STAGE OLYMPIQUE DE MONTPELLIER 2013

Du 19 au 29 août 2013

Avant-propos

Le stage de Montpellier a été organisé par l'association Animath.

Son objet a été de rassembler des jeunes passionné-e-s par les mathématiques et de les faire travailler sur des exercices en vue de la formation des équipes qui représenteront la France à plusieurs compétitions internationales, à savoir l'Olympiade Internationale de Mathématiques en Afrique du Sud en juillet 2014, l'Olympiade Balkanique de Mathématiques en mai 2014, les Olympiades Européennes pour Filles en Turquie en avril 2014 ainsi que les Olympiades Balkaniques Junior de Mathématiques en Macédoine en juin 2014.

Une attention particulière a été apportée au recrutement de collégien-ne-s brillant-e-s en vue de les préparer aux Olympiades Internationales pendant plusieurs années.

Nous tenons à remercier l'Internat d'Excellence de Montpellier pour son excellent accueil.

Les Animatheux


Céline Abraham


Samuel Bach

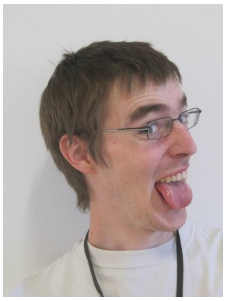

Razvan Barbulescu


Pierre Bertin

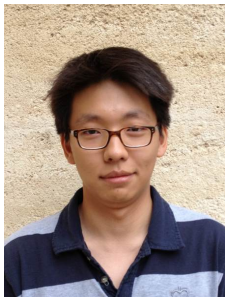

Margaret Bilu


Thomas Budzinski


Guillaume Conchon-Kerjan


Vincent Jugé


Igor Kortchemski


Joon Kwon


Matthieu Lequesne


François Lo Jacomo


Jean-François Martin


Roxane Morel


Vincent Mouly


Louis Nebout


Victor Quach

Les élèves


Julien Alamelle


Etienne Apers


Noélie Bacq


Thibault Bajodek


Henry Bambury


Augustin Bariant

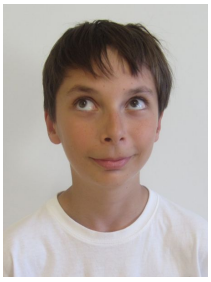

Sébastien Baumert


Moïse Blanchard


Solange Boucheron


Vincent Bouis


Pierre Bras


Félix Breton


Pablo Bustillo


Nicolas Champseix


Louis Charnavel


Elodie Cholieu

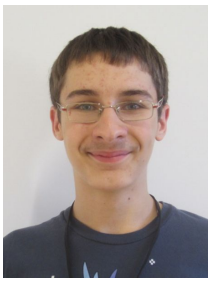

Pierre Clarou


Guillaume Clisson


Baptiste Collet


Edwige Cyffers


Colin Davalo

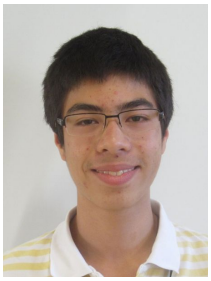

Timothée Defourne

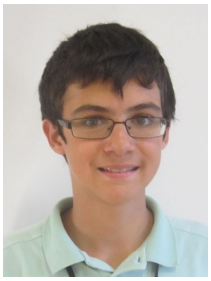

Morine Delhelle

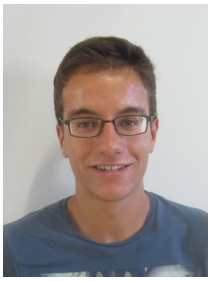

Julie Devaux


Clara Ding


Matthieu Dolbeault

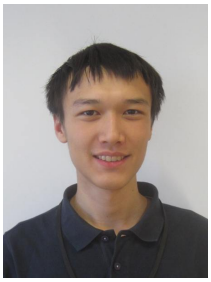

Antoine Dupuis


Thibault
Fay de Lestrac


Romain Fouilland

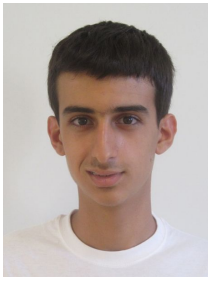

Marc Ganet

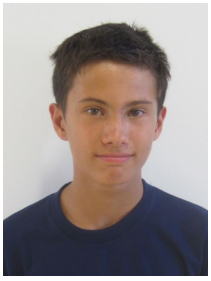
Olivier Garçonnet


Charles Gassot


Solène Gomez


Ilyes Hamdi

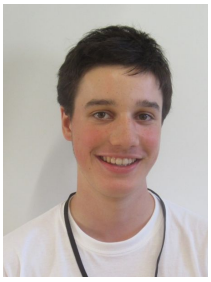

Yassine Hamdi


Maxence Lagarde

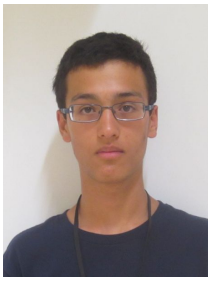

Marc Lamberet


Paul Laubie

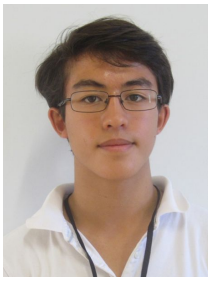

Julie Lauquin


Adrien Lemercier


Jérémy Lengelé


Félix Lequen


Clément Lezane


Adrien Lopez


Charles Madeline-Derou


Christian Michon


Marc Michoux


Arthur Nebout


Florent Noisette


Cédric Ollivier


Tobias Parker


Eva Philippe


Myriam Qrichi Aniba


Raphaël Ruimy


Pascal Sedlmeier


Thomas Sepulchre


Antoine Séré


Adam Siegel


Elie Studnia


Alexandre Thiault


Arthus Vanet

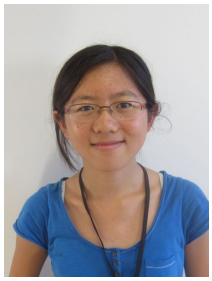

Lucie Wang

Table des matières

I. Déroulement du stage

Pour la deuxième année consécutive, le stage a eu lieu à l'Internat d'Excellence de Montpellier, pendant dix jours (du 19 août vers midi au 29 août vers midi) avec plus de 60 élèves, grâce à une nouvelle subvention de Cap' Maths, et malgré la diminution de la subvention du Ministère (DGESCO). Parmi les 270 candidats au test de sélection, nous en avons finalement accepté 62, de 13 à 17 ans (âge moyen : 15,7 ans), dont 12 filles (en prévision des Olympiades Européennes de Filles), 11 jeunes nés en 1999 (en prévision des Olympiades Balkaniques Junior), et nous avons poursuivi notre effort de préparation sur plusieurs années. 17 animateurs d'âge moyen inférieur à 25 ans - la plupart étant d'anciens stagiaires, six d'entre eux avaient moins de vingt ans - ont assuré les $168 + \epsilon$ heures de cours, les soirées, les tests, la muraille, le polycopié (plus de 400 pages : un record !)...

Le stage était structuré différemment des précédents. Nous avions deux périodes de quatre jours (20 - 23 août et 24 - 27 août), trois de cours et travaux dirigés, un test le matin du quatrième jour, de quatre heures pour le groupe D des avancés, de trois heures pour chacun des autres groupes, et une visite de la ville l'après-midi de ce quatrième jour. Enfin, le mercredi 28 août, dernier jour du stage, était consacré à des cours non sanctionnés par un test, sur des sujets un peu plus larges que la stricte préparation olympique. Les tests étaient corrigés le soir même, les soirées étaient libres les veilles de tests ainsi que le dernier jour (soirée spéciale sans contrôle d'heure de coucher). Le premier soir était une simple prise de contact, deux conférences ont été proposées : « la cryptographie : de vraies mathématiques ! » le 20 août et « théorie des jeux combinatoires » le 25 août, ainsi que des présentations des compétitions mathématiques : « des tournois pas comme les autres : ITYM et le TFJM » le 21 août et « Animath et les Olympiades de Mathématiques » le 24 août. Comme l'an passé, l'horaire des repas était : petit-déjeuner à 8 h, déjeuner à 12 h 30, dîner à 19 h, les soirées commençaient à 20 h 30 (y compris la correction des tests) et les élèves devaient être couchés à 23 h 30, mais ce n'était pas toujours le cas. Malgré des contrôles systématiques, nous n'obtenions pas que tous les élèves soient au moins dans leur chambre avant minuit.

Le lundi 19 août, jour de l'arrivée, après la présentation du stage (14 h 30) au cours de laquelle chaque stagiaire a reçu un nouveau tee-shirt, un bic Animath et deux DVD « Dimensions » et « Chaos », chaque élève a été convoqué à une heure précise, entre 16 h et 18 h 20, pour un entretien individuel de 20 mn avec un animateur. A partir de ces entretiens, quatre groupes de niveaux ont été constitués. Contrairement à l'an passé, il n'y avait pas de « groupe par défaut », chaque élève ayant obligatoirement passé l'entretien, et les groupes valaient pour l'ensemble du stage vu qu'ils ne traitaient pas les mêmes sujets en même temps : les groupes A et B de débutants (collège et lycée) commençaient par les stratégies de base, le groupe C par la géométrie et le groupe D par l'arithmétique. Certains enseignants pouvaient ainsi assurer deux ou trois cours de géométrie (par exemple) à différents groupes. Ces groupes étaient plus

équilibrés que l'an passé : 14 élèves en D, 20 en C, 19 en B et 9 en A. Certaines séances étaient consacrées à des sujets différents des thèmes traditionnels : un cours de logique pour chacun des groupes A et B, des cours de polynômes pour les groupes C et D, et surtout, le dernier jour, des cours sortant du cadre traditionnel (un sur les automates pour le groupe C et un sur la théorie de Galois pour le groupe D par exemple).

Quelques liens utiles pour poursuivre le travail réalisé pendant ce stage :
- Le site d'Animath : http ://www.animath.fr
- Le site MathLinks : http ://www.mathlinks.ro
- Les polycopiés de stages olympiques précédents :
  http ://www.animath.fr/spip.php ?article260
- Les cours de l'Olympiade Française de Mathématiques :
  http ://www.animath.fr/spip.php ?article255

		Groupe A	Groupe B	Groupe C	Groupe D
Lundi 19/08		Arrivé, accueil des élèves et première évaluation			
Mardi	9h - 12h	Cours de stratégies de base (Pierre)	Cours de logique (Vincent J.)	Cours de géométrie (Igor)	Cours d'arithmétique (Louis)
	14h - 17h+ϵ	Cours/TD de stratégies de base (François)	Cours/TD de stratégies de base (Razvan)	TD de géométrie (Jean-François)	TD d'arithmétique (Vincent M.)
	20h30 -22h	Conférence : La cryptographie, de vraies maths ! (Razvan)			
Mercredi	9h - 12h	Cours de logique (Vincent J.)	Cours de stratégies de base (Igor)	Cours/TD de géométrie (Jean-François)	Cours/TD d'arithmétique (Razvan)
	14h - 17h+ϵ	TD de stratégies de base (Guillaume)	TD de stratégies de base (Vincent M.)	TD de géométrie (Pierre)	Cours/TD géométrie (Louis)
	20h30 -22h30	Présentation du TFJM^2 et de l'ITYM			
Jeudi	9h - 12h	Cours d'algèbre (Roxane & Matthieu)	Cours d'algèbre (Margaret)	Cours de polynômes (Igor)	Cours de géométrie (François)
	14h - 17h+ϵ	TD d'algèbre (Vincent M.)	TD d'algèbre (Guillaume)	TD de polynômes (Pierre)	TD de géométrie (Jean-François)
	20h30 - 21h 30	Soirée libre			
Vendredi	9h - 12h	Test			
	Après-midi	Visite de Montpellier			
	20h30 - 21h 30	Correction du Test			
Samedi	9h - 12h	Cours de géométrie (Pierre)	Cours de géométrie (François)	Cours d'arithmétique (Samuel)	Cours de combinatoire (Vincent J.)
	14h - 17h+ϵ	TD de géométrie (Igor)	TD de géométrie (Louis)	TD d'arithmétique (Céline)	TD de combinatoire (Victor)
	20h30 - 21h 30	Présentation des différentes olympiades internationales			
Dimanche 25/08	9h - 12h	Cours/TD de géométrie (Thomas)	Cours/TD de géométrie (Roxane & Matthieu)	Cours/TD d'arithmétique (François)	Cours/TD de combinatoire (Margaret)
	14h - 17h+ϵ	Cours/TD d'arithmétique (Victor)	Cours/TD d'arithmétique (Joon)	Inégalités (Guillaume)	Polynômes (Samuel)
	20h30 - 21h 30	Conférence : La théorie des jeux combinatoires (Louis)			
Lundi	9h - 12h	Cours d'arithmétique (Louis)	Cours d'arithmétique (Thomas)	Cours d'éq. fonctionelles (Jean-François)	Cours d'inégalités (Joon)
	14h - 17h+ϵ	TD d'arithmétique (Céline)	TD d'arithmétique (Vincent J.)	TD d'éq. fonctionnelles (Guillaume)	TD d'inégalités (Margaret)
	20h30 - 21h 30	Soirée libre			
Mardi	9h - 12h	Test			
	Après-midi	Autre visite de Montpellier			
	20h30 - 21h 30	Correction du Test			
Mercredi	9h - 12h	Théorie des graphes (Margaret)	Fonctions (François)	Dénombrabilité (Louis)	Théorie de Galois (Samuel)
	14h - 17h+ϵ	Fonctions (Thomas)	Théorie des graphes (Joon)	Automates (Vincent J.)	Probabilités (Igor)
	20h30 - 21h 30	Soirée/nuit libre			
Jeudi	Matinée	Brunch puis départ			

II. Première période

Contenu de cette partie

1 Groupe A : stratégies de base

1 Cours de stratégies de base : principe des tiroirs, invariants

- Principe des tiroirs -

S'il y a $(n+1)$ chaussettes à ranger dans n tiroirs, alors il existe au moins un tiroir qui contient au moins deux chaussettes.

Exercice 1 On colorie tous les points du plans en rouge et noir. Montrer qu'il existe deux points de la même couleur distants de 1 mètre exactement.

Exercice 2 Dans un internat à Montpellier, il y a 62 stagiaires. Certains se connaissent, et d'autres pas. On suppose que si A connaît B alors B connaît A. Montrer qu'il existe deux stagiaires qui connaissent exactement le même nombre de personnes.

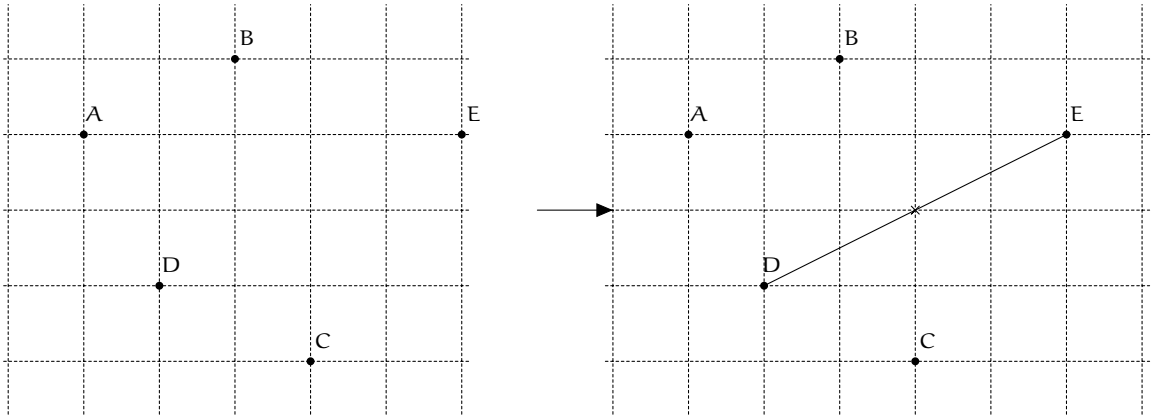
Exercice 3 Un être humain possède entre 0 et 500000 cheveux. Montrer qu'il y a deux Montpelliérains qui ont exactement le même nombre de cheveux.

Exercice 4 Soit x un nombre réel. Montrer qu'il existe une infinité de fractions $\frac{p}{q}$ telles que

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Exercice 5 On place 201 points sur un damier 10 cm $\times$10 cm. Montrer que l'on peut trouver 3 points qui forment un triangle d'aire inférieure à 0.5 cm^2.

Exercice 6 On place 5 points sur un grille. Montrer que l'on peut en trouver deux parmi eux qui forment un segment dont le milieu est lui aussi sur la grille :



- Invariants -

Exercice 7 Trente-six ampoules sont rangées en grille 6×6. On dispose de un interrupteur pour chaque ligne, qui quand il est utilisé éteint toutes les ampoules allumées de la ligne et allume les éteintes. De même il y a un interrupteur pour chaque colonne. Igor affirme : "quand je suis arrivé il y avait exactement une ampoule allumée, mais après avoir manipulé certains interrupteurs j'ai réussi à toutes les éteindre". Qu'en pensez-vous ?

Exercice 8 Soit N le nombre de façons qu'il est possible de paver un échiquer avec 32 dominos. Exprimer en fonction de N le nombre de pavage d'un échiquier auquel on a retiré deux coins opposés par 31 dominos.

Exercice 9 On fait un jeu : on commence avec une pile de 2013 jetons. On retire un jeton, puis on coupe la pile en deux petites piles (pas forcément égales). À chaque étape on enlève un jeton à l'une des piles et on coupe une pile en deux (pas forcément la même). Le but du jeu est d'arriver à une configuration où toutes les piles sont hautes de 3 jetons, est-ce possible ? (Si on retire un jeton à une pile de 1 jeton, on considère qu'on a une pile de 0 jetons)

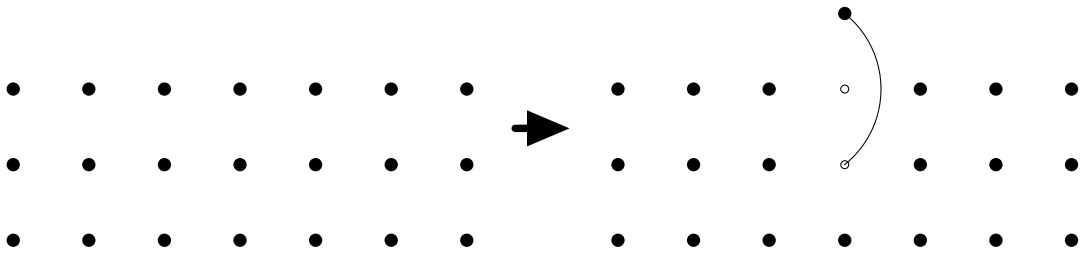
Exercice 10 Vingt-deux arbres sont disposés en rond. Sur chaque arbre se pose un corbeau. À chaque minute, deux corbeaux s'envolent de leurs arbres et se posent sur un arbre voisin. Est-il possible qu'après un certain temps tous les corbeaux soient sur le même arbre ?

Exercice 11 On considère un triplet de nombres réels (a, b, c). On peut effectuer l'action suivante : on choisit x et y deux des nombres du triplet et on les remplace par $(x - y)/\sqrt{2}$ et $(x + y)/\sqrt{2}$. Peut-on passer du triplet initial $(2, \sqrt{2}, 1/\sqrt{2})$ au triplet final $(1, \sqrt{2}, 1 + \sqrt{2})$?

Exercice 12 Sur une île vivent 34 caméléons. Au départ 7 sont jaunes, 10 sont verts et 17 sont rouges. Lorsque deux caméléons de couleurs différentes se rencontrent, ils prennent tous les deux la troisième couleur. Si deux caméléons de la même couleur se rencontrent, rien ne se passe. Un an plus tard ils sont tous de la même couleur. Laquelle ? (Démontrez que c'est la seule possible).

Exercice 13 Un tetramino est une figure formée de 4 carrés (pensez à Tetris). Trouvez le nombre m de tetramino distincts (on dit que deux tetraminos sont identiques si on peut les superposer en les faisant pivoter mais sans les retourner). Est-il possible de paver un rectangle $4 \times m$ avec un tetramino de chaque sorte ?

Exercice 14 (Un Solitaire Infini)($\star$) Vous connaissez tous les règles du solitaire : il y a des billes sur un plateau, on élimine des billes en sautant par dessus avec une autre bille, etc. Maintenant on considère le plan et on place des billes sur tous les points entiers du demi-plan négatif. Le but du jeu est de mettre une bille le plus haut possible en un nombre fini de coups. Le dessin montre comment mettre une bille à hauteur 1. Quelle est la hauteur maximale que l'on peut atteindre ?



- Solutions des exercices -

Solution de l'exercice 1 On prend trois points qui forment un triangle equilatéral de côté 1. Il y a 3 points qui peuvent être de deux couleurs différentes. Il y a donc au moins deux points de la même couleur.

Solution de l'exercice 2 Définissons nos chaussettes et nos tiroirs : les chaussettes sont les 62 stagiaires, et les tiroirs correspondent au nombre de gens connus. Chacun connaît entre entre 0 et 61 personnes, ce qui nous donne 62 tiroirs. Mais il est impossible que quelqu'un connaisse tout le monde et quelqu'un d'autre ne connaisse personne : si quelqu'un connaît tout le monde, alors tout le monde le connaît et du coup tout le monde connaît au moins une personne. Ainsi on ne peut utiliser que 61 tiroirs, il y a donc deux élèves qui connaissent le même nombre de personnes.

Solution de l'exercice 3 C'est une simple application du principe des tiroirs.

Solution de l'exercice 4 Tout d'abord on multiplie les deux côtés de l'inégalité par q :

$$|qx - p| < \frac{1}{q}.$$

Pour choisir p c'est évident, il faut prendre l'entier le plus proche de qx. Nous allons démontrer la proposition suivante : pour tout entier q, il existe un entier $a \leqslant q$ et un entier p tel que $|ax - p| < \frac{1}{q}$. Ensuite on aura fini, puisque

$$\left|x - \frac{p}{a}\right| < \frac{1}{aq} \leqslant \frac{1}{a^2}.$$

Démontrons notre proposition. On prend $x, 2x, \dots qx$ et on ne regarde que la partie après la virgule. Si l'une d'entre elles est entre 0 et $\frac{1}{q}$, on a gagné. Sinon, on divise le segment $[0,1]$ en q segments : $\left[0, \frac{1}{q}\right]$, $\left[\frac{1}{q}, \frac{2}{q}\right]$, etc. Comme aucun n'est dans le premier segment, cela signifie qu'il y a q points répartis dans $(q-1)$ segments. Par le principe des tiroirs, il y en a deux qui sont dans le même segment. Disons qu'ils correspondent à mx et nx. Comme les deux points sont dans un segment de largeur $\frac{1}{q}$, ils sont distants de moins de $\frac{1}{q}$. Ainsi il existe un entier p tel que :

$$|mx - nx - p| < \frac{1}{q}.$$

Enfin on prend $a = m - n$ (ou $a = n - m$ si $n > m$) et on a gagné.

Solution de l'exercice 5 On sépare le damier en 100 cases de 1cm $\times$ 1cm. Comme il y a 201 points, par le principe des tiroirs, il y a une case qui contient 3 points. Il ne reste plus qu'à démontrer que si un triangle est inclus dans un carré de côté 1, alors l'aire du triangle est inférieure à 0.5.

Solution de l'exercice 6 Un point est sur la grille ssi ses coordonnées (x, y) sont toutes les deux entières. Soient A et B de coordonnées respectives (x_1, y_1) et (x_2, y_2), le milieu du segment $[AB]$ sera le point de coordonnées $\left(\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2}\right)$. Le milieu sera sur la grille ssi ses coordonnées sont entières, ssi x_1 et x_2 sont de même parité, et y_1 et y_2 aussi. Les parités des coordonnées d'un point de la grille peuvent prendre quatre valeurs différentes : (paire, paire) ; (paire, impaire) ; (impaire, paire) et (impaire, impaire). Comme on a 5 points pour 4 classes, il y a deux points qui ont les mêmes parités, et leur milieu est sur la grille.

Solution de l'exercice 7 On remarque que quel que soit l'interrupteur utilisé, on ne change jamais la parité du nombre d'ampoules allumées. Donc soit Igor ment, soit il a cassé les ampoules à force de jouer avec.

Solution de l'exercice 8 Lorsqu'on enlève les deux coins opposés d'un échiquier, il reste 32 cases noires et 30 cases blanches. Mais quelle que soit la façon de poser un domino, il recouvre toujours un case noire et une case blanche. Il est donc impossible de paver l'échiquier écorné avec des dominos.

Solution de l'exercice 9 On remarque que chaque étape du jeu consiste à enlever un jeton et rajouter une pile. Donc la quantité "nb de jetons + nb de piles" ne change jamais. Au départ on a 2013 jetons et une pile, ce qui donne 2014, et si arrivait à n piles de 3 jetons (donc $3n$ jetons), on aurait $4n$. Mais 2014 n'est pas divisible par 4, donc c'est impossible.

Solution de l'exercice 10 Supposons que les arbres sont alternés entre des cerisiers et des pommiers. On va compter le nombre de corbeaux posés sur des cerisiers. Au début il y a 11 corbeaux sur des cerisiers, et à la fin soit 0, soit 22 selon l'espèce de l'arbre sur lequel tous les corbeaux sont posés. Mais à chaque étape, on peut vérifier que le nombre de corbeaux sur des cerisiers reste le même, augmente de 2 ou diminue de 2. En particulier il ne change pas de parité. On ne peut donc pas passer de 11 à 22 ou 0.

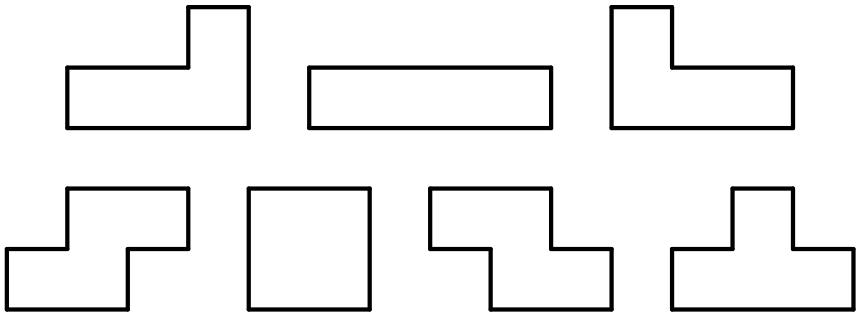
Solution de l'exercice 11 Je vous laisse vérifier l'equation suivante :

$$\left(\frac{x+y}{\sqrt{2}}\right)^2 + \left(\frac{x-y}{\sqrt{2}}\right)^2 + z^2 = x^2 + y^2 + z^2.$$

Ainsi la somme des carrés des trois nombres du triplet ne change jamais. Il suffit maintenant de vérifier que la somme des carrés du triplet initial n'est pas la même que celle du triplet final.

Solution de l'exercice 12 Un peu de manipulations permet de montrer que l'on peut finir avec tous les caméléons rouges. Montrons qu'il est impossible de finir avec seulement des caméléons verts. Nous allons considérer la quantité "nb de rouges - nb de verts". Quand deux caméléons se rencontrent, cette quantité va soit rester constante, soit augmenter de 3, soit diminuer de 3. Ainsi si on veut qu'elle finisse à 0, il faut qu'elle commence à un multiple de 3. Mais au départ, elle vaut 10.

Solution de l'exercice 13 Il est facile de vérifier qu'il y a 7 pièces différentes au Tetris :



Ensuite, passons au pavage d'un rectangle 4×7. Si on colorie les cases en échiquier, on se retrouve avec 14 cases blanches et 14 noires. Tous les tetraminos recouvrent 2 cases noires et 2 blanches, quelle que soit la manière de les mettre, sauf le T, qui recouvre 3 blanches et 1 noire ou 3 noires et 1 blanche. Il est donc impossible de faire le pavage.

Solution de l'exercice 14 Il est facile de faire monter une bille à hauteur 1, 2 et 3, et avec un peu de patience on peut en faire monter une à hauteur 4, mais c'est la limite. Notons φ le nombre d'or, qui vérifie $\varphi^2 = \varphi + 1$:

$$\varphi = \frac{1+\sqrt{5}}{2}.$$

Ensuite il faut faire la somme sur tous les points de coordonnées (x, y) sur lesquelles il y a des billes de $\varphi^{y-|x|}$. Je laisse au lecteur le soin de vérifier que cette quantité reste constante ou diminue lorsqu'on fait sauter les billes et que dans la position de départ elle vaut φ^5. Ceci démontre qu'il est impossible de faire monter une bille à hauteur 5 ou plus.

2 Cours/TD de stratégies de base

- La Récurrence -

Le principe de récurrence est fondamentalement lié à la notion de nombre entier : chaque fois que l'on doit démontrer qu'un résultat est vrai pour tout entier à partir d'un certain rang, que ce soit en arithmétique, géométrie, algèbre... on peut être amené à raisonner par récurrence.

La démonstration par récurrence repose sur le fait que tout entier n possède un suivant $n+1$, et que si l'on « gravit marche après marche » l'ensemble $\mathbb{N}$ des entiers naturels, en partant de 0, en allant d'un entier au suivant et en recommençant indéfiniment, on parcourt ainsi intégralement $\mathbb{N}$.

On va donc démontrer qu'une propriété est vraie pour l'entier $n = 0$ (initialisation), puis que si elle est vraie pour un entier $n \geqslant 0$ quelconque, elle est encore vraie pour l'entier suivant $n+1$ (induction) : on déduit de cela que la propriété est vraie pour tout entier naturel n. C'est le raisonnement par récurrence.

On notera que les deux parties de la démonstration sont toutes deux importantes, même si la première est souvent assez évidente. Il ne faut pas oublier d'initialiser la récurrence, donc de démontrer que la propriété est vraie pour $n = 0$. On peut démarrer la récurrence en une valeur autre que 0, par exemple en 1, 2, $\cdots$ ou K ; il faudra alors prouver (initialisation) que la propriété est vraie pour $n = K$, puis (induction) que pour $n \geqslant K$, si elle est vraie pour n elle l'est encore pour $n+1$.

On notera également que l'induction connait quelques variantes. Par exemple, il arrive que l'on ait à démontrer que si la propriété est vraie en outre pour tout entier $k \leqslant n$, alors elle est vraie pour $n+1$.

Exercice 1

Soient a, b et u trois réels, $a \neq 1$, et (u_n) une suite définie par : $u_0 = u$ et pour tout $n \geqslant 0$, $u_{n+1} = au_n + b$. Démontrer que pour tout $n \geqslant 0$, $u_n = a^n u + b\frac{a^n-1}{a-1}$.

Exercice 2

a) Montrer que pour tout $n \geqslant 1$, $\sum_{k=1}^{n} \frac{1}{k^2} \leqslant 2 - \frac{1}{n}$.
b) Montrer que pour tout $n \geqslant 2$, $\frac{1}{n^2-n} - \frac{1}{n^2+n} > \frac{2}{n^3}$
c) En déduire que pour tout $n \geqslant 1$, $\sum_{k=1}^{n} \frac{1}{k^3} \leqslant \frac{5}{4}$

Exercice 3

Montrer que pour tout $n \geqslant 1$, il existe un multiple de 2^n de n chiffres tous égaux à 1 ou 2.

Exercice 4

Soient n et a deux entiers strictement positifs, tels que $n \geqslant 2$ et $a \leqslant n!$. Montrer qu'il existe $k < n$ et k entiers $d_1, d_2, ...d_k$ deux à deux distincts divisant chacun $n!$ tels que $a = d_1 + d_2 + \cdots + d_k$.

Exercice 5

On considère la suite de Fibonacci (F_n) définie par : $F_0 = 0, F_1 = 1$ et pour tout $n \geqslant 1$ $F_{n+1} = F_n + F_{n-1}$. Soit $\Phi = \frac{1+\sqrt{5}}{2}$ la racine positive de l'équation : $x^2 = x+1$. Montrer que pour tout $n \geqslant 0$, $F_{n+1} - \Phi F_n = \left(-\frac{1}{\Phi}\right)^n$.

Exercice 6

$2n+1$ élèves sont placés de telle sorte que les distances entre deux d'entre eux sont toutes différentes. A un moment donné, chacun d'eux tire sur l'élève le plus proche de lui avec un pistolet à eau.

a) Montrer qu'il existe deux élèves qui se tirent mutuellement dessus,

b) Montrer qu'au moins un des élèves n'est pas visé.

Exercice 7

a) Soient quatre points d'un plan. Montrer qu'au moins un des quatre triangles qu'ils forment n'est pas acutangle (c'est-à-dire ayant tous ses angles strictement inférieurs à 90°).

b) Soient n points d'un plan, avec $n \geqslant 5$. Montrer qu'au plus 70% des triangles qu'ils forment sont acutangles.

Exercice 8

Montrer que pour toute paire d'entiers strictement positifs k et n, il existe k entiers strictement positifs (non nécessairement distincts) $m_1, m_2, \cdots, m_k$ tels que :

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right)\left(1 + \frac{1}{m_2}\right)\cdots\left(1 + \frac{1}{m_k}\right)$$

On commencera par montrer que si c'est vrai pour la paire k, n c'est également vrai pour la paire $k+1, 2n$

Solution de l'exercice 1

Comme le résultat doit être démontré pour tout $n \geqslant 0$, c'est en $n = 0$ qu'on va l'initialiser.

Si $n = 0$, $a^n = 1$, ce qui donne bien $u_0 = u$, conforme à la définition de (u_n) : l'initialisation est terminée.

Quant à l'induction : supposons que pour un $n \geqslant 0$ donné, $u_n = a^n u + b\frac{a^n-1}{a-1}$ (hypothèse de récurrence). Par définition, $u_{n+1} = au_n + b = a\left(a^n u + b\frac{a^n-1}{a-1}\right) + b = a^{n+1}u + b\frac{a^{n+1}-a}{a-1} + b\frac{a-1}{a-1} = a^{n+1}u + b\frac{a^{n+1}-1}{a-1}$ ce qui achève la démonstration.

Solution de l'exercice 2

a) L'initialisation est immédiate. Pour $n = 1$, l'inégalité est manifestement vraie : $1 \leqslant 2 - \frac{1}{1}$. Supposons maintenant (hypothèse de récurrence) que, pour un certain n, $\sum_{k=1}^{n} \frac{1}{k^2} \leqslant 2 - \frac{1}{n}$. Il en résulte que : $\sum_{k=1}^{n+1} \frac{1}{k^2} \leqslant 2 - \frac{1}{n} + \frac{1}{(n+1)^2}$. Il suffit de prouver que ce second membre est lui-même inférieur à $2 - \frac{1}{n+1}$ pour conclure que l'inégalité est vraie au rang suivant $n+1$, donc, par récurrence, qu'elle est vraie pour tout n. Or $\left(2 - \frac{1}{n} + \frac{1}{(n+1)^2}\right) - \left(2 - \frac{1}{n+1}\right) = \frac{-1}{n(n+1)^2} < 0$, d'où le résultat.

b) Il s'agit là d'un simple calcul qui nous servira pour la question suivante : $\frac{1}{n^2-n} - \frac{1}{n^2+n} = \frac{(n^2+n)-(n^2-n)}{(n^2-n)(n^2+n)} = \frac{2n}{n^4-n^2} = \frac{2}{n^3-n} > \frac{2}{n^3}$ car $n^3 - n < n^3$. On remarquera que $n^2 - n = (n-1)n$ et $n^2 + n = n(n+1)$.

c) En s'inspirant du a), on va montrer non pas directement que la somme est inférieure à $\frac{5}{4}$, mais qu'elle est inférieure à $\frac{5}{4}$ moins une fonction de n qui, lorsqu'on ajoute le terme suivant de la somme, fait apparaître la même fonction au rang suivant. Pour s'inspirer plus directement de la question b), on va supposer que la relation est vraie au rang $n-1$ et montrer qu'elle est vraie pour n. Concrètement, la relation que l'on va chercher à démontrer (hypothèse de récurrence) est : $\sum_{k=1}^{n} \frac{1}{k^3} \leqslant \frac{5}{4} - \frac{1}{2(n^2+n)}$. Commençons par initialiser la récurrence : pour $n = 1$, $1 \leqslant \frac{5}{4} - \frac{1}{4}$. C'est pour que cette initialisation soit vraie qu'on a choisi la constante $\frac{5}{4}$, car cette constante ne joue aucun rôle dans la partie induction. Si l'on avait démarré notre récurrence en $n = 2$, on aurait pu choisir une autre constante, $\frac{29}{24}$ qui est donc une meilleure majoration de la somme des inverses des cubes.

Mais terminons la démonstration de notre récurrence : si la relation $\sum_{k=1}^{n} \frac{1}{k^3} \leqslant \frac{5}{4} - \frac{1}{2(n^2+n)}$ est vraie au rang $n-1$, donc si $\sum_{k=1}^{n-1} \frac{1}{k^3} \leqslant \frac{5}{4} - \frac{1}{2(n^2-n)}$, alors $\sum_{k=1}^{n} \frac{1}{k^3} \leqslant \frac{5}{4} - \frac{1}{2(n^2-n)} + \frac{1}{n^3} < \frac{5}{4} - \frac{1}{2(n^2+n)}$ d'après le b), donc l'inégalité est vraie au rang suivant n, et par récurrence elle est vraie pour tout entier n.

Solution de l'exercice 3

Pour $n = 1$, 2 est multiple de 2. Essayons les premières valeurs de n : pour $n = 2$, 12 est multiple de 4, puis 112 de 8, 2112 de 16, 22112 de 32 etc... L'idée est, pour passer au rang suivant, d'ajouter un premier chiffre, 1 ou 2. En effet, si a_n est divisible par 2^n, a_n ayant n chiffres tous égaux à 1 ou 2 (hypothèse de récurrence), les deux nombres : $10^n + a_n$ et $2 \cdot 10^n + a_n$ ont tous deux $n+1$ chiffres tous égaux à 1 ou 2. Il reste donc à prouver que l'un des deux est multiple de 2^{n+1}.

Or si l'on pose $a_n = 2^n \times b_n$, $10^n + a_n = 2^n \times (5^n + b_n)$: si b_n est impair, $5^n + b_n$ est pair, donc $10^n + a_n$ est divisible par 2^{n+1}. Maintenant, si b_n est pair, c'est : $2 \cdot 10^n + a_n = 2^n \times (2 \cdot 5^n + b_n)$ qui est divisible par 2^{n+1} car $2 \cdot 5^n + b_n$ est pair. Que b_n soit pair ou impair, on peut trouver un a_{n+1} de $n+1$ chiffres tous égaux à 1 ou 2 qui soit divisible par 2^{n+1} : c'est précisément ce qu'on devait démontrer.

Solution de l'exercice 4

Nous allons prouver par récurrence sur $n \geqslant 2$ l'hypothèse H_n suivante : « pour tout entier naturel non nul $a \leqslant n!$, il existe des entiers $k < n$ et $d_1 > d_2 > \cdots > d_k$ divisant tous $n!$, tels que $a = d_1 + d_2 + \cdots + d_k$ ».

Tout d'abord, H_2 est clairement vraie : il suffit de prendre $k = 1$ et $d_1 = a$. Supposons maintenant H_n, et prouvons H_{n+1} : soit $a \leqslant (n+1)!$ un entier naturel non nul. Tout d'abord, appliquons H_n à l'entier $\left\lfloor \frac{a}{n+1} \right\rfloor$: il existe un entier $k < n$ et des entiers $d_1 > \cdots > d_k$ divisant $n!$ tels que $\left\lfloor \frac{a}{n+1} \right\rfloor = \sum_{i=1}^{k} d_i$. Soit alors d'_{k+1} le reste de la division euclidienne de a par $n+1$: notons que les entiers $(n+1)d_i$ divisent tous $(n+1)!$. Ensuite :

- si $d_{k+1} = 0$, on pose $k' = k$ et $d'_i = (n+1)d_i$ pour $i \leqslant k$;
- sinon, on pose $k' = k+1$, $d'_i = (n+1)d_i$ pour pour $i \leqslant k$, et $d'_{k+1} = d_{k+1}$.

Dans les deux cas, on se rend compte que les entiers $k' < n+1$ et $d'_1 > \cdots > d'_{k'}$ conviennent. Cela prouve que H_{n+1} est vraie, ce qui clôt la récurrence et l'exercice.

Solution de l'exercice 5

Pour initialiser la récurrence, on vérifie que la relation est vraie pour $n = 0$: $F_1 - \Phi F_0 = 1 - 0 = \left(\frac{-1}{\Phi}\right)^0$. On peut encore, bien que ce ne soit pas indispensable, vérifier cette relation au rang $n = 1$: $F_2 - \Phi F_1 = 1 - \Phi = \left(\frac{-1}{\Phi}\right)^1$. Le principal avantage de cette seconde vérification est de nous rappeler une formule dont nous aurons besoin par la suite : $1 - \Phi = \frac{-1}{\Phi}$.

Supposons maintenant (hypothèse de récurrence) qu'au rang n on ait : $F_{n+1} - \Phi F_n = \left(\frac{-1}{\Phi}\right)^n$, et déduisons en cette même relation au rang suivant $n+1$. Par définition de la suite de Fibonacci, $F_{n+2} - \Phi F_{n+1} = (F_{n+1} + F_n) - \Phi F_{n+1} = (1 - \Phi)F_{n+1} + F_n$. Or, nous venons de le voir : $1 - \Phi = \frac{-1}{\Phi}$, donc $F_{n+2} - \Phi F_{n+1} = \frac{-1}{\Phi}(F_{n+1} - \Phi F_n) = \left(\frac{-1}{\Phi}\right)^{n+1}$ puisque, par hypothèse de récurrence, $F_{n+1} - \Phi F_n = \left(\frac{-1}{\Phi}\right)^n$.

Solution de l'exercice 6

a) Parmi toutes les distances entre deux élèves, deux à deux distinctes par hypothèse, l'une est plus petite que toutes les autres. Les deux élèves situés à cette distance minimale se tirent dessus mutuellement.

b) Initialisons la récurrence : pour $2n + 1 = 3$, parmi trois élèves, deux se tirent mutuellement dessus, et personne ne tire sur le troisième, qui n'est donc pas visé. Le résultat est bien vrai.

Maintenant, considérons $2n + 3$ élèves. Deux d'entre eux, A et B, se tirent mutuellement dessus. Parmi les $2n + 1$ autres, soit l'un au moins tire sur A ou B, et au maximum $2n$ élèves autres que A et B sont visés, l'un au moins n'est pas visé. Soit les $2n + 1$ autres se tirent dessus entre eux, et on peut utiliser l'hypothèse de récurrence pour affirmer que l'un d'eux au moins n'est pas visé.

On notera que ce résultat n'est vrai que pour un nombre impair d'élèves : pour un nombre pair, il est possible de les positionner de sorte qu'ils se tirent mutuellement dessus deux à deux.

Solution de l'exercice 7

a) Il s'agit d'une question élémentaire de géométrie, qui nous sera utile pour la question b. Soit les quatre points forment un quadrilatère convexe, auquel cas, la somme des quatre angles du quadrilatère étant égale à 360°, l'un au moins des quatre angles est supérieur ou égal à 90°, donc l'un au moins des quatre triangles n'est pas acutangle. Soit un des points est à l'intérieur du triangle formé par les trois autres, auquel cas les trois angles de sommets ce point ont pour somme 360°, l'un au moins de ces trois angles est supérieur ou égal à 120°, a fortiori à 90°.

b) Initialisons la récurrence avec cinq points. Ils déterminent dix triangles. Mais ils déterminent également cinq sous-ensembles de quatre points. Chaque triangle appartient à deux sous-ensembles de quatre points, et chaque sous-ensemble de quatre points contient au moins un triangle non acutangle. Donc en comptant deux fois chaque triangle, on en a au moins cinq non acutangles. Il y en a donc au moins 2,5 parmi 10 non acutangles. Mais comme le nombre de triangles non acutangles est nécessairement entier, il y en a au moins 3 parmi 10 non acutangles, donc au plus 70% de triangles acutangles.

L'induction va consister à prouver que la proportion maximale p_n de triangles acutangles ne peut que diminuer quand n augmente. Considérons $n + 1$ points. Ils contiennent $n + 1$ sous-ensembles de n points. Dans chaque sous-ensemble, il y a : $\binom{n}{3}$ triangles, dont au plus $p_n \cdot \binom{n}{3}$ acutangles. Si l'on additionne, on trouvera chaque triangle $n-2$ fois. Donc le nombre de triangles acutangles parmi les $n + 1$ points est au maximum : $p_n \cdot \binom{n}{3} \cdot \frac{n+1}{n-2} = p_n \cdot \binom{n+1}{3}$:

comme il y a $\binom{n+1}{3}$ triangles, la proportion $p_{n+1} \leqslant p_n$, ce qui achève la démonstration.

Solution de l'exercice 8

Cet exercice est le problème 1 de l'Olympiade Internationale 2013. C'est une variante de la démonstration par récurrence.

Commençons, comme proposé, par prouver que si c'est vrai pour k et n, c'est vrai pour $k+1$ et $2n$. Pour k, n, le membre de gauche s'écrit : $\frac{2^k+n-1}{n}$. Pour $k+1, 2n$: $\frac{2^{k+1}+2n-1}{2n}$. Le quotient des deux est : $\frac{2^{k+1}+2n-1}{2^{k+1}+2n-2}$. En d'autres termes, si $m_{k+1} = 2^{k+1} + 2n - 2$, $1 + \frac{2^{k+1}-1}{2n} = \left(1 + \frac{2^k-1}{n}\right)\left(1 + \frac{1}{m_{k+1}}\right)$. Donc si le résultat est vrai pour k et n, il est encore vrai, avec un facteur de plus, pour $k+1$ et $2n$.

On démontre pareillement que si c'est vrai pour k et n, c'est vrai pour $k+1$ et $2n-1$, avec un $(k+1)$-ème facteur. $1 + \frac{2^{k+1}-1}{2n-1} = \frac{2^{k+1}+2n-2}{2n-1} = \left(1 + \frac{2^k-1}{n}\right)\left(1 + \frac{1}{2n-1}\right)$.

Maintenant, il faut initialiser la récurrence : pour $k = 1$, le résultat est immédiat quel que soit n, avec $m_1 = n$. Pour $n = 1$, il est tout aussi immédiat quel que soit k avec $m_1 = m_2 = \cdots = m_k = 1$. Donc d'après ce qu'on vient de démontrer, il est encore vrai pour $n = 2$ et $k \geqslant 2$. Mais il est aussi vrai pour $n = 2$ et $k = 1$. On en déduit qu'il est vrai pour $n = 4$ et $n = 3$ et $k \geqslant 2$, à quoi s'ajoute le cas démontré séparément $n = 4$ ou 3 et $k = 1$. Plus généralement, si (pour $N \geqslant 1$) le résultat est vrai pour tout entier $n \leqslant 2N$, et tout k, alors il est vrai en particulier pour $n = N+1$, donc pour $n = 2N+2$ et $p = 2N+1$ et $k \geqslant 2$. Mais il est vrai aussi, par ailleurs, pour $n = 2N+2$ et $p = 2N+1$ et $k = 1$. Donc en définitive, s'il est vrai pour tout entier $n \leqslant 2N$ et tout k, il est vrai pour tout entier $n \leqslant 2N+2$ et tout k, donc par récurrence il est vrai pour tout n et tout k.

3 Cours de logique

- Introduction : pourquoi la logique ? -

Ce cours consiste en une introduction à la logique. Les concepts qui y sont présentés sont simples, mais à la base de tout raisonnement mathématique. Aussi est-il très important de les maîtriser si l'on tient à explorer, seul, en cours ou à l'aide d'un livre, le monde merveilleux des mathématiques.

À l'image de toutes les disciplines scientifiques, les mathématiques cherchent à fournir une modélisation du monde. Cependant, l'approche choisie est différente de celles de la plupart des disciplines dites expérimentales. Ainsi, en biologie, on travaille sur le vivant ; en chimie, sur les interactions entre les différents composants de la matière, tels que les atomes, les ions et les molécules ; dans les deux cas, l'objet d'intérêt peut être appréhendé par l'expérience, et un des buts de son étude est d'en trouver une modélisation aussi simple et précise que possible.

Au contraire, les mathématiques concernent l'étude d'objets entièrement issus de l'esprit humain, et dont on peut donc espérer qu'ils soient parfaitement définis. En particulier, la complexité d'une simple paramécie est terrifiante, tandis que celle de l'ensemble vide l'est beaucoup moins. Travailler sur des objets simples permet alors au mathématicien d'énoncer des assertions extrêmement précises : si le concept d'être vivant est très flou, ce n'est pas le cas du nombre π.

Il convient alors d'utiliser un vocabulaire adapté pour énoncer ces assertions que l'on peut rendre aussi précises que l'on souhaite. C'est le rôle de la *logique*, qui englobe en particulier le concept de *raisonnement*. Qu'est-ce qui peut faire qu'une assertion soit *vraie* ou *fausse* ? Ou bien simplement que cette assertion ait un sens ? C'est ce que nous allons voir ci-dessous.

- La formalisation de la logique -

Si Paris est la capitale du Mali…

Qu'est-ce qu'un raisonnement ? C'est une suite d'énoncés tels que, si le premier énoncé de la suite est vrai, alors on peut raisonnablement se convaincre que le deuxième énoncé est vrai, puis le troisième, etc, jusqu'au dernier énoncé, qui est donc vrai. En particulier, le concept de raisonnement n'est absolument pas réservé aux mathématiques : quand un papa dit à son enfant « **si tu ne manges pas ton gratin de courgettes, tu seras privé de glace au chocolat** », l'enfant en *déduit* qu'il a tout intérêt à manger son gratin de courgettes (sauf si, bien évidemment, il préfère la glace à la pistache).

Il a donc, ne serait-ce qu'intuitivement, élaboré le raisonnement suivant :

1. Si je ne mange pas mes courgettes, je n'aurai pas de chocolat.
2. Or, j'aime tant le chocolat que je serais prêt à manger également des courgettes pour pouvoir en déguster.
3. Je vais donc manger des courgettes, et ainsi je pourrai ensuite manger du chocolat.

Notons cependant que ce raisonnement est, en toute généralité, *faux* ! En effet, la seule chose que l'enfant sait est que, s'il ne mange pas ses courgettes, il ne mangera pas de chocolat non plus. Mais si son papa est un logicien sadique, il se peut très bien que l'enfant n'ait pas droit à de la glace au chocolat *même s'il a mangé ses courgettes* ! Et oui : le papa a simplement dit « **si tu ne manges pas ton gratin de courgettes, tu seras privé de glace au chocolat** », mais n'a pas rajouté « **si tu manges ton gratin de courgettes, tu auras le droit de manger de la glace au chocolat** ».

C'est là l'une des difficultés que crée la langue française (de même que nombre d'autres langues) quand on essaie d'appréhender le raisonnement logique de manière précise : la deuxième partie de la phrase (celle que n'a pas rajoutée le papa) était sous-entendue dans ses propos : quel monstre oserait ainsi manipuler ses enfants, et surtout subir les pleurs assourdissants qui suivront à coup sûr la découverte d'un tel traquenard ? Il convient donc de faire très attention à distinguer *implication* et *équivalence*.

Dans notre exemple, l'assertion du papa était une simple implication : « **si A, alors B** ». Mais son enfant l'a interprété comme une équivalence : « **si A, alors B, et si (non A), alors (non B)** ». En outre, *implication* n'est pas *causalité*. Ainsi, la phrase « **si Paris est la capitale du Mali, alors Paris est la capitale du Togo** » est…*vraie* !

Ce que je viens de dire peut vous paraître évident, mais l'expérience montre que c'est loin d'être le cas pour tout le monde. En particulier, notons bien que l'on a dit « **si Paris est la capitale du Mali, alors Paris est la capitale du Togo** », et non pas « **si Paris *était* la capitale du Mali, alors Paris *serait* la capitale du Togo** ». Dans le premier cas, on dit qu'une assertion fausse implique une autre assertion fausse ; dans le deuxième cas, on essaie d'imaginer (de manière totalement floue) une situation où la première assertion serait vraie, et on se demande si la deuxième assertion serait vraie aussi : les deux cas de figure n'ont rien à voir !

Une fois encore, il faut donc se méfier des raccourcis de raisonnement auxquels on est habitué quand on parle dans la vie de tous les jours : on utilise un vocabulaire peu précis, parfois à mauvais escient, mais la situation est si simple que tout le monde comprend quand même ce que l'on veut dire, et ce même sans y faire attention. Cependant, quand on tient à énoncer des assertions précises et à les démontrer rigoureusement, et que ces assertions ne sont plus des évidences, alors il faut prendre garde de ne pas dire n'importe quoi, et choisir judicieusement les mots que l'on emploie devient indispensable !

C'est pour éviter cet écueil que les mathématiciens ont inventé leurs propres notations : chacun des symboles que l'on pourra ainsi utiliser a un sens bien précis, qu'il convient de connaître avant de l'utiliser, et qui permet d'énoncer des assertions aussi précises que possible, donc qui ont une chance d'être vraie. On pourrait se passer de telles notations et rédiger les mathématiques comme on le faisait dans l'Antiquité ou à la Renaissance. Mais le moindre exercice de $4^{\text{ème}}$ prendrait alors des pages et des pages, ce qui ne serait guère pratique.

Dans la suite, nous verrons donc quelques unes de ces notations mathématiques, mais surtout leur signification, ainsi que la manière de (ne pas) les utiliser : utiliser de telles notations à mauvais escient peut rendre un texte complètement inintelligible !

Exercice 1 Durant la première guerre mondiale, un militaire remarqua que, alors que presque toutes les parties des avions rentrés du combat portaient des traces d'impacts de balles, ce n'était jamais le cas du cockpit. Il annonça alors à ses supérieurs que le cockpit était fragile, et qu'il fallait le renforcer. Êtes vous d'accord avec cette conclusion ?

Si oui, donner un exemple de raisonnement aussi précis que possible, qui sera à même de convaincre n'importe quel général ; si non, expliquer tout aussi soigneusement pourquoi le militaire a tort.

De l'usage des symboles mathématiques

J'espère que les paragraphes précédents vous ont convaincu que les mathématiques étaient en fait du Français (ou de l'Anglais, de l'Allemand, de l'Esperanto, bref, votre langue préférée). Plus précisément, tous les symboles mathématiques, qui peuvent donner à cette discipline une apparence cryptique, sont en fait des raccourcis pour éviter de faire des vraies phrases tellement longues qu'elles en deviendraient illisibles.

Sans plus traîner, voyons donc les principaux de ces symboles, que l'on utilise en logique :

- $\neg$, la *négation* : on dit que « la négation de A » (ce que l'on note aussi « $\neg$ A », « $\overline{\text{A}}$ » ou « non A ») est vraie si et seulement si A est faux.
- $\wedge$, la *conjonction* : on dit que « A et B » (ce que l'on note aussi « A $\wedge$ B » ou « A $\cdot$ B ») est vrai si et seulement si A et B sont tous les deux vrais.
- $\vee$, la *disjonction* : on dit que « A ou B » (ce que l'on note aussi « A $\vee$ B » ou « A + B ») est vrai si et seulement si, au choix, soit A est vrai, soit B est vrai (soit les deux).
- $\Rightarrow$, l'*implication* : on dit que « A implique B » (ce que l'on note aussi « A $\Rightarrow$ B ») si et seulement si, au choix, soit A est faux, soit B est vrai (soit les deux).
- $\Leftrightarrow$, l'*équivalence* : on dit que « A est équivalent à B » (ce que l'on note aussi « A $\Leftrightarrow$ B ») si et seulement si, au choix, soit A et B sont tous les deux faux, soit ils sont tous les deux vrais.

Insistons une fois encore sur la locution « si et seulement si » : au paragraphe précédent, la papa disait « si A, alors B » alors qu'il pensait en fait « B si et seulement si A ». En particulier,

dans ses propos, rien ne l'empêchait de punir son enfant même si ce dernier était sage, alors qu'il pensait en fait récompenser le charmant bambin de sa sagesse éventuelle.

D'autre part, **attention** ! S'il est utile de connaître ces notations, au cas où on les rencontre un jour, il est très important de ne les utiliser qu'avec parcimonie ! En particulier, il est toujours plus sage de noter la négation, la disjonction et la conjonction avec des mots français (en écrivant « non », « ou » et « et ») plutôt qu'en utilisant des symboles cabalistiques, surtout dans une copie écrite à la va-vite et à l'écriture chancelante.

En particulier, voici le modèle-type, mais maintes fois rencontré, de ce qu'il ne faut *surtout pas faire* :

Prouvons qu'il existe une infinité d'entiers pairs. Supposons qu'il existe un nombre fini d'entiers pairs. Donc n pair maximal $\Rightarrow$ n+2 pair $\Rightarrow$ n n'est pas maximal $\Rightarrow$ impossible, d'où le résultat.

Évidemment, cet extrait de copie d'élève est une caricature inventée pour l'occasion, mais les incorrections qu'elle contient sont cependant couramment rencontrées dans une copie mathématique. Le début de la solution proposée est correct, mais les choses se gâtent à la phrase « Donc n pair … » En effet :

- L'entier n n'est nulle part défini : il faut *toujours* définir les objets que l'on utilise *avant* de les utiliser, ne serait-ce que de manière informelle ! Ici, l'entier n désigne implicitement l'entier pair maximal dont on a supposé (de manière erronée) l'existence.
- Marquer « impossible » en fin de ligne est sympathique ; faire une vraie phrase où l'on marque clairement que la situation évoquée ici est impossible serait beaucoup mieux !
- En faisant fi des précédentes remarques, on a montré que l'existence d'un entier pair maximal était impossible, mais le lien avec la finitude éventuelle de l'ensemble des entiers pairs n'apparait nulle part. En particulier, écrire « donc » en début de phrase laisse penser que la suite d'implications ici écrite dépend de la finitude supposée de l'ensemble des nombres pairs, alors que cette suite d'implications est vraie en toute généralité.

Il aurait plutôt fallu écrire quelque chose comme :

Prouvons qu'il existe une infinité d'entiers pairs. Supposons qu'il existe un nombre fini d'entiers pairs. Il en existe alors un maximal, que l'on note n. Puisque n est pair, alors n+2 est pair aussi, donc n ne peut pas être le plus grand entier pair, ce qui contredit sa définition. On en conclut que notre supposition aboutissait à une situation impossible, ce qui montre bien qu'elle était fausse, c'est-à-dire qu'il existe une infinité d'entiers pairs.

Il est important de se rappeler que savoir s'exprimer en mathématiques, c'est avant tout s'avoir s'exprimer en Français ! Le but, quand on écrit une rédaction mathématique, n'est pas simplement d'avoir raison, mais de convaincre l'autre que l'on a raison. Une copie vraie mais inintelligible ne vaut donc guère mieux qu'une copie fausse.

Exercice 2 Montrer soigneusement qu'il existe une infinité d'entiers impairs divisibles par 2013.

Logique booléenne et tables de vérité

Maintenant que l'on a découvert quelques symboles logiques ainsi que leur signification et la manière de les utiliser, faisons le lien avec ce que l'on appelle la logique *booléenne*. Ici, on identifie une assertion fausse à l'entier 0, et une assertion vraie à l'entier 1. En effet, en logique, on ne s'intéresse qu'au caractère faux ou vrai des assertions étudiées !

Par exemple, les assertions « Paris est la capitale du Mali » et « Paris est la capitale du Togo » sont fausses, donc toutes les deux identifiées à 0 : du point de vue de la logique, ces deux assertions sont strictement équivalentes. Au contraire, l'assertion « si Paris est la capitale du Mali, alors Paris est la capitale du Togo » est vraie, donc identifiée à 1, et est logiquement équivalente à toute autre assertion vraie.

La logique booléenne a un avantage certain, puisque l'on peut considérer toutes les assertions étudiées comme appartenant à l'ensemble $\{0,1\}$. En particulier, on peut ainsi redéfinir les *connecteurs logiques* mentionnés dans la partie précédente :

$\neg$: $\neg a = 1 - a$.

$\wedge$: $a \wedge b = a \times b$.

$\vee$: $a \vee b = \max\{a, b\}$.

$\Rightarrow$: $a \Rightarrow b = \max\{1 - a, b\}$.

$\Leftrightarrow$: $a \Leftrightarrow b = a \times b + (1 - a) \times (1 - b)$.

On peut aussi voir cela dans des *tables de vérité* :

a	**0**	**1**
$\neg a$	1	0

a	**0**	**0**	**1**	**1**
b	**0**	**1**	**0**	**1**
$a \wedge b$	0	0	0	1
$a \vee b$	0	1	1	1
$a \Rightarrow b$	1	1	0	1
$a \Leftrightarrow b$	1	0	0	1

C'est de là que viennent les notations $\cdot$ et $+$ utilisées pour symboliser la conjonction et la disjonction : la conjonction peut vraiment être considérée comme un produit, tandis que la disjonction peut être vue comme une addition (à ceci près que l'on impose la relation $1+1 = 1$, car le résultat d'une disjonction ne peut prendre que les valeurs 0 et 1).

On reconnaît bien là le fait que l'assertion « si Paris est la capitale du Mali, alors Paris est la capitale du Togo » est vraie : puisque « Paris est la capitale du Mali » et « Paris est la capitale du Togo » sont identifiées à l'entier 0, alors l'assertion « si Paris est la capitale du Mali, alors Paris est la capitale du Togo » est identifiée à l'entier $(0 \Rightarrow 0) = \max\{1 - 0, 0\} = 1$.

En outre, l'utilisation de tables de vérité rend particulièrement efficace, dans certains cas, la démonstration de certaines propositions. Par exemple, on peut se demander à quelles conditions sur a, b et c la proposition $a \Rightarrow (b \Leftrightarrow c)$ est vraie. Il suffit alors de faire une table de vérité, certes un peu plus grande que celles montrées ci-dessus :

a	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**
b	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**
c	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**
$b \Leftrightarrow c$	1	0	0	1	1	0	0	1
$a \Rightarrow (b \Leftrightarrow c)$	1	1	1	1	1	0	0	1

Ici, on constate que la proposition $a \Rightarrow (b \Leftrightarrow c)$ est vraie dès lors que $a = 0$, ou bien que $b = c$ (ce dont on aurait certes pu se douter dès le départ), et faux dans les autres cas.

Exercice 3 Montrer que toute fonction $f : \{0,1\} \times \{0,1\} \to \{0,1\}$ peut s'écrire à partir des connecteurs logiques $\vee$, $\wedge$ et $\neg$. Peut-on généraliser le résultat aux fonctions $f : \{0,1\}^n \to \{0,1\}$?

Quantificateurs existentiel et universel

Deux autres symboles que vous avez pu déjà rencontrer, mais qui ne sont pas encore mentionnés ici, sont les symboles de *quantification* :

- $\forall$, le quantificateur *universel* : si E est un ensemble et $P(x)$ est une propriété, dépendant d'un élément x de E (et qui peut donc être vraie ou fausse selon l'élément considéré), alors on dit que « pour tout x appartenant à E, $P(x)$ est vraie » (ce que l'on note « $\forall x \in E, P(x)$ ») si et seulement si la propriété $P(x)$ est vraie pour tous les éléments x de E.
- $\exists$, le quantificateur *existentiel* : si E est un ensemble et $P(x)$ est une propriété, dépendant d'un élément x de E (et qui peut donc être vraie ou fausse selon l'élément considéré), alors on dit que « il existe un élément x de E tel que $P(x)$ est vraie » (ce que l'on note « $\exists x \in E, P(x)$ ») si et seulement si la propriété $P(x)$ est vraie pour au moins un élément x de E.

Intuitivement, le quantificateur universel consiste en fait en une immense conjonction, qui regrouperait tous les éléments de E : par exemple, si E est un ensemble fini, contenant les trois éléments a, b et c, alors $\forall x \in E, P(x)$ est une assertion vraie si et seulement si $P(a)$, $P(b)$ et $P(c)$ sont toutes les trois vraies, ce que l'on peut aussi écrire $P(a) \wedge P(b) \wedge P(c)$. Mais utiliser le quantificateur universel est pratique quand E est un ensemble très grand, voire un ensemble infini ! ou alors quand on ne connaît pas bien les éléments de E.

De même, le quantificateur existentiel consiste en fait en une immense disjonction, qui regrouperait tous les éléments de E : dans le même exemple que précédemment, $\exists x \in E, P(x)$ est une assertion vraie si et seulement si au moins l'une des assertions $P(a)$, $P(b)$ et $P(c)$ est vraie, ce que l'on peut aussi écrire $P(a) \vee P(b) \vee P(c)$.

Cependant, et de même que pour les connecteurs logiques tels que $\Rightarrow$ et $\vee$, il faut faire attention à la façon dont on utilise les symboles $\forall$ et $\exists$ et, dans le doute, mieux vaut mettre explicitement « pour tout x appartenant à l'ensemble E… » En particulier, il faut bien prendre garde de ne jamais utiliser ces quantificateurs si l'on ne sait pas dans quel ensemble E on peut choisir l'élément x. Et, bien sûr, de même qu'il faut à tout prix éviter d'écrire « $\Rightarrow$ » au lieu de « donc », ou bien « $\Leftrightarrow$ » au lieu de « ce qui est équivalent à » ou « c'est-à-dire », on n'utilise pas les symboles « $\forall$ » et « $\exists$ » en guise d'abbréviation : gare à celui qui écrira « `merci ∀ !` » à la fin d'une lettre de remerciements !

Enfin, il faut bien évidemment prendre garde de ne jamais définir deux fois le même objet, et de se rappeler que les *variables* définies à l'aide d'un quantificateur existentiel ou universel sont muettes :

- les assertions « $\forall x \in E, P(x)$ » et « $\forall \zeta \in E, P(\zeta)$ » sont équivalentes (quand bien même le symbole ζ fait beaucoup plus savant qu'un banal x) ;
- l'assertion « $\exists x \in E, \forall x \in F, P(x)$ » n'a aucun sens, car la variable x était déjà définie (dans la partie « $\exists x \in E$ ») quand on tente de la redéfinir (dans la partie « $\forall x \in F$ »).

Jouer avec les formules logiques

L'intérêt des connecteurs logiques et des quantificateurs est d'exprimer simplement des formules mathématiques. Cependant, certaines formules peuvent être difficiles à manipuler, de même qu'il peut être difficile de se faire une intuition sur le sens mathématique de la proposition qu'elles représentent. Une idée est donc de simplifier les formules, et également de reconnaître certains cas où l'on aurait envie, mais à tort, de croire que certaines formules sont équivalentes alors qu'elles ne le sont pas.

Tout d'abord, voici quelques relations que l'on peut trouver entre les connecteurs logiques, et que l'on peut facilement vérifier à l'aide de tables de vérité :

- **A est équivalent à B** si et seulement si **A et B s'impliquent l'un l'autre**.
- **A implique B** si et seulement si **(non A) ou B** est vrai.
- **A ou B** est vrai si et seulement si **non ((non A) et (non B))** est vrai.
- **A et B** est vrai si et seulement si **non ((non A) ou (non B))** est vrai.
- **non(non A)** est vrai si et seulement si **A** est vrai.

Les deux dernières lignes sont aussi connues sont le nom de *lois de De Morgan*, en hommage à celui qui les a identifiées pour la première fois, et du fait de leur importance.

a	**0**	**1**
$\neg a$	1	0
$\neg(\neg a)$	0	1

$a \equiv \neg(\neg a)$

a	**0**	**0**	**1**	**1**
b	**0**	**1**	**0**	**1**
$a \Leftrightarrow b$	1	0	0	1
$a \Rightarrow b$	1	1	0	1
$b \Rightarrow a$	1	0	1	0
$(a \Rightarrow b) \wedge (b \Rightarrow a)$	1	0	0	1

$a \Leftrightarrow b \equiv (a \Rightarrow b) \wedge (b \Rightarrow a)$

a	**0**	**0**	**1**	**1**
b	**0**	**1**	**0**	**1**
$a \Rightarrow b$	1	1	0	1
$\neg a$	1	1	0	0
$(\neg a) \vee b$	1	1	0	0

$a \Rightarrow b \equiv (\neg a) \vee b$

a	**0**	**0**	**1**	**1**
b	**0**	**1**	**0**	**1**
$a \vee b$	0	1	1	1
$\neg(a \vee b)$	1	0	0	0
$\neg a$	1	1	0	0
$\neg b$	1	0	1	0
$(\neg a) \wedge (\neg b)$	1	0	0	0

$\neg(a \vee b) \equiv (\neg a) \wedge (\neg b)$

a	**0**	**0**	**1**	**1**
b	**0**	**1**	**0**	**1**
$a \wedge b$	0	0	0	1
$\neg(a \wedge b)$	1	1	1	0
$\neg a$	1	1	0	0
$\neg b$	1	0	1	0
$(\neg a) \vee (\neg b)$	1	1	1	0

$\neg(a \wedge b) \equiv (\neg a) \vee (\neg b)$

On peut faire encore plus fort et toujours transformer une formule logique en une formule équivalente, mais :

- sans symbole $\Rightarrow$, $\Leftrightarrow$, et
- où les symboles $\neg$ apparaissent toujours aussi à droite que possible.

Concrètement, on commence par faire disparaître tous les symboles $\Rightarrow$ ou $\Leftrightarrow$ en utilisant les relations ci-dessus. Puis il s'agit de faire passer un symbole $\neg$ « à droite » d'un connecteur $\neg$, $\vee$ ou $\wedge$, ou d'un quantificateur $\forall$ ou $\exists$. On procède alors en faisant les transformations suivantes :

- « $\neg(\forall \mathbf{x} \in \mathbf{E}, \mathbf{P}(\mathbf{x}))$ » devient « $\exists \mathbf{x} \in \mathbf{E}, \neg\mathbf{P}(\mathbf{x})$ ».
- « $\neg(\exists \mathbf{x} \in \mathbf{E}, \mathbf{P}(\mathbf{x}))$ » devient « $\forall \mathbf{x} \in \mathbf{E}, \neg\mathbf{P}(\mathbf{x})$ ».
- « $\neg(\mathbf{a} \wedge \mathbf{b})$ » devient « $(\neg\mathbf{a}) \vee (\neg\mathbf{b})$ ».
- « $\neg(\mathbf{a} \vee \mathbf{b})$ » devient « $(\neg\mathbf{a}) \wedge (\neg\mathbf{b})$ ».
- « $\neg(\neg\mathbf{a})$ » devient « $\mathbf{a}$ ».

On a déjà montré, ci-dessus, que les trois dernières simplifications étaient légitimes. Quant aux deux premières, on se convainc facilement qu'elles fonctionnes si on se rappelle que les quantificateurs existentiel et universel représentent respectivement des disjonctions et des conjonctions « géantes ».

Cela dit, si on le préfère, on peut aussi constater directement que ces simplifications fonctionnent : dire « **il est faux que la proposition** $P(x)$ **soit vérifiée pour tout** $x \in E$ » revient à dire « **il existe au moins un** $x \in E$ **tel que la proposition** $P(x)$ **n'est pas vérifiée** », ou encore « **il existe au moins un** $x \in E$ **tel que la proposition** $\neg P(x)$ **est vérifiée** ». De même, dire « **il est faux que la proposition** $P(x)$ **soit vérifiée pour au moins un** $x \in E$ » revient à dire « **pour tout** $x \in E$**, la proposition** $P(x)$ **n'est pas vérifiée** », ou encore « **pour tout** $x \in E$**, la proposition** $\neg P(x)$ **est vérifiée** ». Devant la lourdeur de telles phrases, on comprend vite l'intérêt de l'utilisation du langage mathématique et de ses symboles.

Enfin, de même que l'ordre des mots est important en Français, l'ordre des mots ou des symboles est important en mathématique. Ainsi, les phrases « **La France a battu la Suisse 3 à 0** » et « **La Suisse a battu la France 3 à 0** » n'ont pas du tout la même signification, alors qu'on s'est contenté d'y échanger les places de deux mots. De même, l'ordre des connecteurs et quantificateurs est très important. Par exemple, on peut dire que tout enfant a une maman : « **pour tout élément E de l'ensemble des enfants, il existe un élément M de l'ensemble des mamans tel que M est la maman de E** ». Cette phrase est très différente de la suivante, et qui signifie que tous les enfants du monde ont la même maman : « **il existe un élément M de l'ensemble des mamans tel que, pour tout élément E de l'ensemble des enfants, M est la maman de E** ».

Pour résumer, notons que :

- on peut toujours échanger deux occurrences successives du quantificateur universel : les assertions « $\forall x \in E, \forall y \in F, P(x,y)$ » et « $\forall y \in F, \forall x \in E, P(x,y)$ » sont équivalentes ;
- on peut toujours échanger deux occurrences successives du quantificateur existentiel : les assertions « $\exists x \in E, \exists y \in F, P(x,y)$ » et « $\exists y \in F, \exists x \in E, P(x,y)$ » sont équivalentes ;
- on ne peut *pas* échanger deux quantificateurs universel et existentiel (a priori) : les assertions « $\forall x \in E, \exists y \in F, P(x,y)$ » et « $\exists y \in F, \forall x \in E, P(x,y)$ » ne sont en général pas équivalentes ;
- on peut toujours faire passer les symboles $\neg$ le plus à droite possible (en faisant comme indiqué ci-dessus) ;
- on peut toujours modifier le nom d'une variable introduite à l'aide d'un quantificateur existentiel ou universel (mais alors il faut faut faire attention de modifier le nom de cette variable à chaque fois qu'elle apparait ensuite, et à ne pas réutiliser un nom de variable déjà utilisé) ;
- on peut toujours faire passer le quantificateur universel à gauche des connecteurs **ou** et **et** : les assertions « $(\forall x \in E, P(x,y)) \vee Q(y))$ » et « $\forall x \in E, (P(x,y) \vee Q(y))$ » sont équivalentes, de même que les assertions « $(\forall x \in E, P(x,y)) \wedge Q(y))$ » et « $\forall x \in E, (P(x,y) \wedge Q(y))$ » sont équivalentes ;
- on peut toujours faire passer le quantificateur existentiel à gauche des connecteurs **ou** et **et** : les assertions « $(\exists x \in E, P(x,y)) \vee Q(y))$ » et « $\exists x \in E, (P(x,y) \vee Q(y))$ » sont équivalentes, de même que les assertions « $(\exists x \in E, P(x,y)) \wedge Q(y))$ » et « $\exists x \in E, (P(x,y) \wedge Q(y))$ » sont équivalentes.

On peut se dire qu'il y a là beaucoup de règles à retenir : ce n'est pas totalement faux, mais on peut aussi les réinventer en direct tant elles sont naturelles : une méthode pratique est de

regarder ce que de telles règles (celles-ci ou d'autres qu'on aura voulu inventer) donnent sur des exemples simples, ou encore de se rappeler que les quantificateurs ne sont rien d'autre que des conjonctions et des disjonctions géantes.

Exercice 4 On dit qu'une suite $(u_n)_{n\in\mathbb{N}}$ a une limite $L \in \mathbb{R}$ si et seulement si $\forall \varepsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\varepsilon > 0 \wedge n \geqslant N) \Rightarrow |L - u_n| \leqslant \varepsilon$. Cette définition est-elle équivalente aux définitions suivantes ?

1. $\forall \varepsilon \in \mathbb{R}, \varepsilon \leqslant 0 \vee (\exists N \in \mathbb{N}, \forall n \in \mathbb{N}, |L - u_n| \leqslant \varepsilon \vee n < N)$;
2. $\forall \varepsilon \in \mathbb{R}, \forall n \in \mathbb{N}, \exists N \in \mathbb{N}, (\varepsilon > 0 \wedge n \geqslant N) \Rightarrow |L - u_n| \leqslant \varepsilon$;
3. $\forall \varepsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\varepsilon > 0 \wedge n > N) \Rightarrow |L - u_n| < \varepsilon$;
4. $\exists N \in \mathbb{N}, \forall \varepsilon \in \mathbb{R}, \forall n \in \mathbb{N}, (\varepsilon > 0 \wedge n \geqslant N) \Rightarrow |L - u_n| \leqslant \varepsilon$.

- Différents types de raisonnements -

Le raisonnement par équivalences successives

Nous avons raconté, ci-dessus, en quoi la logique traitait des assertions qui sont soit vraies, soit fausses. En outre, nous avons vu comment lier certaines de ces assertions à d'autres, au moyen de *connecteurs logiques* comme la disjonction et l'équivalence. Il nous faut maintenant nous intéresser au *raisonnement*, c'est-à-dire à ce qui permet de dire, sachant que certaines propositions sont vraies, qu'une autre proposition est vraie (ou fausse).

Le premier de ces modes de raisonnement est le raisonnement *par équivalences successives*. Il vise à répondre à des questions du type : « **Quels sont les entiers** n **tels que la propriété** $P(n)$ **soit vraie ?** » Pour répondre à une telle question, on cherche des propriétés $P_1, P_2, \dots, P_k$ telles que, quel que soit l'entier n considéré, $P(n) \Leftrightarrow P_1(n) \Leftrightarrow P_2(n) \Leftrightarrow \cdots \Leftrightarrow P_k(n)$. Alors on peut dire que les entiers n tels que la propriété $P(n)$ est vraie sont exactement les entiers n tels que la propriété $P_k(n)$ est vraie.

Notons, au passage, que ce genre de raisonnements n'a d'intérêt que si la propriété P_k apparaît comme plus simple ou plus naturelle que la propriété P elle-même. Sinon, point n'était besoin de s'embêter, on aurait pu se contenter de l'assertion (évidente mais peu informative) selon laquelle « **Les entiers** n **tels que la propriété** $P(n)$ **est vraie sont les entiers tels que la propriété** $P(n)$ **est vraie.** »

Le raisonnement par analyse et synthèse

Dans certains cas, il est difficile de procéder par équivalences successives : comment trouver la suite de propriétés $P_1, P_2, \dots, P_k$ qui fonctionnera ? On peut alors recourir à un autre type de raisonnement, *a priori* plus facile à trouver : le raisonnement *par analyse et synthèse*. Lui aussi vise à répondre aux questions du type : « **Quels sont les entiers** n **tels que la propriété** $P(n)$ **soit vraie ?** » Cependant, le processus suivi est différent.

Dans un premier temps, on cherche des propriétés $P_1, P_2, \dots, P_k$ telles que, quel que soit l'entier n considéré, $P(n) \Rightarrow P_1(n) \Rightarrow P_2(n) \Rightarrow \cdots \Rightarrow P_k(n)$: il s'agit de la phase d'*analyse*. Puis, dans un deuxième temps, on cherche d'autres propriétés $Q_1, Q_2, \dots, Q_\ell$ telles que, quel que soit l'entier n considéré, $P_k(n) \Rightarrow Q_1(n) \Rightarrow Q_2(n) \Rightarrow \cdots \Rightarrow Q_\ell(n) \Rightarrow P(n)$: c'est la phase de *synthèse*.

On peut alors en déduire que $P(n) \Rightarrow P_k(n)$ et que $P_k(n) \Rightarrow P(n)$, ce qui signifie que $P(n)$ et $P_k(n)$ sont des propriétés équivalentes. Notons que le raisonnement par équivalences successives est, dans un sens, un cas particulier du raisonnement par analyse et synthèse, où l'on aurait choisi $Q_1 = P_{k-1}, Q_2 = P_{k-2}, \dots, Q_\ell = P_1$. Cependant, s'il est possible de procéder directement par équivalences successives, il est alors souvent plus simple d'exposer le résultat obtenu.

En outre, il est bien sur possible d'inverser l'ordre des phases d'analyse et de synthèse, voire de mélanger les deux. De manière générale, on pourra toujours se permettre de mélanger plusieurs types de raisonnement différents ; mais alors il faudra veiller à rester très clair sur le type de raisonnement que l'on est en train de suivre : il faut que le lecteur ait toujours une idée assez précise du cheminement suivi dans le raisonnement, ce sans quoi il sera vite perdu, donc dans l'impossibilité de le comprendre.

Exercice 5 Identifier l'ensemble des paires (x, y) de nombres réels telles que $2x + y = 5$ et $x - 3y = 6$. On procédera de deux manières différentes :

1. par équivalences successives ;
2. par analyse et synthèse.

Le raisonnement par contraposée

Le raisonnement par contraposée est utile quand on veut démontrer des implications. Il vise à répondre à une question du type : « **Montrer que A $\Rightarrow$ B.** »

Il consiste simplement à montrer une *autre* implication que celle demandée, à savoir l'implication « (non B) $\Rightarrow$ (non A) ». En effet, en utilisant une table de vérité, on constate aisément que les deux propriétés « A $\Rightarrow$ B » et « (non B) $\Rightarrow$ (non A) » sont équivalentes :

A	**0**	**0**	**1**	**1**
B	**0**	**1**	**0**	**1**
$A \Rightarrow B$	1	1	0	1
$\neg A$	1	1	0	0
$\neg B$	1	0	1	0
$(\neg B) \Rightarrow (\neg A)$	1	1	0	1

$A \Rightarrow B \equiv (\neg B) \Rightarrow (\neg A)$

Le raisonnement par l'absurde

Le raisonnement par l'absurde repose sur le principe du *tiers exclus* : soit une propriété A est vraie, soit elle est fausse. Le raisonnement par l'absurde vise à répondre à une question du type : « **Montrer que la propriété A est fausse.** »

Il consiste alors à supposer que la propriété A est vraie, puis, sous cette hypothèse, à aboutir à une absurdité. En d'autres termes, il s'agit de trouver des propriétés $P_1, P_2, \dots, P_k$ telles que $A \Rightarrow P_1 \Rightarrow P_2 \Rightarrow \cdots \Rightarrow P_k$, où P_k est une propriété notoirement fausse. On en déduit alors que la propriété A ne pouvait être vraie et, puisqu'elle est nécessairement soit vraie soit fausse, elle est fausse.

En particulier, dès lors que l'on souhaite montrer qu'une propriété A est fausse, on peut toujours supposer, sans perte de généralité. En effet, dans la vie, il y a deux cas de figure :

soit la propriété A est fausse, auquel cas on a déjà gagné ; soit elle est vraie, et c'est le seul cas intéressant, donc le cas dans lequel on décide de se placer.

On notera cependant que de nombreux lecteurs tendent à considérer l'utilisation du raisonnement par l'absurde comme assez lourd : si on peu montrer directement que A est fausse, pourquoi s'embêter à supposer d'abord que A est vraie, et ainsi s'encombrer d'une hypothèse inutile ? De manière générale, en effet, plus une preuve est simple, mieux elle sera comprise, et plus son auteur sera content.

Enfin, notons le raisonnement par l'absurde n'est qu'un cas particulier du raisonnement par contraposée : en effet, pour montrer la propriété « non A » — c'est-à-dire la propriété « **Vrai** $\Rightarrow$ (non A) » — on a en fait montré la propriété « A $\Rightarrow$ **Faux** ».

Exercice 6 Identifier l'ensemble des entiers naturels non nuls n tels que n^n est pair.

Le raisonnement par récurrence

Le raisonnement par récurrence fait suite à la question naïve : jusqu'où savez-vous compter ? Poser cette question à un enfant en bas-âge est généralement délectable, car quand il annonce un nombre (par exemple « un million »), on peut lui demander : « alors tu ne sais pas compter jusqu'à un million un ? » Ce à quoi il répondra invariablement « si, bien sûr ! »

De manière générale, quand on sait compter de 1 jusqu'à n et qu'on sait compter de n jusqu'à $n+1$, alors on sait compter de 1 jusqu'à $n+1$. Puis, si l'on sait compter de $n+1$ jusqu'à $n+2$, alors on sait en fait compter de 1 jusqu'à $n+2$. Et ainsi de suite. C'est cet *ainsi de suite* que le raisonnement par récurrence permet de formaliser.

Le raisonnement par récurrence vise à répondre à une question du type : « **Montrer que la propriété** $P(n)$ **est vraie pour tout entier naturel** n**.** » Il consiste en 3 étapes (que l'on peut traiter dans l'ordre qu'on veut, mais qui sont usuellement présentées dans cet ordre) :

1. L'initialisation : On montre que la propriété $P(0)$ est vraie.
2. L'hérédité : On montre que, si n est un entier naturel tel que $P(n)$ est vraie, alors $P(n+1)$ est vraie aussi.
3. La conclusion : On en conclut que $P(n)$ est vraie pour tous les entiers naturels.

Pourquoi cela marche-t-il ? Montrons-le avec un raisonnement par l'absurde, et supposons qu'il existe moins un entier naturel n tel que $P(n)$ est fausse. Alors l'ensemble $E = \{n \in \mathbf{N} : P(n) \text{ fausse}\}$ des entiers naturels n tels que $P(n)$ est fausse est un ensemble non vide. Par conséquent, il admet un élément minimal, que l'on notera m. Puisque $P(0)$ est vraie, on sait que $m > 0$. En particulier, puisque $m-1$ est un entier naturel strictement inférieur à m, on en conclut que $P(m-1)$ est vraie. Mais alors la phase d'hérédité nous prouve que $P(m)$ est vraie aussi, ce qui contredit le fait que m appartienne à l'ensemble E ! Notre supposition était donc fausse, ce qui clôt notre démonstration.

Notons ici que, dans tous les cas, on pourra remplacer un raisonnement par récurrence par un raisonnement par l'absurde similaire à celui présenté ci-dessus. En particulier, de manière générale, quand on veut montrer qu'une propriété $P(n)$ est vraie pour tous les entiers naturel n, il peut toujours être pratique de procéder par l'absurde, en supposant que l'ensemble E est non vide, puis se concentrer sur un élément remarquable de E : son minimum, son maximum (si E est nécessairement fini, par exemple dans le cas d'une propriété $P(n)$ vraie dès que $n \geqslant 2013^{2013}$), un nombre premier qui appartiendra éventuellement à E, etc.

Ce type de généralisation nous permet d'ailleurs d'utiliser un raisonnement par *récurrence forte*, analogue au raisonnement par récurrence :

1. L'initialisation : On montre que la propriété $P(0)$ est vraie.
2. L'hérédité : On montre que, si n est un entier naturel tel que $P(k)$ est vraie pour tous les entiers naturel $k \leqslant n$, alors $P(n+1)$ est vraie aussi.
3. La conclusion : On en conclut que $P(n)$ est vraie pour tous les entiers naturels.

Une fois encore, la légitimité du raisonnement par récurrence s'observe facilement si l'on considère l'ensemble E des entiers naturels n tels que $P(n)$ est fausse.

Enfin, voici une chose à laquelle il convient de faire extrêmement attention : dans la plupart des cas, le problème que vous étudierez ne vous demandera pas de montrer une propriété que l'on montre directement par récurrence. Souvent, ce sera à vous d'inventer une propriété, que vous prouverez par récurrence, puis à l'aide de laquelle vous pourrez résoudre l'exercice. Il convient alors d'être vigilant et d'exprimer très clairement quelle est la propriété que l'on veut montrer par récurrence : on ne saurait trop vous conseiller, avant toute démonstration par récurrence, d'énoncer explicitement la propriété $P(n)$ que l'on entend démontrer. En effet, en pratique, il n'est pas rare de voir un élève prétendre démontrer une propriété P par récurrence, mais ne pas utiliser la bonne initialisation (montrant une propriété $Q(0)$ plus faible que la propriété $P(0)$) ou se tromper dans la phase d'hérédité (en utilisant une hypothèse du type « **si** $Q(n)$ **est vraie, alors** $P(n+1)$ **est vraie** » pour une propriété $Q(n)$ plus forte que la propriété $P(n)$) !

Exercice 7 Soit (u_n) la suite réelle telle que $u_0 = 3$ et $u_{n+1} = \sqrt{2+u_n}$. Montrer que la suite (u_n) est bien définie et strictement décroissante.

- Conclusion : a-t-on tout raconté ici ? -

Ce cours constitue une simple introduction à la logique : on y a donc donné quelques idées simples à la base du raisonnement mathématique, et qu'il est absolument nécessaire de maîtriser si l'on tient à mener quelque raisonnement que ce soit. En particulier, rappelons ici les quelques grands principes qu'il convient de ne jamais oublier :

- ne jamais utiliser une notion ou un objet non encore défini ;
- dans le doute, toujours préférer écrire une phrase claire en Français plutôt que d'aligner des symboles dont la signification sera douteuse ;
- ne pas confondre implication, corrélation et équivalence ;
- toujours rester aussi clair que possible sur le déroulement de la démonstration que l'on est en train d'écrire : si l'on parle de raisonnement par l'absurde au lieu de parler de raisonnement par analyse et synthèse, on perdra le lecteur à coup sûr !
- ne pas oublier qu'une démonstration non comprise par le lecteur est assimilable à une démonstration fausse.

Si ce domaine vous intéresse, vous découvrirez plus tard qu'il est en effet très profond, et passionnant, avec des résultats tels que :

- l'étude des propriétés exprimables dans un certain vocabulaire (par exemple avec les connecteurs logiques et les quantificateurs mentionnés ci-dessus) ;
- l'apparition de paradoxes, qui montrent qu'on peut facilement énoncer des définitions dénuées de sens (que dire de l'ensemble de tous les ensembles ?) ;

– l'existence de propriétés vraies mais non démontrables, ou encore « ni vraies ni fausses » (ce sont des propriétés dont on peut supposer qu'elles sont vraies ou fausses, et ce sans aboutir à une contradiction) : et oui, ça parait fou, mais c'est pourtant vrai !

- Solutions des exercices -

Solution de l'exercice 1 Nous allons montrer ici que le militaire a **raison**. On peut supposer, sans prendre trop de risques, que les balles ennemies arrivent à peu près uniformément sur la surface de l'avion ; en particulier, il est certain que les cockpits doivent recevoir des balles, comme toutes les autres parties de l'avion. Or, nul avion dont le cockpit a été touché par une balle n'est rentré à bon aéroport. On en conclut donc que, dès lors qu'un avion est touché par une balle, il est condamné au crash. Cela signifie que le cockpit est **très** fragile, et donc qu'il faut en effet songer à le renforcer !

Solution de l'exercice 2 On pourrait utiliser un raisonnement par l'absurde, comme dans le cours qui précède. Cependant, on peut également fournir une preuve directe. En effet, pour tout entier naturel n, notons que $2013(2n+1)$ est un entier impair divisble par 2013 ; en outre, ces entiers sont deux à deux distincts. Il s'ensuit donc que ces entiers sont en nombre infini et que, *a fortiori*, il existe une infinité d'entiers impairs divisibles par 2013.

Solution de l'exercice 3 On va ruser un peu, et fournir une construction générique permettant de représenter toute fonction $f : \{0,1\}^n \to \{0,1\}$ à partir des connecteurs logiques $\vee$, $\wedge$ et $\neg$. En effet, rien que dans le cas $n = 2$, on a 2 valeurs possibles pour chacun des 2^2 éléments de $\{0,1\}^2$, soit $2^{2^2} = 16$ fonctions possibles : dans le cas général, il existe 2^{2^n} fonctions $f : \{0,1\}^n \to \{0,1\}$ possibles, et il serait peine perdue d'exxayer de les énumérer toutes.

La construction que nous allons utiliser est la *forme normale disjonctive*. Elle est très pratique, puisque deux formules de logique propositionnelle (sans quantificateurs) sont identiques si et seulement si elles ont même forme normale disjonctive : et, puisque deux formules de logique propositionnelle peuvent être interprétées comme des fonctions $f : \{0,1\}^n \to \{0,1\}$, il nous suffit de définir la forme normale disjonctive pour ces 2^{2^n} fonctions possibles.

Pour ce faire, fixons une fonction f. On note F l'ensemble des n-uplets $(x_1, x_2, \ldots, x_n)$ tels que $f(x_1, x_2, \ldots, x_n) = 1$. Ensuite, à chaque tel n-uplet x, on associe une conjonction X, appelée *forme normale disjonctive* de f : on choisit $X = \left(\bigwedge_{x_i=0} (\neg v_i)\right) \wedge \left(\bigwedge_{x_i=1} v_i\right)$. Puis on associe à f la disjonction $\bigvee_{x \in F} X$. Remarquons que, alors que nous avons noté les variables de f par $x_1, x_2, \ldots, x_n$, les variables utilisées dans la formule associée à la fonction f sont $v_1, v_2, \ldots, v_n$. Cependant, à ce renommage près (délibérément choisi ici, pour ne pas confondre les x_i et les v_i), on vérifie facilement que $\bigvee_{x \in F} X$ représente effectivement la fonction f.

Solution de l'exercice 4 Nous allons montrer que la définition d'une suite $(u_n)_{n \in \mathbb{N}}$ ayant une limite $L \in \mathbb{R}$ — que nous noterons « définition 0) » pour des raisons pratiques — est équivalente aux définitions 1) et 3), mais pas aux définitions 2) et 4).

1. Transformons progressivement notre définition 0) en des définitions qui lui sont équivalentes :

   0) est équivalent à $\forall \varepsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \neg(\varepsilon > 0 \wedge n \geqslant N) \vee |L - u_n| \leqslant \varepsilon$
   est équivalent à $\forall \varepsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \varepsilon \leqslant 0 \vee n < N \vee |L - u_n| \leqslant \varepsilon$
   est équivalent à $\forall \varepsilon \in \mathbb{R}, \varepsilon \leqslant 0 \vee (\exists N \in \mathbb{N}, \forall n \in \mathbb{N}, n < N \vee |L - u_n| \leqslant \varepsilon)$
   est équivalent à 1).

2. Il nous suffit de remarquer que la suite $(u_n)_{n\in\mathbb{N}}$ telle que tout $u_n = 0$ et le réel $L = -2$ satisfont la définition 2) mais pas 0) :
   - Dans la définition 0), si on prend $\varepsilon = 1$, alors $|L - u_N| > \varepsilon$ (alors que $\varepsilon > 0$ et que $N \geqslant N$) quelque soit $N \in \mathbb{N}$.
   - Dans la définition 2), si on prend de manière systématique $N = n + 1$, on remarque que l'assertion $\varepsilon > 0 \wedge n \geqslant N$ est nécessairement fausse, donc que la définition 2) est nécessairement satifsaite.
3. Montrons que les définitions 0) et 3) s'impliquent mutuellement :

   0) est équivalent à $\forall \varepsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\varepsilon > 0 \wedge n \geqslant N) \Rightarrow |L - u_n| \leqslant \varepsilon$
   est équivalent à $\forall \epsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\epsilon/2 > 0 \wedge n \geqslant N) \Rightarrow |L - u_n| \leqslant \epsilon/2$
   est équivalent à $\forall \epsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\epsilon > 0 \wedge n \geqslant N) \Rightarrow |L - u_n| \leqslant \epsilon/2$
   implique $\forall \epsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\epsilon > 0 \wedge n \geqslant N) \Rightarrow |L - u_n| < \epsilon$
   implique $\forall \epsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\epsilon > 0 \wedge n > N) \Rightarrow |L - u_n| < \epsilon$
   implique 3)

   3) est équivalent à $\forall \varepsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\varepsilon > 0 \wedge n > N) \Rightarrow |L - u_n| < \varepsilon$
   est équivalent à $\forall \varepsilon \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (\varepsilon > 0 \wedge n \geqslant N + 1) \Rightarrow |L - u_n| < \varepsilon$
   implique $\forall \varepsilon \in \mathbb{R}, \exists M \in \mathbb{N}, \forall n \in \mathbb{N}, (\varepsilon > 0 \wedge n \geqslant M) \Rightarrow |L - u_n| < \varepsilon$
   implique $\forall \varepsilon \in \mathbb{R}, \exists M \in \mathbb{N}, \forall n \in \mathbb{N}, (\varepsilon > 0 \wedge n \geqslant M) \Rightarrow |L - u_n| \leqslant \varepsilon$
   implique 0).
4. Il nous suffit de remarquer que la suite $(u_n)_{n\in\mathbb{N}}$ telle que tout $u_n = \frac{1}{n+1}$ et le réel $L = 0$ satisfont la définition 0) mais pas 3) :
   - Dans la définition 3), si on prend $\varepsilon = \frac{1}{N+2}$, alors $|L - u_N| > \varepsilon$ (alors que $\varepsilon > 0$ et que $N \geqslant N$) quelque soit $N \in \mathbb{N}$.
   - Dans la définition 0), si on prend de manière systématique $N = 1$ quand $\varepsilon \leqslant 0$ et $N > \frac{1}{\varepsilon}$ quand $\varepsilon > 0$, on remarque que soit l'assertion $\varepsilon > 0 \wedge n \geqslant N$ est fausse, soit l'assertion $|L - u_n| \leqslant \varepsilon$ est vraie, de sorte que la définition 0) est nécessairement satifsaite.

Solution de l'exercice 5 Comme demandé dans l'énoncé, identifions l'ensemble des paires (x, y) de nombres réels telles que $2x + y = 5$ et $x - 3y = 6$ en procédant d'abord par équivalences successives, puis par analyse et synthèse.

1. Transformons ici le système d'équations $\{2x+y = 5, x-3y = 6\}$ en des systèmes d'équations qui lui sont équivalents :

   $\{2x + y = 5, x - 3y = 6\}$ est équivalent à $\{y = 5 - 2x, x = 3y + 6\}$
   est équivalent à $\{y = 5 - 2x, x = 21 - 6x\}$
   est équivalent à $\{y = 5 - 2x, 7x = 21\}$
   est équivalent à $\{x = 3, y = -1\}$

   Donc l'ensemble des paires (x, y) solutions de notre système d'équation est l'ensemble $\mathcal{S} = \{(3, -1)\}$.
2. Recommençons le travail en procédant par analyse et synthèse : si $2x+y = 5$ et $x-3y = 6$, alors $x = 3y + 6$, donc $2(3y + 6) + y = 7y + 12 = 5$; il s'ensuit que $7y = -7$, c'est-à-dire $y = -1$, puis $x = 3y + 6 = 3$. Réciproquement, on vérifie aisément que la paire $(x, y) = (3, -1)$ est bien une solution au problème, donc que l'ensemble des solutions recherché est l'ensemble $\mathcal{S} = \{(3, -1)\}$.

Solution de l'exercice 6 Nous allons montrer que l'ensemble recherché est l'ensemble des entiers pairs. Pour ce faire, nous allons procéder par analyse et synthèse. Dans un premier temps (l'analyse), montrons que les entiers recherchés sont nécessairement pairs ; nous aboutirons à ce résultat en démontrant sa contraposée : si n est impair, alors n^n est impair aussi.

Ce dernier résultat est obtenu à la suite d'une récurrence, où nous montrons en fait la propriété $P(k)$ suivante : si n est impair, alors n^k est impair aussi. L'initialisation, pour $k = 0$, est évidente : en effet, $n^0 = 1$ est bien impair ; il s'ensuit que $P(0)$ est effectivement vraie. De surcroit, soit k un entier naturel tel que $P(k)$ est vraie : si n est impair, alors $n^{k+1} = n \times n^k$ est le produit de deux nombres impairs, donc est un nombre impair lui-même ; cela prouve la propriété $P(k)$. On en déduit que la propriété $P(k)$ set vraie quel que soit l'entier naturel k considéré : en particulier, si n est impair, $P(n)$ montre bien que n^n est impair également.

Procédons maintenant à la phase de synthèse, et montrons que, si n est pair, n^n est pair aussi : si n est pair, alors 2 divise n, donc 2 divise $n \times n^{n-1} = n^n$ aussi, et n^n est bien pair !

En conclusion, l'ensemble recherché est bien l'ensemble des entiers pairs.

Solution de l'exercice 7 Que peut signifier le fait que la suite (u_n) soit *bien définie* ? Cela veut tout simplement dire que chacun des termes $2 + u_n$ doit être positif ou nul, de sorte que l'on puisse en extraire la racine carrée. Prouvons donc tout cela à l'aide d'une unique récurrence, et prouvons la propriété $P(k)$ = « les termes u_k et u_{k+1} sont bien définis, et tels que $u_k > u_{k+1} \geqslant 0$ ».

Tout d'abord, notons que $u_0 = 3$, donc que $u_1 = \sqrt{5}$, de sorte que $P(0)$ est vraie. Supposons maintenant que $P(k)$ est vraie, et montrons $P(k+1)$. D'une part, d'après $P(k)$, on sait que $u_{k+1} \geqslant 0$ est bien défini, de sorte que $2 + u_{k+1} \geqslant 0$ et que $u_{k+2} = \sqrt{2 + u_{k+1}}$ est également bien défini. En outre, $P(k)$ indique également que $u_k > u_{k+1}$; puisque la fonction $x \mapsto \sqrt{2+x}$ est strictement croissante sur l'intervalle $[0, +\infty[$, on en déduit que $u_{k+1} = \sqrt{2+u_k} > \sqrt{2+u_{k+1}} = u_{k+2}$, ce qui montre $P(k+1)$. Ainsi, la propriété $P(k)$ est vraie pour tout entier naturel k, ce qui clôt cette solution.

4 TD de stratégies de base

- Énoncé des exercices -

Exercice 1 Au premier jour d'un congrès, n scientifiques se serrent la main. Montrer qu'à n'importe quel moment, le nombre des scientifiques ayant serré un nombre impair de mains est pair.

Exercice 2 Montrer que pour tout entier naturel n, il existe un multiple de n à n chiffres et qui s'écrit uniquement avec des 0 et des 1.

Exercice 3 Waldetrade et Zénobie jouent au jeu suivant : sur un 2014-gone régulier, chacune trace tour à tour une diagonale. La dernière à tracer une diagonale qui ne coupe aucune autre diagonale déjà tracée remporte la partie. Qui gagne ?

Exercice 4 Un roi se trouve dans un coin d'un damier $m \times n$. Tour à tour, Anthelme et Brunehaut le déplacent selon la règle des échecs (d'une case, on peut accéder à ses 8 voisines). Le premier qui repasse par une case déjà visitée a perdu. Qui gagne ?

Exercice 5 Sur un cours d'eau circulaire sont disposés n hors-bords, et ils ont au total juste assez de carburant pour faire le tour du cercle. Montrer qu'un certain hors-bord peut réaliser ce

tour sans tomber en panne, en prenant le carburant des hors-bords stationnés sur son chemin.

Exercice 6 On place des tours sur un échiquier $n \times n$ de sorte que, si la case (i, j) est libre, alors il y a au moins n tours sur la i-ème ligne et j-ème colonne. Montrer qu'il y a au moins $n^2/2$ tours sur l'échiquier.

Exercice 7 On dispose de 7 longueurs, entre 1 cm et 12 cm. Montrer qu'on peut en trouver trois qui sont les longueurs des côtés d'un triangle non aplati.

Exercice 8 On colorie chaque point du plan en blanc ou en noir. Montrer qu'il existe un triangle équilatéral dont les sommets sont de la même couleur.

Exercice 9 On considère un damier d'échecs 8×8. On choisit un bord de départ et on appelle *zigzag* un chemin qui rejoint le bord opposé en passant sur exactement 8 cases blanches et aucune noire. Combien y a-t-il de *zigzags* ?

Exercice 10 On considère six points du plan, trois d'entre eux n'étant jamais alignés. On colorie en rouge ou en bleu tous les segments reliant entre eux deux des six points. Montrer qu'il existe un triangle monochrome.

Exercice 11 Maintenant, on dispose de n couleurs. Montrer que $3n!$ points suffisent pour être sûr d'avoir un triangle monochrome.

- Solutions des exercices -

Solution de l'exercice 1 Notons $a_1, \cdots, a_n$ les nombres de poignées de mains échangées à un certain moment. Après une poignée de main, deux scientifiques comptent une salutation de plus, donc la somme $a_1 + \cdots + a_n$ est paire. L'énoncé demande de montrer qu'il y a un nombre pair de a_i impairs : mais la somme des a_j pairs est paire, donc par soustraction, la somme des a_i impairs est également paire. Il y a donc un nombre pair de a_i impairs.

Solution de l'exercice 2 Considérons les nombres $1, 11, \cdots, 1\ldots1$ (ce dernier ayant n chiffres 1). Si l'un d'entre eux est multiple de n, on rajoute des 0 derrière jusqu'à ce qu'on ait n chiffres, et on a le multiple cherché.

Sinon, deux d'entre eux, le i-ème et le j-ème avec $1 \leqslant i < j \leqslant n$ ont le même reste dans la division euclidienne par n selon le principe des tiroirs : en effet, le reste 0 étant éliminé (aucun multiple de n), il reste $n - 1$ restes pour n entiers. Donc leur différence $1..10..0$ avec i zéros et $j - i$ chiffres 1 est multiple de n. De nouveau, on rajoute des 0 derrière jusqu'à ce qu'on ait n chiffres.

Solution de l'exercice 3 Waldetrade l'emporte à coup sûr : elle trace une grande diagonale dans le 2014-gone qui le sépare en deux polygones symétriques par rapport à cette diagonale. Zénobie ne peut tracer de diagonale qui traverse celle tracée par Waldetrade, donc elle en trace une dans un des deux polygones obtenus. Waldetrade n'a plus qu'à tracer la même diagonale dans l'autre polygone. Elle procède ainsi à chaque nouveau tracé de Zénobie jusqu'à ce que cette dernière soit obligée de perdre en traçant une diagonale de trop.

Solution de l'exercice 4 Le résultat dépend de la parité du produit nm.

Si nm est pair, on peut partitionner la grille en dominos de taille 1×2. Le roi se trouve dans un des dominos. Anthelme le bouge dans l'autre partie du domino, dans lequel on n'a

désormais plus le droit de retourner. Brunehaut est donc obligée de bouger le roi dans un autre domino, qu'Anthelme complète au coup suivant, et ainsi de suite jusqu'à ce que Brunehaut soit bloquée. Ainsi, Anthelme a une stratégie gagnante.

Si nm est impair, on partitionne de la même manière la grille en laissant une case seule dans un coin : la case où se trouve le roi initialement. Cette fois-ci, Anthelme commence les dominos et Brunehaut les finit : elle a donc une stratégie gagnante.

Solution de l'exercice 5 Tant qu'à faire, autant exposer deux solutions. Les plus courtes étant les meilleures, et le meilleur étant gardé pour la fin, on commence par une récurrence sur n.

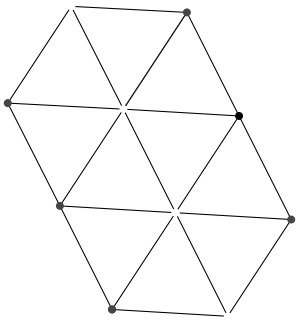
L'initialisation à $n = 1$ est évidente. On suppose le rang $n \geqslant 1$, et on considère $n + 1$ hors-bords. Il y en a au moins 1 qui a assez de carburant pour aller au suivant (sinon, ils n'auraient pas assez de carburant à eux tous), et on peut alors remplacer ces deux hors-bords par un seul, positionné à l'endroit où se trouve le premier des deux, ayant la somme de leurs quantités de carburant. On se ramène ainsi au cas où il y a n hors-bords, supposé résolu par hypothèse de récurrence.

Utilisons le principe de l'extremum : on imagine un hors-bord (fictif) avec suffisamment d'essence qui fait le tour en prenant l'essence des n hors-bords sur son chemin. En atteignant un certain hors-bord, sa jauge d'essence sera minimale. Alors ce hors-bord peut réaliser le tour souhaité.

Solution de l'exercice 6 Considérons la ligne ou colonne ayant le moins de tours, mettons une ligne. Elle contient k tours. Si $k \geqslant \frac{n}{2}$, alors sur les n lignes il y a bien au moins $n \times n/2$ tours. Sinon, sur chacune des $n - k$ colonnes dont la case en commun avec la ligne en question est vide, il y a au moins $n - k$ tours. Quant aux k autres colonnes, elles ont chacune au moins k tours (par définition de k). Ce qui fait, au total, au moins $(n-k)^2+k^2$ tours, soit $n^2/2+\frac{(n-2k)^2}{2} \geqslant n^2/2$.

Solution de l'exercice 7 Soit $l_1 \leqslant \cdots \leqslant l_7$ les longueurs dont on dispose. Supposons par l'absurde qu'on ne puisse former de triangle avec trois quelconques d'entre elles : par l'inégalité triangulaire, $l_3 \geqslant l_2 + l_1$. Or $l_2, l_1 \geqslant 1$, donc $l_3 \geqslant 2$. De même, $l_4 \geqslant l_3 + l_2 \geqslant 3$, $l_5 \geqslant l_4 + l_3 \geqslant 5$, etc. et on trouve $l_7 \geqslant 13$, or $l_7 \leqslant 12$ d'après l'énoncé, ce qui est une contradiction. Donc on peut bien former un triangle non dégénéré.

Solution de l'exercice 8 Considérons un hexagone régulier tel que son centre soit, disons, blanc. La figure suivante illustre la seule répartition possible des couleurs aux sommets sans triangle équilatéral monochrome.



On fait de même avec un hexagone régulier de même taille et dont le centre est un sommet blanc de l'hexagone précédent. Alors on a formé un triangle équilatéral aux sommets noirs.

Solution de l'exercice 9 On va compter plus généralement de manière récursive le nombre de chemins distincts (sur des cases blanches !) qui arrivent sur une case blanche donnée. Considérons B une case blanche ; comme les zigzags ne peuvent « revenir en arrière » (sinon il faudrait plus de 8 cases pour traverser l'échiquier), il y a au plus deux cases blanches qui peuvent mener à B. S'il y en a deux, B_1 et B_2, le nombre de chemins arrivant en B est alors la somme des nombres des cases B_1 et B_2. S'il n'y en a qu'une, B_1, alors autant de chemins arrivent en B_1 qu'en B.

Ainsi, le nombre de zigzags sera la somme des 4 nombres de chemins des 4 cases blanches sur le bord d'arrivée. On écrit bien sûr 1 sur les 4 cases du bord de départ, et on remonte ligne par ligne selon le procédé récursif décrit plus haut. On trouve 296 zigzags.

Solution de l'exercice 10 Soient A, B, C, D, E, F les six sommets. Depuis A partent au moins trois segments de la même couleur d'après le principe des tiroirs. Sans perte de généralité, les segments $[AB]$, $[AC]$, $[AD]$ sont bleus. Et, si $[BC]$ ou $[CD]$ ou $[DB]$ est bleu, alors ABC ou ACD ou ADB est bleu. Sinon, BCD est rouge, donc il y a bien un triangle monochrome.

Solution de l'exercice 11 On procède par récurrence sur n, en notant $R_3(n)$ le nombre minimal de sommets cherché.

Trouvons d'abord une formule liant $R_3(n+1)$ à $R_3(n)$: partant d'un sommet A quelconque, si on a $(n+1)(R_3(n)-1)+1$ autres sommets, alors il y aura au moins $R_3(n)$ segments ayant A pour extrémité qui seront de la même couleur, disons bleu, d'après le principe des tiroirs. Posons $m = R_3(n)$. Comme dans l'exercice précédent, en notant $B_1, \cdots B_m$ les autres extrémités de ces segments bleus, si $[B_iB_j]$ est bleu alors AB_iB_j est bleu. Sinon, il reste n couleurs pour colorier les segments de $R_3(n)$ sommets, donc il y aura nécessairement un triangle monochrome. On en déduit, en comptant le nombre de sommets de notre graphe :

$$R_3(n+1) \leqslant (n+1)R_3(n) - n + 1$$

Sachant que $R_3(2) = 6 = 3 \times 2!$, on peut montrer par récurrence que $R_3(n) \leqslant 3n!$: en effet, pour l'hérédité, on a bien $R_3(n+1) \leqslant (n+1)R_3(n) \leqslant 3(n+1)!$.

En tenant mieux compte de la correction en $-(n-1)$ qui décroît avec n (ici, on a juste utilisé le fait qu'elle était négative), on peut obtenir des majorations un petit peu plus fines (en améliorant la constante : $e = 2,7182818...$ au lieu de 3).

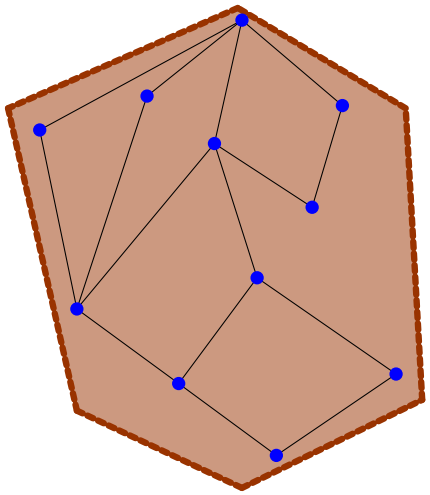


FIGURE 1 – Circuit sur une carte.

2 Groupe B : stratégies de base

1 Cours de logique

Voir le cours de logique du groupe A de la Section 3 commençant page 26.

2 Cours/TD de stratégies de base : coloriages, invariants

Coloriages

Exercice 1 Le plancher est pavé avec des dalles de type 2×2 et 1×4. Une dalle s'est brisée. Peut-on réaranger les dalles de façon à remplacer la dalle brisée avec une nouvelle dalle de l'autre type ?

Exercice 2 On appelle tétromino une dalle de 4 carrés en forme de I, □, Z, T et L. Peut-on paver un rectangle avec une pièce de chaque type ?

Exercice 3 On enlève les quatre coins à un rectangle $n \times n$. Est-il possible de le recouvrir avec des L-tétrominos ?

Exercice 4 On colorie le plan en 2 couleurs. Montrer qu'il y a un rectangle dont tous les sommets ont la même couleur. Généralisez.

Exercice 5 Les villes d'un pays sont connectées par TGV comme dans la Figure 1. Peut-on faire un circuit qui passe exactement une fois par chaque ville ?

Exercice 6 On transforme le mot W en insérant, en effaçant ou en ajoutant au bout XXX où X est un mot formé des chiffres 0 et 1. Peut-on obtenir 10 à partir de 01 ?

Invariants

Exercice 7 Sur l'Île de Pâques vivent des caméléons qui peuvent changer de couleur selon leur gré en bleus, blanc et rouge. Quand deux caméléons de couleurs différentes se rencontrent de manière accidentelle ils ont peur et prennent tous les deux la troisième couleur. À un moment donné on a 12 caméléons bleus, 25 blancs et 8 rouges. Est-il possible que tous les caméléons deviennent blancs ?

Exercice 8 Les nombres $a_1, \ldots, a_n$ valent 1 ou -1. On pose $a_{n+1} = a_1$, $a_{n+2} = a_2$ et $a_{n+3} = a_3$. Sachant que $S = a_1a_2a_3a_4 + a_2a_3a_4a_5 + \cdots + a_na_{n+1}a_{n+2}a_{n+3}$ vaut 0, montrer que n est divisible par 4.

Exercice 9 Les entiers relatifs a, b, c, d ne sont pas tous égaux. À chaque itération on remplace (a, b, c, d) par $(a - b, b - c, c - d, d - a)$. Montrer qu'au moins un des quatre nombres va devenir arbitrairement grand en valeur absolue.

Exercice 10 Les entiers de 1 à n sont écrits dans l'ordre. On échange deux nombres. Un mouvement consiste à échanger n'importe quels deux entiers. Montrer qu'on ne peut pas retrouver l'ordre initial (croissant) dans un nombre pair de mouvements.

Exercice 11 On part de quatre triangles rectangles qui sont congruents. À chaque étape on choisit un triangle, on trace l'hauteur issue de l'angle droit et on considère les deux nouveaux triangles. Est-il possible de rendre tous les triangles non-congruents ?

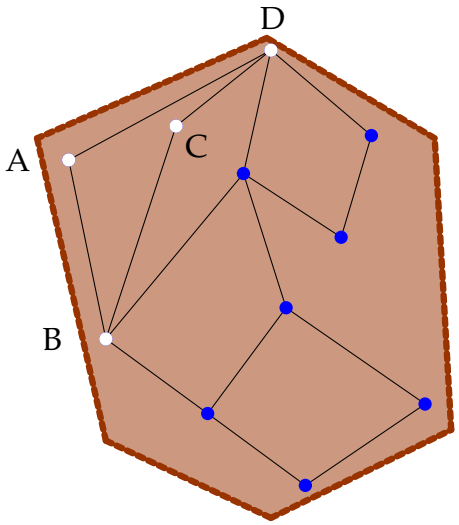
- Solutions des exercices de coloriages -

Solution de l'exercice 1 On colorie la première ligne en carrés bleus et rouges en commençant par bleu, la deuxième en noir et blanc en commençant par noir. Ensuite on continue avec des lignes alternées bleu-rouge et noir-blanc en commençant toujours par bleu et noir respectivement. Alors les dalles 2 x 2 couvrent exactement un carré de chaque couleur. Une dalle 4 x 1 couvre 2 carrés d'une couleur et 2 d'une autre. Ainsi les deux types de dalles ne sont pas interchangeables.

Solution de l'exercice 2 Le rectangle à recouvrir est de taille 4 x 5. On le colorie en blanc et noir comme un échiquier, ayant donc 10 carrés noirs et 10 blancs. Alors on voit que chacune des pièces I, □, Z et L couvre 2 carrés noirs et 2 blancs. Ce n'est pas le cas pour le T qui a 3 carrés de la même couleur. Ainsi, les 5 pièces ne peuvent pas couvrir un nombre égal de carrés blancs et noirs.

Solution de l'exercice 3 Réponse : $n = 4k + 2$. On doit paver $n^2 - 4$ carrés avec des dalles de 4 carrés, donc n doit est pair. On colorie le rectangle en lignes noires et blanches qui s'alternent. Alors chaque dalle recouvre soit 3 carrés blancs et 1 noirs soit le contraire. Ainsi, on doit avoir un nombre pair de dalles pour couvrir le même nombre de carrés blancs et noirs. Ainsi $n^2 - 4 \equiv 0 \bmod 8$, donc $n \equiv 2 \bmod 4$. Il est facile de faire une construction pour tout n de ce type.

Solution de l'exercice 4 On résout le problème pour n couleurs. On considère un rectangle de largeur n et de longueur n^{n+1} que l'on découpe en carrés de taille 1. Ainsi chaque segment parallèle à la larguer à $n + 1$ points sommets. Le nombre de tels segments est $n^{n+1} + 1$ qui est plus grand que le nombre de coloriages différents de $n + 1$ points. Ainsi on a deux segments qui sont coloriés de la même façon. Chacun de ces deux segments contient au moins une



couleur deux fois. Quatre points de cette couleur sur les deux segments identiques forment un rectangle monochrome.

Solution de l'exercice 5 On appelle « circuit hamiltonien » un circuit passant exactement une fois par chaque sommet d'un graphe. La question est donc ici de décider si, oui ou non, notre graphe contient un circuit hamiltonien. En toute généralité, cette question est *difficile* : il est aisé de vérifier qu'un circuit marche ou ne marche pas, mais trouver un circuit hamiltonien ou montrer qu'il n'en existe pas sont deux des problèmes les plus difficiles que l'on puisse concevoir.

Heureusement, ici, il existe une manière simple de montrer que le graphe n'admet pas de circuit hamiltonien. En effet, observons attentivement les sommets A, B, C et D, en blanc, sur notre nouvelle figure, et imaginons un circuit hamiltonien éventuel. Avant et après chaque occurrence de A et C, on devrait passer par B et D ; notre chemin ne transitant que deux fois par des arêtes touchant B et D, il devrait donc contenir un cycle A B C D A ou bien A D C B A : dans les deux cas, notre chemin ne consisterait donc pas en un circuit hamiltonien, ce qui clôt l'exercice.

Solution de l'exercice 6 On doit trouver un invariant qui tient compte des positions de chacun des chiffres 1. Pour $W = w_1 w_2 \cdots$ on pose $I(W) = \sum i w_i$. Quand on ajoute ou insère XXX, chaque lettre du mot X reçoit les indices i, $i+k$ et $i+2k$ pour un indice i et pour k la longueur de X. La partie de W qui est déplacée pour insérer XXX a été décalée de $3k$. Ainsi $I(W)$ mod 3 est un invariant. Comme $I(01) = 2$ et $I(10) = 1$, il est impossible de passer de 01 à 10.

- Solutions des exercices d'invariants -

Solution de l'exercice 7 On note n_1, n_2 et n_3 le nombre de caméléons bleus, blancs et rouges respectivement. À chaque rencontre, les différences $n_1 - n_2$, $n_1 - n_3$ et $n_2 - n_3$ ne changent pas modulo 3. Au début on a $n_1 - n_2 \equiv 12 - 25 \equiv 2 \bmod 3$. On nous demande d'avoir $n_2 = 45$ et $n_1 = 0$ donc $n_1 - n_2 \equiv 0 \bmod 3$. Il est donc impossible que tous les caméléons deviennent blancs.

Solution de l'exercice 8 On décide de changer le signe de certain des nombres a_i et de regarder les nouvelles valeurs de S. Quand on change le signe d'un nombre a_i avec $i \in [1, n]$, la nouvelle valeur de S est son ancienne valeur plus

$$\pm 2a_i \left(a_{i-3}a_{i-2}a_{i-1} + a_{i-2}a_{i-1}a_{i+1} + a_{i-1}a_{i+1}a_{i+2} + a_{i+1}a_{i+2}a_{i+3}\right).$$

Comme la parenthèse a 4 termes impairs, sa valeur est paire. Ainsi, S ne change jamais son reste modulo 4. Maintenant, on change le signe de tous les nombres a_i de façons qu'il soient tous positifs. Alors $S = n$, donc n a le même reste que la valeur initiale de S, soit n est divisible par 4.

Solution de l'exercice 9 Ce qu'on apprend dans cet exercice est qu'un type de fonction invariante à regarder sont les tailles. Par cela on comprend la valeur absolue du plus grand nombre, la somme des valeurs aboslues, la somme des carrés et autres. Dans ce cas précis on regarde $a^2 + b^2 + c^2 + d^2$. Si on met un indice n pour la valeur des nombres après n itérations alors on remarque que $a_n + b_n + c_n + d_n = 0$ indépendamment de n. Ensuite on a

$$\begin{aligned} a_{n+1}^2 + b_{n+1}^2 + c_{n+1}^2 + d_{n+1}^2 &= (a_n - b_n)^2 + (b_n - c_n)^2 = (c_n - d_n)^2 + (d_n - a_n)^2 \\ &= 2(a_n^2 + b_n^2 + c_n^2 + d_n^2) - 2(a_n b_n + b_n c_n + c_n d_n + d_n a_n). \end{aligned}$$

Or l'égalité $a_n + b_n + c_n + d_n = 0$ doit nous aider à simplifier l'expression. On a

$$0 = (a_n + b_n + c_n + d_n)^2 = (a_n + c_n)^2 + (b_n + d_n)^2 - 2(a_n b_n + b_n c_n + c_n d_n + d_n a_n).$$

Solution de l'exercice 10 C'est une propriété très connue des permutations, listes des nombres de 1 à n dans n'importe quel ordre. Si i et j sont deux nombres de 1 à n avec $i < j$ on dit qu'il sont dans le bon ordre si i apparaît à gauche de j dans notre liste. Sinon on dit que le couple (i, j) est une inversion de notre permutation. Un invariant classique est des permutations est la signature : si σ est une permutation on pose $\varepsilon(\sigma) = 1$ si elle a un nombre pair d'inversion er -1 si elle a un nombre impair. Pour résoudre l'exercice il suffit de montrer qu'à chaque échange on change le signe de ε.

Sans restreindre la généralité on peut supposer qu'on échange i et j avec $i < j$. D'abord, l'échange de i et de j rajoute l'inversion (i, j). Soit k un nombre qui se trouve entre i et j. Si k est plus petit que i, alors l'échange de i et j remplace l'inversion (k, i) par l'inversion (k, j). De même si $k > j$ l'inversion (j, k) est remplacée par l'inversion (i, k). Si $i < k < j$ alors l'échange de i et j rajoute ou enlève 2 inversions. Dans tous les cas, l'échange de i et j change la parité du nombre d'inversions, donc le signe de ε.

Solution de l'exercice 11 On note 1 l'hypoténuse des triangles de départ et p et q les deux côtés. Chaque découpage d'un triangle T produit deux triangles semblables à T, de rapport p et respectivement q. Ainsi tous les triangles T obtenus au cours du processus sont caractérisés par les entiers m et n tels que T a un rapport $p^m q^n$ avec les triangles initiaux. Chaque découpage remplace un triangle (m, n) par un triangle $(m+1, n)$ et un triangle $(m, n+1)$. À un ensemble de triangles on associe la fonction

$$I = \sum \frac{1}{2^{m+n}},$$

qui est invariante pour les découpages. Comme au début I vaut 4, elle doit valoir 4 à la fin. Supposons par l'absurde qu'après un nombre fini d'étapes on a seulement des triangles non-congruents. Soit M et N deux bornes pour les m et les n qui interviennent dans un ensemble de triangles. Alors $\sum \frac{1}{2^m} \leqslant 2 - \frac{1}{2^{M+1}}$ et $\sum \frac{1}{2^n} \leqslant 2 - \frac{1}{2^{N+1}}$ où les sommes sont sur tous les m et n de notre ensemble. Finalement

$$I < \left(2 - \frac{1}{2^{M+1}}\right)\left(2 - \frac{1}{2^{N+1}}\right) < 4$$

ce qui est une contradiction.

3 Cours de stratégies de base

- Raisonnement par récurrence -

Le raisonnement par récurrence vise à répondre à une question du type : « **Montrer que la propriété** $P(n)$ **est vraie pour tout entier naturel** n**.** » Il consiste en 3 étapes :

1. L'initialisation : On montre que la propriété $P(0)$ est vraie.
2. L'hérédité : On montre que, si n est un entier naturel tel que $P(n)$ est vraie, alors $P(n+1)$ est vraie aussi.
3. La conclusion : On en conclut que $P(n)$ est vraie pour tous les entiers naturels.

Si on sait monter sur la première marche d'un escalier et qu'on sait monter d'une marche à la suivante, alors on peut gravir tout l'escalier. Telle est l'idée du raisonnement par récurrence.

On renvoie à la partie du cours de logique consacré à la récurrence pour une preuve (voir page 36).

Exemple 2.1. Pour un entier $n \geqslant 1$, soit P_n la propriété « $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ ». Montrons que P_n est vraie pour tout entier $n \geqslant 1$ par récurrence sur n.

- (Initialisation) Il est clair que P_1 est vérifiée.
- (Hérédité) Supposons P_n vérifié. Montrons P_{n+1}. En utilisant l'hypothèse de récurrence, on a

$$\begin{aligned} 1 + 2 + \cdots + (n+1) &= (1 + 2 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}. \end{aligned}$$

On en déduit que P_n est vérifiée pour tout entier $n \geqslant 1$.

Exercice 1 Montrer que

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solution de l'exercice 1 Pour un entier $n \geqslant 1$, soit P_n la propriété

$$\text{« } 1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}\text{ ».}$$

Montrons que P_n est vérifiée pour tout entier $n \geqslant 1$ par récurrence sur n.

- (Initialisation) Il est clair que P_1 est vérifiée.
- (Hérédité) Supposons P_n vérifiée. Montrons P_{n+1}. En utilisant l'hypothèse de récurrence, on a

$$\begin{aligned}1^2+2^2+\cdots+(n+1)^2 &= \left(1^2+2^2+\cdots+n^2\right)+(n+1)^2\\ &= \frac{n(n+1)(2n+1)}{6}+(n+1)^2\\ &= \frac{(n+1)(n(2n+1)+6(n+1))}{6}=\frac{(n+1)(2n^2+7n+6)}{6}\\ &= \frac{(n+1)(n+2)(2n+3)}{6}.\end{aligned}$$

On en déduit que P_n est vérifiée pour tout entier $n \geqslant 1$.

Exercice 2 Trouver tous les entiers $n \geqslant 0$ tels que $2^n \geqslant n^2$.

Solution de l'exercice 2 On voit que $n = 0, 1, 2, 4$ conviennent mais pas $n = 3$. Montrons ensuite que $2^n \geqslant n^2$ pour tout entier $n \geqslant 4$. Pour un entier $n \geqslant 4$, soit P_n la propriété « $2^n \geqslant n^2$ ». Montrons que P_n est vérifiée pour tout entier $n \geqslant 4$ par récurrence sur n.

- (Initialisation) On a vu que P_4 est vérifiée.
- (Hérédité) Supposons P_n vérifiée. Montrons P_{n+1}. En utilisant l'hypothèse de récurrence, on a

$$2^{n+1} \geqslant 2 \cdot 2^n \geqslant 2n^2.$$

Il suffit donc de montrer que $2n^2 \geqslant (n+1)^2$. Pour cela, on écrit

$$2n^2-(n+1)^2 = n^2-2n-1 = (n-1)^2-2,$$

qui est bien positif car $n-1 \geqslant 3$.

On en déduit que P_n est vérifiée pour tout entier $n \geqslant 4$. Ainsi, $2^n \geqslant n^2$ pour tout entier positif sauf pour $n = 3$.

Exercice 3 À Mathland, deux villes sont toujours reliées soit par une ligne aérienne, soit un canal navigable (à double sens). Montrer qu'il est possible de choisir un moyen de transport, tel que, en partant de n'importe quelle ville, on puisse atteindre n'importe quelle autre ville uniquement à l'aide de ce moyen de transport.

Solution de l'exercice 3 Notons n le nombre de villes. Pour avoir une intuition de ce qui se passe, il est conseillé de tester différentes configurations pour des petites valeurs de n. Pour $n = 2$, il n'y a un qu'un seul moyen de transport. Pour $n = 3$, soient A, B, C les trois villes. Sans perte de généralité, supposons que $A - B$ est une ligne aérienne. Alors soit C peut être relié à A ou B par une ligne aérienne, auquel cas l'avion convient, soit C est relié à A et B par un canal, auquel cas le bateau convient.

Cela suggère de démontrer que la véracité de la proposition suivante par récurrence [1] sur n :

1. il faut toujours connaître la propriété *précise* que l'on veut prouver afin d'éviter les mauvaises surprises (par exemple lors de deux récurrences imbriquées ou autre réjouissances de ce type).

P_n : « Pour toute configuration de n villes, il existe un moyen de transport vérifiant les conditions requises. »

- (Initialisation) On a déjà vu que P_2 est vérifiée.
- (Hérédité) Soit $n \geqslant 2$ un entier et supposons que P_n est vraie. Montrons que P_{n+1} est satisfaite. Considérons A une ville quelconque et appliquons la propriété P_n à la configuration des n villes restantes. Sans perte de généralité, supposons que c'est l'avion qui convient. Alors de deux choses l'une : soit il existe une ligne aérienne reliant A à une autre ville, auquel cas l'avion convient, soit A est relié à toutes les autres villes par un canal, auquel cas le bateau convient.

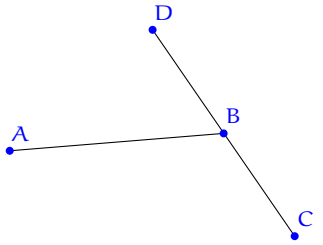
Exemple 2.2. Un exemple d'application de récurrence forte sera vu en cours d'arithmétique, où la récurrence forte sera utilisée pour démontrer l'unicité de la décomposition en facteurs premiers d'un nombre entier.

- Principe extrémal -

Commençons par quelques exemples.

Exemple 2.3. Soit Ω un ensemble de points du plan. On suppose que tout point de Ω est le milieu d'un segment dont les extrémités sont dans Ω. Prouvons que l'ensemble Ω est infini.

Par l'absurde, supposons que l'ensemble Ω est fini. Parmi tous les couples de points de Ω, choisissons-en deux maximisant leur distance. Notons les A et B. Par hypothèse, il existe C et D des points de Ω tels que B est le milieu de $[CD]$.



On voit alors que soit $AC > AB$, soit $AD > AB$. Ceci contredit le caractère maximal de la distance AB. Nous avons abouti à une contradiction : notre hypothèse de départ est donc fausse, et il s'ensuit que l'ensemble Ω est infini.

Exemple 2.4. À chaque point à coordonnées entières du plan on associe un entier positif ou nul. On suppose que l'entier de chaque point à coordonnées entières du plan est la moyenne des nombres de ses quatre voisins (immédiatement à gauche, droite, haut et bas). Prouvons que tous les entiers sont égaux.

Notons m l'entier positif minimal porté par l'un de ces points, et notons a, b, c, d les entiers portés par ses quatre voisins. Par hypothèse, $m \leqslant a, m \leqslant b, m \leqslant c, m \leqslant d$. Si l'une de ces inégalités est stricte, on a alors $m < (a+b+c+d)/4$, ce qui contredit l'égalité $m = (a+b+c+d)/4$. On a donc $a = b = c = d = m$, autrement dit les quatre voisins de m portent la même valeur m. De proche en proche, on en déduit que tous les entiers sont égaux (un raisonnement rigoureux ferait appel à une récurrence).

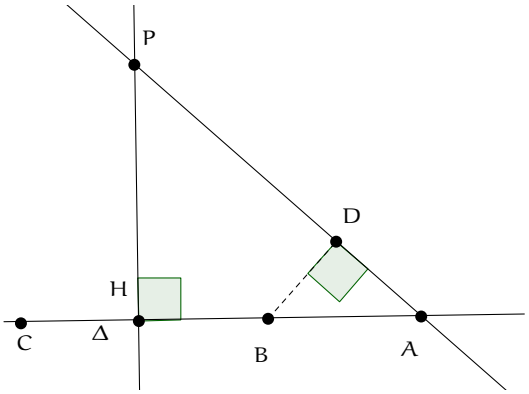
Exemple 2.5. Au stage olympique, chaque élève connaît exactement trois autres élèves. Prouvons qu'on peut partager les élèves en deux groupes de sorte que chacun ne connaisse qu'une seule personne dans son groupe.

Parmi tous les partages possibles en deux groupes, regardons le nombre total de connaissances qu'il y a cumulées en restant à l'interieur de son groupe. Choisissons le partage qui minimise ce nombre. Prouvons que celui-ci convient. Par l'absurde, supposons que dans le partage il existe un élève, appelons le A, qui connaisse au moins deux personnes dans son groupe. Dans l'autre groupe, il y a au plus une personne qu'il connaît : en changeant A de groupe on diminuerait ainsi le nombre total de connaissances qu'il y a cumulées en restant à l'interieur de son groupe, ce qui contredit la minimalité supposée du partage initial.

On conclut par le célébre problème de Sylvester, posé par Sylvester en 1893, résolu par Gallai en 1933 par une méthode compliquée. Kelly a donné la solution qui suit en 1948.

Exemple 2.6. Soit S un ensemble fini de points du plan tel que si deux points appartiennent à S, alors il en existe un troisième appartenant à la droite formée par ces deux points. Alors l'ensemble S est formé de points alignés.

Pour prouver cette assertion, raisonnons par l'absurde et supposons que tous les points ne soient pas alignés. Parmi tous les couples (P, Δ) de points $P \in S$ et de droites Δ passant par deux points de S, choisissons-en un qui mimimise la distance de P à Δ. Notons (P, Δ) un tel couple. Soit H le projeté orthogonal de P sur Δ. Par hypothèse, il existe au moins trois points de S sur Δ, et donc forcément deux du même côté par rapport à H, disons A et B. Quitte à renommer les points, supposons que B est plus proche de P que A.



Alors le couple formé par le point B et la droite (AP) contredit la minimalité de (P, Δ) car $BD < HP$. Ceci est absurde. Ainsi, tous les points sont alignés.

Une autre manière de formuler le résultat de Sylvester est de dire que pour tout ensemble fini de points non alignés il existe une droite passant par exactement deux points de l'ensemble (pourquoi ?).

Les exemples précédents partagent une même idée : considérer un élément maximisant ou minimisant une certaine quantité. Plus précisément, nous avons utilisé les deux propriétés suivantes :

(i) Tout ensemble *fini* non vide de nombres entiers (ou réels) admet un plus petit élément ainsi qu'un plus grand élément (qui ne sont pas nécessairement uniques).

(ii) Tout ensemble non vide (éventuellement infini) de nombres entiers positifs ou nuls admet un plus petit élément.

On dit qu'on utilise un *principe extrémal* lorsqu'on applique ces propriétés. Comme nous l'avons vu, le principe extrémal permet d'exhiber des configurations auxquels on souhaite arrive (mais parfois pas de manière explicite), ou bien d'introduire un nouvel objet qu'on peut utiliser.

- Exercices d'application -

Exercice 4 On place les n^2 entiers $1, 2, \ldots, n^2$ dans un tableau $n \times n$ (sans répétition). On dit que deux cases sont voisines si elles ont au moins un point en commun. Prouver qu'il existe deux cases voisines dont la différence des valeurs vaut au moins $n + 1$.

Exercice 5 On se donne un ensemble fini de points dans le plan, de cardinal pair, trois quelconques d'entre eux non alignés. Montrer qu'on peut les relier par des segments sorte que chaque point soit relié à exactement un autre et que les segments ne se coupent pas.

Exercice 6 Soit $n \geqslant 3$ un entier. On considère un ensemble de n droites dans le plan tel que deux quelconques ne soient pas parallèles. On suppose que par l'intersection de deux quelconques de ces droites passe une autre droite de l'ensemble. Prouver que toutes les droites sont concourantes.

Exercice 7 À un tournoi, chaque compétitrice rencontre chaque autre compétitrice exactement une fois. Il n'y a pas de match nul. À l'issue de la compétition, chaque joueuse fait une liste qui contient les noms des joueuses qu'elle a battues, ainsi que les noms des joueuses qui ont battu les joueuses qu'elle a battues.

Montrer qu'il existe une liste qui contient le nom de toutes les autres joueuses.

Exercice 8 Un ensemble (fini) S de personnes vérifie la propriété suivante : deux personnes connaissant le même nombre de personnes n'ont jamais de connaissance commune. Prouver qu'il existe une personne connaissant exactement une autre.

- Solutions des exercices -

Solution de l'exercice 4 Raisonnons par l'absurde en supposant que les différences des valeurs de deux cases voisines sont toujours au plus n. Notons A la case dont la valeur est 1 et B la case dont la valeur est n^2. Il existe un chemin de longueur au plus $n - 1$ reliant A à B en ne passant que par des cases voisines. La différence entre les valeurs des cases B et A vaut donc au plus $n(n-1)$, qui est strictement inférieur à $n^2 - 1$, absurde.

Solution de l'exercice 5 Considérons la façon de relier les points qui minimise la somme des longueurs des segments, avec pour unique contrainte que chaque point soit extrémité d'exactement un segment. Supposons, par l'absurde, que l'on a deux segments AD et BC qui se coupent en un point O (par hypothèse, celui-ci est forcément différent de A, B, C, et D). Si, à la place des segments AD et BC on choisit CD et AB, alors tout point est relié à exactement un autre. Par minimalité de la somme des longueurs, on en déduit :

$$AD + BC \leqslant AB + CD. \tag{II.1}$$

Pour la même raison, on a :

$$AD + BC \leqslant AC + BD. \tag{II.2}$$

En sommant les deux équations, on trouve

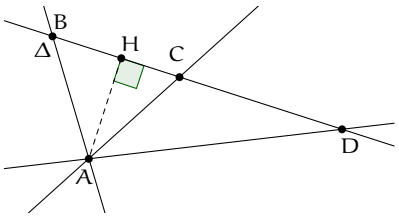
$$2 \cdot (AD + BC) \leqslant (AC + CD) + (AB + BD) \tag{II.3}$$

Par l'inégalité triangulaire dans les triangles AOB, BOD, DOC et COA, on a :

$$AC + AB + BD + DC \leqslant CO + OA + OA + OB + OB + OD + OD + OC = 2 \cdot (AD + BC), \tag{II.4}$$

et on n'a pas égalité sinon A, B, et O seraient alignés, donc A, B, et C aussi, ce qui est exclu par l'hypothèse. Ainsi on a une contradiction avec l'équation (II.3). Donc dans la solution minimale, il n'y a pas de segments qui se coupent.

Solution de l'exercice 6 La preuve est très proche de la preuve du problème de Sylvester : on choisit le couple (P, Δ) où P est un point d'intersection et Δ une droite de l'ensemble ne contenant pas P qui minimise la distance de P à Δ. Notons B, C, D les points d'intersection de trois droites de l'ensemble passant par A avec Δ. Soit H le projeté orthogonal de A sur Δ. Sans perte de généralité, nous pouvons supposer que C et D sont du même côté de P sur Δ et que C est plus proche de H que D. Ainsi la distance de C à (AD) est plus petite que la distance de A à Δ, absurde.



Solution de l'exercice 7 Soit A la joueuse ayant gagné le plus de matchs. S'il n'existait pas de liste contenant le nom de toutes les autres joueuses, il existerait une joueuse B ayant gagné contre A ainsi que contre toutes les personnes battues par A. Donc B aurait gagné plus de matchs que A, absurde.

Solution de l'exercice 8 Soit A la personne ayant le plus grand nombre de connaissances n. Considérons l'ensemble E formé par les nombres de personnes que connaissent les connaissances de A. Ainsi E est constitué de n entiers appartenant à $\{1, 2, \ldots, n\}$. Par hypothèse, ils sont également deux à deux différents. On en déduit que $E = \{1, 2, \ldots, n\}$. En particulier, il existe une personne connaissant exactement une autre.

- Coefficients binomiaux -

La Combinatoire est un sous-art des mathématiques qui consiste à compter et à étudier des structures discrètes (finies). De nombreux problèmes difficiles sont formulés de manière très simple (mais la résolution nécessite des outils avancés). Le but de ce cours est de présenter quelques réflexes et idées de bases pouvant être utiles dans la résolution d'exercices de combinatoire de type olympiades ayant un rapport avec les coefficients binomiaux.

Faute de temps, cette partie n'avait pas été abordée pendant le cours de combinatoire.

1) Définitions

On rappelle qu'un ensemble E est une collection d'éléments dont l'ordre n'a pas d'importance (ainsi, les ensembles $\{2,3\}$ et $\{3,2\}$ sont les mêmes ensembles). On note $x \in A$ si x appartient à l'ensemble A. Si A et B sont deux ensembles, on écrit $A \subset B$ et on dit que A est inclus dans B si chaque élément de A appartient au B. L'ensemble vide, qui ne contient aucun élément, est noté $\emptyset$. On note $\mathrm{Card}(A)$ (on prononce « cardinal de A ») le nombre d'éléments de A. On dit que A est infini si $\mathrm{Card}(A) = \infty$, fini sinon.

Définition 2.7. Pour des entiers $0 \leqslant k \leqslant n$, on note $\binom{n}{k}$ (et on prononce « k parmi n ») le nombre de manières de choisir un sous-ensemble à k éléments d'un ensemble à n éléments différents. Pour $k > n$, on pose $\binom{n}{k} = 0$.

Il est clair que dans la définition précédente, $\binom{n}{k}$ ne dépend pas de l'ensemble à n éléments différents considéré.

Exemple 2.8. On a $\binom{4}{2} = 6$, car les sous-ensembles à 2 éléments de $\{1,2,3,4\}$ sont $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{3,4\}$ et il y en a 6

Pour un entier $n \geqslant 1$, rappelons la notation $n! = 1 \cdot 2 \cdot 3 \cdots n$.

Proposition 2.9. Le nombre de manières d'ordonner n éléments est $n!$.

Démonstration. Nous avons n possibilités pour choisir le premier élément, $n-1$ possibilités pour le deuxième, et ainsi de suite jusqu'au dernier élément pour lequel nous avons une seule possibilité. Le résultat en découle. □

Proposition 2.10. Pour des entiers $0 \leqslant k \leqslant n$, on a :

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}.$$

Démonstration. Comptons de deux manières différentes le nombre de suites à k éléments qu'on peut créer en utilisant les n éléments d'un ensemble à n éléments différents.

D'une part, comme pour la proposition précédente, nous avons n choix pour le premier terme de la suite ; $n-1$ choix pour le deuxième, et ainsi de suite jusqu'au k-ième élément pour lequel nous avons $n-k+1$ choix. Finalement, il y a en tout $n \cdot (n-1) \cdots (n-k+1)$ suites à k éléments.

D'autre part, pour créer une suite à k éléments, on peut commencer par choisir les k éléments qui vont constituer la suite ($\binom{n}{k}$ possibilités), puis les ordonner ($k!$ manières possibles de les ordonner). Il y a donc en tout $k! \cdot \binom{n}{k}$ suites à k éléments. □

Remarque 2.11. Reformulé différemment, $\binom{n}{k}$ est le nombre de manière de choisir k boules parmi n boules différentes si on ne tient pas compte de l'ordre de leurs tirages.

2) Propriétés combinatoires

Exercice 9 Pour des entiers $0 \leqslant k \leqslant n$, on a :

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Solution de l'exercice 9 *Première méthode :* On utilise la formule $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ et le résultat en découle immédiatement.

Deuxième méthode : On remarque que choisir k éléments parmi n revient à choisir $n-k$ éléments parmi n qu'on ne choisira pas.

L'exercice précédent, bien que facile, est assez représentatif des exercices ayant pour but de prouver des relations d'égalité entre coefficients binomiaux. Très souvent, il y a toujours (au moins) deux approches possibles : remplacer les coefficients binomiaux par leur formule et ramener le problème à un exercice de manipulation de relations algébriques, ou bien d'interpréter de manière combinatoire les deux termes de part et d'autre de l'égalité et de prouver qu'ils sont égaux. La deuxième approche est biensûr bien plus élégante et fournit très souvent des preuves courtes, mais requiert davantage d'ingéniosité.

Exercice 10 Soient $0 \leqslant k \leqslant n$ des entiers (avec $(k,n) \neq (0,0)$). Alors :

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Solution de l'exercice 10 *Première méthode :* On utilise la formule.

Seconde méthode : On démontre ce résultat de manière combinatoire. Considérons l'ensemble $\{1,2,\dots,n\}$ et dénombrons ses sous-ensembles à k éléments. Il y en a $\binom{n-1}{k}$ qui ne contiennent pas n et il y en a $\binom{n-1}{k-1}$ qui contiennent n. Le résultat en découle.

Exercice 11 Pour $0 \leqslant k \leqslant n$, on a :

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Solution de l'exercice 11 *Première méthode :* On utilise la formule exprimant $\binom{n}{k}$ (le faire).

Seconde méthode : Démontrons ce résultat de manière combinatoire en comptant de deux manières différentes le nombre de sous-ensembles de $\{1,2,\dots,n\}$ de cardinal k ayant un élément distingué (qu'on appellera chef). Tout d'abord, il suffit de choisir un sous-ensemble de cardinal k ($\binom{n}{k}$ choix), puis de choisir un chef (k choix indépendants). On obtient donc en tout $k\binom{n}{k}$ possibilités.

Exercice 12 Pour un entier $n \geqslant 1$, on a

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Solution de l'exercice 12 *Première méthode :* Si on n'a pas d'idée comment commencer de manière astucieuse, on peut essayer de procéder par récurrence sur n. Pour $n = 1$, le résultat est clair. Supposons le résultat acquis au rang n et montrons-le au rang $n+1$ en écrivant, avec

l'exercice 4 :

$$\begin{aligned}\sum_{k=0}^{n+1}\binom{n+1}{k} &= 1+\sum_{k=1}^{n+1}\left(\binom{n}{k}+\binom{n}{k-1}\right)\\ &= \sum_{k=1}^{n}\binom{n}{k}+\sum_{k=0}^{n}\binom{n}{k}\\ &= 2^n+2^n \qquad \text{(par hypothèse de récurrence)}\\ &= 2^{n+1},\end{aligned}$$

Seconde méthode : Démontrons ce résultat de manière combinatoire en comptant le nombre N de sous-ensembles de $\{1,2,\dots,n\}$. D'une part, pour un entier $0 \leqslant k \leqslant n$, il y a $\binom{n}{k}$ sous-ensembles à k éléments. En sommant le tout, on voit que $N = \sum_{k=0}^{n}\binom{n}{k}$.

Mais, pour construire un sous-ensemble de $\{1,2,\dots,n\}$, on a le choix de choisir 1 ou non, 2 ou non, et ainsi de suite jusqu'à n. On a donc $N = 2^n$, ce qui conclut.

En particulier, la solution précédente montre qu'il existe 2^n sous-ensembles d'un ensemble à n éléments.

Proposition 2.12 (Formule du binôme de Newton)**.** Soient x, y des nombres réels et $n \geqslant 1$ un entier. Alors :

$$\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} = (x+y)^n.$$

Démonstration. Première méthode : par récurrence sur n (s'entraîner à le faire).

Seconde méthode : lorsqu'on développe $(x+y)\cdot(x+y)\cdots(x+y)$, pour trouver le coefficient devant $x^k y^{n-k}$, parmi les n termes $(x+y)$, il faut en choisir k pour lesquels on garde le x et qui vont donner un terme x^k, et les $n-k$ autres termes pour lesquels on sélectionne y vont donner le terme y^{n-k}. Le résultat s'ensuit. □

Exercice 13 Quel est le cardinal moyen d'un sous-ensemble de $\{1,2,\dots,n\}$?

Solution de l'exercice 13

Première méthode (d'après une idée d'élèves) : On regroupe un ensemble avec son complémentaire. Si $A \subset \{1,2,\dots,n\}$, on note A^c l'ensemble des entiers de $\{1,2,\dots,n\}$ qui ne sont pas dans A. Notons N ce cardinal moyen. Alors :

$$\begin{aligned}N &= \frac{1}{2^n}\sum_{A\subset\{1,2,\dots,n\}}\mathrm{Card}(A) = \frac{1}{2^n}\sum_{A\subset\{1,2,\dots,n\}}\frac{\mathrm{Card}A+\mathrm{Card}(A^c)}{2}\\ &= \frac{1}{2^n}\sum_{A\subset\{1,2,\dots,n\}}\frac{n}{2} = \frac{1}{2^n}\cdot\frac{n}{2}2^n = \frac{n}{2}.\end{aligned}$$

Autre méthodes : Il faut évaluer la somme

$$S_n = \frac{1}{2^n}\sum_{k=0}^{n}k\binom{n}{k}.$$

Si on ne sait pas commencer, il faut étudier les premiers cas : $n = 1, 2, \ldots$. On trouve toujours $S_n = n/2$. Essayer donc de démontrer cela.

Seconde méthode : Si on n'a pas d'idée, on peut procéder par récurrence sur n.

Troisième méthode, plus avancée. Considérons le polynôme $P_n(x) = \sum_{k=0}^{n} \binom{n}{k} x^k$. D'après a formule du binôme de Newton, $P_n(x) = (1+x)^n$. Dérivons cette égalité par rapport à x :

$$\sum_{k=0}^{n} k\binom{n}{k} x^{k-1} = n(1+x)^{n-1}.$$

Évaluons alors cette quantité en $x = 1$:

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}.$$

Le résultat en découle.

Exercice 14 Prouver que pour $0 \leqslant m \leqslant n$:

$$\sum_{k=0}^{n} \binom{n}{k}\binom{k}{m} = \binom{n}{m} 2^{n-m}.$$

Solution de l'exercice 14 On remarque d'abord que seuls les k tels que $k \geqslant m$ contribuent de manière non nulle. On va procéder à un double comptage en comptant le nombre N de sous-ensembles A, B de $\{1, 2, \ldots, n\}$ tels que $A \subset B$ et $\mathrm{Card}(A) = m$. En effet, d'une part, pour construire A, B on peut d'abord choisir A de cardinal m ($\binom{n}{m}$ choix), puis rajouter un sous-ensemble quelconque de l'ensemble $\{1, 2, \ldots, n\}$ privé des éléments de A, qui a $n-m$ éléments (et donc 2^{n-m} choix indépendants). En ainsi, $N = \binom{n}{m} 2^{n-m}$.

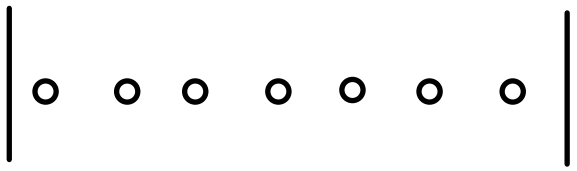
D'autre part, pour construire A, B on peut d'abord choisir B de cardinal quelconque entre m et n (si B est de cardinal k, $\binom{n}{k}$ choix), puis choisir A de cardinal m comme sous-ensemble de B ($\binom{k}{m}$ choix si B est de cardinal k). Ainsi, $N = \sum_{k=0}^{n} \binom{n}{k}\binom{k}{m}$.

Exercice 15 Combien y a-t-il de chemins sur $\mathbb{Z}^2$ issus de $(0,0)$, faisant des pas $+(1,0)$ ou $+(0,1)$, et finissant en (m,n), où $m, n \geqslant 0$?

Solution de l'exercice 15 Un tel chemin doit faire $m+n$ pas, dont m fois $+(1,0)$ et n fois $+(0,1)$. Il suffit donc de choisir parmi les $m+n$ pas possibles la position des m qui font $+(1,0)$. Le nombre total vaut donc $\binom{m+n}{m}$.

Exercice 16 De combien de manières peut-on placer 5 pièces identiques dans 3 poches différentes ?

Solution de l'exercice 16 Considérons la figure suivante (avec deux barres) :



Remplaçons chaque rond soit par une pièce, soit par une barre de sorte qu'il y ait en tout 2 barres et 5 pièces. Les pièces entre les deux Premières barres seront contenues dans la Première poche, les pièces entre la deuxième barre et la troisième barre seront contenues dans la seconde poche, et finalement les pièces entre la troisième barre et la quatrième barre seront contenues dans la troisième poche.

Ainsi, placer 5 pièces identiques dans 3 poches différentes, revient à choisir la position des 2 barres parmi 7 positions possibles. La réponse est donc $\binom{7}{2} = 21$.

Plus généralement, en procédant de la même façon, on voit qu'il y a $\binom{a+b-1}{b-1} = \binom{a+b-1}{a}$ manières de placer a pièces identiques dans b poches différentes.

4 TD de stratégies de base

- Exercices -

Exercice 1 15 élèves ont attrapés 100 tiques. Montrer que deux élèves ont attrapé le même nombre de tiques.

Exercice 2 Soit α un nombre réel tel que $\alpha + \frac{1}{\alpha} \in \mathbb{Z}$. Montrer que, pour tout $n \in \mathbb{N}$, $\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$.

Exercice 3 (application de la récurence forte) Montrer que pour tout $n \in \mathbb{N}^*$, on peut trouver k nombres premiers $p_0, \ldots, p_{k-1}$ tels que $\prod_{i \in k} p_i = n$.

NB. On admet que le produit de zéro nombre premier vaut 1.

- Solutions -

Solution de l'exercice 1 On raisonne par l'absurde. On note $t_0, t_1, \ldots, t_{14}$ les nombres de tiques des élèves, supposés distincts. Quitte à intervertir les élèves, on peut donc supposer $t_0 < t_1 < \ldots < t_{14}$. Comme ce sont des entiers, on a alors $0 \leqslant t_0$, $t_1 \geqslant t_0 + 1 \geqslant 1$, et ainsi de suite jusqu'à $t_{14} \geqslant 14$.

Le nombre total T de tiques vérifie alors $T \geqslant 0 + 1 + \ldots + 14 = 105$, soit $100 \geqslant 105$, ce qui est absurde.

Solution de l'exercice 2 On procède par récurence sur n. En fait, on montre par récurence la proposition $P(n) = (\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$ ET $\alpha^{n-1} + \frac{1}{\alpha^{n-1}} \in \mathbb{Z})$.

Initialisation : $\alpha + \frac{1}{\alpha} \in \mathbb{Z}$ et $\alpha^0 + \frac{1}{\alpha^0} = 2 \in \mathbb{Z}$.

Hérédité : on suppose P vraie au rang n. Déjà, $\alpha^{n+1-1} + \frac{1}{\alpha^{n+1-1}} = \alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$ par hypothèse de récurence. Ensuite,

$$\alpha^{n+1} + \frac{1}{\alpha^{n+1}} = \alpha^{n+1} + \frac{1}{\alpha^{n+1}} + \alpha^{n-1} + \frac{1}{\alpha^{n-1}} - \alpha^{n-1} - \frac{1}{\alpha^{n-1}} = (\alpha + \frac{1}{\alpha})(\alpha^n + \frac{1}{\alpha^n}) - (\alpha^{n-1} + \frac{1}{\alpha^{n-1}})$$

qui est entier, comme somme de produits d'entiers.

Conclusion : pour tout $n \geqslant 1$, $P(n)$ est vrai, donc en particulier, $\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$

Solution de l'exercice 3 On procède par récurence forte sur n.

Initialisation : le cas $n = 1$ est admis par l'énoncé.

Hérédité : on suppose que, pour tout k tel que $1 \leqslant k < n$, k se décompose comme produit de facteurs premiers. On distingue alors deux cas :

.Si n est premier, alors $n = n$, donc n se décompose comme le produit d'un nombre premier.

.Sinon, par définition de la non primitude, $n = ab$ avec $a \neq 1$ et $b \neq 1$. On a alors $a = \dfrac{n}{b} < n$ et de même, $b < n$. Donc, par hypothèse de récurence forte, $a = \prod_{i \in r} p_i$ et $b = \prod_{j \in r'} p'_j$, donc $n = ab = p_0 p_1 \dots p_{r-1} p'_0 \dots p'_{r'-1}$.

- Principe des tiroirs -

Si on cherche à ranger $n + 1$ chaussettes (ou pigeons) dans n tiroirs (ou trous de pigeon), on sait qu'au moins un tiroir contient au moins deux chaussettes.

Plus généralement, si on cherche à ranger au moins $(kn + 1)$ objets dans n ensembles, on sait qu'au moins un des ensembles contient au moins $k + 1$ objets.

De même, si on cherche à ranger au plus $kn - 1$ pigeons dans n tiroirs, au moins un trou de pigeon contiendra au plus $k - 1$ chaussettes.

Exercice 4 Dans un groupe de 2013 personnes, certaines se connaissent et d'autre non. On admet que si A connait B, alors B connais également A. Montrer qu'il y a deux personnes ayant le même nombre de connaissances.

Solution de l'exercice 4 On suppose d'abord qu'une des personnes connaît tout le monde. Dans ce cas, tout le monde la connaît, donc personne ne connait personne. Les nombres d'amis possibles pour une personne donnée sont donc les entiers de 1 à 2012, soit 2012 possibilités. Comme il y a 2013 élèves, par le principe des trous de chaussettes, deux personnes ont le même nombre de connaissances.

De même, si personne n'a 2012 connaissances, les nombres d'amis possibles pour une personne donnée sont les entiers de 0 à 2011, ce qui conclut.

3 Groupe C : géométrie

1 Cours de géométrie

Si ABC est un triangle, on note $a = BC, b = AC, c = AB$, $\widehat{A} = \widehat{BAC}, \widehat{B} = \widehat{ABC}, \widehat{C} = \widehat{ACB}$. On note S l'aire de ABC, H son orthocentre, G son centre de gravité, I le centre de son cercle inscrit, O le centre de son cercle circonscrit et R le rayon de son dernier.

- Mini-cours sur le produit scalaire -

Rappels sur les vecteurs Un vecteur du plan $\mathbb{R}^2$ est la donnée d'une direction, d'un sens et d'une longueur. On note $\overrightarrow{0}$ le vecteur nul. La norme d'un vecteur $\overrightarrow{u}$, notée $\|u\|$, est la longueur de $\overrightarrow{u}$. Deux points A et B du plan définissent un vecteur $\overrightarrow{AB}$. Si O est un point fixé du plan, à un vecteur $\overrightarrow{u}$ on peut associer de manière unique un point, noté $P_{\overrightarrow{u}}$, tel que $\overrightarrow{OP_{\overrightarrow{u}}} = \overrightarrow{u}$.

Si $(O, \overrightarrow{i}, \overrightarrow{j})$ est un repère (pas forcément orthogonal ni orthonormal) du plan, on dit que $\binom{x}{y}$ (ou indifféremment (x, y)) sont les coordonnées du vecteur $\overrightarrow{u}$ si $\binom{x}{y}$ sont les coordonnées dans $(O, \overrightarrow{i}, \overrightarrow{j})$ du point $P_{\overrightarrow{u}}$. On note alors $\overrightarrow{u}\binom{x}{y}$.

Si $\overrightarrow{u}\binom{x}{y}$ et $\overrightarrow{v}\binom{x'}{y'}$ sont deux vecteurs, on note $\overrightarrow{u} + \overrightarrow{v}$ le vecteur de coordonnées $\binom{x+x'}{y+y'}$, et pour tout réel λ on note $\lambda \cdot \overrightarrow{u}$ (ou indifféremment $\lambda\overrightarrow{u}$) le vecteur de coordonnées $\binom{\lambda x}{\lambda y}$.

Pour tous points A, B du plan, on a $\overrightarrow{AB} = -\overrightarrow{BA}$ et pour tous points A, B, C du plan on a $\overrightarrow{AB} = \overrightarrow{AC} + \overrightarrow{CB}$ (relation de Chasles).

Définition du produit scalaire et premières propriétés À partir de maintenant, on travaille dans un repère **orthonormal** $(O, \overrightarrow{i}, \overrightarrow{j})$.

Définition 3.1. Le produit scalaire de deux vecteurs $\overrightarrow{u}\binom{x}{y}$ et $\overrightarrow{v}\binom{x'}{y'}$ est le nombre réel noté $\overrightarrow{u} \cdot \overrightarrow{v}$ défini par

$$\overrightarrow{u} \cdot \overrightarrow{v} = xx' + yy'.$$

Voici quelques conséquences immédiates de cette définition :

Proposition 3.2.
(i) Pour tout nombre réel λ, $(\lambda\overrightarrow{u}) \cdot \overrightarrow{v} = \overrightarrow{u} \cdot (\lambda\overrightarrow{v}) = \lambda(\overrightarrow{u} \cdot \overrightarrow{v})$. Pour cette raison, on note ce nombre $\lambda\overrightarrow{u} \cdot \overrightarrow{v}$.
(ii) Pour tous vecteurs $\overrightarrow{u}, \overrightarrow{v}$ et $\overrightarrow{w}$, on a $\overrightarrow{u} \cdot \overrightarrow{v} = \overrightarrow{v} \cdot \overrightarrow{u}$ et $(\overrightarrow{u} + \overrightarrow{v}) \cdot \overrightarrow{w} = \overrightarrow{u} \cdot \overrightarrow{w} + \overrightarrow{v} \cdot \overrightarrow{w}$.
(iii) Pour tout vecteur $\overrightarrow{u}\binom{x}{y}$, $\overrightarrow{u} \cdot \overrightarrow{u} = x^2 + y^2 = \left\|\overrightarrow{u}\right\|^2$. On écrit souvent $\overrightarrow{u}^2$ pour désigner ce nombre.
(iv) Si $\overrightarrow{u}$ ou $\overrightarrow{v}$ sont nuls, $\overrightarrow{u} \cdot \overrightarrow{v} = 0$. Par contre, la réciproque est fausse (par exemple si $\overrightarrow{u}\binom{1}{0}$ et $\overrightarrow{u}\binom{0}{1}$).
(v) Si $\overrightarrow{u} = \lambda\overrightarrow{v}$ avec $\lambda \in \mathbb{R}$, on a $\overrightarrow{u} \cdot \overrightarrow{v} = \lambda \|v\|^2$.

On utilisera très souvent la propriété (iii) pour écrire $AB^2 = \overrightarrow{AB} \cdot \overrightarrow{AB}$ et utiliser ensuite le calcul vectoriel. Donnons maintenant différentes expressions du produit scalaire.

Théorème 3.3. Soient $\vec{u}$ et $\vec{v}$ deux vecteurs. On a :

(i) $\vec{u} \cdot \vec{v} = \frac{1}{2}\left(\|\vec{u}+\vec{v}\|^2 - \|\vec{u}\|^2 - \|\vec{v}\|^2\right)$.

(ii) Lorsque $\vec{u}$ et $\vec{v}$ son non nuls, $\vec{u} \cdot \vec{v} = \|\vec{u}\| \cdot \|\vec{v}\| \cdot \cos(\vec{u}, \vec{v})$, où $(\vec{u}, \vec{v})$ est l'angle orienté entre les vecteurs $\vec{u}$ et $\vec{v}$.

Une conséquence importante de l'assertion (i) est que le produit scalaire ne dépend pas de la base orthonormée choisie.

Démonstration. Pour (i), écrivons

$$\|\vec{u}+\vec{v}\|^2 = (\vec{u}+\vec{v}) \cdot (\vec{u}+\vec{v}) = \vec{u} \cdot \vec{u} + \vec{v} \cdot \vec{v} + 2\vec{u} \cdot \vec{v} = \|\vec{u}\|^2 + \|\vec{v}\|^2 + 2\vec{u} \cdot \vec{v}.$$

Le résultat en découle.

Pour (ii), plaçons-nous dans le repère orthonormé direct $(O, \vec{i}, \vec{j})$ où $\vec{i} = \frac{\vec{u}}{\|\vec{u}\|}$ (on a vu que (i) implique que le produit scalaire ne dépend pas de la base orthonormée choisie). Alors, en notant $\alpha = (\vec{u}, \vec{v})$, on a $\vec{u}\begin{pmatrix}\|\vec{u}\|\\0\end{pmatrix}$ et $\vec{v}\begin{pmatrix}\|\vec{v}\|\cos(\alpha)\\\|\vec{v}\|\sin(\alpha)\end{pmatrix}$. Ainsi, $\vec{u} \cdot \vec{v} = \|\vec{u}\| \cdot \|\vec{v}\| \cdot \cos(\alpha)$, d'où le résultat. □

On prouve de même que

$$(\vec{u}-\vec{v})^2 = \vec{u}^2 - 2\vec{u} \cdot \vec{v} + \vec{v}^2, \qquad (\vec{u}+\vec{v})(\vec{u}-\vec{v}) = \vec{u}^2 - \vec{v}^2.$$

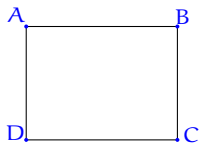
L'intérêt du Théorème 3.3 est d'exprimer la produit scalaire de manière "géométrique", c'est-à-dire sans faire intervenir les coordonnées. Un corollaire crucial est le suivant.

Théorème 3.4. Deux vecteurs $\vec{u}$ et $\vec{v}$ sont orthogonaux si, et seulement si, $\vec{u} \cdot \vec{v} = 0$.

Démonstration. D'après le théorème de Pythagore, $\vec{u}$ et $\vec{v}$ sont orthogonaux si, et seulement si, $\|\vec{u}+\vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2$. D'après le Théorème 3.3, ceci est équivalent au fait que $\vec{u} \cdot \vec{v} = 0$. □

Ainsi, l'utilisation du produit scalaire est particulièrement adaptée lorsque nous sommes en présence de droites orthogonales (mais pas que !), comme l'illusteront les applications qui suivent.

Exemple 3.5. Soit $ABCD$ un rectangle tel que $AB = 4$ et $BC = 3$. Calculons $\overrightarrow{AC} \cdot \overrightarrow{DB}$.

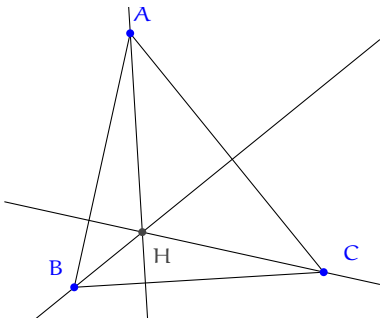


On a

$$\overrightarrow{AC} \cdot \overrightarrow{DB} = (\overrightarrow{AB} + \overrightarrow{BC}) \cdot \overrightarrow{DB} = \overrightarrow{AB} \cdot \overrightarrow{DB} + \overrightarrow{BC} \cdot \overrightarrow{DB} = AB^2 - BC^2 = 7.$$

On aurait également pu passer en coordonnées.

Exemple 3.6. Montrons que les trois hauteurs d'un triangle ABC sont concourantes en utilisant le produit scalaire. Soit H l'intersection des hauteurs issues de B et de C.



Nous allons montrer que $\overrightarrow{AH} \cdot \overrightarrow{BC} = 0$. Pour cela, on écrit :

$$0 = \overrightarrow{BH} \cdot \overrightarrow{AC} = (\overrightarrow{BA} + \overrightarrow{AH}) \cdot \overrightarrow{AC} = \overrightarrow{BA} \cdot \overrightarrow{AC} + \overrightarrow{AH} \cdot \overrightarrow{AC}.$$

De même,

$$0 = \overrightarrow{CH} \cdot \overrightarrow{AB} = \overrightarrow{CA} \cdot \overrightarrow{AB} + \overrightarrow{AH} \cdot \overrightarrow{AB}.$$

Or $\overrightarrow{BA} \cdot \overrightarrow{AC} = \overrightarrow{AC} \cdot \overrightarrow{BA} = \overrightarrow{CA} \cdot \overrightarrow{AB}$. D'où $\overrightarrow{AH} \cdot \overrightarrow{AC} = \overrightarrow{AH} \cdot \overrightarrow{AB}$, et donc

$$\overrightarrow{AH} \cdot (\overrightarrow{AC} - \overrightarrow{AB}) = \overrightarrow{AH} \cdot \overrightarrow{BC} = \overrightarrow{0},$$

ce qui conclut.

Comme dans les exemples précédents, il est parfois utile de décomposer des vecteurs suivant des directions orthogonales pour calculer des produits scalaires.

Exercice 1 Soient $n \geqslant 3$ un entier et $A_1A_2 \cdots A_n$ un polygône régulier inscrit dans un cercle Γ de centre O et de rayon R. Soit M un point de Γ. Prouver que

$$\sum_{i=1}^{n} A_iM^2 = 2nR^2.$$

Concluons par une propriété très utile :

Proposition 3.7. Soient A, B, C, D des points du plan avec $A \neq B$ et $C \neq D$. Les droites (AB) et (CD) sont perpendiculaires si, et seulement si, $AC^2 + BD^2 = AD^2 + BC^2$.

Démonstration. Il suffit d'écrire :

$$\begin{aligned} AC^2 + BD^2 - AD^2 - BC^2 &= (\overrightarrow{AB} + \overrightarrow{BC})^2 + (\overrightarrow{AD} - \overrightarrow{AB})^2 - \overrightarrow{AD}^2 - \overrightarrow{BC}^2 \\ &= 2AB^2 + 2\overrightarrow{AB} \cdot (\overrightarrow{BC} - \overrightarrow{AD}) \\ &= 2\overrightarrow{AB} \cdot (\overrightarrow{BC} - \overrightarrow{BD}) = 2\overrightarrow{AB} \cdot \overrightarrow{DC}, \end{aligned}$$

ce qui conclut. □

On trouvera une jolie utilisation de ce résultat à l'Exemple 3.21.

Applications du produit scalaire Nous donnons ici quelques applications. On rappelle sans preuve la loi des sinus :

$$\frac{a}{\sin \widehat{A}} = \frac{b}{\sin \widehat{B}} = \frac{c}{\sin \widehat{C}} = 2R = \frac{abc}{2S}.$$

Formule d'Al-Kashi

Proposition 3.8 (Formule d'Al-Kashi)**.** Soit ABC un triangle. On a

$$a^2 = b^2 + c^2 - 2bc\cos\widehat{A}.$$

Démonstration. On écrit :

$$\begin{aligned} a^2 = BC^2 = \overrightarrow{BC}^2 = (\overrightarrow{BA} + \overrightarrow{AC})^2 = AB^2 + AC^2 + 2\overrightarrow{BA}\cdot\overrightarrow{AC} &= AB^2 + AC^2 - 2\overrightarrow{AB}\cdot\overrightarrow{AC} \\ &= b^2 + c^2 - 2bc\cos\widehat{A}. \end{aligned}$$

□

Identité du parallélogramme

Proposition 3.9 (Identité du parallélogramme)**.** Soit $ABCD$ un parallélogramme. Alors $AC^2 + BD^2 = 2(AB^2 + AD^2)$.

Démonstration. En prenant $\vec{u} = \overrightarrow{AB}$ et $\vec{v} = \overrightarrow{AD}$, ceci provient du fait que

$$(\vec{u} + \vec{v})^2 + (\vec{u} - \vec{v})^2 = 2(\vec{u}^2 + \vec{v}^2).$$

□

Formule de la médiane

Proposition 3.10 (Formules de la médiane)**.** Soit ABC un triangle et I le milieu de $[AB]$. Alors :

$$\text{(i)}\quad AC^2+BC^2 = 2IC^2+\frac{1}{2}AB^2, \quad \text{(ii)}\quad AC^2-BC^2 = 2\overrightarrow{CI}\cdot\overrightarrow{BA}, \quad \text{(iii)}\quad \overrightarrow{CA}\cdot\overrightarrow{CB} = CI^2-\frac{1}{4}AB^2.$$

Démonstration. Pour (i), on écrit

$$AC^2 + BC^2 = \overrightarrow{AC}^2 + \overrightarrow{BC}^2 = (\overrightarrow{AI} + \overrightarrow{IC})^2 + (\overrightarrow{BI} + \overrightarrow{IC})^2 = 2IC^2 + 2(\overrightarrow{AI} + \overrightarrow{BI})\cdot\overrightarrow{IC} + AI^2 + BI^2.$$

Comme $\overrightarrow{AI} + \overrightarrow{BI} = \overrightarrow{0}$ et $AI^2 + BI^2 = AB^2/2$, le résultat en découle.

Les preuves des autres assertions sont similaires et sont laissées en exercice. □

Géométrie analytique

Le produit scalaire est également utile en géométrie analytique pour calculer les coordonnées de divers points lorsque de l'orthogonalité est mise en jeu :

(i) Soient A, B, C trois points différents du plan. Comment trouver l'équation de la droite perpendiculaire à (AB) passant par (C) ? Un point M appartient à cette droite si, et seulement si, $\overrightarrow{CM}\cdot\overrightarrow{AB} = 0$. Ainsi, si $A\binom{x_A}{y_A}$, $B\binom{x_B}{y_B}$ et $C\binom{x_C}{y_C}$, l'équation de la droite perpendiculaire à (AB) passant par C est caractérisée par l'équation

$$(x - x_C)(x_B - x_A) + (y - y_C)(y_B - y_A) = 0.$$

(ii) Deux droites de coefficients directeurs respectifs k et k' sont perpendiculaires si, et seulement si, $kk' = -1$. On rappelle que le coefficient directeur d'une droite d'équation $ax + by + c = 0$ est $(-b, a)$. Ainsi, un vecteur orthogonal à cette droite (on dit aussi vecteur normal) est (a, b).

Relations trigonométriques

Rappelons sans preuve les relations suivantes (qu'on vérifie aisément grâce à un cercle trigonométrique) : On rappelle également que $\cos^2(x) + \sin^2(x) = 1$.

$$\begin{array}{llll} \cos(-x) = \cos(x) & & \sin(-x) = -\sin(x) & \\ \cos(\pi - x) = -\cos(x) & & \sin(\pi - x) = \sin(x) & \\ \cos(\pi + x) = -\cos(x) & & \sin(\pi + x) = -\sin(x) & \\ \cos\left(\frac{\pi}{2} + x\right) = -\sin(x) & & \sin\left(\frac{\pi}{2} + x\right) = \cos(x) & \\ \cos\left(\frac{\pi}{2} - x\right) = \sin(x) & & \sin\left(\frac{\pi}{2} - x\right) = \cos(x) & \end{array}$$

Les relations suivantes sont cruciales et absolument à connaître.

Théorème 3.11 (Formules d'addition trigonométriques)**.** (i) On a

$$\cos(a - b) = \cos(a)\cos(b) + \sin(a)\sin(b), \quad \cos(a + b) = \cos(a)\cos(b) - \sin(a)\sin(b).$$

(ii) On a

$$\sin(a - b) = \sin(a)\cos(b) - \cos(a)\sin(b), \quad \sin(a + b) = \sin(a)\cos(b) + \cos(a)\sin(b).$$

(iii) On a

$$\tan(a - b) = \frac{\tan(a) - \tan(b)}{1 + \tan(a)\tan(b)}.$$

Démonstration. Pour (i), introduisons les points U et V de coordonnées $U\binom{\cos(a)}{\sin(a)}$ et $V\binom{\cos b}{\sin(b)}$. Ainsi, $b - a$ est l'angle (modulo 2π) orienté $(\overrightarrow{OU}, \overrightarrow{OV})$. Comme $OU = OV = 1$, en calculant de deux manières différentes le produit scalaire $\overrightarrow{OU} \cdot \overrightarrow{OV}$, on obtient :

$$\cos(a - b) = \overrightarrow{OU} \cdot \overrightarrow{OV} = \cos(a)\cos(b) + \sin(a)\sin(b).$$

La seconde relation s'en déduit en prenant $-b$ à la place de b.

Pour (ii), il suffit d'écrire que $\sin(a + b) = \cos(\pi/2 - a - b)$ et d'utiliser (i).

Finalement, (iii) est une conséquence de (i) et (ii), laissée en exercice. □

En particulier, noter que

$$\begin{aligned} \cos(2a) &= \cos^2(a) - \sin^2(a) = 2\cos^2(a) - 1 = 1 - 2\sin^2(a) \\ \sin(2a) &= 2\sin(a)\cos(a) \\ \tan(2a) &= \frac{2\tan(a)}{1 - \tan^2(a)}. \end{aligned}$$

Ces dernières formules s'appellent les *formules de duplication*. Noter aussi que le théorème 3.11 implique que

$$\begin{aligned} \cos(a) + \cos(b) &= 2\cos\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right) \\ \cos(a) - \cos(b) &= -2\sin\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right) \\ \sin(a) + \sin(b) &= 2\sin\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right) \\ \sin(a) - \sin(b) &= 2\sin\left(\frac{a-b}{2}\right)\cos\left(\frac{a+b}{2}\right). \end{aligned}$$

Exercice 2 Soit ABC un triangle.

(i) Prouver que $\overrightarrow{OA} \cdot \overrightarrow{OB} = R^2 - c^2/2$.

(ii) Prouver que $\overrightarrow{OH} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}$.

(iii) Prouver que $OH^2 = 9R^2 - a^2 - b^2 - c^2$.

- Puissance d'un point par rapport à un cercle -

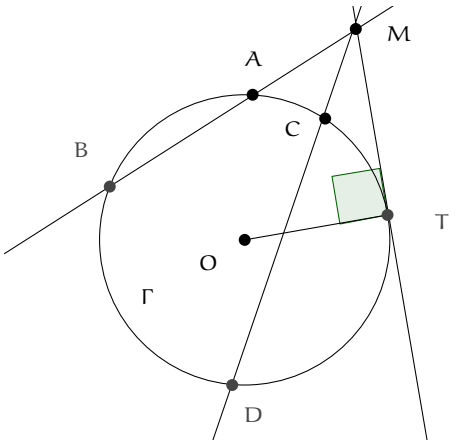
Si A, B, C sont trois points alignés, on rappelle que $\overline{AB}\cdot\overline{AC}$, produit algébrique des longeurs AB et AC, est égal par définition à $\overrightarrow{AB} \cdot \overrightarrow{AC}$.

Définition et premières propriétés

Définition 3.12 (et propriété)**.** Soit Γ un cercle de centre O de rayon R. Soit M un point quelconque du plan. Si deux droites passant par M coupent Γ respectivement en A, B et C, D alors

$$\overline{MA} \cdot \overline{MB} = \overline{MC} \cdot \overline{MD}.$$

Ce réel est aussi égal à $OM^2 - R^2$ et est appelé puissance du point M par rapport au cercle Γ et est noté $P_\Gamma(M)$.



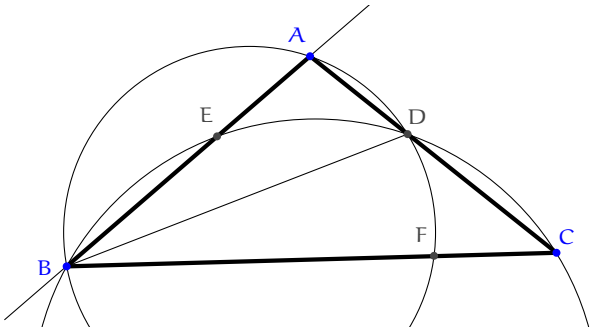
Démonstration. Soit A' le point diamétralement opposé à A sur Γ, de sorte que $\widehat{MBA'} = \pi/2$ et $\overrightarrow{OA'} = \overrightarrow{AO}$. Alors

$$\overline{MA} \cdot \overline{MB} = \overrightarrow{MA} \cdot \overrightarrow{MB} = \overrightarrow{MA} \cdot \overrightarrow{MA'} = (\overrightarrow{MO} + \overrightarrow{OA}) \cdot (\overrightarrow{MO} - \overrightarrow{OA}) = OM^2 - R^2.$$

On montre exactement de la même manière que $\overline{MC} \cdot \overline{MD} = OM^2 - R^2$. □

Remarque 3.13. $P_\Gamma(M) = 0$ si, et seulement si, $M \in \Gamma$ et $P_\Gamma(M) > 0$ si, et seulement si, M est à l'exterieur de Γ. Par ailleurs, si M est à l'extérieur de Γ et T est le point de contact avec Γ d'une tangente à Γ issue de M, alors $P_\Gamma(M) = MT^2$.

Exemple 3.14 (Olympiade de Saint-Pétersbourg 1996)**.** À titre d'exemple, résolvons le problème suivant. Soit ABC un triangle et D le pied de la bissectrice issue de $\widehat{B}$. On note E le second point d'intersection du cercle circonscrit du triangle de BDC avec (AB) et F le second point d'intersection du cercle circonscrit du triangle ABD avec (BC). Montrons que $AE = CF$.



En calculant de deux manières possibles les puissances, on a

$$AE \cdot AB = AD \cdot AC, \qquad CB \cdot CF = CD \cdot CA.$$

On en déduit que

$$\frac{AE}{CF} = \frac{AD \cdot CB}{AB \cdot CD}.$$

Or $AD/CD = AB/CB$ car (BD) est la bissectrice de $\widehat{B}$.

Réciproquement, les assertions suivantes sont vérifiées (leur preuve est laissée en exercice).

Proposition 3.15. (i) Soient A, B, C, D des points distincts non alignés. Si (AB) et (CD) sont sécantes en un point M tel que $\overline{MA} \cdot \overline{MB} = \overline{MC} \cdot \overline{MD}$ alors les points A, B, C, D sont cocycliques.

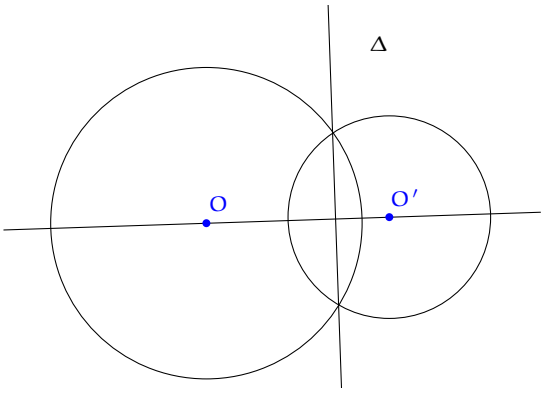
(ii) Soit ABT un triangle. Si un point M de la droite (AB) vérifie $\overline{MA} \cdot \overline{MB} = MT^2$, alors (MT) est tangente au cercle Γ circonscrit au triangle ABT.

Axe radical

Définition 3.16 (et propriété)**.** Soient Γ et Γ' deux cercles de centres respectifs O et O' distincts, de rayons respectifs R et R'. Alors l'ensemble des points M qui ont même puissance par rapport à ces deux cercles est une droite Δ perpendiculaire à (OO'). Par ailleurs, le point d'intersection P des droites Δ et (OO') vérifie

$$2\overline{OO'} \cdot \overline{\omega P} = R^2 - R'^2,$$

où ω est le milieu de $[OO']$. La droite Δ est appelée axe radical des deux cercles Γ et Γ'.



Démonstration. L'égalité $P_\Gamma(M) = P_{\Gamma'}(M)$ est équivalente à $MO^2 - R^2 = MO'^2 - R'^2$. Or

$$MO^2 - MO'^2 = (\overrightarrow{MO} - \overrightarrow{MO'})(\overrightarrow{MO} + \overrightarrow{MO'}) = \overrightarrow{O'O} \cdot (2\overrightarrow{M\omega} + \overrightarrow{\omega O'} + \overrightarrow{\omega O}) = 2\overrightarrow{O'O} \cdot \overrightarrow{M\omega}.$$

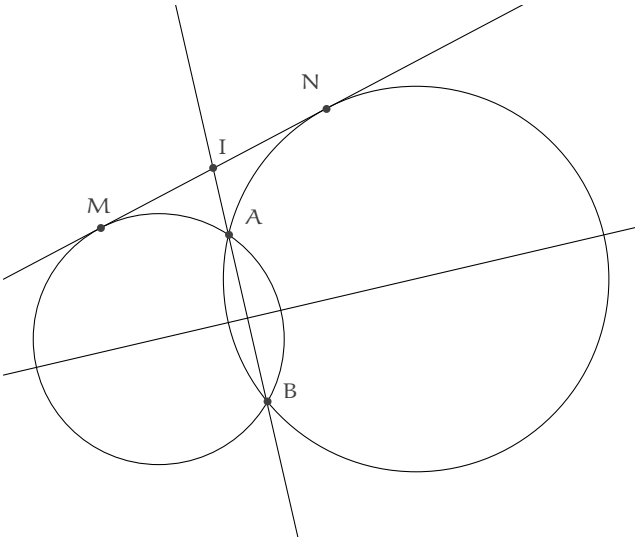
Ainsi, l'ensemble des points M tels que $P_\Gamma(M) = P_{\Gamma'}(M)$ est l'ensemble des points M tels que

$$2\overrightarrow{O'O} \cdot \overrightarrow{M\omega} = R^2 - R'^2.$$

Le résultat en découle. □

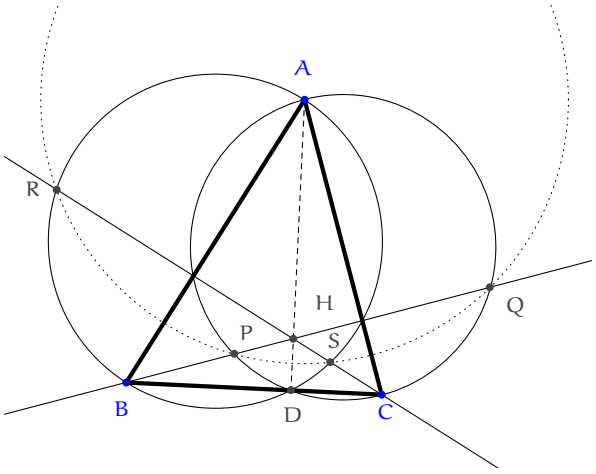
Remarque 3.17. Si Γ et Γ' sont sécants, leur axe radical est la droite passant par leurs points d'intersection.

Exemple 3.18. Soient Γ_1, Γ_2 deux cercles qui se coupent en A et en B. Soit Δ une droite tangente aux deux cercles en M et en N. Montrons que (AB) coupe le segment $[MN]$ en son milieu.



La puissance de I par rapport au premier cercle vaut $IM^2 = IA \cdot IB$. La puissance de I par rapport au deuxième cercle vaut $IA \cdot IB = IN^2$. On en déduit que $IM^2 = IN^2$, d'où $IM = IN$.

Exemple 3.19. Soit ABC un triangle acutangle. La perpendiculaire à (AC) passant par B coupe le cercle de diamètre $[AC]$ en P et Q, et la droite perpendiculaire à (AB) passant par C coupe le cercle de diamètre $[AB]$ en R et S. Montrons que P, Q, R, S sont cocycliques.

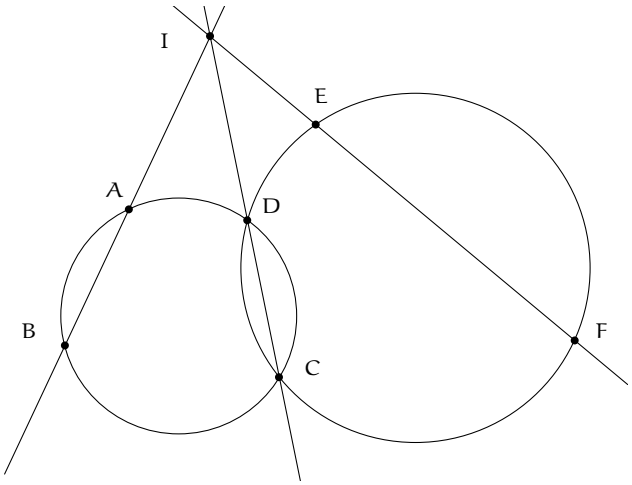


Soit D le pied de la hauteur issue de A dans le triangle ABC et soit H son orthocentre. Le point D appartient au cercle de diamètre [AB], donc $HS \cdot HR = HA \cdot HD$. De même, D appartient au cercle de diamètre [AC], donc $HP \cdot HQ = HA \cdot HD$. Donc $HP \cdot HQ = HR \cdot HS$, ce qui implique que P, Q, R, S sont cocycliques.

Théorème 3.20. Soient ABCD et CDEF deux quadrilatères inscrits dans deux cercles Γ_1, Γ_2. On suppose que parmi les droites (AB), (CD) et (EF) il n'y en a pas deux qui soient parallèles. Alors les droites (AB), (CD) et (EF) sont concourantes si, et seulement si, les points A, B, E et F sont cocycliques.

Ce résultat dit que les axes radicaux de trois cercles sont soit concourants, soit parallèles.

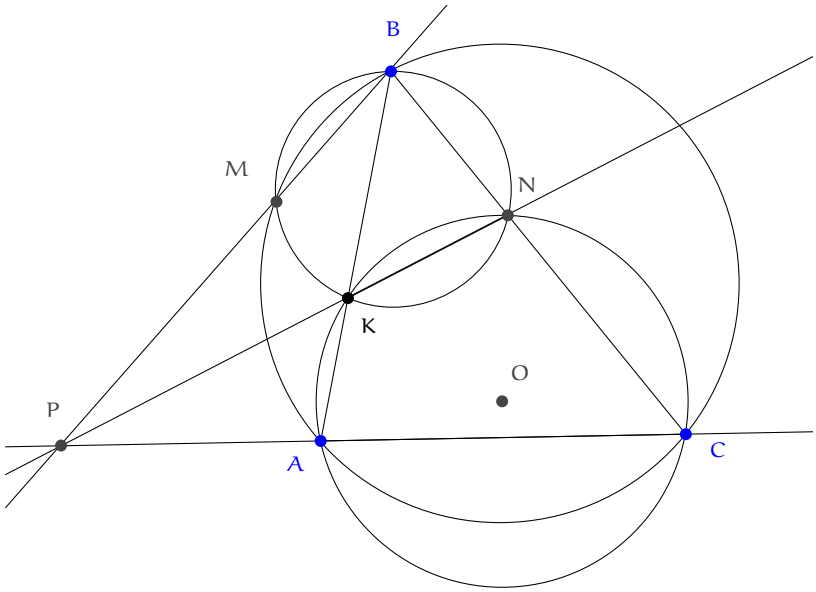
Démonstration.



Supposons d'abord que les trois droites soient concourantes. Alors la puissance de I par rapport au cercle de gauche vaut $IA \cdot IB = ID \cdot IC$. La puissance de I par rapport au cercle de droite vaut $ID \cdot IC = IE \cdot IF$. On en déduit que $IA \cdot IB = IE \cdot IF$, et donc que A, B, F, E sont cocycliques.

Réciproquement, si A, B, F, E sont cocycliques, notons I le point d'intersection des droites (AB) et (EF). La puissance de I par rapport au cercle circonscrit à ABFE vaut $IA \cdot IB = IE \cdot IF$. Donc I a même puissance par rapport aux deux cercles de la figure. I est donc sur leur axe radical, qui est (DC). Les trois droites (AB), (CD) et (EF) sont donc concourantes en I. □

Exemple 3.21. (IMO 1985/5) Un cercle de centre O passe par les points A et C d'un triangle ABC et recoupe les segments [AB] et [BC] en respectivement K et N ($K \neq N$). On suppose que les cercles circonscrits aux triangles ABC et KBN se recoupent en un point M différent de B. Prouvons que l'angle $\widehat{OMB}$ est un angle droit.



Soit P l'intersection des trois axes radicaux (AC), (KN) et BM. D'après la Proposition 3.7, pour prouver que (OM) et (BP) sont perpendiculaires, il suffit de vérifier que $OB^2 - OP^2 = MB^2 - MP^2$.

Comme $\widehat{PCN} = \widehat{AKN} = \widehat{BMN}$, les points P, C, N, M sont cocycliques. En notant r le rayon du cercle circonscrit de AKC, il vient :

$$PM \cdot PN = PC \cdot PA = OP^2 - r^2.$$

De même,

$$BM \cdot BP = BN \cdot BC = OB^2 - r^2.$$

Ainsi,

$$OB^2 - OP^2 = BM \cdot BP - PM \cdot PB = BP(BM - PM) = (BM + PM)(BM - PM) = BM^2 - PM^2,$$

d'où le résultat.

Exercices d'application **Exercice 3** Soit ABC un triangle isocèle en B. Les tangentes en A et B au cercle circonscrit Γ de ABC se coupent en D. Soit E le second point d'intersection de (DC) avec Γ. Prouver que (AE) coupe [DB] en son milieu.

Exercice 4 Soit ABC un triangle, H son orthocentre. Soient M un point de [AB] et N un point de [AC]. Les cercles de diamètre BN et CM se coupent en P et Q. Montrer que P, Q et H sont alignés.

Exercice 5 (IMO 2000/1) Soient Ω_1 et Ω_2 deux cercles qui se coupent en M et en N. Soit Δ la tangente commune aux deux cercles, qui est plus proche de M que de N. Δ est tangente à Ω_1 en A et à Ω_2 en B. La droite passant par M et parallèle à Δ rencontre Ω_1 en C et Ω_2 en D. Soient E l'intersection des droites (CA) et (BD), P le point d'intersection de droites (AN) et (CD) et Q le point d'intersection des droites (BN) et (CD). Montrer que EP = EQ.

Exercice 6 (USAMO 1998) Soient Γ_1 et Γ_2 deux cercles concentriques, avec Γ_2 à l'intérieur de Γ_1. Soient A, B deux points appartenant à respectivement Γ_1 et Γ_2 tels que (AB) est tangente à Γ_2.

Soit C le deuxième point d'intersection de (AB) avec Γ_1 et soit D le milieu de $[AB]$. Une droite passant par A coupe Γ_2 en E et F de sorte que les médiatrices de $[DE]$ et $[CF]$ se coupent en un point M de la droite (AB). Calculer le rapport AM/MC.

Exercice 7 Soient ABC un triangle et D, E deux points appartenant respectivement à $[AB]$ et $[AC]$ tels que (DE) et (BC) soient parallèles. Soit P un point à l'intérieur du triangle ADE. Soient F et G les points d'intersection de (DE) avec respectivement les droites (BP) et (CP). Soit Q le deuxième point d'intersection des cercles circonscrits des triangles PDG et PFE. Prouver que les points A, P, Q sont alignés.

Exercice 8 (IMO 1995) Soient A, B, C, D quatre points distincts d'une droite (dans cet ordre). Les cercles de diamètre $[AC]$ et $[BD]$ se coupent en X et Y. La droite (XY) coupe (BC) en Z. Soit P un point de la droite (XY) autre que Z. La droite (CP) recoupe le cercle de diamètre $[AC]$ en M, et la droite (BP) recoupe le cercle de diamètre $[BD]$ en N. Prouver que les droites $(AM), (DN)$ et (XY) sont concourantes.

Exercice 9 (Chine 1997) Soient A, B, C, D quatre points sur un cercle Γ. On suppose que les droites (AB) et (DC) se coupent en P et que les droites (AD) et (BC) se coupent en Q. Soient E et F les deux points de tangence des tangentes à Γ issues de Q. Prouver que P, E, F sont alignés.

- Quelques configurations à connaître en géométrie du triangle -

Rappels On rappelle sans démonstration les résultats suivants :

- les symétriques de l'orthocentre d'un triangle par rapport à ses côtés appartiennent à son cercle circonscrit (on peut le retrouver en faisant une chasse aux angles).
- Si P est le pied de la bissectrice intérieure issue de A dans un triangle ABC, alors $\frac{PB}{PC} = \frac{AB}{AC}$ (on peut le retrouver en utilisant la loi des sinus).

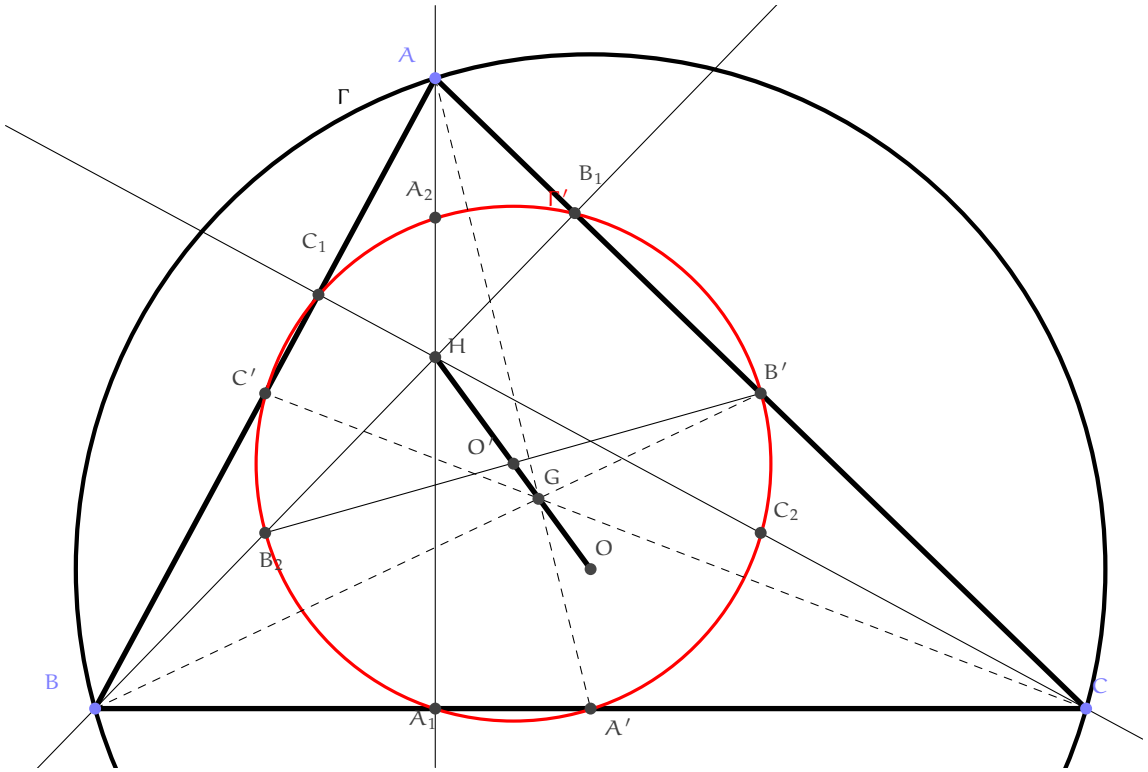
On rappelle qu'il est parfois utile de faire une esquisse de figure rapidement à main levée pour choisir la configuration initiale donnant la meilleure figure possible. Par meilleure, on entend une figure sans symétries ajoutées (comme des triangles isocèles qui n'en sont pas forcément), sans alignements supplémentaires, etc. Ensuite il est utile de travailler sur une grande figure tracée avec les instruments. Si des propriétés remarquables semblent apparaître (égalité de longueurs, alignements), il est utile de faire une figure dans une autre configuration pour voir s'il s'agit une coincidence ou non.

Cercle d'Euler

Théorème 3.22. (i) On a $\overrightarrow{OH} = 3\overrightarrow{OG}$.

(ii) Les points suivants sont tous cocycliques : les milieux des côtés du triangle ABC, les pieds des hauteurs de ABC, les milieux des segments $[AH], [BH], [CH]$. Le cercle passant par tous ces points est appelé *cercle d'Euler* de ABC. Par ailleurs, le rayon du cercle d'Euler vaut $R/2$.

(iii) Les triangles ABC, ABH, BCH et CAH ont même cercle d'Euler, et leurs cercles circonscrits ont tous même rayon.



Ce résultat, ainsi que sa preuve, sont à retenir.

Démonstration. (i) On a déjà vu que $\overrightarrow{OH} = \overrightarrow{OA}+\overrightarrow{OB}+\overrightarrow{OC}$. Comme G est le centre de gravité de ABC, on a $\overrightarrow{GA} + \overrightarrow{GB} + \overrightarrow{GC} = \overrightarrow{0}$. Donc

$$\overrightarrow{OH} = (\overrightarrow{OG} + \overrightarrow{GO}) + (\overrightarrow{OG} + \overrightarrow{GB}) + (\overrightarrow{OG} + \overrightarrow{GC}) = 3\overrightarrow{OG}.$$

(ii) Soit Γ le cercle circonscrit de ABC. Notons A', B' et C' les milieux respectifs de $[BC]$, $[AC]$ et $[AB]$; notons également A_1, B_1 et C_1 les pieds respectifs des hauteurs issues de A, B et C.

ÉTAPE 1 : Soit $\mathcal{H}$ l'homothétie de centre G et de rapport $-1/2$. Étudions l'image de Γ par $\mathcal{H}$. Le centre de gravité étant situé au tiers de chaque médiane, $\mathcal{H}$ transforme A en A', B en B' et C en C'. Ainsi, l'image de Γ par $\mathcal{H}$ est le cercle circonscrit de $A'B'C'$ qu'on note Γ'. Ainsi, le rayon de Γ' est $R/2$. Soit O' son centre. On a donc $\overrightarrow{GO'} = -\frac{1}{2}\overrightarrow{GO}$. Or $\overrightarrow{OH} = 3\overrightarrow{OG}$. On en déduit que O' est le milieu de $[OH]$.

ÉTAPE 2 : Soit h l'homothétie de centre H et de rapport 2. D'après ce qui précède, h transforme un cercle de centre O' et de rayon r en un cercle de centre O et de rayon $2r$. On en déduit que h transforme Γ' en Γ. En particulier Γ' contient $h(A), h(B), h(C)$ et donc les milieux des segments $[AH]$, $[BH]$, $[CH]$ appartiennent à Γ'.

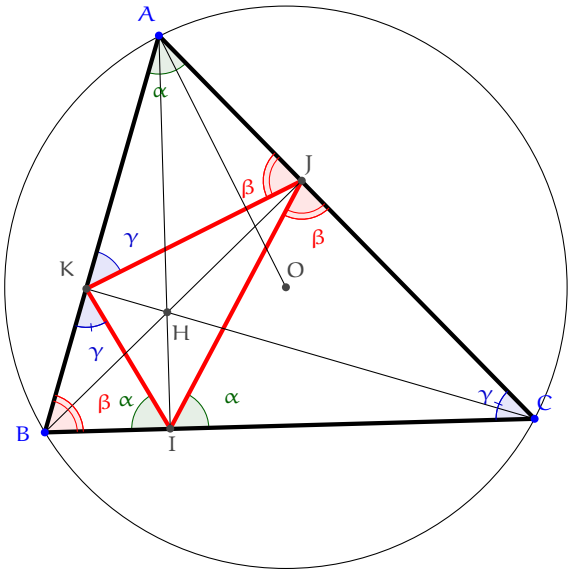
ÉTAPE 3 : Pour montrer que $A_1 \in \Gamma'$, montrons que $O'A_1 = O'A$.Soit O'_1 le projeté orthogonal de O' sur (BC). Comme $(HA_1) \parallel (OA')$ et comme O' est le mileu de $[OH]$, le théorème de Thalès assure que O'_1 est le milieu de $[A_1A']$. Il s'ensuit que O'_1 appartient à la médiatrice de ce dernier segment et donc $O'A_1 = O'A$. On montre de même que $B_1, C_1 \in \Gamma'$.

(iii) Le cercle Γ' passe par les milieux de tous ces triangles. Ils ont donc même cercle d'Euler et donc même rayon, car d'après (ii) ce rayon vaut $R/2$.

□

Triangle orthique et théorème de Nagel Soit ABC un triangle non rectangle. Soient I, J, K les pieds respectifs des hauteurs issues de A, B, C. Le triangle IJK est appelé *triangle orthique* de ABC

Théorème 3.23. (i) On a les égalités d'angles suivantes :



(ii) Théorème de Nagel : les bissectrices des angles $\widehat{BAC}$ et $\widehat{IAO}$ sont confondues.

(iii) Les droites $(OA), (OB), (OC)$ sont perpendiculaires aux côtés de IJK.

(iv) Les droites (IJ) et (IK) sont symétriques par rapport à la hauteur (AI).

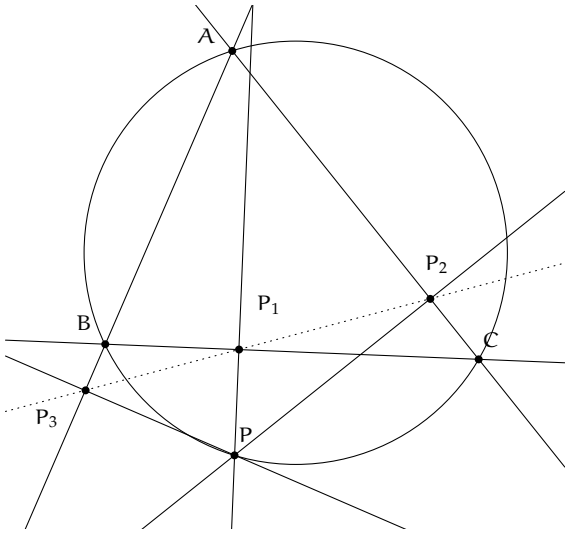
Démonstration. La première assertion provient d'une simple chasse aux angles. Les autres assertions sont alors des conséquences faciles (pour (ii), on utilise par exemple que $\widehat{OAC} = 90° - \beta/2 = \widehat{BAI}$). □

Droites de Simson et de Steiner On définit ici la notion importante de droite de Simson et étudions quelques unes de es propriétés. Dans cette partie, on garde les notations introduites dans les différents énoncés.

Théorème 3.24. Soit Γ un cercle et A, B, C trois points de Γ. Soit P un point du plan, P_1, P_2, P_3 ses projections respectives sur les droites $(BC), (CA), (AB)$. Montrer que les points P_1, P_2, P_3 sont alignés si et seulement si P appartient à Γ.

Lorsque A, B, C, D sont cocycliques, la droite passant pas P_1, P_2, P_3 est appelée *droite de Simson*, et on la notera Δ_P.

Démonstration. On traitera le cas où les points sont dans la confiuration de la figure, les autres se traitent de façon similaire.

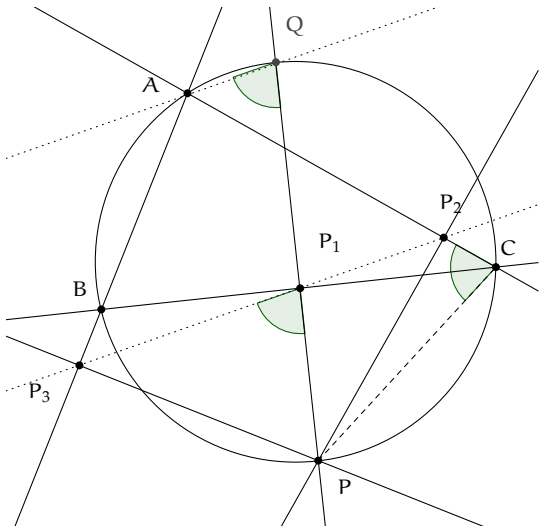


Les points P, P_1, B, P_3 d'une part, P, A, P_2, P_3 d'autre part sont cocycliques. En en déduit que $\widehat{PP_3P_1} = \widehat{PBP_1} = \widehat{PBC}$ et $\widehat{PP_3P_2} = \widehat{PAP_2} = \widehat{PAC}$. Or, les points P, Q, R sont alignés si et seulement si $\widehat{P_1P_3P_2} = 0$, soit $\widehat{PP_3P_1} = \widehat{PP_3P_2}$, donc si et seulement si $\widehat{PBC} = \widehat{PAC}$, donc si et seulement si les points A, B, C, P sont cocycliques. □

Proposition 3.25. On reprend les notations du Théorème 3.24. On suppose que $P \in \Gamma$. Notons Q le point où (PP_1) recoupe Γ (si (PP_1) est tangente à Γ on pose $Q = P$).

Alors (AQ) et Δ_P sont parallèles.

Démonstration. On traitera le cas où les points sont dans la confiuration de la figure, les autres se traitent de façon similaire.



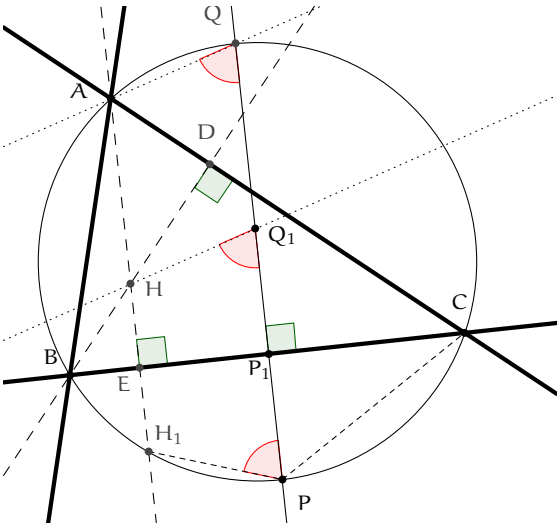
Les points Q, A, C, P étant cocycliques, on a $\widehat{AQP} = \widehat{ACP}$. Par ailleurs, les points P_1, P_2, C, P étant cocycliques (sur le cercle de diamètre $[CP]$), on a $\widehat{P_3P_1P} = \widehat{ACP}$. On en déduit que $\widehat{AQP} = \widehat{P_3P_1P}$, et donc que Δ_P et (AQ) sont parallèles. □

Théorème 3.26. On suppose que $P \in \Gamma$. Notons respectivement Q_1, Q_2, Q_3 les symétriques de P par rapport aux droites $(BC), (AC), (AB)$.

(i) Les points Q_1, Q_2, Q_3 sont alignés sur une droite notée $\mathcal{D}_P$ et appelée *droite de Steiner*. De plus Δ_P et $\mathcal{D}_P$ sont parallèles.

(ii) L'orthocentre H du triangle ABC appartient à la droite de Steiner $\mathcal{D}_P$.

Démonstration.

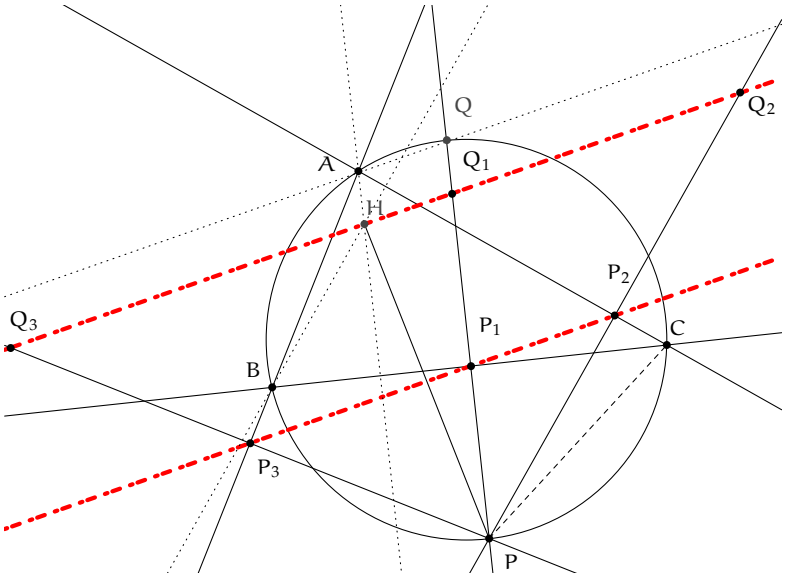


Comme la droite de Simson est parallèle à (AQ), il suffit de prouver que (HQ_1) est parallèle à (AQ) (on montrerait de même que (HQ_2) et (HQ_3) sont parallèles à (AQ)).

Notons H_1 le symétrique de H par rapport à (BC). On sait que H_1 appartient à Γ. Par symétrie, $\widehat{HQ_1P} = \widehat{Q_1PH_1}$. Comme H_1, A, P, Q sont cocycliques, on $\widehat{Q_1PH_1} = 180° - \widehat{HAQ}$. Comme (AH) et (QP_1) sont parallèles (car perpendiculaires à (BC)), il vient $180° - \widehat{HAQ} = \widehat{AQP_1}$. On en déduit que (AQ) et (HQ_1) sont parallèles, ce qui clôt la preuve. □

Théorème 3.27. On suppose que $P \in \Gamma$. Alors le milieu de $[PH]$ appartient à la droite de Simson

Démonstration. Comme P_1, P_2, P_3 sont les milieux respectifs de $[PQ_1]$, $[PQ_2]$, $[PQ_3]$, la droite de Steiner est l'image de la droite de Simson par une homothétie de centre P et de rapport 2. Comme H appartient à la droite de Steiner, on en déduit que le milieu de $[HP]$ appartient à la droite de Simson.



□

Proposition 3.28. Soient $P, P' \in \Gamma$. Montrer que les droites de Simson de P et P' sont perpendiculaires si, et seulement si, P et P' sont diamétralement opposés sur Γ.

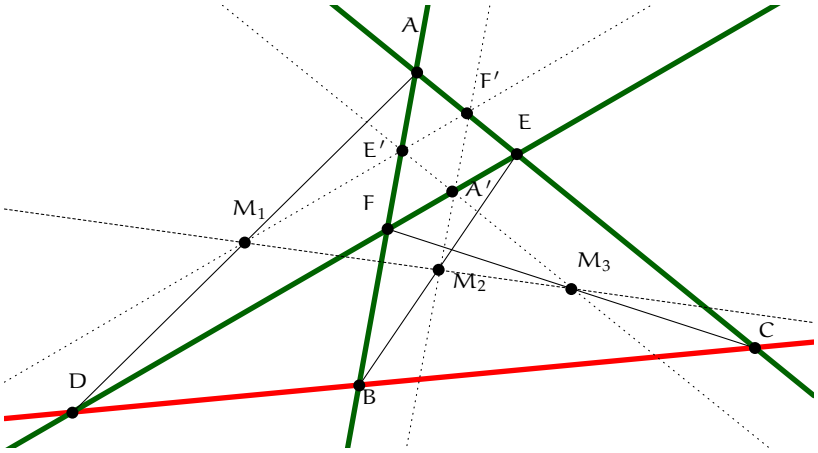
Démonstration. Notons Q' le point où $(P'P'_1)$ recoupe Γ. D'après la Proposition 3.25, il suffit de prouver que (AQ) et (AQ') sont perpendiculaires si, et seulement si, P et P' sont diamétralement opposés sur Γ. Or (AQ) et (AQ') sont perpendiculaires si, et seulement si, $[QQ']$ est un diamètre de Γ. On voit aisément que c'est le cas si, et suelement si, P et P' sont diamétralement opposés. □

Exercice 10 Soient $P, P' \in \Gamma$ deux points diamétralement opposés. Prouver que les droites de Simson de P et P' se coupent en un point du cercle d'Euler de ABC.

Quadrilatères complets On explore ici quelques propriétés des quadrilatères complets, qui sont des figures detérminées par quatre droites distinctes, sécantes deux à deux, l'intersection de trois quelconques d'entre elles étant vides. Plus précisément, soit ABC un triangle. On suppose qu'une droite Δ coupe $(BC), (CA), (AB)$ en respectivement D, E, F. On parle de quadrilatère complet $BCEF$.

Théorème 3.29 (Droite de Newton d'un quadrilatère complet)**.** Soient M_1, M_2, M_3 les milieux respectifs de $[AD], [BE], [CF]$. Les points M_1, M_2, M_3 sont alignés sur une droite appelée *droite de Newton* du quadrilatère complet.

Démonstration.



Soient A', E', F' les milieux respectifs de $[EF], [FA], [AE]$. Alors M_1, E', F' sont alignés, ainsi que M_2, F', A' et ainsi que M_3, A', E'. D'après le théorème de Thalès, les triplets M_1, E', F' et M_2, F', A' et M_3, A', E' sont constitués de points alignés.

Appliquons le théorème de Ménélaüs au triangle AEF et la droite passant par D, B, C

$$\frac{\overline{DE}}{\overline{DF}} \cdot \frac{\overline{BF}}{\overline{BA}} \cdot \frac{\overline{CA}}{\overline{CE}} = 1.$$

D'après le théorème de Thalès, on a $\overline{DE} = 2\overline{M_1F'}$, $\overline{DF} = 2\overline{M_1E'}$, $\overline{BF} = 2\overline{M_2A'}$, $\overline{BA} = 2\overline{M_2F'}$, $\overline{CA} = 2\overline{M_3E'}$, $\overline{CE} = 2\overline{M_3A'}$. On en déduit que

$$\frac{\overline{M_1F'}}{\overline{M_1E'}} \cdot \frac{\overline{M_3E'}}{\overline{M_3A'}} \cdot \frac{\overline{M_2A'}}{\overline{M_2F'}} = 1.$$

□

Théorème 3.30 (Point de Miquel d'un quadrilatère complet)**.**

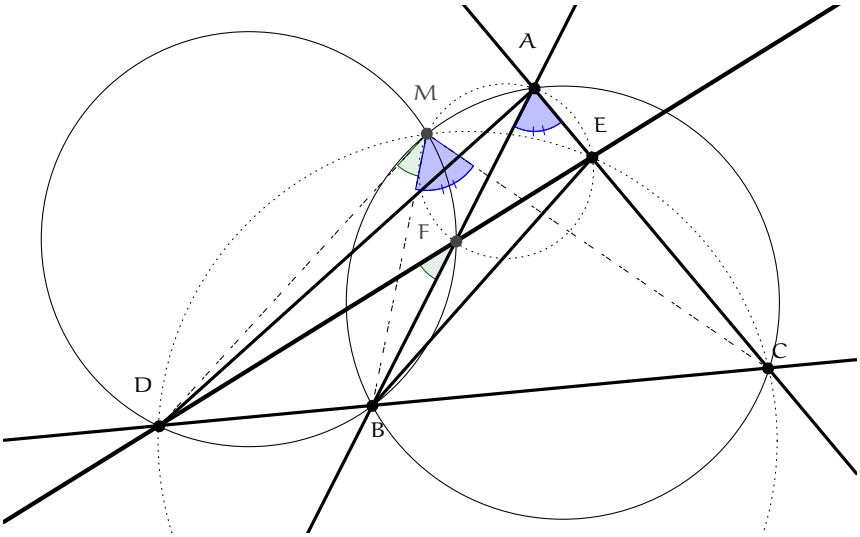
(i) Les quatres cercles Γ_1, Γ_2, Γ_3 et Γ_4 circonscrits respectivement aux triangles ABC, DBF, AEF et DCE sont concourants en un point appelé *point de Miquel* du quadrilatère complet.

(ii) Les centres de Γ_1, Γ_2, Γ_3 et Γ_4 appartiennent un même cercle $\mathcal{M}$, appelé *cercle de Miquel* du quadrilatère complet.

(iii) Le point de Miquel appartient au cercle de Miquel.

Démonstration. On fait les démonstrations dans les configurations des figures (sinon il faudrait utiliser des angles orientés).

(i)

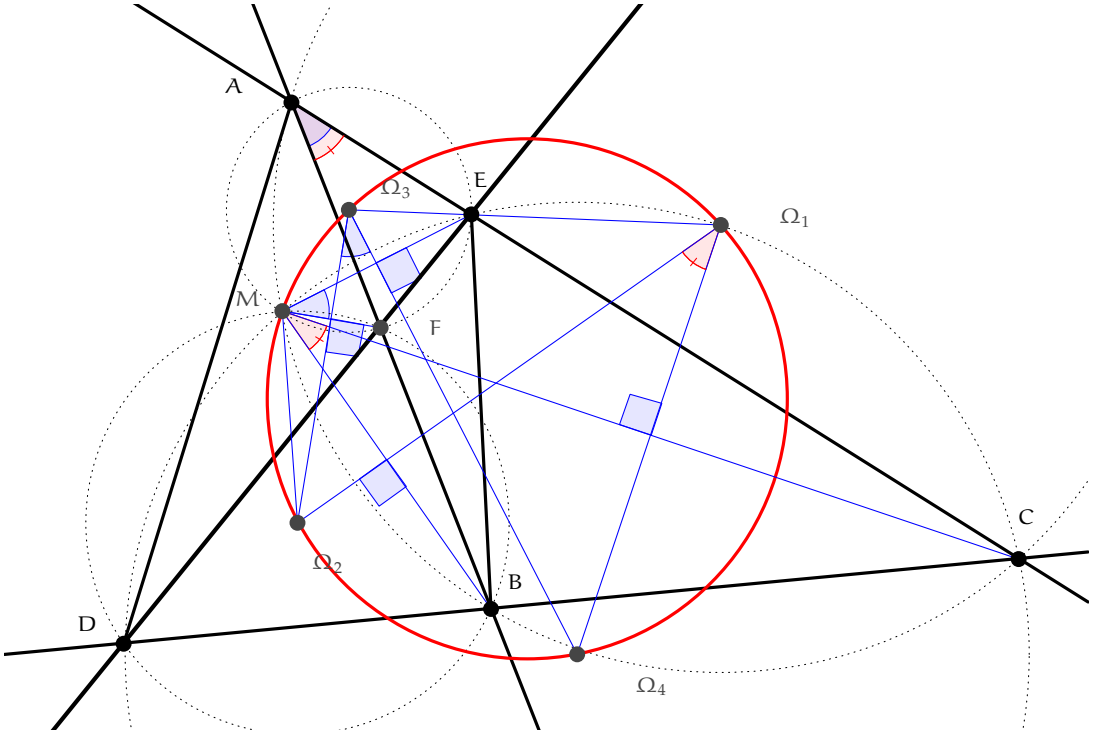


Soit M le point d'intersection des cercles circonscrits à ABC et DBF. Montrons que M appartient au cercle circonscrit de DEC (la preuve est similaire pour AEF). Par cocyclicité on a

$$\widehat{DMB} = \widehat{DFB}, \qquad \widehat{BMC} = \widehat{BAC}.$$

Donc $\widehat{DMC} = \widehat{FEC}$. On en déduit que D, M, E, C sont cocycliques.

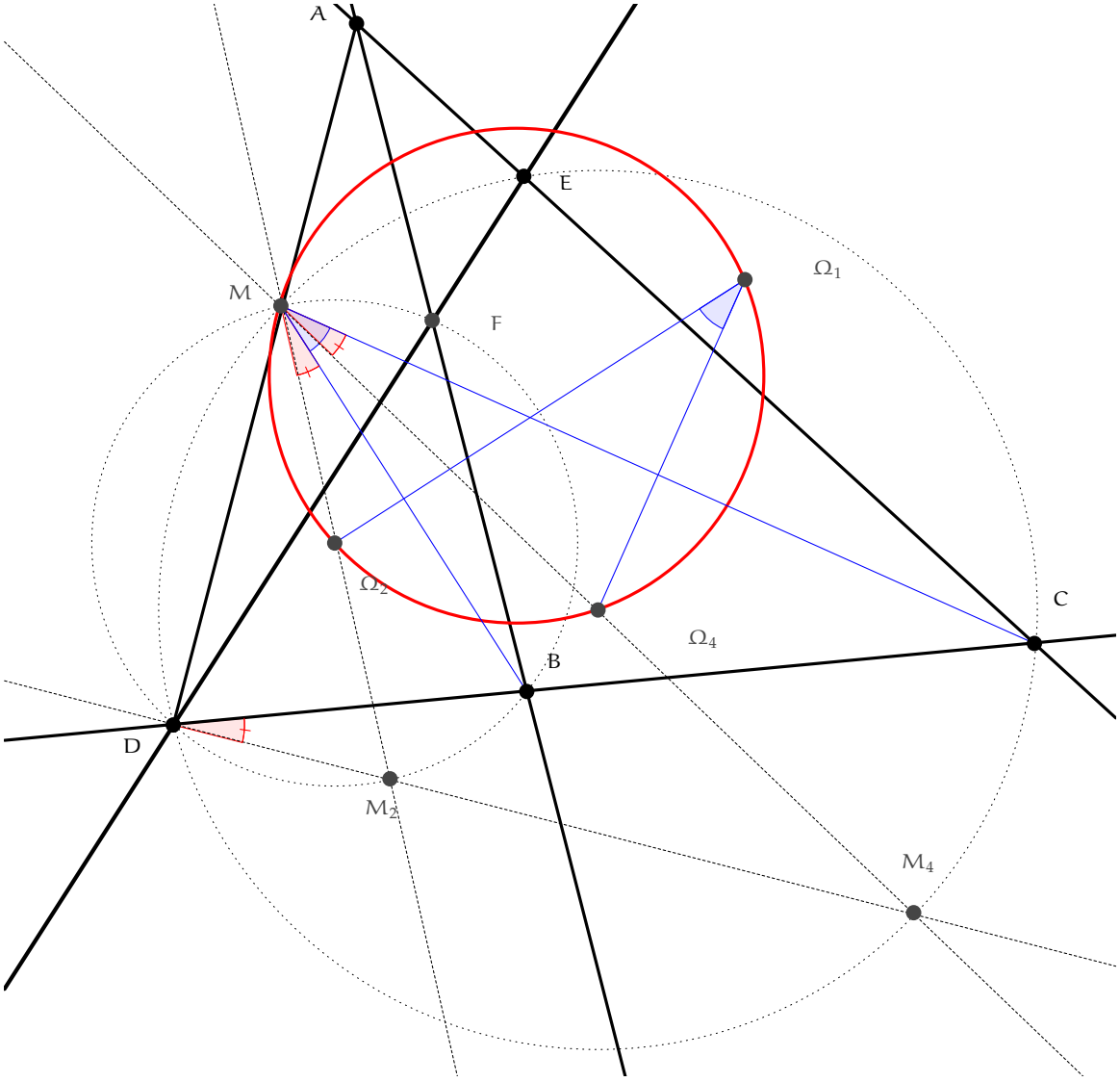
(ii)



Comme $(MF) \perp (\Omega_2\Omega_3)$ et $(\Omega_3\Omega_4) \perp (EM)$, on a $\widehat{FME} = \Omega_2\Omega_3\Omega_4$. De même, $\widehat{BMC} = \Omega_2\widehat{\Omega_1}\Omega_4$.

Or par cocyclicité de A, E, F, M, on a $\widehat{FME} = \widehat{FAE}$ et par cocyclicité de A, M, B, C on a $\widehat{FAE} = \widehat{BAC} = \widehat{BMC}$. Ainsi, $\Omega_2\Omega_3\Omega_4 = \Omega_2\widehat{\Omega_1}\Omega_4$, ce qui prouve que les quatre centres sont cocycliques.

(iii)



Montrons que $\Omega_1, \Omega_2, \Omega_4, M$ sont cocycliques. Pour cela, soient M_2 et M_4 les points diamétralement opposés de M sur respectivement Ω_2 et Ω_4.Alors $\widehat{MDM_2}$ et $\widehat{MDM_4}$ sont des angles droits, et donc D, M_2, M_4 sont alignés. On en déduit que

$$\widehat{\Omega_2 MB} = \widehat{M_2 MB} = \widehat{M_2 DB} = \widehat{M_4 DC} = \widehat{\Omega_4 MC}.$$

Il s'ensuit que $\Omega_2 M \Omega_4 = \widehat{BMC}$. Or on a vu dans la preuve de (ii) que $\widehat{BMC} = \widehat{\Omega_2 \Omega_1 \Omega_4}$. Ceci conclut.

□

Finalement, le fait suivant, utile et à retenir, est laissé en exercice.

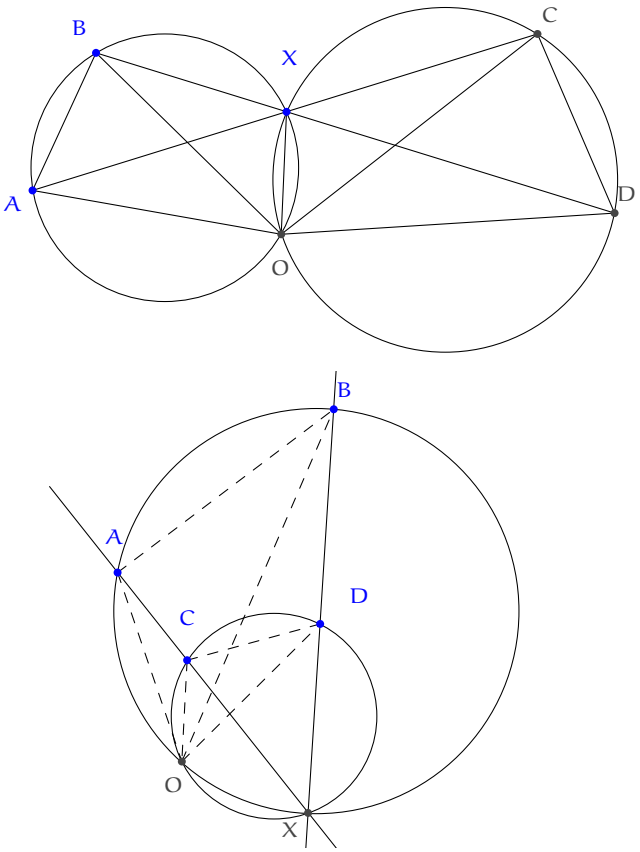
Exercice 11 En gardant les notations précédentes, montrer que le point M appartient à la droite (AD) si, et seulement si, les points B, F, E, C sont cocycliques.

Nous concluons cette section par une autre propriété utile du point de Miquel, qui permet de retrouver le centre d'une similitude connaissant un segmet et son image. On rappelle

qu'une similitude directe de centre O est la composée d'une rotation et d'une homothétie (les deux de centre O) et que si ABCD n'est pas un parallélogramme, il existe une unique similitude directe envoyant A sur B et C sur D.

Théorème 3.31. Soient A, B, C, D quatre points du plan tels que (AC) et (BD) ne soient pas parallèles. Soit X le point d'intersection des droites (AC) et (BD). Soit O le second point d'intersection des cercles circonscrits des triangles ABX et CDX. Alors O est le centre de la similitude directe envoyant A sur C et B sur D, ainsi que le centre de la similitude directe envoyant A sur B et C sur D.

Démonstration.



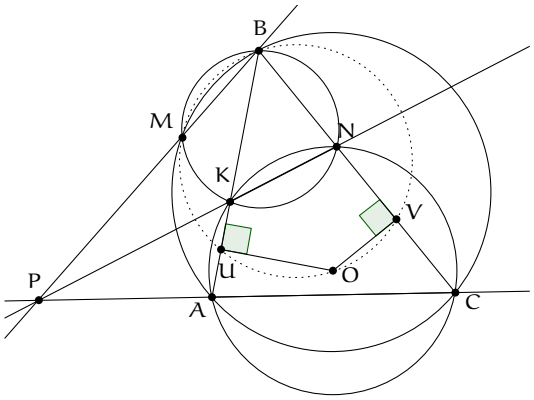
Ceci provient d'une simple chasse aux angles, qui montre que les triangles AOC et BOD sont semblables, ainsi que les triangles AOB et CPD. □

En particulier, si O est le centre d'une similitude directe qui envoie A sur C et B sur D (ou A sur B et C sur D), alors si M est le point de Miquel du quadrilatère ABDC et X est le point d'intersection de (AC) et (BD), alors A, B, M, X sont cocycliques ainsi que C, D, O, M.

Une conséquence immédiate du théorème précédent est que le point de Miquel M d'un quadrilatère ABCD est le centre de la similitude directe qui envoie A sur D et B sur C, ainsi que le centre de la similitude directe qui envoie A sur B et D sur C.

À titre d'illustration, démontrons l'affirmation de l'Exemple 3.21 en utilisant ce résultat. Rappelons son contenu : un cercle de centre O passe par les points A et C d'un triangle ABC et recoupe les segments [AB] et [BC] en respectivement K et N ($K \neq N$). On suppose que les

cercles circonscrits aux triangles ABC et KBN se recoupent en un point M différent de B. Il s'agissait de prouver que l'angle $\widehat{OMB}$ est un angle droit.



Comme dans l'Exemple 3.21 (ou en utilisant l'exercice 11), les droites (MB), (KN) et (AC) sont concourantes en un point P. Notons U et V les milieux respectifs de $[AK]$ et $[CN]$. M est le centre de la similitude directe envoyant $[AK]$ sur $[NC]$. M est donc aussi le centre de la similitude directe envoyant $[KU]$ sur $[NV]$, ce qui implique que les points M, B, U, V sont cocycliques. Or, puisque $\widehat{OUB} = \widehat{OVB} = 90°$, les points U, B, V, O appartiennent au cercle de diamètre $[BO]$. Donc M appartient également à ce dernier cercle, ce qui implique que $\widehat{OMB} = 90°$.

Pour approfondir cette partie, nous ne saurions trop vivement conseiller la lecture de http://yufeizhao.com/olympiad/cyclic_quad.pdf

Bissectrices, cercles inscrit et exinscrits

Théorème 3.32. Soit I le centre du cercle inscrit d'un triangle ABC et I_a le centre de son cercle exinscrit Γ_a "de l'angle $\widehat{A}$". Soit A' le milieu de $[BC]$ et soient D et D_1 les points de contacts respectifs du cercle inscrit de Γ_a avec (BC).

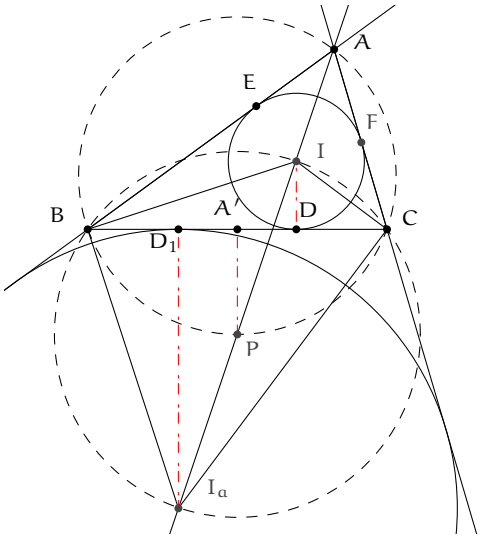
(i) D et D_1 sont symétriques par rapport à A'.

(ii) Notons E, F les points de contacts respectifs du cercle inscrit avec $[AB]$ et $[AC]$. En notant $p = (a + b + c)/2$, on a

$$CD_1 = BD = p - b, \quad BD_1 = CD = p - c, CE_1 = p - b.$$

On calcule similairement les autres longueurs faisant intervenir les points de contacts du cercle inscrit et des autres cercles circonscrits.

Démonstration.



(i) Soit P le milieu de $[II_a]$. Prouvons que P appartient au cercle circonscrit de ABC. Comme $\widehat{I_aBI} = \widehat{I_ACI} = 90°$, P est le centre cercle passant par B, I, C, I_a. En particulier, P appartient à la médiatrice de $[BC]$. Or il est bien connu que la médiatrice de $[BC]$ coupe (IA) en un point appartenant au cercle circonscrit de ABC.

point d'intresection de la droite (AI) avec le cercle circonscrit de ABC. Il est bien connu que P appartient à la médiatrice de $[BC]$. Par ailleurs, comme $\widehat{I_aBI} = \widehat{I_ACI} = 90°$, $[II_a]$ est le diamètre du cercle passant par B, I, C, I_a. En particulier, le projeté orthogonal de P sur (BC) est A'. Puisque les projetés orthogonaux sur (BC) de I_a et I sont respectivement D_1 et D, A' est bien le milieu de D_1D, d'où le résultat.

(ii) Posons $x = AE = AF, y = BF = BD, z = CD = CE$. Comme $BD + DC = BC$, on a $y + z = a$. De même, $z + x = b$ et $x + y = c$. On en déduit que $x + y + z = p$, puis $x = p - a$, $y = p - b$ et $z = p - c$. Comme D_1 et D sont symétriques par rapport à A', on a aussi $CD_1 = BD = p - b$ et $PD_1 = CD = p - c$.

□

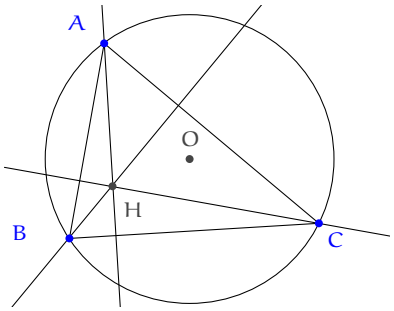
- Solution des exercices -

Solution de l'exercice 1 En remarquant que $\overrightarrow{OA_1} + \overrightarrow{OA_2} + \cdots + \overrightarrow{OA_n} = \overrightarrow{0}$, écrivons

$$\begin{aligned}\sum_{i=1}^{n} A_iM^2 &= \sum_{i=1}^{n} (\overrightarrow{OM} - \overrightarrow{OA_i}) \cdot (\overrightarrow{OM} - \overrightarrow{OA_i}) \\ &= \sum_{i=1}^{n} \left(2R^2 - 2\overrightarrow{OM} \cdot \overrightarrow{OA_i}\right) \\ &= 2nR^2 - 2\overrightarrow{OM} \cdot \left(\sum_{i=1}^{n} \overrightarrow{OA_i}\right) = 2nR^2,\end{aligned}$$

ce qui conclut.

Solution de l'exercice 2



(i) On écrit :

$$\overrightarrow{OA} \cdot \overrightarrow{OB} = R^2 \cos \widehat{AOB} = R^2 \cos(2\widehat{C}) = R^2(1 - 2\sin^2(\widehat{C})) = R^2 - c^2/2,$$

où pour la dernière égalité on a utilisé le fait que $2R = c/\sin \widehat{C}$ d'après la loi des sinus.

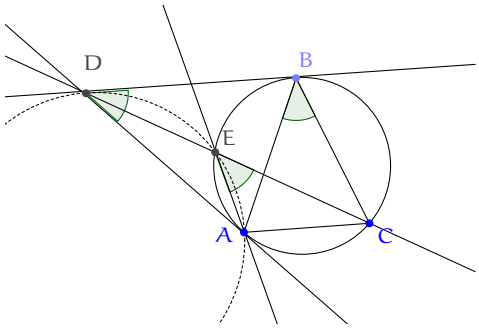
(ii) Il suffit de vérifier que si le point H' est défini par la relation $\overrightarrow{OH'} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}$, alors $\overrightarrow{AH'} \cdot \overrightarrow{BC}$ et $\overrightarrow{BH'} \cdot \overrightarrow{AC}$, ce qui se fait exactement comme dans l'Exemple 3.6.

(iii) On écrit :

$$\begin{aligned} OH^2 &= \overrightarrow{OH}^2 = (\overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}) \cdot (\overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}) \\ &= 3R^2 + 2(R^2 - a^2/2) + 2(R^2 - b^2/2) + 2(R^2 - c^2/2), \end{aligned}$$

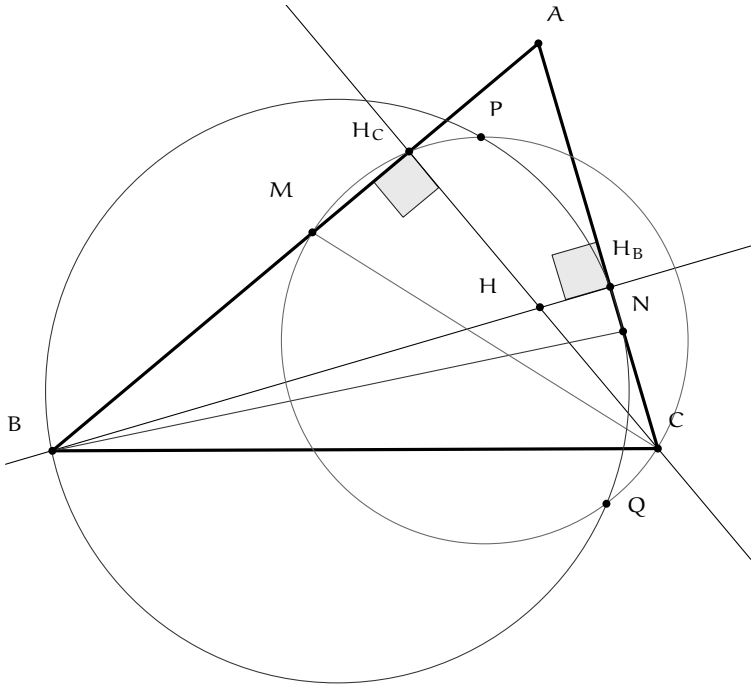
d'où le résultat.

Solution de l'exercice 3



D'après l'Exemple 3.18, il suffit de vérifier que le cercle circonscrit de ADE est tangent à (DB). Ceci provient d'une petite chasse aux angles : $\widehat{ADB} = 180° - 2\widehat{ABD} = \widehat{ABC} = \widehat{AEC}$.

Solution de l'exercice 4

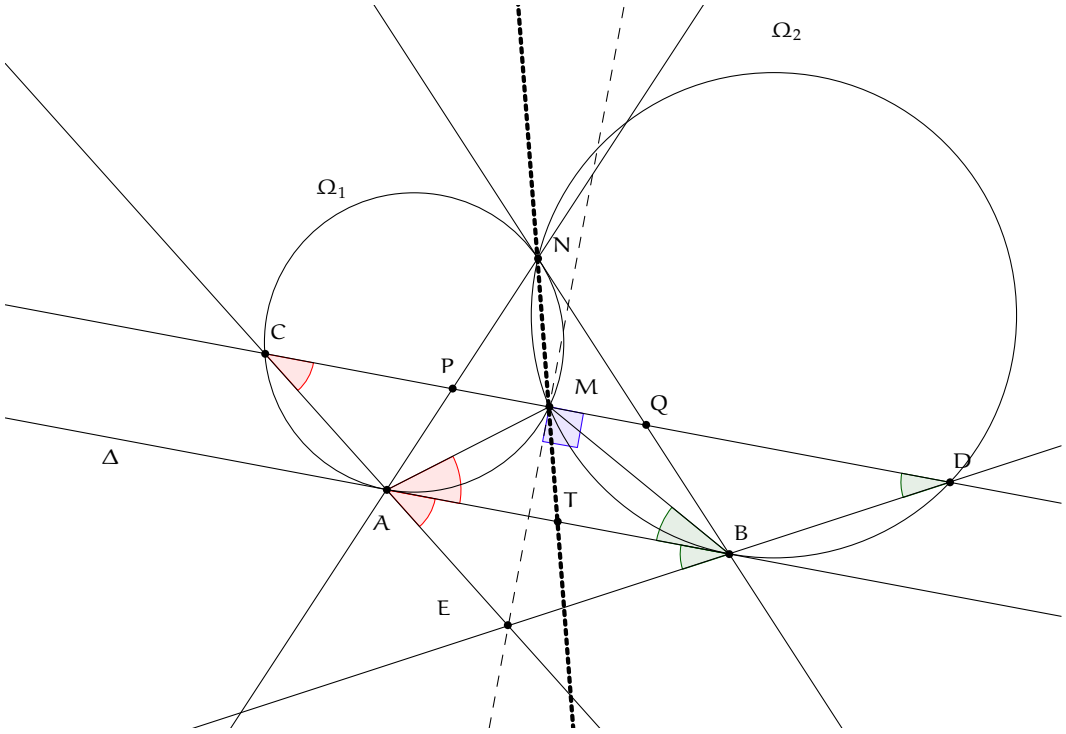


Nous allons montrer que H a la même puissance par rapport aux deux cercles de la figure, ce qui impliquera que H est sur leur axe radical, qui est (PQ).

Pour cela, comme $(BH_B) \perp (AC)$, H_B est sur le cercle de diamètre $[BN]$. La puissance de H par rapport au cercle de diamètre $[BN]$ vaut donc $-HB \cdot HH_B$. De même, la puissance de H par rapport au cercle de diamètre $[CM]$ vaut $-HC \cdot HH_C$.

Or les points B, H_C, H_B, C sont cocycliques : ces points sont situés sur le cercle de diamètre $[BC]$. On en déduit que $-HB \cdot HH_B = -HH_C \cdot HC$, ce qui conclut.

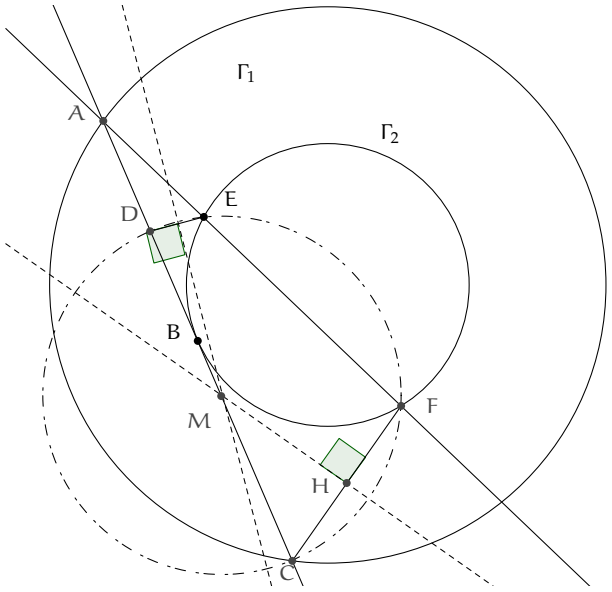
Solution de l'exercice 5



Il suffit d'être logique, qualité qui permet de résoudre nombre d'exercices de géométrie : une chasse aux angles s'impose, et montre que $\widehat{ABE} = \widehat{CDE} = \widehat{MBA}$, la dernière égalité étant d'une importance capitale. De même, $\widehat{BAE} = \widehat{MAB}$. Ces égalités impliquent que M et E sont images l'un de l'autre par la symétrie par rapport à la droite (AB). Les droites (ME) et (AB) sont orthogonales, puis les droites (ME) et (PQ) sont orthogonales.

Il faut également savoir reconnaître les situations classiques : ici, en notant T l'intersection des droites (MN) et (AB), il faut savoir que $TA = TB$ (voir Exemple 3.18). Le théorème de Thalès montre alors que M est le milieu de $[PQ]$. En somme, (ME) est la médiatrice de $[PQ]$. E est donc bien équidistant de P et de Q.

Solution de l'exercice 6

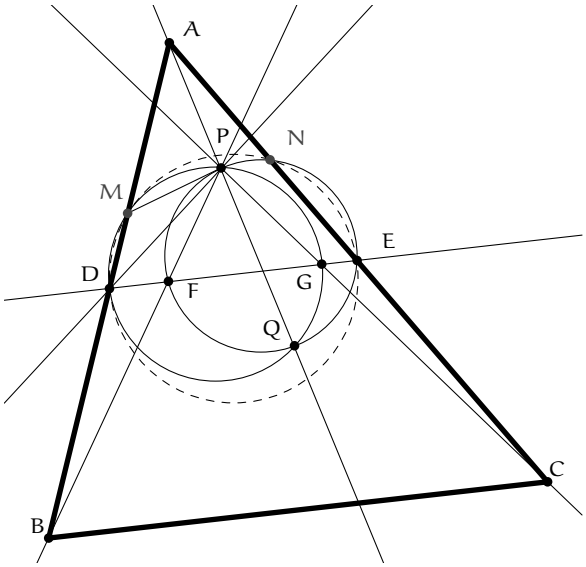


En calculant la puissance de A par rapport à Γ_1, on obtient $AE \cdot AF = AB^2 = AD \cdot AC$. Donc D, C, F, E appartiennent à un même cercle Ω, de sorte que M est le centre de Ω. On en déduit que $[DC]$ est un diamètre de Ω puis que M est le milieu de $[DC]$. D'où :

$$\frac{MC}{AC} = \frac{DC}{2AC} = \frac{3}{2 \cdot 4} = \frac{3}{8}.$$

Donc $AM/MC = 3/5$.

Solution de l'exercice 7

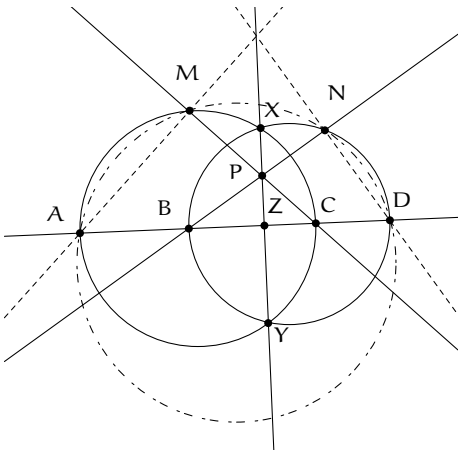


Soient M le second point d'intersection du cercle circonscrit de PDG avec (AB), et N le second point d'intersection du cercle circonscrit de EPF avec (AC). Sans perte de généralité, supposons que M et N appartiennent respectivement à $[AB]$ et $[AC]$ (les autres cases sont similaires). Alors

$$\widehat{ABC} = \widehat{ADG} = 180° - \widehat{BDG} = 180° - \widehat{MPC},$$

ce qui implique que B, M, P, C sont cocycliques. De même, B, P, N, C sont cocycliques. Ainsi, B, C, N, P, M sont cocycliques. Donc $\widehat{ANM} = \widehat{ABC} = \widehat{ADE}$, donc M, N, D, E sont également cocycliques. Donc $AD \cdot AM = AE \cdot AD$. Ainsi A a même puissance par rapport aux cercles circonscrits de PDG et EPF, et appartient donc à (PQ) qui est leur axe radical.

Solution de l'exercice 8

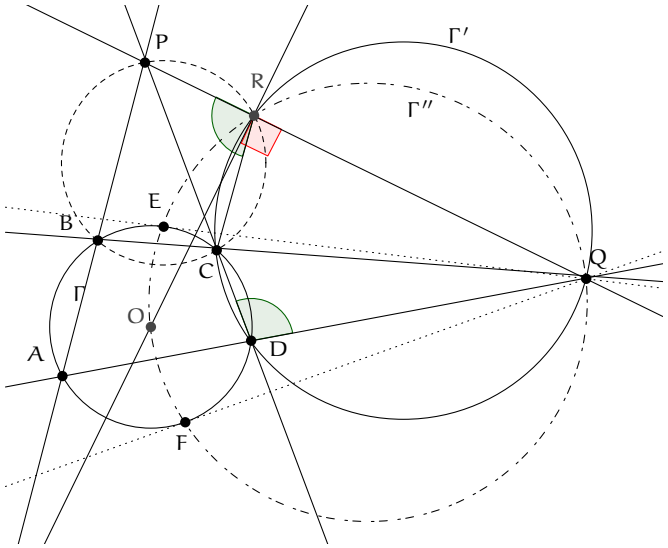


Le point P appartenant à l'intersection des trois axes radicaux, les ponts M, N, C, B sont cocycliques. Par ailleurs, comme

$$\widehat{MND} = 90° + \widehat{MNB} = 90° + \widehat{MCA} = 180° - \widehat{MAD},$$

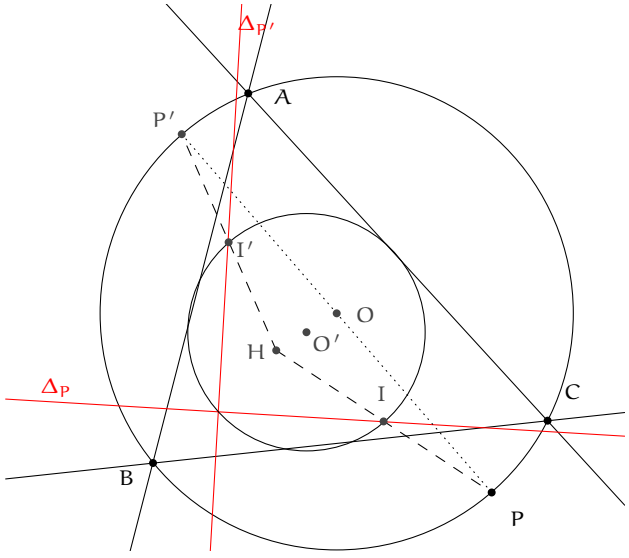
les points A, M, N, D sont cocycliques. Les droites $(AM), (DN)$ et (XY) sont ainsi les axes radicaux de trois cercles et sont donc concourantes (elles ne peuvent pas être parallèles).

Solution de l'exercice 9



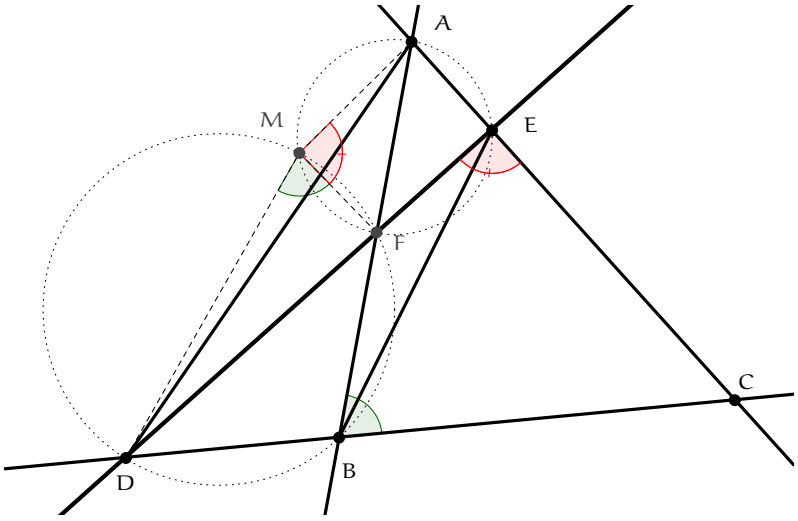
Soit O le centre de Γ et soit R le second point d'intersection du cercle circonscrit Γ′ à QCD avec (PQ) (R est le point de Miquel du quadrilatère complet). Comme $\widehat{PRC} = \widehat{QDC} = \widehat{ABC}$, on rappelle que les points P, R, C, B sont cocycliques. D'après l'Exemple 3.21, (OR) et (PQ) sont perpendiculaires, ce qui implique que Q, F, O, E, R sont cocycliques sur un cercle Γ″. L'axe radical de Γ et Γ′ est (CD), l'axe radical de Γ′ et Γ″ est (QR). Comme ils s'intersectent en P, il en découle que P appartient à l'axe radical de Γ et Γ″, qui n'est autre que (EF).

Solution de l'exercice 10



Soit O le centre de Γ. Soit Γ′ le cercle d'Euler de ABC et notons O′ son centre. Notons I et I′ les milieux respectifs de [PH] et [P′H]. On a déjà vu que Γ′ est l'image de Γ par une homothétie de centre H et de rapport 1/2. On en déduit que I et I′ appartiennent au cercle d'Euler. Comme [PP′] est un diamètre de Γ, [II′] est un diamètre de Γ′. Si R est le point d'intersection des deux droites de Simson, les droites (RI) et (RI′) sont perpendiculaires. Ainsi, R appartient au cercle de diamètre [II′], qui n'est autre que le cercle d'Euler.

Solution de l'exercice 11



Faisons la preuve dans la configuration de la figure. Par cocyclicité de D, M, F, B on a $\widehat{DMF} = \widehat{FBC}$ et par cocyclicité de M, A, E, F on a $\widehat{FMA} = \widehat{DEC}$. Ainsi, D, M, A sont alignés, si et seulement si, $\widehat{FBC} + \widehat{FEC} = 180°$, autrement dit si, et seulement si, F, E, C, B sont cocycliques.

2 Cours/TD de géométrie : similitudes

Question philosophique : qu'est-ce que la géométrie ? S'agit-il de l'étude de certaines figures en termes d'angles, de distances ... ? La distance d'une figure donnée au bord du tableau ne nous intéresse pourtant pas. L'étude de certaines propriétés de certaines figures ? Certes, mais comment définir exactement ces propriétés ? Qu'est-ce qui distingue la propriété pertinente "A, B et C sont alignés" et la propriété inintéressante "(AB) est perpendiculaire au bord du tableau" ? Ou, moins caricaturalement, la propriété "$AB = 1\text{cm}$", moyennement intéressante de la plupart des points de vue mathématiques.

Un moyen pertinent de définir ces propriétés est : "l'ensemble des propriétés invariantes par une certaine classe de transformations". Par exemple, si on veut s'intéresser aux distances, on peut considérer les propriétés invariantes par isométries (translations, rotations, réflexions...) ; si on veut s'intéresser aux rapports de longueurs, aux angles, on peut considérer les propriétés invariantes par similitudes ; si on veut s'intéresser au parallélisme, aux milieux, on peut considérer les propriétés invariantes par transformation affines ; si on veut s'intéresser aux alignements, aux points harmoniques, on peut considérer les propriétés invariantes par transformation projective (voir cours du groupe D).

Il est donc naturel de tenter de comprendre en profondeur ces transformations. Nous considérerons ici les similitudes directes.

- Cours -

Définition 3.33. On appelle similarité toute transformation (i.e. fonction bijective) du plan qui conserve les angles orientés, ou, de manière équivalente, envoie les triangles sur des triangles directement semblables.

Remarques 3.34. – L'équivalence entre conservation des angles orientés et des triangles directement semblables n'est pas immédiatement évidente pour les triangles plats. Toutefois, étant donné trois points A, B et C alignés, pour montrer que le rapport AB/AC est

conservé, il suffit de considérer un point P en dehors de la droite et de considérer les triangles ABP et ACP, prouvant que les rapports AB/AP et AP/AC seront conservés. Une astuce du même genre permettra de toujours mettre de côté ce genre de cas résiduels. C'est un bon exercice pour le lecteur pointilleux de remplir les trous...
- On connaît déjà bon nombre de similarités. Translations, rotations, homothéties et similitude directes (voir définition 3.41) sont des similarités. De plus, il est évident que la composition de deux similarités est une similarité.
- Le terme "similarité" est un anglicisme. Le terme approprié est similitude directe, mais cela induit une confusion avec la notion propre au plan de la définition 3.41. Le théorème 3.42 en devient d'ailleurs particulièrement limpide...

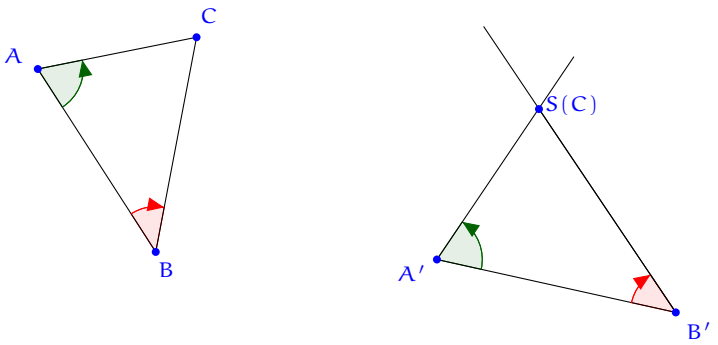
Théorème 3.35. Étant donnés quatre points $A \neq B$ et $A' \neq B'$, il existe une unique similarité S telle que :

$$\begin{array}{rcccl} S & : & A & \longmapsto & A' \\ & & B & \longmapsto & B'. \end{array}$$

Démonstration. On pourrait raisonner directement dans l'esprit du théorème 3.42, mais la preuve naturelle a son intérêt.

Unicité.

Montrons que pour tout point C du plan, cette condition fixe l'image de C par S. On suppose $C \notin (AB)$. Par conservation des angles orientés, l'image de C doit être sur la droite formant en B′ un angle $\widehat{ABC}$ avec la droite (AB). De même, elle doit être sur la droite formant en A′ un angle $\widehat{BAC}$ avec (AB). L'intersection de ces deux droites, uniquement déterminée, est donc le point recherché.



Existence.

On va exhiber une similarité avec cette propriété en composant différentes similarités classiques (translations, rotations, homothéties...) de manière à s'approcher de plus en plus du but souhaité.

Dans un premier temps, afin d'envoyer déjà A sur A', on utilise la translation t de vecteur $\overrightarrow{AA'}$:

$$\begin{array}{rccc} t & : & A & \longmapsto & A' \\ & & B & \longmapsto & B''. \end{array}$$

On utilise ensuite la rotation ρ de centre A' et d'angle $\widehat{B''A'B'}$:

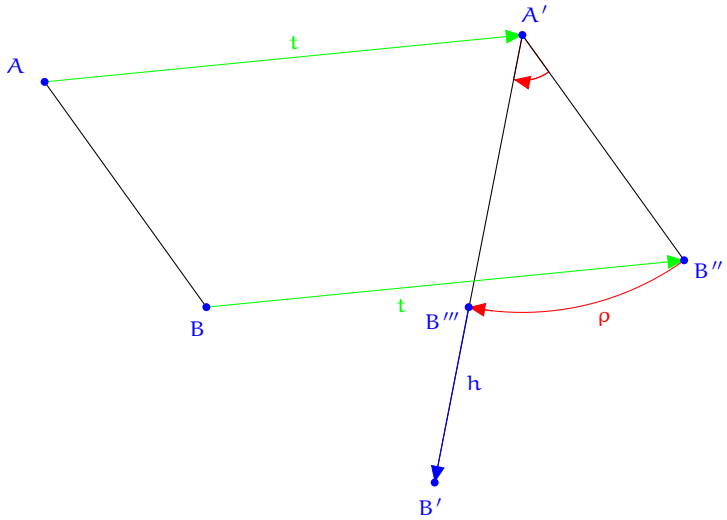
$$\begin{array}{rccc} \rho & : & A' & \longmapsto & A' \\ & & B'' & \longmapsto & B'''. \end{array}$$

Comme par construction $B''' \in (A'B')$, on peut finalement utiliser l'homothétie h de centre A' et de rapport $A'B'/A'B'''$:

$$\begin{array}{rccc} h & : & A' & \longmapsto & A' \\ & & B''' & \longmapsto & B'. \end{array}$$

□

Finalement, $S = h \circ \rho \circ t$ convient par construction.



Définition 3.36. On appelle centre d'une similarité un point fixe de cette similarité.

Exemple 3.37. Une translation de vecteur non nul n'a aucun centre, une rotation ou une homothétie en a un et la transformation identité admet tous les points du plan comme centre.

Remarque 3.38. L'unicité du théorème précédent appliquée à l'identité montre que, hormis l'identité, toute similarité a au plus un point fixe.

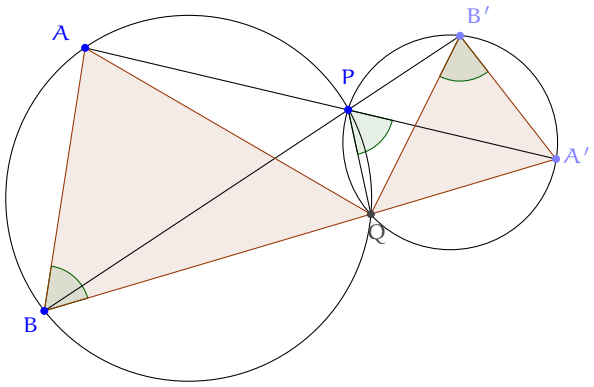
Le théorème suivant, essentiel, montre que l'on connaît bien le centre d'une similitude :

Théorème 3.39. Soit A, B, A' et B' supposés en position générale (un couple ne peut être obtenu à partir de l'autre par translation ou homothétie). Soit P le point d'intersection de (AA') et (BB'). Soit $\mathcal{C}_1$ et $\mathcal{C}_2$ les cercles circonscrits à PAB et $PA'B'$ et Q leur deuxième point d'intersection.

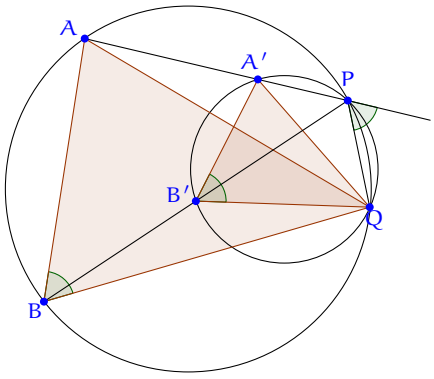
Alors, Q est le centre de la similitude envoyant A et B sur A' et B'.

Démonstration. Soit S l'unique similitude envoyant A et B sur A' et B'. On cherche à montrer que S envoie Q sur lui-même. D'après la démonstration de l'unicité de cette similitude, il suffit de vérifier que ABQ et $A'B'Q$ sont directement semblables. On procède par chasse aux angles. Il suffit de montrer que $\widehat{ABQ} = \widehat{A'B'Q}$, l'égalité $\widehat{BAQ} = \widehat{B'A'Q}$ se montrant de manière similaire.

$\widehat{ABQ} = 180° - \widehat{APQ} = \widehat{A'PQ} = \widehat{A'B'Q}$. □



Remarque 3.40. Bien sûr, il faudrait écrire cette démonstration en termes d'angles orientés. Ce que le lecteur pointilleux est invité à faire. Il est d'ailleurs important de se familiariser avec les deux configurations :



On remarque de plus en utilisant les triangles semblables de la démonstration précédente que cette similarité peut facilement être vue comme la composée d'une rotation (d'angle $\widehat{AQA'}$) et d'une homothétie (de rapport QA'/QA) de centre Q.

Définition 3.41. Une similitude directe de centre Q est la composée d'une rotation de centre Q et d'une homothétie de centre Q. Elle est caractérisée par son angle de rotation et son facteur de dilatation.

On a donc le théorème important suivant :

Théorème 3.42. Toute similarité est soit une translation soit une similitude directe.

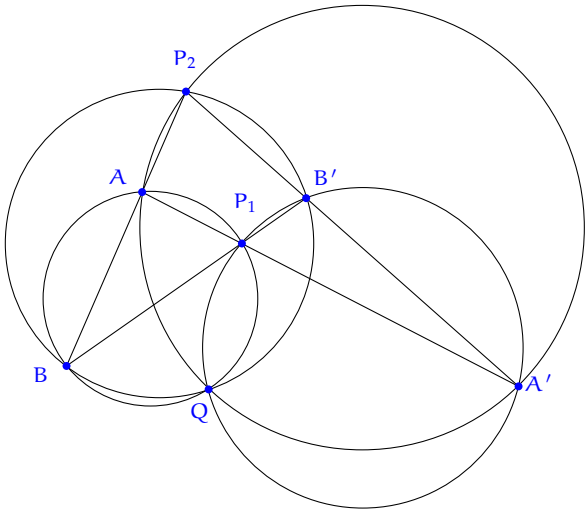
De plus, on voit toujours dans la même figure grâce aux mêmes triangles semblables que la similitude directe de centre Q, d'angle $\widehat{AQB} = \widehat{A'QB'}$ et de rapport de dilatation $QB/QA = QB'/QA'$ envoie A sur B et A′ sur B′. En laissant au lecteur le cas particulier des homothéties, on obtient le théorème important suivant :

Théorème 3.43. Si une similitude directe envoie A sur A′ et B sur B′, alors la similitude envoyant A sur B et A′ sur B′ a même centre.

En appliquant le théorème 3.39 aux deux similitudes précédentes, on obtient le résultat bien connu suivant, qui (pour l'intersection des cercles) se démontre également par chasse aux angles (exercice !) :

Théorème 3.44. Soit A, B, A′ et B′ en position générale. Soit $P_1 = (AA') \cap (BB')$ et $P_2 = (AB) \cap (A'B')$. Alors les cercles circonscrits à P_1AB, $P_1A'B'$, P_2AA' et P_2BB' sont concourants en un point Q, appelé point de Miquel du quadrilatère complet $AA'BB'$.

Il est le centre de la similitude directe envoyant A sur A′ et B sur B′ ainsi que de celle envoyant A sur B et A′ sur B′.



Remarque 3.45. On considérera essentiellement ce point comme centre des similitudes directes précédentes. Mais il est également d'une importance primordiale en géométrie projective unidimensionnelle complexe en tant que centre de l'involution échangeant les 6 sommets du quadrilatère complet (pour comprendre la phrase précédente ... allez au club de mathématiques discrètes de Lyon !).

Remarque 3.46. Il peut souvent être intéressant de regarder les similitudes d'un point de vue complexe : c'est en fait juste les fonctions affines. Voir notamment la première question de l'exercice 2 du test.

- Exercices -

Dans tous les exercices, les points sont ou ne sont pas supposés en position générale (à la discrétion du lecteur pointilleux !). Face à un exercice où les points ne sont pas en position générale mais où les techniques de ce cours semblent prometteuses, une bonne stratégie est de dire que, par un argument de continuité (en considérant les points de l'exercice comme des fonctions continues quand écrits en analytique), on peut les supposer en position générale.

Exercice 1 Soit $ABCD$ un quadrilatère, E et F sur $[AD]$ et $[BC]$ respectivement tels que $\frac{AE}{ED} = \frac{BF}{FC}$. Soit $S = (EF) \cap (AB)$ et $T = (EF) \cap (CD)$.

Montrer que les cercles circonscrits aux triangles SAE, SBF, TCF et TDE sont concourants.

Exercice 2 Soit $ABCD$ un quadrilatère avec $AD = BC$ et P l'intersection de ses diagonales. Soit F et E des points variables sur les segments $[AD]$ et $[BC]$ respectivement de manière à avoir $BE = DF$. On pose R et Q les points d'intersections de (EF) avec (AC) et (BD) respectivement.

Montrer que le cercle circonscrit à PQR a un deuxième point fixe quand E et F varient.

Exercice 3 Soit ABC un triangle inscrit dans un cercle Γ, P un point variable sur le petit arc AB. Soit I et J les centres des cercles inscrits des triangles ACP et BCP respectivement. On considère P le point d'intersection de Γ et du cercle circonscrit au triangle PIJ.

Montrer que Q reste fixe quand P varie.

Exercice 4 Soit Γ_1 et Γ_2 deux cercles s'intersectant en P et Q. Soit A_1 et B_1 deux points variables sur Γ_1 et A_2 et B_2 les deuxièmes points d'intersection de Γ_2 avec (A_1P) et (B_1P) respectivement. Soit $C = (A_1B_1) \cap (A_2B_2)$.

Montrer que le centre O du cercle circonscrit au triangle CA_1A_2 reste sur un cercle fixe quand A_1 et A_2 varient.

L'exercice suivant est important per se et souvent utilisé (il faut par contre penser à le redémontrer ... ou citer ce poly !).

Exercice 5 Soit $ABCD$ un quadrilatère convexe inscrit dans un cercle de centre O, P le point d'intersection des diagonales et Q le deuxième point d'intersection des cercles circonscrits aux triangles APD et BPC.

Montrer que $\widehat{OQP} = 90°$.

Exercice 6 Soit ABC un triangle, E et D des points sur les côtés $[AB]$ et $[AC]$ de manière à avoir $BE = CD$. Soit P l'intersection des diagonales du quadrilatère $BEDC$ et Q le deuxième point d'intersection des cercles circonscrits à EPB et DPC. Soit K et L les milieux respectifs de $[BE]$ et $[CD]$ et R le point d'intersection de la perpendiculaire à (QK) passant par K et de la perpendiculaire à (QL) passant par L.

Montrer que :

a) Q est sur la bissectrice de l'angle $\widehat{BAC}$.
b) R est sur le cercle circonscrit au triangle ABC.

Exercice 7 Soit ABC un triangle et Γ son cercle circonscrit. On considère trois points A_1, B_1 et C_1 sur les côtés $[BC]$, $[CA]$ et $[AB]$ respectivement. On note A_3, B_3 et C_3 les symétriques de A_1, B_1 et C_1 par rapport aux milieux de leurs côtés respectifs. On note A_2, B_2 et C_2 les deuxièmes points d'intersection de Γ avec les cercles circonscrits à AB_1C_1, BC_1A_1 et CA_1B_1 respectivement.

Montrer que les triangles $A_2B_2C_2$ et $A_3B_3C_3$ sont semblables.

On peut également trouver un type d'exercice légèrement différent à propos du point de Miquel et des similitudes : une figure ou apparaît de manière évidente une similitude directe particulière et son centre. Le théorème 3.44 permet alors de trouver des points cocycliques.

Exercice 8 Soit $ABCDE$ un pentagone convexe vérifiant les relations $\widehat{BAC} = \widehat{CAD} = \widehat{DAE}$ et $\widehat{CBA} = \widehat{DCA} = \widehat{EDA}$. Soit $P = (BD) \cap (CE)$.

Montrer que la droite (AP) coupe le segment $[CD]$ en son milieu.

Exercice 9 Soit $ABCDEF$ un hexagone inscriptible vérifiant $AB = CD = EF$. Soit $Z = (AC) \cap (BD)$, $X = (CE) \cap (DF)$ et $Y = (EA) \cap (FB)$.

Montrer que XYZ et BDF sont semblables.

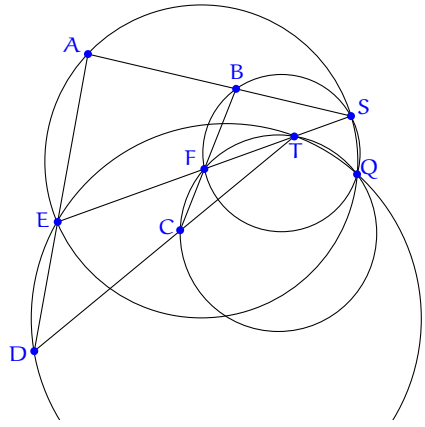
Enfin, comme pour les autres transformations (translation, homothéties, rotations...), il est intéressant de considérer ce que donne la composition de similitudes directes. Afin d'inviter le lecteur curieux à explorer ce champ de possibilités, je conclus sur un exercice dans cette direction.

Exercice 10 Soit Γ_1, Γ_2 et Γ_3 trois cercles avec $A; B = \Gamma_1 \cap \Gamma_2$, $C; D = \Gamma_2 \cap \Gamma_3$ et $E; F = \Gamma_3 \cap \Gamma_1$. On considère P_1 sur Γ_1 et on note P_2 le deuxième point d'intersection de (P_1A) et Γ_2, P_3 le deuxième d'intersection de (P_3C) et Γ_3, P_4 le deuxième point d'intersection de (P_3E) et Γ_1, P_5 le deuxième point d'intersection de (P_4B) et Γ_2, P_6 le deuxième point d'intersection de (P_5D) et Γ_3 et enfin P_7 le deuxième point d'intersection de (P_6F) et Γ_1.

Montrer que $P_7 = P_1$.

- Solutions -

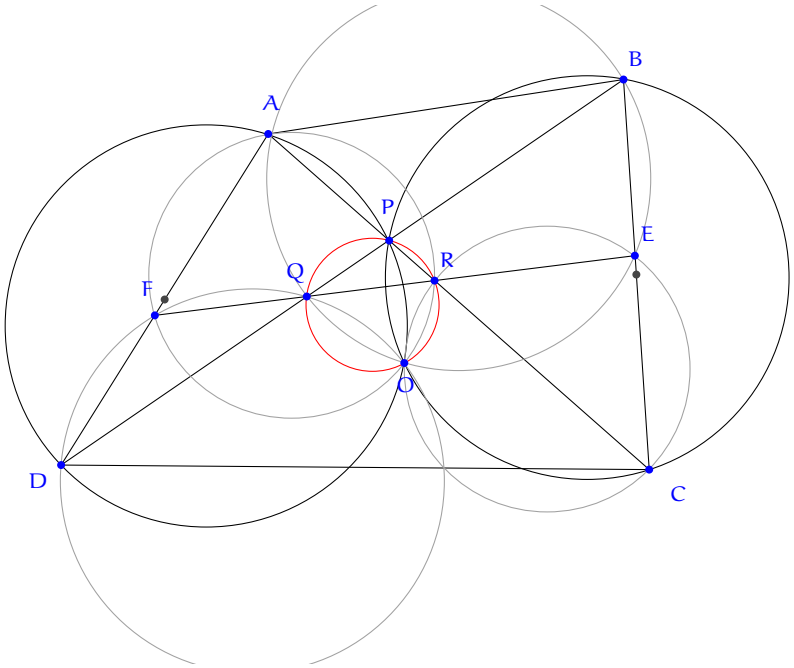
Solution de l'exercice 1



D'après l'égalité sur les rapports de longueur, la similitude directe envoyant A sur B et D sur C envoie également E sur F. En utilisant le théorème 3.44 pour les couples de points

$(E, D) \mapsto (F, C)$, on obtient que son centre est sur les cercles circonscrits à TCF et TDE. En l'utilisant sur les couples de points $(A, E) \mapsto (B, F)$, ce centre est également sur les cercles circonscrits à SAE et SBF. D'où la conclusion.

Solution de l'exercice 2

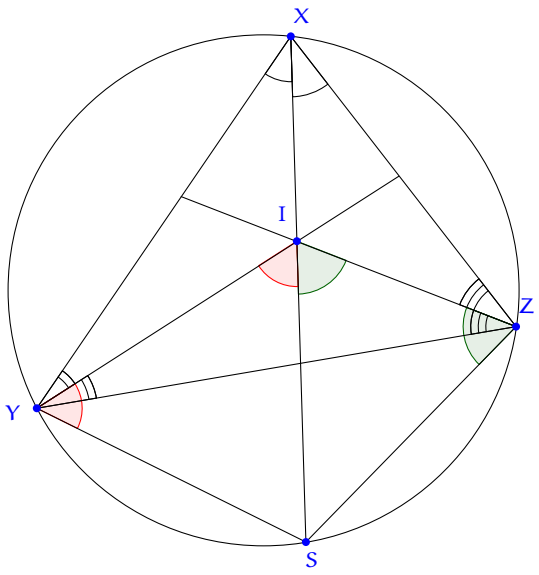


Il existe clairement en utilisant les égalités de longueur une similitude envoyant les points A, F et D sur les points C, E et B respectivement.

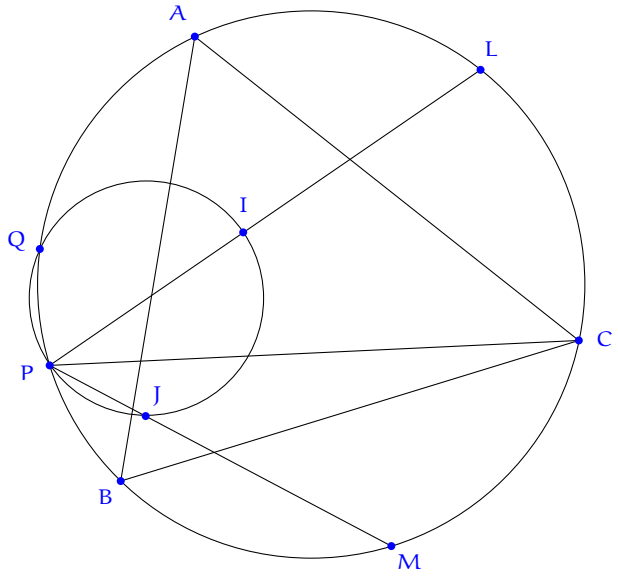
Il est naturel d'introduire son centre O et quelques dessins peuvent nous convaincre que c'est vraisemblablement le point recherché. En utilisant successivement le théorème principal pour les couples $(A, F) \mapsto (C, E)$, $(F, D) \mapsto (E, B)$ et $(D, A) \mapsto (B, C)$, on sait que O est sur le cercle circonscrit aux triangles ARF, ERC, FQD, BQE, APD et BPC. En particulier (en utilisant les deux derniers triangles), il est fixe. Il est donc suffisant (et probablement raisonnablement aisé au vu de tous les autres cercles...) de démontrer que O, P Q et R sont cocycliques.

Or, le théorème de Miquel appliqué au quadrilatère AFPQ prouve qu'il suffit de démontrer que O est sur le cercle circonscrit à ARF, DPA et DFQ. D'où la conclusion.

Solution de l'exercice 3 On rappelle le théorème du pôle Sud, visiblement pertinent dans cet exercice et démontrable grâce à une chasse aux angles élementaire (exercice !).



Si XYZ est un triangle inscrit dans un cercle $\mathcal{C}$, I son centre du cercle inscrit et S le deuxième point d'intersection de (XI) avec $\mathcal{C}$. Alors, S est le milieu de l'arc YZ et, plus précisément, $SY = SI = SZ$.

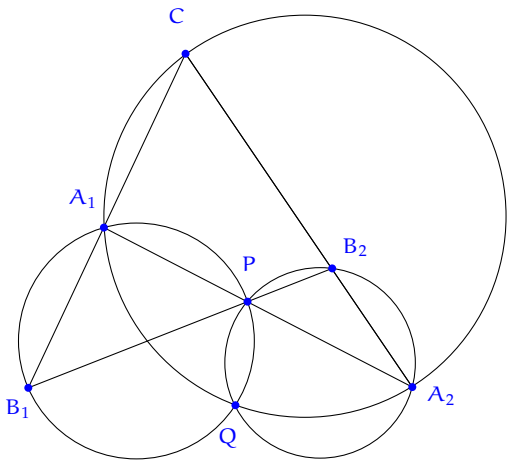


On est dans la situation classique avec deux cercles qui s'intersectent, on connaît bien un des points d'intersection et c'est l'autre qui nous intésse. On cherche donc à compléter le quadrilatère. De manière naturelle, on introduit donc les points fixes L et M, milieux respectifs des petits arcs AC et BC. D'après le théorème du pôle Sud, P, I et L ainsi que P, J et M sont alignés.

D'après le théorème 3.44, Q est le centre de la similitude S envoyant I sur J et L sur M. (Comme toujours se pose la question de quelle similitude choisir : pourquoi pas celle envoyant I sur L et J sur M ? Et comme souvent la réponse sera qu'on connaît mieux la première

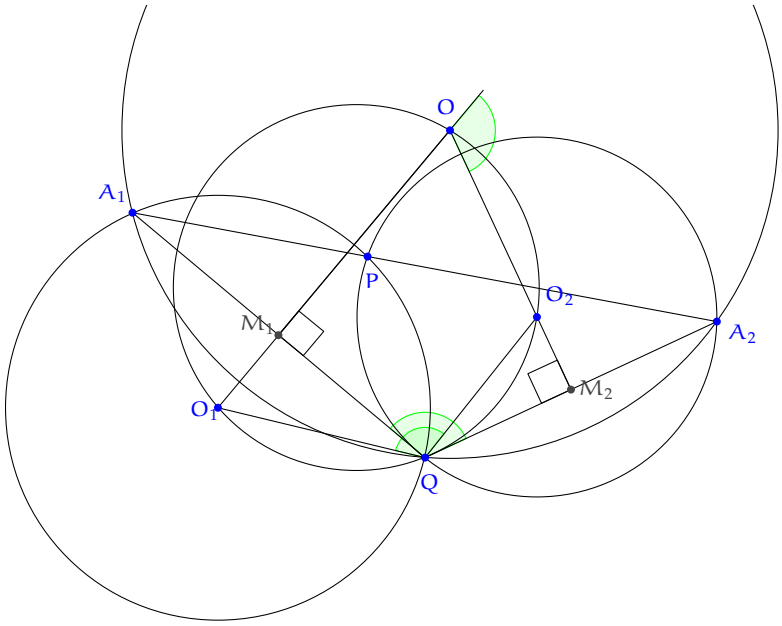
similitude parce que l'on maîtrise bien les longueurs impliquées.) Cette similitude envoyant le point fixe L sur le point fixe M, pour prouver qu'elle est fixe (et donc Q également), il suffit de montrer que son angle de rotation et son rapport de dilatation sont fixes (un petit dessin convaincra le lecteur sceptique...). Or, l'angle vaut $\widehat{LQM}$ qui est fixe d'après le théorème de l'angle inscrit et le rapport de dilatation vaut JM/IL qui vaut CM/CL d'après le théorème du pôle Sud, d'où la conclusion.

Solution de l'exercice 4



On voit qu'on est naturellement dans une situation du type théorème de Miquel dans le quadrilatère $A_1B_1A_2B_2$. En particulier, le cercle circonscrit à CA_1A_2 passe par Q.

Cette remarque est positive pour de nombreuses raisons : on se rend compte que les points B_1 et B_2 sont inutiles (O peut être défini comme le centre du cercle circonscrit à A_1QA_2), ce qui permet de simplifier la figure et de perdre un degré de liberté.



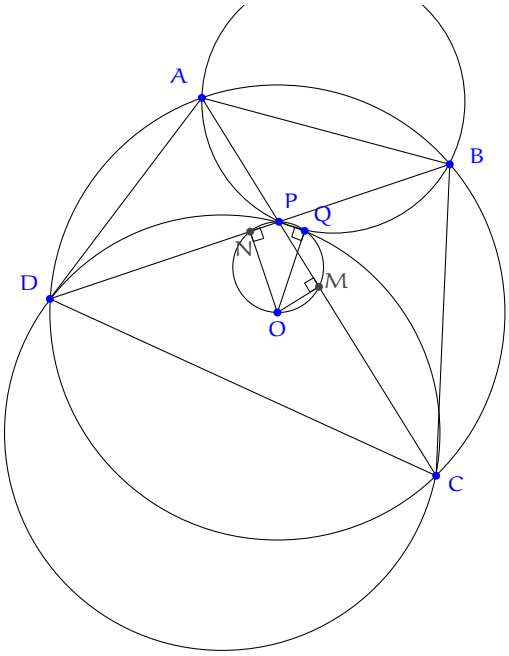
La question naturelle est maintenant : quel va être ce cercle que parcourra O ? Le plus simple est de considérer les cas limites : quand A_1 tend vers Q, A_2 et donc O également. Quand A_1 tend vers P, A_2 tend vers un point de Γ_2 et O devient donc le centre O_2 du cercle Γ_2. De même, quand A_2 tend vers P, O tend vers le centre O_1 de Γ_1.

On cherche donc à montrer que O, O_1, O_2 et Q sont cocycliques. Il faut naturellement travailler avec des angles orientés, mais on se passera (exercice...).

Notons M_1 et M_2 les milieux respectifs de $[A_1Q]$ et $[A_2Q]$. En utilisant les angles droits dus aux médiatrices, M_1, O, M_2 et Q sont cocycliques, d'où $\widehat{O_1OO_2} = 180° - \widehat{A_1QA_2}$.

Or, la similitude de centre Q qui envoie A_1 sur A_2 envoie O_1 sur O_2 (d'après par exemple le théorème 3.44 appliqué à $(A_1, B_1) \mapsto (A_2, B_2)$). D'où $\widehat{A_1QA_2} = \widehat{O_1QO_2}$, ce dont on déduit $\widehat{O_1OO_2} = 180° - \widehat{O_1QO_2}$, et la conclusion par le théorème de l'angle inscrit.

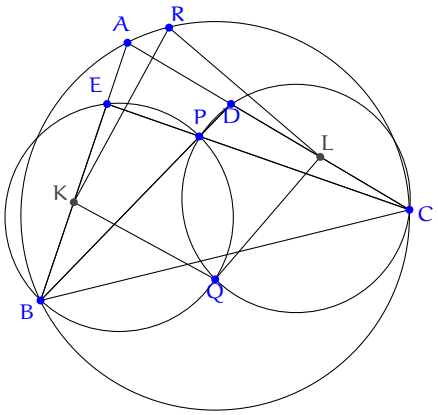
Solution de l'exercice 5 Il est naturel pour obtenir des angles droits de considérer les milieux M et N de [AC] et [BD].



On considère la similitude de centre Q qui envoie A sur B et C sur D. Elle envoie le segment [AC] sur le segment [BD] et en particulier M sur N. En utilisant le théorème 3.44 avec les couples $(A, M) \mapsto (B, N)$, M, N, P et Q sont cocycliques. Or, en utilisant l'angle droit des médiatrices, il et clair que M, N, P et O sont cocycliques.

D'où finalement M, N, P Q et O cocycliques et $\widehat{OQP} = 90°$ par le théorème de l'angle inscrit.

Solution de l'exercice 6

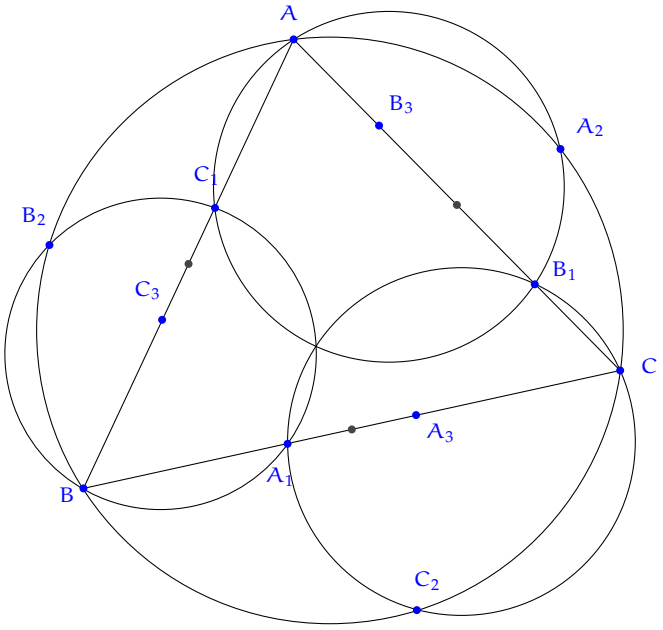


a) Q est le centre de la similitude ρ envoyant B sur D et E sur C. Comme BE = CD, son facteur de dilatation est 1 i.e. c'est une rotation. En particulier, en appelant Q_1 et Q_2 les projections de Q sur (AB) et (CD), comme ρ envoie Q_1 sur Q_2, $QQ_1 = QQ_2$, i.e. Q est sur la bissectrice (le lecteur attentif remarquera qu'il faut vérifier que c'est bien la bissectrice intérieure, ce qui se fait facilement par un argument de continuité en regardant le cas extrémal).

b) On remarque dans un premier temps que ρ envoie K sur L. En particulier, QK = QL, d'où également RK = RL. De plus, l'angle de la rotation est $\widehat{KQL}$ mais est également, la droite (EB) étant envoyé sur la droite (CD), l'angle entre les droites (BA) et (CA). En

particulier, A, K, Q et L sont cocycliques d'après le théorème de l'angle inscrit. Comme il est également clair que K, Q, L et R sont cocycliques, K, Q, L, A et R sont cocycliques. Le but de l'exercice est donc de montrer que R est le centre de la similitude envoyant K sur L et B sur C. Soit R′ le centre de cette similitude. R′ comme R est sur le cercle circonscrit à KQL. De plus, comme KB = LC, cette similitude est une rotation, d'où, comme pour R, R′K = R′L. Ainsi, R et R′ font partie des deux points d'intersection de la médiatrice de [KL] et du cercle circonscrit à KAL et un argument fumeux de positionnement (le lecteur pointilleux remarquera que c'est formalisable sans trop de difficulté) montre que c'est en fait les mêmes. D'où la conclusion.

Solution de l'exercice 7



On a visiblement de nombreuses similitudes naturelles dans cette figure et qui dit similitudes dit triangles semblables. Après étude de quelques figures, il semble que l'on puisse montrer que $C_2AB \sim CB_3A_3$.

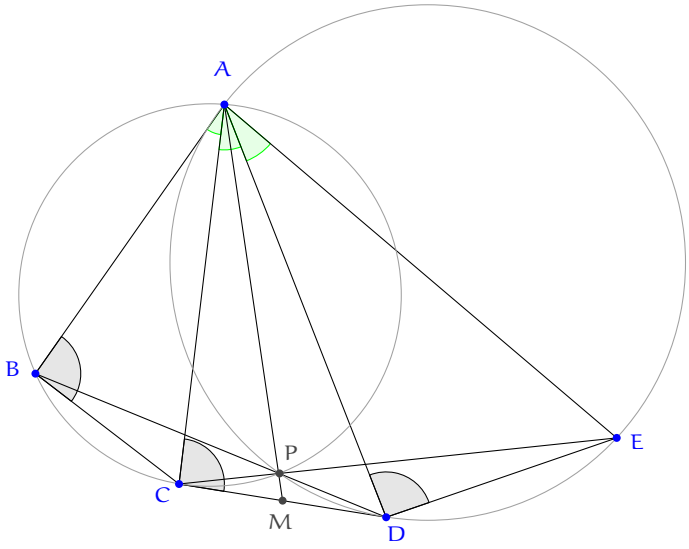
Effectivement, $\widehat{AC_2B} = \widehat{B_3CA_3}$ d'après le théorème de l'angle inscrit. Comme A_3 et B_3 sont plutôt défini en termes de longueur, on cherche également à démontrer que $CB_3/CA_3 = C_2A/C_2B$. Or, le rapport de dilatation de la similitude de centre C_2 envoyant B sur A et A_1 sur B_1 vaut selon la manière de le calculer C_2A/C_2B ou AB_1/BA_1 qui vaut exactement CB_3/CA_3. On a donc bien $C_2AB \sim CB_3A_3$. Cycliquement, on sait que $A_2BC \sim AC_3B_3$ et $B_2CA \sim BA_3C_3$.

On connaît maintenant très bien tous les angles. Philosophiquement, on sait donc qu'il suffit de faire une chasse aux angles. Effectivement :

$$\begin{aligned}\widehat{B_2A_2C_2} &= \widehat{B_2AC_2} = \widehat{BAC_2} + \widehat{B_2AC} - \widehat{BAC} \\ &= \widehat{A_3B_3C} + \widehat{BC_3A_3} - \widehat{BAC} = \widehat{B_3A_3C_3}.\end{aligned}$$

D'où la conclusion en raisonnant cycliquement.

Solution de l'exercice 8

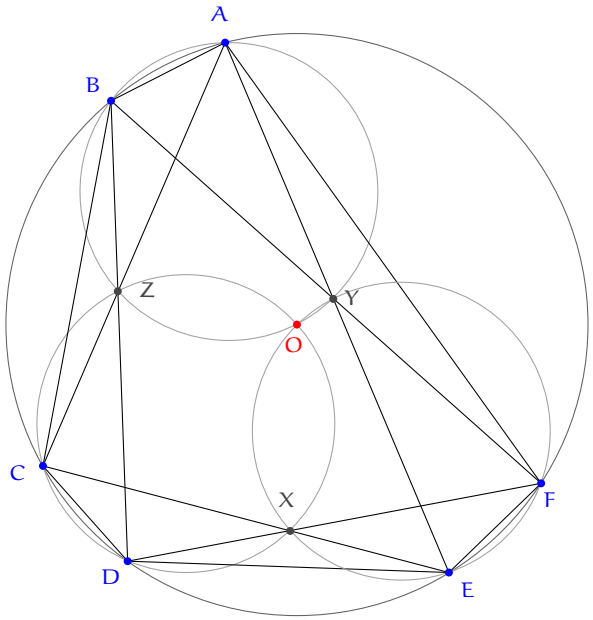


On se rend immédiatement compte qu'il existe une similitude de centre A qui envoie B sur C, C sur D puis D sur E.

Donc, d'après le théorème 3.44 appliqué au couple de point $(B, D) \mapsto (C, E)$, A est sur le cercle circonscrit Γ_1 à PBC et Γ_2 à PDE. Ici, l'exercice commence à avoir bien la tête d'un exercice d'Igor, on essaye donc de montrer que Γ_1 est tangent à (CD). Or c'est vrai d'après la récriproque du théorème de l'angle inscrit comme $\widehat{BAC} = \widehat{DCA}$. De même, comme $\widehat{DEA} = 180° - \widehat{EAD} - \widehat{EDA} = 180° - \widehat{CAD} - \widehat{ACD} = \widehat{CDA}$, Γ_2 est également tangent à (CD).

Finalement, en notant $M = (AP) \cap (CD)$, M est sur l'axe radical de Γ_1 et Γ_2 et on peut donc écrire $MC^2 = \mathcal{P}_{\Gamma_1}(M) = \mathcal{P}_{\Gamma_2}(M) = MD^2$ et la conclusion.

Solution de l'exercice 9



On a clairement une rotation (donc une similitude) de centre le centre du cercle O qui

envoie A sur B, C sur D et E sur F.

En utilisant le théorème 3.44 sur le couple $(A, C) \mapsto (B, D)$, A, B, Z et O sont cocycliques. Or, de même, en l'utilisant sur le couple $(A, E) \mapsto (B, F)$, A, B, Y et O sont cocycliques.

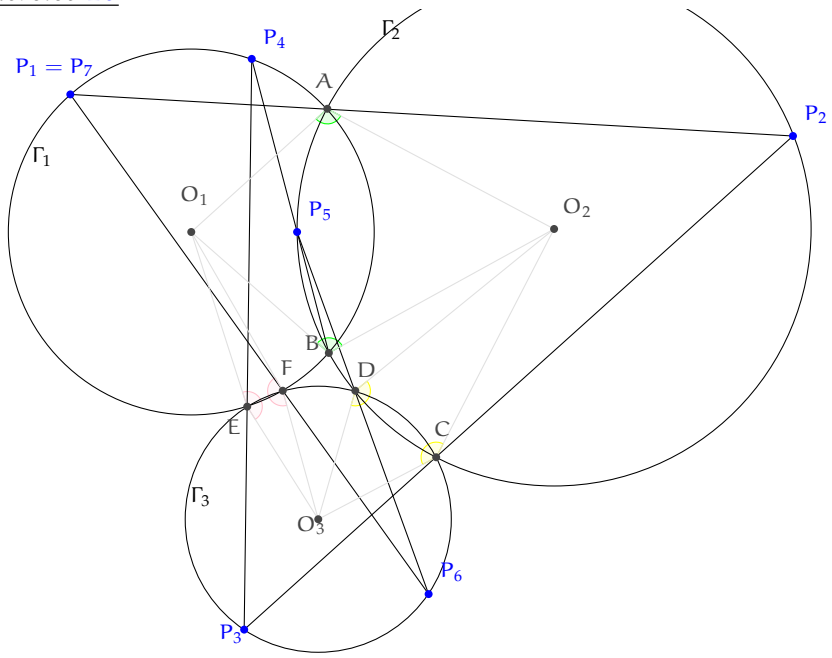
Ainsi, A, B, Z, O, Y sont cocycliques, et de la même manière également C, Z, O, X, D et E, X, O, Y, F.

Encore une fois, philosophiquement parlant, avec tant de cercles on connaît tous les angles, donc une simple chasse aux angles devrait suffire pour terminer. Effectivement :

$$\begin{aligned}\widehat{ZXY} &= \widehat{ZXO} + \widehat{OXY} \\ &= \widehat{ODZ} + \widehat{OFY} \\ &= \widehat{ODB} + \widehat{OFB} \\ &= \widehat{OBD} + \widehat{OBF} \\ &= \widehat{DBF}.\end{aligned}$$

On conclut cycliquement.

Solution de l'exercice 10



On considère ϕ_B la similitude de centre B qui envoie P_1 sur P_2 et Γ_1 sur Γ_2. De même, on considère ϕ_D la similitude de centre D qui envoie P_2 sur P_3 et Γ_2 sur Γ_3. on définit de manière similaire ϕ_F, ϕ_A, ϕ_C et ϕ_E.

On note $\Phi = \phi_E \circ \phi_C \circ \phi_1 \circ \phi_F \circ \phi_D \circ \phi_B$. On a alors $P_7 = \Phi(P_1)$. Or, l'angle de rotation de Φ vaut $(BO_1, BO_2) + (DO_2, DO_3) + (FO_3, FO_1) + (AO_1, AO_2) + (CO_2, CO_3) + (EO_3, EO_1) = 0$ en éliminant les termes correspondants (voir figure). De même, le facteur de dilatation de Φ vaut $r_2/r_1 \cdot r_3/r_2 \cdot r_1/r_3 \cdot r_2/r_1 \cdot r_3/r_2 \cdot r_1/r_3 = 1$.

Φ est donc l'identité, d'où la conclusion.

3 TD de géométrie : barycentres

- Barycentres -

Soient ABC un triangle et (α, β, γ) un triplet de réels tels que $\alpha + \beta + \gamma \neq 0$.

Définition 3.47. Le barycentre des points pondérés (A, α), (B, β) et (C, γ) est l'unique point G tel que

$$\alpha\overrightarrow{GA} + \beta\overrightarrow{GB} + \gamma\overrightarrow{GC} = \overrightarrow{0}.$$

Pour vous représenter physiquement le barycentre, imaginez que le triangle ABC est un mobile et que l'on a accroché un poids de α grammes au point A, un poids de β grammes en B et un de γ grammes en C. Le point G est le point par lequel il faut tenir le mobile pour que tout soit en équilibre.

Pour construire ce barycentre, et pour vérifier qu'il est bien unique, on utilise la condition suivante :

Proposition 3.48. Soit O un point quelconque du plan, alors

$$\overrightarrow{OG} = \frac{\alpha}{\alpha+\beta+\gamma}\overrightarrow{OA} + \frac{\beta}{\alpha+\beta+\gamma}\overrightarrow{OB} + \frac{\gamma}{\alpha+\beta+\gamma}\overrightarrow{OC}.$$

Pour démontrer cette proposition, il suffit de remplacer $\overrightarrow{OA}$ par $\overrightarrow{OG} + \overrightarrow{GA}$, pareil pour les deux autres, et d'utiliser la définition.

Faisons une pause un instant pour regarder le barycentre de 2 points : soit G le barycentre des points (A, α) et (B, β). En utilisant la proposition avec A à la place de O, on trouve

$$\overrightarrow{AG} = \frac{\beta}{\alpha+\beta}\overrightarrow{AB}.$$

Le point G est donc le point de la droite (AB) tel que $AG = \frac{\beta}{\alpha+\beta}AB$. En particulier, $\frac{AG}{GB} = \frac{\beta}{\alpha}$. Je souligne cette identité puisqu'elle sera très importante par la suite.

- Coordonnées barycentriques -

Soit ABC un triangle fixé.

Définition 3.49. Pour tout point G du plan on peut associer un triplet de réels (α, β, γ) tel que G soit le barycentre de (A, α), (B, β) et (C, γ). On appelle ce triplet les coordonnées barycentriques de G, et il est unique à un coefficient multiplicatif près.

Pour montrer cette propriété, on utilise l'existence et l'unicité de coordonnées du point G dans le repère $(A, \overrightarrow{AB}, \overrightarrow{AC})$, et on utilise la première propriété des barycentres.

Comme on peut multiplier les triplets par un coefficient multiplicatif quelconque, on met à part triplet particulier qui vérifie $\alpha + \beta + \gamma = 1$: on l'appelle les coordonées barycentriques homogènes de G.

Discutons un peu un des avantages des coordonnées barycentriques : dans ce système, on a $A : (1, 0, 0)$, $B : (0, 1, 0)$ et $C : (0, 0, 1)$, ce qui est très facile à retenir.

De plus les droites ont des équations d'une forme facile à retenir : un point G de coordonnées barycentriques (α, β, γ) apparient à une droite d ssi

$$u\alpha + v\beta + w\gamma = 0,$$

où (u, v, w) est un triplet de réels particulier à d, unique à coefficient multiplicatif près. Pour la démonstration, allez voir l'exercice 3 plus bas.

- Associativité des barycentres -

Une propriété très pratique des barycentres est la suivante :

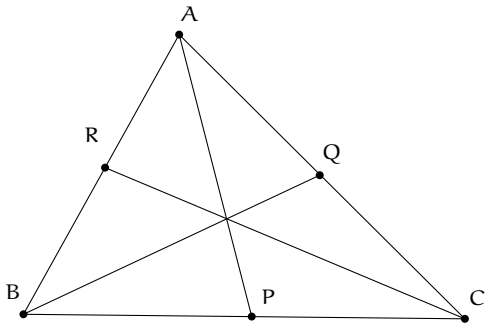
Proposition 3.50 (associativité des barycentres)**.** Soit $P : (\alpha_P, \beta_P, \gamma_P)$ et $Q : (\alpha_Q, \beta_Q, \gamma_Q)$. Soit G le barycentre de $(P, \lambda), (Q, \mu)$, alors G est le barycentre de

$$\left(A, \lambda\frac{\alpha_P}{\alpha_P+\beta_P+\gamma_P} + \mu\frac{\alpha_Q}{\alpha_Q+\beta_Q+\gamma_Q}\right),$$
$$\left(B, \lambda\frac{\beta_P}{\alpha_P+\beta_P+\gamma_P} + \mu\frac{\beta_Q}{\alpha_Q+\beta_Q+\gamma_Q}\right),$$
$$\left(C, \lambda\frac{\gamma_P}{\alpha_P+\beta_P+\gamma_P} + \mu\frac{\gamma_Q}{\alpha_Q+\beta_Q+\gamma_Q}\right).$$

Cette propriété est un peu dure à utiliser sous cette forme, mais permet de construire plus facilement le barycentre de 3 points. Soit $G : (\alpha, \beta, \gamma)$. On introduit M le barycentre de (B, β) et (C, γ), alors G est le barycentre de (A, α) et $(M, \beta + \gamma)$. Pour le construire, on place d'abord le point M sur (BC) tel que $BM = \frac{\gamma}{\beta+\gamma}BC$, puis on place G sur AM tel que $AG = \frac{\beta+\gamma}{\alpha+\beta+\gamma}AM$.

Maintenant si on fait le raisonnement à l'envers : soit $G : (\alpha, \beta, \gamma)$ et soit M le point d'intersection de AG avec BC. Alors M est le barycentre de (B, β) et (C, γ), et $\frac{BM}{MC} = \frac{\gamma}{\beta}$.

- Théorème de Ceva -



Théorème 3.51 (Ceva)**.** Soit ABC un triangle et P, Q, et R des points de BC, AC et AB respectivement. Les droites AP, BQ et CR sont concourantes ssi

$$\frac{BP}{PC}\cdot\frac{CQ}{QA}\cdot\frac{AR}{RB} = 1.$$

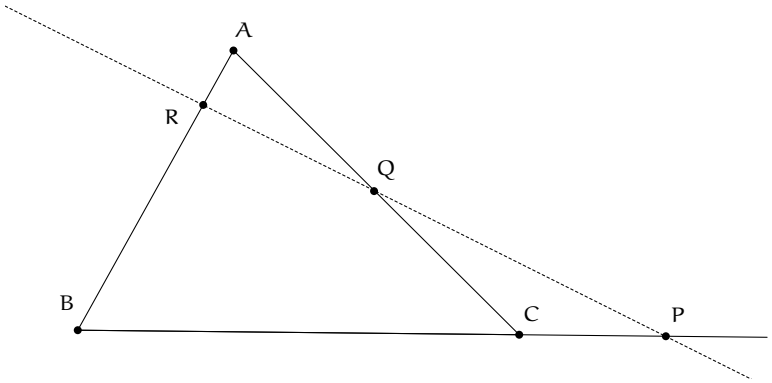
NB. Ici, et dans toute cette partie, les longueurs sont algébriques.

La démonstration utilise la section précédente. Supposons que les trois droites se coupent au point G de coordonnées barycentriques (α, β, γ). Comme P est le point d'intersection de AG avec BC, cela signifie que P est le barycentre de (B, β) et (C, γ), et $\frac{BP}{PC} = \frac{\gamma}{\beta}$. De même $\frac{CQ}{QA} = \frac{\alpha}{\gamma}$ et $\frac{AR}{RB} = \frac{\beta}{\alpha}$, et

$$\frac{BP}{PC}\cdot\frac{CQ}{QA}\cdot\frac{AR}{RB} = \frac{\gamma}{\beta}\cdot\frac{\alpha}{\gamma}\cdot\frac{\beta}{\alpha} = 1.$$

Pour montrer la réciproque, supposons que le produit est égal à 1, et notons G le point d'intersection de AP et BQ, et (α, β, γ) ses coordonnées. On en déduit que $\frac{BP}{PC} = \frac{\gamma}{\beta}$ et $\frac{CQ}{QA} = \frac{\alpha}{\gamma}$. Ensuite, comme $\frac{BP}{PC} \cdot \frac{CQ}{QA} \cdot \frac{AR}{RB} = 1$, $\frac{AR}{RB} = \frac{\beta}{\alpha}$, et R est bien le point d'intersection de CG avec AB.

Il est aussi possible de montrer le théorème de Ménélaüs grâce aux coordonnées barycentriques :



Théorème 3.52 (Ménélaüs)**.** Soit ABC un triangle et P, Q, et R des points de BC, AC et AB respectivement. Les P, Q et R sont alignés ssi

$$\frac{BP}{PC} \cdot \frac{CQ}{QA} \cdot \frac{AR}{RB} = -1.$$

Remarque 3.53. Pour déterminer le signe de $\frac{BP}{PC}$, on dit que si BP et PC sont de sens différents (ie si P est à l'extérieur du segment [BC]), alors le quotient est négatif.

La démonstration du théorème fait l'objet de l'exercice 6.

- Exercices -

Dans tous les exercices, ABC est un triangle, $BC = a$, $AC = b$ et $AB = c$. J'utiliserai la notation [ABC] pour l'aire du triangle ABC.

Exercice 1 Utilisez Ceva pour montrer que les médianes sont concourantes et exprimer les coordonnées barycentriques de G. Idem pour les bissectrices et I et les hauteurs et H.

Exercice 2 (Point de Gergonne) Soient P, Q, R les points de contact du cercle inscrit avec les trois côtés. Montrer que AP, BQ et CR sont concourantes. Trouver les coordonnées barycentriques du point d'intersection.

Soit P′ le point de contact du cercle exinscrit en A avec BC, Q′ le point de contact du cercle exinscrit en B avec AC et R′ le point de contact du cercle exinscrit en C avec AB etc. Montrer que AP′, BQ′ et CR′ qont concourantes. Trouver les coordonnées barycentriques du point d'intersection.

Exercice 3 En coordonnées barycentriques, calculer l'équation d'une droite passant par A, d'une droite quelconque.

($\star$) Calculer l'équation d'un cercle, puis celle du cercle circonscrit à ABC en particulier.

Exercice 4 Montrez Ceva trigonométrique : Soit ABC un triangle et P, Q, et R des points de BC, AC et AB respectivement. Les droites AP, BQ et CR sont concourantes ssi

$$\frac{\sin(\widehat{BAP})}{\sin(\widehat{PAC})} \cdot \frac{\sin(\widehat{CBQ})}{\sin(\widehat{QBA})} \cdot \frac{\sin(\widehat{ACR})}{\sin(\widehat{RCB})} = 1.$$

Exercice 5 Soit P un point à l'intérieur du triangle. Montrer que P a pour coordonnées barycentriques $([BPC], [PCA], [PAB])$.

Exercice 6 Utilisez les coordonnées barycentriques pour montrer le théorème de Ménélaüs : Soit ABC un triangle et P, Q et R des points de BC, AC et AB respectivement. Les points P, Q, R sont alignés ssi

$$\frac{BP}{PC} \cdot \frac{CQ}{QA} \cdot \frac{AR}{RB} = -1$$

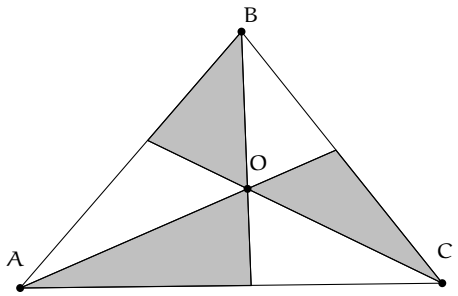
Exercice 7 Soit d une droite passant par A. La conjuguée isogonale de d est la symétrique de d par rapport à la bissectrice de $\widehat{A}$. Montrer que trois droites passant par A, B et C respectivement sont concourantes ssi leurs conjuguées isogonales (par rapport à A, B, C respectivement) sont concourantes. Si le point d'intersection des isogonales a pour coordonnées barycentriques (α, β, γ), quelles sont les coordonnées barycentriques du point d'intersection des trois droites initiales ?

Exercice 8 Soit $ABCDEF$ un hexagone régulier, M un point de la diagonale AC et N un point de CE tels que

$$\frac{AM}{AC} = \frac{CN}{CE} = r.$$

Que dire de r si B, M et N sont alignés ?

Exercice 9 Soit ABC un triangle et O un point à l'intérieur. On trace les droites AO, BO, CO qui coupent le triangle en 6 :



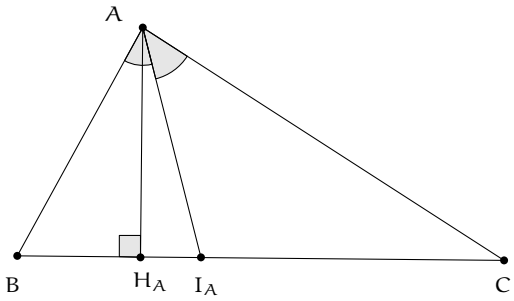
Montrer que l'aire noire est égale à l'aire blanche ssi O est sur une médiane.

Exercice 10 Soit ABC un triangle et P, Q, R les pieds des bissectrices. Montrer que si B, P, Q, R sont cocycliques, alors

$$\frac{b}{a+c} = \frac{a}{b+c} + \frac{c}{a+b}.$$

- Solutions des exercices -

Solution de l'exercice 1 La démonstration pour G est facile et $G : (1,1,1)$. Occupons-nous de I :



Utilisons la loi des sinus dans le triangle BAI_A :

$$\frac{BI_A}{\sin(\widehat{BAI_A})} = \frac{AI_A}{\sin(\widehat{B})} \text{ donc } BI_A = AI_A \frac{\sin(\widehat{A}/2)}{\sin(\widehat{B})}.$$

De même :

$$I_AC = AI_A \frac{\sin(\widehat{A}/2)}{\sin(\widehat{C})}.$$

$$\frac{BI_A}{I_AC} = \frac{\sin(\widehat{C})}{\sin(\widehat{B})}.$$

$$\frac{BI_A}{I_AC} \cdot \frac{CI_B}{I_BA} \cdot \frac{AI_C}{I_CB} = \frac{\sin(\widehat{C})}{\sin(\widehat{B})} \cdot \frac{\sin(\widehat{A})}{\sin(\widehat{C})} \cdot \frac{\sin(\widehat{B})}{\sin(\widehat{A})} = 1.$$

Donc les trois bissectrices sont bien concourantes. Maintenant pour les coordonnées barycentriques. Par les propriétés du barycentre, si $I : (\alpha, \beta, \gamma)$, et que I_A est l'intersection de AI avec BC, alors I_A est le barycentre de (B, β) et (C, γ), et donc $\frac{BI_A}{I_AC} = \frac{\gamma}{\beta}$. Essayons de trouver des poids qui vérifient $\frac{\gamma}{\beta} = \frac{\sin(\widehat{C})}{\sin(\widehat{B})}$. Le triplet $(\sin(\widehat{A}), \sin(\widehat{B}), \sin(\widehat{C}))$ marche :

$$I : (\sin(\widehat{A}), \sin(\widehat{B}), \sin(\widehat{C})).$$

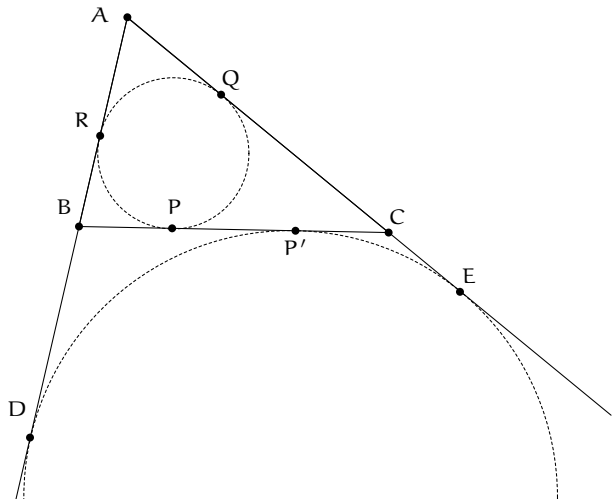
Par la loi des sinus, $\frac{a}{\sin(\widehat{A})} = \frac{b}{\sin(\widehat{B})} = \frac{c}{\sin(\widehat{C})}$, donc on peut aussi utiliser le triplet

$$I : (a, b, c).$$

L'intersection des hauteurs se fait de la même manière, j'en laisse l'exercice au lecteur. Les coordonnées barycentriques de H sont

$$H : (\tan(\widehat{A}), \tan(\widehat{B}), \tan(\widehat{C})).$$

Solution de l'exercice 2 Commençons par la figure :



Faisons le cercle inscrit en premier. Par les propriétés des bissectrices, $AQ = AR$ (si vous voulez vous en convaincre, regardez les triangles AIQ et AIR : ce sont deux triangles rectangles qui ont l'hypothénuse en commun et $IQ = IR$), et de même cycliquement. Notons $x = AQ = AR$, $y = BP = BR$ et $z = CP = CQ$.

$$\frac{BP}{PC} \cdot \frac{CQ}{QA} \cdot \frac{AR}{RB} = \frac{y}{z} \cdot \frac{z}{x} \cdot \frac{x}{y} = 1.$$

Comme dans l'exo précédent, on trouve que les coordonnées barycentriques du point d'intersection sont $\left(\frac{1}{x}, \frac{1}{y}, \frac{1}{z}\right)$. Essayons d'exprimer x, y et z de façon plus satisfaisante. On sait que $a = y + z$, $b = x + z$ et $c = x + y$. Il est facile d'en déduire les formules suivantes :

$$x = \frac{b + c - a}{2},\ y = \frac{a + c - b}{2},\ z = \frac{a + b - c}{2}.$$

Attaquons nous maintenant aux cercles exinscrits. Je note D et E les points de contact du cercle exinscrit en A avec AB et AC respectivement. Comme dans la partie précédente, $BD = BP'$ et $CP' = CE$ et $AD = AE$. On a les équations suivantes :

$$x + y + BP' = x + z + CP' \quad \text{et} \quad BP' + CP' = BC = y + z.$$

On en déduit facilement que $BP' = z$ et $CP' = y$. La fin de la preuve est facile, AP', BQ' et CR' sont concourantes, le point d'intersection a pour coordonnées barycentriques (x, y, z).

Solution de l'exercice 3 Prenons une droite d qui passe par A, et soit P l'intersection de cette droite avec BC. Soient ν et w des poids tels que P soit le barycentre de (B, ν) et (C, w). Un point de coordonnées barycentriques (α, β, γ) est sur la droite d ssi

$$\frac{\gamma}{\beta} = \frac{BP}{PC} = \frac{w}{\nu} \text{ ssi } \beta w - \gamma \nu = 0.$$

Pour une droite quelconque, prenons P et Q deux points de la droite de coordonnées barycentriques homogènes (x_1, y_1, z_1) et (x_2, y_2, z_2). Un point $M : (\alpha, \beta, \gamma)$ est sur la droite PQ ssi il existe deux réels λ et μ tels que M soit le barycentre de (P, λ) et (Q, μ).

$$M : (\lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2, \lambda z_1 + \mu z_2).$$

Je vais un peu tricher et utiliser des propriétés d'algèbre linéaire que vous verrez en prepa. L'équation précédente veut dire que le vecteur (α, β, γ) est combinaison linéaire des deux vecteurs (x_1, y_1, z_1) et (x_2, y_2, z_2), ce qui est équivalent à

$$\det \begin{pmatrix} x_1 & x_2 & \alpha \\ y_1 & y_2 & \beta \\ z_1 & z_2 & \gamma \end{pmatrix} = 0$$

ce qui revient à l'équation suivante :

$$(y_1z_2 - z_1y_2)\alpha + (z_1x_2 - x_1z_2)\beta + (x_1y_2 - y_1x_2)\gamma = 0.$$

Donc les droites en coordonnées barycentriques ont une équation du type :

$$u\alpha + v\beta + w\gamma = 0,$$

pour un triplet de réels (u, v, w) unique à un coefficient multiplicatif près.

En ce qui concerne les cercles, c'est un cauchemar. L'équation est de la forme

$$-a^2\beta\gamma - b^2\gamma\alpha - c^2\alpha\beta + (u\alpha + v\beta + w\gamma)(\alpha + \beta + \gamma) = 0,$$

pour un triplet de réels (u, v, w) unique.

Solution de l'exercice 4 Appliquons la loi des sinus dans les triangles BAP et PAC :

$$\frac{BP}{\sin(\widehat{BAP})} = \frac{AP}{\sin(\widehat{B})} \quad \text{et} \quad \frac{PC}{\sin(\widehat{PAC})} = \frac{AP}{\sin(\widehat{C})}.$$

$$\frac{BP}{PC} = \frac{\sin(\widehat{BAP})}{\sin(\widehat{PAC})}\frac{\sin(\widehat{C})}{\sin(\widehat{B})}.$$

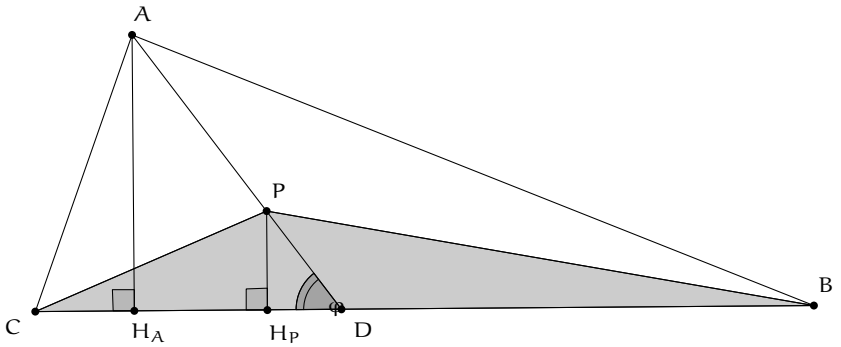
$$\frac{BP}{PC} \cdot \frac{CQ}{QA} \cdot \frac{AR}{RB} = \frac{\sin(\widehat{BAP})}{\sin(\widehat{PAC})} \cdot \frac{\sin(\widehat{CBQ})}{\sin(\widehat{QBA})} \cdot \frac{\sin(\widehat{ACR})}{\sin(\widehat{RCB})}.$$

Le théorème de Ceva classique est donc equivalent au théorème de Ceva trigonométrique.

Solution de l'exercice 5 Soit P un point de coordonnées barycentriques (α, β, γ). Je veux montrer que le triplet $([BPC], [PCA], [PAB])$ est aussi un jeu de coordonnées barycentriques de P, c'est-à-dire que les deux triplets sont proportionneles l'un à l'autre. Montrons que

$$\frac{\alpha}{\alpha + \beta + \gamma} = \frac{[BPC]}{[BPC] + [PCA] + [PAB]} = \frac{[BPC]}{[ABC]},$$

les deux autres équations se font de la mème manière.



On note D l'intersection de AP avec BC, et on note φ l'angle $\widehat{ADC}$. D'après les propriétés des barycentres, P est le barycentre de (A, α) et $(D, \beta + \gamma)$ et

$$\frac{PD}{AD} = \frac{\alpha}{\alpha + \beta + \gamma}.$$

Maintenant calculons les deux aires qui nous intéressent :

$$[PBC] = \frac{1}{2} BC \cdot PH_P = \frac{1}{2} BC \cdot PD \sin(\varphi) \quad \text{et} \quad [ABC] = \frac{1}{2} BC \cdot AD \sin(\varphi).$$

En faisant le quotient de ces deux égalités on trouve le résultat voulu.

$$P : ([BPC], [PCA], [PAB]).$$

Solution de l'exercice 6 Nous allons utiliser le résultat de l'exo 3 qui dit que les droites ont pour équation $u\alpha + v\beta + w\gamma = 0$. Faisons le premier sens : on suppose que les trois points sont alignés, et soit $u\alpha + v\beta + w\gamma = 0$ l'équation de cette droite. Soit $(\alpha_P, \beta_P, \gamma_P)$ un triplet de coordonnées barycentriques de P. Comme P est sur BC, $\alpha_P = 0$, et comme P est sur la droite qui passe par P, Q, R, $v\beta_P + w\gamma_P = 0$. Le point P est le barycentre de (B, β_P) et (C, γ_P), donc

$$\frac{BP}{PC} = \frac{\gamma_P}{\beta_P} = \frac{-v}{w}.$$

On trouve de même

$$\frac{CQ}{QA} = \frac{-w}{u} \quad \text{et} \quad \frac{AR}{RB} = \frac{-u}{v}.$$

$$\frac{BP}{PC} \cdot \frac{CQ}{QA} \cdot \frac{AR}{RB} = \frac{-v}{w} \cdot \frac{-w}{u} \cdot \frac{-u}{v} = -1.$$

Pour faire l'autre sens, on suppose $\frac{BP}{PC} \cdot \frac{CQ}{QA} \cdot \frac{AR}{RB} = -1$. Soit d la droite PQ d'équation $u\alpha + v\beta + w\gamma = 0$. Comme P et Q sont sur la droite, on peut utiliser le même raisonnement qu'avant pour montrer

$$\frac{BP}{PC} = \frac{-v}{w} \quad \text{et} \quad \frac{CQ}{QA} = \frac{-w}{u}.$$

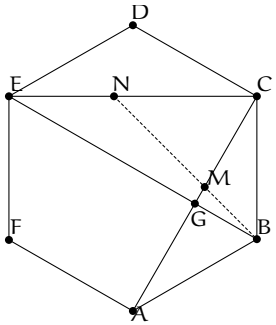
On utilise ensuite l'égalité $\frac{BP}{PC} \cdot \frac{CQ}{QA} \cdot \frac{AR}{RB} = -1$ pour montrer que

$$\frac{AR}{RB} = \frac{-u}{v},$$

et il est facile de vérifier ensuite que R est bien sur la droite.

Solution de l'exercice 7 La démonstration est quasi immédiate avec Ceva trigonométrique. Si un point a pour coordonnées barycentriques (α, β, γ), alors son conjugué isogonal a pour coordonnées $\left(\frac{a^2}{\alpha}, \frac{b^2}{\beta}, \frac{c^2}{\gamma}\right)$.

Solution de l'exercice 8 Commençons par faire la figure, en rajoutant G le point d'intersection de AC et BE (par les symétries de l'hexagone, G est le milieu de AC) :



Considérons le triangle CEG : les points M, N et B sont sur GC, CE et EG respectivement, et sont alignés, nous pouvons donc utiliser Ménélaüs :

$$\frac{GM}{MC}\cdot\frac{CN}{NE}\cdot\frac{EB}{BG}=-1.$$

Calculons les trois quotients :

$$GM = AM - AG = rAC - \frac{1}{2}AC \quad \text{donc} \quad \frac{GM}{MC} = \frac{(r-1/2)AC}{(1-r)AC}) = \frac{2r-1}{2-2r}.$$

$$\frac{CN}{NE} = \frac{rCE}{CE - rCE} = \frac{r}{1-r}.$$

Pour le dernier quotient on va calculer EB et BG en utilisant les propriétés de l'hexagone régulier. Soit c la longueur du côté de l'hexagone, EB est une grande diagonale et mesure 2c (on divise l'hexagone en 6 triangles equilatéraux et ça saute aux yeux), et $BG = c/2$ (AG est l'axe de symétrie de l'un des petits triangles equilatéraux), $\frac{EB}{BG} = -4$. Donc r vérifie l'équation suivante

$$\begin{array}{rrcl} & -4\cdot\frac{2r-1}{2-2r}\cdot\frac{r}{1-r} & = & -1 \\ \text{ssi} & 2(2r-1)r & = & (1-r)^2 \\ \text{ssi} & 4r^2-2r & = & r^2-2r+1 \\ \text{ssi} & r & = & \pm\frac{\sqrt{3}}{3}. \end{array}$$

Le réel r vaut soit $\sqrt{3}3$, soit $-\sqrt{3}/3$.

Solution de l'exercice 9 Soit (α,β,γ) les coordonnées barycentriques de O et P, Q, R les points d'intersection respectifs de AO et BC, BO et AC, CO et AB. On veut trouver une condition nécessaire et suffisante pour que l'aire noire soit la moitié de l'aire totale. Vérifiez que les deux conditions ci dessous sont bien équivalentes :

$$[AOQ] + [BOR] + [COP] = \frac{1}{2}[ABC]$$

$$\text{ssi} \quad [APC] + [BQA] + [CRB] = \frac{3}{2}[ABC].$$

Exprimons ces aires en fonction de α, β et γ. Soit h_A la longueur de la hauteur issue de A,

$$[ABC] = \frac{1}{2}BC\cdot h_A \quad \text{et} \quad [APC] = \frac{1}{2}PC\cdot h_A.$$

$$\frac{[APC]}{[ABC]} = \frac{PC}{BC} = \frac{\beta}{\beta+\gamma}.$$

Ainsi l'aire noire est égale à l'aire blanche ssi

$$\frac{\beta}{\beta+\gamma} + \frac{\gamma}{\gamma+\alpha} + \frac{\alpha}{\alpha+\beta} = \frac{3}{2}.$$

Il faut montrer que ceci est équivalent à "O est sur une médiane". Montrons le premier sens. Supposons que O soit sur une médiane, disons la médiane de AB, cela veut dire que $\alpha = \beta$.

$$\frac{\beta}{\beta+\gamma} + \frac{\gamma}{\gamma+\alpha} + \frac{\alpha}{\alpha+\beta} = \frac{\alpha}{\alpha+\gamma} + \frac{\gamma}{\alpha+\gamma} + \frac{\alpha}{2\alpha} = \frac{3}{2}.$$

Maintenant attaquons nous au deuxième sens : on suppose que α, β, γ vérifient

$$\begin{aligned} \frac{\beta}{\beta+\gamma} + \frac{\gamma}{\gamma+\alpha} + \frac{\alpha}{\alpha+\beta} &= \frac{3}{2} \\ \left(\frac{\beta}{\beta+\gamma} - \frac{1}{2}\right) + \left(\frac{\gamma}{\gamma+\alpha} - \frac{1}{2}\right) + \left(\frac{\alpha}{\alpha+\beta} - \frac{1}{2}\right) &= 0 \\ \frac{\beta-\gamma}{\beta+\gamma} + \frac{\gamma-\alpha}{\gamma+\alpha} + \frac{\alpha-\beta}{\alpha+\beta} &= 0 \end{aligned}$$

On peut supposer que $\alpha \geqslant \beta \geqslant \gamma$ (ici je vous truande un peu, je vous laisse chercher pourquoi je suis un truand, et pourquoi ça marche quand même). L'équation devient

$$\frac{\alpha-\beta}{\alpha+\beta} + \frac{\beta-\gamma}{\beta+\gamma} = \frac{\alpha-\gamma}{\alpha+\gamma}.$$

Mais ceci ressemble à une équation de convexité (un peu cachée). Soient

$$f(x) = \frac{1}{x},\ x = \alpha+\beta,\ y = \beta+\gamma, \lambda = \frac{\alpha-\beta}{\alpha-\gamma},\ 1-\lambda = \frac{\beta-\gamma}{\alpha-\gamma}.$$

L'équation que l'on a trouvée se réecrit ainsi :

$$\lambda f(x) + (1-\lambda) f(y) = f(\lambda x + (1-\lambda) y).$$

Mais la fonction $f(x) = 1/x$ est strictement convexe sur $\mathbb{R}+$, donc cette égalité n'a lieu que si $\lambda = 0$, $\lambda = 1$ ou $x = y$. Ces trois cas correspondent à $\alpha = \beta$, $\beta = \gamma$ et $\alpha = \gamma$, donc seulement si O est sur une médiane.

Solution de l'exercice 10 Nous avons vu dans l'exo 1 que le centre du cercle cercle inscrit avait pour coordonnées barycentriques (a, b, c), on peut donc facilement en déduire les coordonnées barycentriques des points de la figure :P : $(0, b, c)$, Q : $(a, 0, c)$, R : $(a, b, 0)$. On regarde le cercle qui passe par B, P, Q et R. Dans l'exo 3 je vous ai dit qu'un cercle avait pour équation

$$-a^2\beta\gamma - b^2\gamma\alpha - c^2\alpha\beta + (u\alpha + v\beta + w\gamma)(\alpha+\beta+\gamma) = 0.$$

Il ne reste plus qu'à déterminer le triplet (u, v, w). Comme le cercle passe par B : $(0, 1, 0)$, on vérifie facilement que $v = 0$. On utilise le fait que P et R sont sur le cercle pour montrer que

$$u = \frac{c^2 b}{a+b} \quad \text{et} \quad v = \frac{a^2 b}{b+c}.$$

Ensuite on utilise le fait que Q est sur le cercle pour montrer que

$$ua + wc = \frac{b^2ac}{a+c} \text{ donc } \frac{a}{a+b} + \frac{c}{b+c} = \frac{b}{a+c}.$$

4 Groupe D : arithmétique

1 Cours d'arithmétique : structure de $\mathbb{Z}/n\mathbb{Z}$

Le but de cette séance est de vous introduire au point du vue moderne sur l'arithmétique, issu de l'algèbre. Rien de ceci n'est officiellement au programme des olympiades, pourtant une bonne connaissance de cette théorie permet de mieux comprendre ce qui se passe, et de prouver quelques résultats très puissants.

- $\mathbb{Z}/n\mathbb{Z}$ -

Soit $n \geqslant 2$ un entier naturel. Quelle est précisement la nature de la formule $a \equiv b \pmod{n}$? Ce n'est pas une vraie égalité : cela veut dire qu'il existe une certaine relation d'équivalence, la relation de congruence, pour laquelle a et b sont en relation. Maintenant, si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, on sait bien que $a+c \equiv b+d \pmod{n}$, et de même avec la multiplication. Ainsi, cette relation possède en fait des propriétés tout à fait similaires à l'égalité, et on aimerait bien dire que « on peut additionner et multiplier les modulo », mais cette phrase n'a aucun sens mathématique. Pour lui donner du sens, on aimerait bien la « transformer » en une véritable égalité, en « faisant de deux entiers congrus modulo n un seul et même nombre ».

Si x est un entier, on appelle *classe d'équivalence de* x *modulo* n l'ensemble des entiers congrus à x modulo n. On note $\overline{x}$ la classe de x. Attention, si $x \equiv y \mod n$, alors $\overline{x}$ et $\overline{y}$ sont deux notations pour un seul et même objet. On obtient exactement n classes d'équivalence : $\overline{0}$, $\overline{1}$, $\ldots$, $\overline{n-1}$, et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de ces classes d'équivalence. On munit $\mathbb{Z}/n\mathbb{Z}$ de deux opérations $+$ et $\times$ en posant $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$. Il y a une subtilité : il faut prouver que ces opérations sont bien définies, c'est-à-dire que les résultats de ces opérations ne dépendent pas des choix des représentants x et y de $\overline{x}$ et $\overline{y}$, par exemple pour $+$, que si $\overline{x} = \overline{x'}$ at $\overline{y} = \overline{y'}$, alors $\overline{x+y} = \overline{x'+y'}$: c'est une simple reformulation du fait que la relation de congruence est compatible avec les opérations.

La construction de $\mathbb{Z}/n\mathbb{Z}$ peut paraître conceptuellement difficile la première fois qu'on la voit, mais en fait, la manipulation de cet ensemble est très simple en pratique : écrire $\overline{x} + \overline{y} = \overline{z}$ est rigoureusement équivalent à écrire $x + y \equiv z \pmod{n}$, par exemple. Pour passer d'une écriture à l'autre, on enlève les barres et on remplace l'égalité par une relation de congruence. Mais l'énorme avantage conceptuel de l'utilisation de $\mathbb{Z}/n\mathbb{Z}$ est, dans le cas de $\mathbb{Z}/5\mathbb{Z}$ par exemple, le fait que $\overline{2}$ et $\overline{7}$ sont *un seul et même nombre*, et non plus simplement congrus. De plus, $\mathbb{Z}/n\mathbb{Z}$ possède une certaine structure algébrique, qui nous permet de réaliser toutes nos opérations en restant à l'intérieur de $\mathbb{Z}/n\mathbb{Z}$, et donc sans avoir à repasser par les entiers.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est donc muni de deux opérations, une addition et une multiplication, toutes deux commutatives et associatives, et telles que

- La loi $+$ admet un élément neutre, $\overline{0}$, tel que pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $x + \overline{0} = x$;
- Tout élément x de $\mathbb{Z}/n\mathbb{Z}$ admet un opposé noté $-x$, tel que $x + (-x) = \overline{0}$ (celui-ci est unique).
- $\times$ est distributive sur $+$ ($(x+y) \times z = x \times z + y \times z$),
- La loi $\times$ admet un élément neutre, $\overline{1}$, tel que pour tout $x \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$, $x \times \overline{1} = x$.

En algèbre, on appelle un tel ensemble un *anneau* (commutatif). Les anneaux sont fondamentaux, car ils apparaissent dans bien des domaines, et les mathématiciens ont donc développé une théorie générale traitant de ce type d'objets. Je n'en dirai pas plus pour l'instant.

- $\mathbb{Z}/p\mathbb{Z}$ -

On commence cette section par un rappel :

Proposition 4.1. On dit que $a \in \mathbb{Z}/n\mathbb{Z}$ est *inversible* s'il existe $b \in \mathbb{Z}/n\mathbb{Z}$, appelé l'*inverse* de a et noté a^{-1}, tel que $a \times b = \overline{1}$. Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\overline{k}$, où k est un entier premier avec n.

Démonstration. C'est une reformulation du théorème de Bézout, en effet on a les équivalences suivantes.

Il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \mod n$
$\Leftrightarrow$ il existe $b \in \mathbb{Z}$ et $k \in Z$ tels que $ab = kn + 1$
$\Leftrightarrow$ a est premier avec n. □

Dans toute la suite, p désignera un nombre premier. On a ainsi que tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ autres que $\overline{0}$ sont inversibles. On appelle *corps* un anneau vérifiant cette propriété. Dans un corps, on dispose donc d'une opération fondamentale qui n'existe pas dans les anneaux : la division. Ainsi, les corps sont des objets algébriques beaucoup plus riches. Par exemple, la théorie des polynômes fonctionne très bien sur les corps, et nous allons donc étudier les polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Noter que de tels polynômes seraient délicats à définir sans l'introduction de $\mathbb{Z}/p\mathbb{Z}$.

Lemme 4.2. Soient a et b dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$, alors $a \times b$ est dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$.

Démonstration. Si on avait $a \times b = \overline{0}$, en multipliant par a^{-1} et b^{-1} on obtiendrait $\overline{1} = \overline{0}$, c'est absurde. □

Ce lemme facile nous permet de définir une notion satisfaisante de degré sur $\mathbb{Z}/p\mathbb{Z}[X]$, l'ensemble des polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. En effet, si P et Q ont pour termes dominants $a \cdot X^k$ et $b \cdot X^l$, alors $ab \cdot X^{k+l}$ sera non nul, et sera le terme dominant de $P \cdot Q$. Nous sommes maintenant en mesure de prouver :

Proposition 4.3. Il y a une notion de division euclidienne sur $\mathbb{Z}/p\mathbb{Z}[X]$: soient A et B dans $\mathbb{Z}/p\mathbb{Z}[X]$ avec B non nul, alors il existe un unique couple (Q, R) de polynômes de $\mathbb{Z}/p\mathbb{Z}[X]$ tels que $A = Q \cdot B + R$, avec $\deg(R) < \deg(B)$.

Démonstration. La preuve est la même que dans $\mathbb{R}[X]$. Pour l'unicité, soit (Q', R') un deuxième tel couple, alors $B \cdot (Q - Q') = R' - R$, puis $Q = Q'$ en examinant les degrés.

Pour l'existence, on vérifie que l'algorithme usuel fonctionne, car le coefficient dominant de B est inversible. Par exemple, pour diviser $A = \overline{5} \cdot X^3 + \overline{2} \cdot X^2 + \overline{5} \cdot X$ par $B = \overline{3} \cdot X^2 + \overline{6} \cdot X + \overline{2}$ dans $\mathbb{Z}/7\mathbb{Z}$, on commence par retrancher $\overline{5} \cdot \overline{3}^{-1} \cdot X \cdot B$ à A, le coefficient dominant de Q doit donc être $\overline{5} \cdot \overline{3}^{-1} \cdot X = \overline{5} \cdot \overline{5} \cdot X = \overline{4} \cdot X$. Il reste $A - \overline{4} \cdot X \cdot B = \overline{6} \cdot X^2 + \overline{4} \cdot X$. On retranche donc $\overline{6} \cdot \overline{3}^{-1} \cdot B$. Au final, on obtient $A = Q \cdot B + R$ avec $Q = \overline{4} \cdot X + \overline{2}$ et $R = \overline{6} \cdot X + \overline{3}$. □

Corollaire 4.4. Soit P dans $\mathbb{Z}/p\mathbb{Z}[X]$, et a une racine de P. Alors P est divisible par $(X-a)$, i.e. il existe Q dans $\mathbb{Z}/p\mathbb{Z}[X]$ tel que $P = (X-a)\cdot Q$.

Démonstration. Soit $P = (X-a)\cdot Q + R$ la division euclidienne de P par $(X-a)$. Alors R est de degré inférieur strictement à 1, donc constant, et l'évaluation de l'expression précédente en a nous donne $R = \overline{0}$. □

Corollaire 4.5. Un polynôme de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$ a au plus n racines.

Démonstration. Soit P de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$. Supposons qu'il admette n racines $a_1, a_2, \ldots, a_n$. D'après le corollaire précédent, il existe une constante c non nulle tel que

$$P = c\cdot \Pi_{i=1}^{n}(X-a_i).$$

Soit alors a une racine de P. On a

$$\overline{0} = c\cdot \Pi_{i=1}^{n}(a-a_i),$$

et, d'après le lemme, un des $(a-a_i)$ est nul, donc a est l'un des a_i. □

Soit a dans $\mathbb{Z}/p\mathbb{Z}$, en appliquant cela au polynôme $X^k - a$, on obtient un résultat important : a a au plus k racines k-ièmes ! Voici un exemple d'application.

Proposition 4.6. Soit a dans $\mathbb{Z}/p\mathbb{Z}\setminus\{\overline{0}\}$. Alors a est un carré si et seulement si

$$a^{\frac{p-1}{2}} = 1.$$

Démonstration. Tout d'abord, si a est un carré différent de $\overline{0}$, on écrit $a = x^2$, et alors $a^{(p-1)/2} = x^{p-1} = 1$ par théorème de Fermat. De plus, par ce que l'on vient de voir, il y a au plus $\frac{p-1}{2}$ solutions à l'équation $a^{(p-1)/2} = 1$. Or, il y a au moins $\frac{p-1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}\setminus\{\overline{0}\}$! En effet, un nombre ayant au plus 2 racines carrées, il y a au moins $\frac{p-1}{2}$ carrés parmi la liste $\overline{1}^2, \overline{2}^2, \ldots, \overline{p-1}^2$. □

Ainsi, par exemple, $\overline{-1}$ est un carré modulo p si et seulement si p est congru à 1 modulo 4. Un petit lemme souvent bien pratique.

- $\mathbb{Z}/n\mathbb{Z}^*$ -

Passons à une étude plus poussée de l'opération la plus intéressante dans $\mathbb{Z}/n\mathbb{Z}$: la multiplication. Seulement, cette multiplication possède quelques propriétés pénibles, comme le fait que le produit de deux éléments non nuls puisse être nul, qui empêchent de dire grand chose d'intéressant. Ainsi, il est naturel de restreindre notre étude à l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, que l'on notera $\mathbb{Z}/n\mathbb{Z}^*$. Algébriquement, cet ensemble est muni d'une opération, la multiplication, qui possède un élément neutre $\overline{1}$, et chaque élément possède un inverse. Un tel ensemble s'appelle un groupe, une structure mathématique très importante. Un autre exemple de groupe est $\mathbb{Z}/n\mathbb{Z}$ tout entier, muni de son addition. Nous prouverons plus loin que dans certains cas ces groupes ont en fait une structure très proche.

J'insiste sur ces questions de structure, car elles sont fondamentales. Selon les ensembles ou les opérations intervenant dans un problème donné, le cadre naturel dans lequel se place le problème change. Ainsi, un problème ne faisant intervenir que des multiplications modulo n « vit » dans $\mathbb{Z}/n\mathbb{Z}^*$, et les outils que l'on peut utiliser pour aborder le problème seront ceux de la théorie des groupes, qui sont très différents de ceux de la théorie des corps par exemple.

Commençons par un rappel : la forme générale du petit théorème de Fermat.

Théorème 4.7. Soit a dans $\mathbb{Z}/n\mathbb{Z}^*$. Alors $a^\varphi = 1$. (On rappelle que φ désigne l'indicatrice d'Euler, et que $\varphi(n)$ est le nombre d'entiers inférieurs à n et premiers avec n, qui est aussi le cardinal de $\mathbb{Z}/n\mathbb{Z}^*$, d'après notre reformulation du théorème de Bézout).

Démonstration. L'idée est d'utiliser le fait que la multiplication par a est une bijection. Appelons $x_1, x_2, \ldots, x_{\phi(n)}$ les éléments de $\mathbb{Z}/n\mathbb{Z}^*$. On a que

$$\{x_1, x_2, \ldots, x_{\phi(n)}\} = \{ax_1, ax_2, \ldots, ax_{\phi(n)}\},$$

et on obtient donc le résultat en comparant le produit de tous les éléments de nos deux ensembles, puis en simplifiant par le produit de x_i. □

Proposition 4.8. Soit x dans $\mathbb{Z}/n\mathbb{Z}^*$. La suite $(x^k)_{k\in\mathbb{Z}}$ est périodique. Appelons $\omega(x)$ sa période. Alors $x^l = 1 \Leftrightarrow \omega(x)|l$.

Démonstration. La seule chose à prouver est la périodicité. Or la suite $(x^k)_{k\in\mathbb{N}}$ prend ses valeurs dans un ensemble fini, il existe donc par principe des tiroirs $p < q$ tels que $x^p = x^q$, et alors $x^{p-q} = 1$, et la suite est $p - q$ périodique. □

Attention, dans cette preuve $p - q$ n'est pas nécessairement l'ordre de x. Calculer l'ordre d'un élément x n'est pas un problème facile : en général, il n'y a pas de méthode plus beaucoup plus intelligente que le calcul des puissances de x. Introduire cet ordre peut pourtant s'avérer très fructueux. Il y a un cas particulièrement agréable : si on dispose d'une relation de type $x^l = 1$: on saura alors que l'ordre divise à la fois l et $\phi(n)$, ce qui peut permettre de le déterminer.

- $\mathbb{Z}/p\mathbb{Z}^*$ -

Étudier les ordres est plus agréable dans $\mathbb{Z}/p\mathbb{Z}^*$, grâce aux bonnes propriétes des polynômes de la forme $X^k - 1$ montrées dans ma deuxième partie.

Définition 4.9. Un *générateur* de $\mathbb{Z}/n\mathbb{Z}^*$ est un élément x de $\mathbb{Z}/n\mathbb{Z}^*$ tel que la suite des puissances de x recouvre tout $\mathbb{Z}/n\mathbb{Z}^*$.

Théorème 4.10. Pour tout p premier, $\mathbb{Z}/p\mathbb{Z}$ possède un générateur.

Pour prouver ce théorème, il faut trouver un moyen de construire des éléments d'ordre donnés. Je commence par un lemme allant dans ce sens. il est vrai de manière générale sur $\mathbb{Z}/n\mathbb{Z}^*$, je l'énonce donc dans ce cadre.

Lemme 4.11. Soient a et b dans $\mathbb{Z}/n\mathbb{Z}^*$ tels que $\omega(a) \wedge \omega(b) = 1$. Alors $\omega(ab) = \omega(a)\omega(b)$.

Démonstration. Tout d'abord, $(ab)^{\omega(a)\omega(b)} = 1$, donc $\omega(ab)|\omega(a)\omega(b)$. Pour terminer, il suffit de prouver que si k est tel que $(ab)^k = 1$, alors k est multiple de $\omega(a)$ et de $\omega(b)$. Or, si $(ab)^k = 1$, en élevant à la puissance $\omega(a)$ on trouve que $b^{k\omega(a)} = 1$, donc que $\omega(b)$ divise $k\omega(a)$, donc $\omega(b)$ divise k par lemme de Gauss. □

Lemme 4.12. Posons $m := \mathrm{PPCM}((\omega(x))_{x\in\mathbb{Z}/n\mathbb{Z}^*})$. Alors il existe dans $\mathbb{Z}/n\mathbb{Z}^*$ un élément d'ordre m.

Démonstration. Décomposons m en facteurs premiers : $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Soit x_i un élément dont l'ordre est un multiple de $p_i^{\alpha_i}$: $\omega(x_i) = k_i p_i^{\alpha_i}$ (un tel x_i existe par définition du PPCM). Posons $y_i := x_i^{k_i}$. On vérifie que y_i est d'ordre $p_i^{\alpha_i}$ et, en utilisant de façon répétée notre lemme précedent, le produit des y_i est d'ordre m. □

Démonstration. Il est temps de finir la preuve du théorème annoncé. Appliquons donc les lemmes à $\mathbb{Z}/p\mathbb{Z}^*$. Soit donc x un élément d'ordre m. On sait que $p-1$ est multiple de tous les ordres des éléments de $\mathbb{Z}/p\mathbb{Z}^*$, il est donc multiple de leur PPCM : m, et donc $m \leqslant p-1$. Or, on sait que le polynôme $X^m - 1$ a au plus m racines, et que les $p-1$ éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont racines de ce polynôme (car m est multiple de tous les ordres), donc on a $p-1 \leqslant m$, puis $p-1 = m$, et notre élément d'ordre m est notre générateur recherché. □

Que veut dire ce théorème ? Choisissons x un générateur. Alors

$$\mathbb{Z}/p\mathbb{Z}^* = \{1, x, x^2, \dots, x^{p-2}\}.$$

La multiplication de telles puissances de x est très facile : il suffit d'ajouter les exposants modulo $p-1$. En fait, ce choix de x permet même d'identifier $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ avec $(\mathbb{Z}/p\mathbb{Z}^*, x)$, via la fonction $k \mapsto x^k$. Ainsi, la structure multiplicative du groupe $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ n'est pas plus compliquée que la structure additive du groupe $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$. Attention, tout n'est pas si rose, car trouver un générateur x n'est pas facile. Toutefois, l'introduction d'un générateur peut faire des miracles dans un problème plutôt théorique. Mentionnons, enfin, qu'il existe des résultats plus généraux, plus difficiles, explicitant pour tout n la structure de $\mathbb{Z}/n\mathbb{Z}^*$. En particulier, on a :

Théorème 4.13. Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ possède un générateur si et seulement si n vaut 2, 4, p^k ou $2p^k$, où p est un nombre premier plus grand que 3.

- Quelques exercices -

Exercice 1 Trouver tous les entiers $n \geqslant 1$ impairs tels que n divise $3^n + 1$.

Exercice 2 Soit p un nombre premier. Trouver tous les entiers k tels que p divise $1^k + 2^k + \dots + (p-1)^k$.

Exercice 3 Soit p un nombre premier impair. Prouver que si q est un diviseur premier de $x^{p-1} + x^{p-2} + \dots + 1$ alors $p = q$ ou p divise $q-1$.

Exercice 4 Combien y-a-t'il d'élements d'ordre k dans $\mathbb{Z}/p\mathbb{Z}^*$?

Exercice 5 Trouver tous les p, q premiers tels que pq divise $2^p + 2^q$.

- Solutions des exercices -

Solution de l'exercice 1 Soit $n > 1$ tel que n divise $3^n + 1$. Une autre façon de le dire est que $3^n \equiv -1 \pmod{n}$, on est donc face à un problème purement multiplicatif. On aimerait bien utiliser le théorème de Fermat, mais il est difficile à exploiter car on contrôle mal $\varphi(n)$. Soit donc p un facteur premier de n, qui est impair. On a $3^{2n} \equiv 1 \pmod{p}$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1 \pmod{p}$. Ainsi ω divise $p-1$. On en déduit que ω divise PGCD$(2n, p-1)$. Si on impose de

plus que p soit le plus petit facteur premier de n, alors nécessairement $\omega = 1$ ou 2 (car un facteur premier de $p-1$ ne peut pas diviser n par minimalité). Dans le premier cas de figure, $3 \equiv 1 \pmod p$ et donc $p = 2$, ce qui est exclu. Dans le deuxième cas, $3^2 \equiv 1 \pmod p$ et donc p divise 8, ce qui est exclu également. On en déduit que $n = 1$.

Solution de l'exercice 2 La somme des puissances k-ièmes va être difficile à manipuler telle quelle. L'idée est d'introduire un générateur x de $\mathbb{Z}/p\mathbb{Z}^*$. En effet,

$$1^k + 2^k + \ldots + (p-1)^k \equiv 1 + x^k + x^{2k} \ldots + x^{(p-2)k} \pmod p.$$

On reconnaît la somme des termes d'une suite géométrique. Ainsi, si $(p-1)|k$, chaque terme de la somme vaut 1, et la somme vaut $p-1$ qui est non nul. Sinon, x^k est différent de 1, $x^k - 1$ est inversible, et la somme vaut $\frac{x^{(p-1)k}-1}{x^k-1}$, qui est nul par théorème de Fermat.

Solution de l'exercice 3 Un tel diviseur q divise $x^p - 1 = (x-1)\left(x^{p-1} + x^{p-2} + ... + 1\right)$ donc l'ordre de x modulo q divise p premier. Si cet ordre est p, comme d'après le théorème de Fermat il divise également $q-1$, p divise $q-1$. Si l'ordre est 1, pour tout k, $x^k \equiv 1 \pmod q$ donc la somme des p termes : $x^{p-1} + x^{p-2} + ... + 1 \equiv p \pmod q$ est divisible par q si et seulement si q divise p, soit $q = p$.

Solution de l'exercice 4 Soit x un générateur de $\mathbb{Z}/p\mathbb{Z}^*$ (le résultat de l'exercice implique l'existence d'un générateur, donc, à moins de vouloir tout reprouver, il faudra de toute façon utiliser ce résultat). Les éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont donc les x^k avec k entre 0 et $p-2$. Quel est l'ordre d'un tel x^k ? C'est le plus petit a tel que ak soit multiple de $p-1$, c'est donc $\frac{\mathrm{PPCM}(p-1,k)}{k}$, autrement dit $\frac{p-1}{\mathrm{PGCD}(p-1,k)}$. Soit donc d un diviseur de $p-1$. L'élément x^k est d'ordre $\frac{p-1}{d}$ si et seulement si $\mathrm{PGCD}(p-1,k) = d$, donc si k est de la forme αd avec α premier avec $\frac{p-1}{d}$. Il y a $\phi(\frac{p-1}{d})$ tels k.

Deux remarques : la notion d'ordre fonctionne aussi dans $(\mathbb{Z}/n\mathbb{Z}, +)$, l'ordre de x étant le plus petit entier n tel que nx soit nul (où nx est défini comme valant $x + x + \ldots + x$ n fois). Un raisonnement identique montre alors que, pour d divisant n, il y a $\phi(d)$ éléments d'ordre d (moralement, notre preuve consistait à, via le choix d'un générateur, se placer dans $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$. On en déduit en comptant selon leur ordre les éléments de $\mathbb{Z}/n\mathbb{Z}$, la très jolie, et importante, identité combinatoire suivante :

$$\phi(n) = \Sigma_{d|n}\phi(d).$$

Solution de l'exercice 5 Remarquons tout d'abord que si $p = 2$, $2q$ divise $4 + 2^q$ si et seulement si soit $q = 2$, soit $2q$ divise 6, puisque, pour tout q impair, q divise $2^{q-1} - 1$, donc $2q$ divise $2^q - 2$. D'où les solutions : $(p,q) = (2,2), (2,3)$ ou $(3,2)$. On supposera désormais p et q impairs. Appelons ω_p et ω_q les ordres de 2 modulo p et q respectivement. Supposons que p divise $2^p + 2^q$, donc $2^{p-1} + 2^{q-1}$ (car 2 est inversible modulo p, on peut donc diviser par 2), comme p divise $2^{p-1} - 1$, p divise $2^{q-1} + 1$, donc p divise $2^{2(q-1)} - 1$. Dès lors, ω_p divise $p-1$ et $2(q-1)$ mais ne divise pas $q-1$. Appelons ν_2 la valuation 2-adique. Le fait que ω_p divise $p-1$ implique que $\nu_2(\omega_p) \leqslant \nu_2(p-1)$, et le fait que ω_p divise $q-1$ mais pas $2(q-1)$ implique que $\nu_2(\omega_p) = 1 + \nu_2(q-1)$ (pour vous en convaincre, regardez les décompositions en facteurs premiers). Or, symétriquement, on a $\nu_2(\omega_q) \leqslant \nu_2(q-1)$, et donc $\nu_2(\omega_p) = 1 + \nu_2(q-1) > \nu_2(\omega_q)$. Symétriquement, $\nu_2(\omega_q) > \nu_2(\omega_p)$, c'est absurde.

2 TD d'arithmétique

- Énoncés -

Exercice 1 Montrer qu'il n'existe pas d'entiers non nuls x, y, z tels que $x^4 + y^4 = z^4$.

Exercice 2 Trouver tous les $n \in \mathbb{N}^*$ tels que $n^2 \mid 2^n + 1$.

Exercice 3 Trouver toutes les paires d'entiers strictement positifs telles que $a^b = b^{(a^2)}$.

Exercice 4 Soit P un polynôme non constant à coeficients entiers, montrer que l'ensemble E des nombres premiers divisant $P(n)$ pour au moins un n est infini.

- Solutions des exercices -

Solution de l'exercice 1 On montre en fait la propriété plus forte qu'il n'est pas possible d'avoir $x^4 + y^4 = z^2$.

Par l'absurde, on suppose que (x, y, z) est la solution de l'équation avec z^2 minimal. On a alors que $x \wedge y \wedge z = 1$. D'après la forme générale des triplets pythagoriciens, on pose

$$x^2 = 2mn \qquad (1)$$
$$y^2 = m^2 - n^2 \qquad (2)$$
$$z = m^2 + n^2 \qquad (3)$$

Avec m et n non nuls, premiers entre eux et de parité opposée. De même, grâce à (2), on a m impair et n pair, donc on pose

$$m = u^2 + v^2$$
$$n = 2uv$$
$$y = u^2 - v^2$$

Avec u et v non nuls, premiers entre eux et de parité opposée. Donc (1) se réécrit

$$x^2 = 4uv(u^2 + v^2)$$

Comme u, v et $u^2 + v^2$ sont deux à deux premiers entre eux, chacun est un carré. On note $u = \tilde{x}^2$, $v = \tilde{y}^2$ et $u^2 + v^2 = \tilde{z}^2$. On a alors

$$\tilde{x}^4 + \tilde{y}^4 = \tilde{z}^2$$

et $\tilde{z} < x^2 < z$, ce qui contredit la minimalité de la solution (x, y, z).

Solution de l'exercice 2 On constate que n est impair. $n = 1$ est solution. Si $n > 1$, on pose p_0 le plus petit diviseur premier de n. Soit $\omega_{p_0}(2)$ l'ordre de 2 modulo p_0. On a

$$\omega_{p_0}(2) \mid 2n$$
$$\omega_{p_0}(2) \nmid n$$
$$\omega_{p_0}(2) \mid p_0 - 1$$

Par minimalité de p_0, n est premier avec $p_0 - 1$, donc $2n \wedge (p_0 - 1) = 2$, donc $\omega_{p_0}(2) \mid 2$, donc $\omega_{p_0}(2) = 2$. Donc $p_0 \mid (2^2 - 1)$ donc $p_0 = 3$.

D'après le théorême LTE, $v_3(2^n + 1^n) = v_3(2 + 1) + v_3(n)$, donc $v_3(n^2) \leqslant 1 + v_3(n)$, donc $v_3(n) \leqslant 1$, donc $v_3(n) = 1$. On note $n = 3m$. On constate que $m = 1$ donne $n = 3$, qui est bien solution.

Sinon, on pose p_1 le plus petit diviseur premier de m. $m^2 \mid \frac{8^m+1}{9}$. Donc

$$\omega_{p_1}(8) \mid 2m$$
$$\omega_{p_1}(8) \nmid m$$
$$\omega_{p_1}(8) \mid p_1 - 1$$

donc, comme précedemment, $\omega_{p_1}(8) = 2$, donc $p_1 \mid 63$, donc $p_1 = 7$.

Il suffit alors de constater que $7 \nmid \frac{8^m+1}{9}$.

Les deux seules solutions sont donc $n = 1$ et $n = 3$.

Solution de l'exercice 3

Lemme 4.14. Si $a^b \geqslant b^a$, alors $b \geqslant a$ ou $b = 2$ ou $b = 1$. Dans le deuxième cas, on a de plus $a \leqslant 4$.

Démonstration.

$$a^b \geqslant b^a \Leftrightarrow b\ln(a) \geqslant a\ln(b) \Leftrightarrow \frac{b}{\ln(b)} \geqslant \frac{a}{\ln(a)}$$

La fonction $f : x \mapsto \dfrac{x}{\ln x}$ est strictement croissante pour $x \geqslant e$, et $f(2) = f(4)$, ce qui conclut la preuve. □

Si $a = 1$, alors $b = 1$ et réciproquement. Par la suite, on suppose que $a \geqslant 2$ et $b \geqslant 2$.

On a $(a^2)^b \geqslant a^b = b^{(a^2)}$, donc, d'après le lemme, $b \geqslant a^2$ ou ($b = 2$ et $a^2 = 3$) ou ($b = 2$ et $a^2 = 4$). $a^2 = 3$ est absurde, et $(2, 2)$ n'est pas solution.

Si $b \geqslant a^2$, et p est un nombre premier, on a $b.v_p(a) = a^2.v_p(b)$, donc $v_p(a) \leqslant v_p(b)$.

Donc $a \mid b$. On pose $b = ac$, on a alors $a^{ac} = (ac)^{(a^2)}$, donc $a^{c-a} = c^a$. c^a est entier, donc $c - a \geqslant 0$. On a donc $a^{c-a} \geqslant (c - a)^a$, donc, comme précedemment, soit $(c - a) \leqslant 2$, soit $c - a \geqslant a$, donc $a \mid c$. Si $c - a = 0$, on retrouve la solution $(1, 1)$, et $c - a \in \{1, 2\}$ abouti à une absurdité.

On note donc $c = da$. On a alors $a^{a(d-1)} = (ad)^a$ soit $a^{d-2} = d$. Cela implique $d \leqslant 4$.

$d = 2$ donne $1 = 0$, ce qui est absurde.

$d = 3$ donne $a = 3$, on a alors $b = 27$, qui est bien solution.

$d = 4$ donne $a = 2$, on a alors $b = 16$, qui est bien solution.

Solution de l'exercice 4 Si $P(0) = 0$, pour tout p, $p \mid P(0)$.

Si $P(0) = 1$, on suppose par l'absurde que $E = p_0, p_1, \ldots, p_k$ est fini. On note alors $\Pi = \prod p_i$. Comme P est non constant, $P(\Pi X)$ non plus, donc il existe $s \in \mathbb{N}$ tel que $P(\Pi s)$ ne soit ni 1 ni -1. De plus, $P(\Pi s) \equiv 1[p_i]$ pour tout i. Soit q un diviseur premier de $P(\Pi s)$, $q \notin E$, d'où contradiction.

Sinon, on pose $a = P(0)$ et on s'intéresse au polynôme $\tilde{P}(X) = \frac{P(aX)}{a}$. $\tilde{P}$ est non constant, à coeficients entiers et tout diviseur de $\tilde{P}(n)$ est dans E, de plus, $\tilde{P}(0) = 1$.

3 Cours/TD d'arithmétique

On utilisera :
- la loi de réciprocité quadratique ;
- le théorème chinois ;
- l'ordre multiplicatif d'un éléments dans $(\mathbb{Z}/p\mathbb{Z})^*$ pour p premier.

Définition 4.15. Si p est un premier et n un entiers relatifs non-nul, alors on appelle valuation de n à p, et on le note $\nu_p n$, le plus grand entier ν tel que p^ν divise n. Par convention on pose $\nu_p 0 = \infty$.

On fait la convention que $a + \infty = \infty$ quand a est un entier relatif ou ∞. La valuation a une série de propriété comme suit.

Théorème 4.16. Soit p un premier et a, b deux entiers relatifs quelconques. Alors on a :

(i) $\nu_p(ab) = \nu_p a + \nu_p b$;

(ii) $\nu_p(a + b) \geqslant \min(\nu_p a, \nu_p b)$ avec égalité si $\nu_p a \neq \nu_p b$.

Démonstration 4.17. **(i)** C'est une conséquence du fait que la décomposition en facteurs premiers est unique.

(ii) On pose $\nu = \min(\nu_a, \nu_b)$. Comme p^ν divise a et b il divise également $a + b$. D'où on trouve l'inégalité.

Supposons maintenant $\nu_p a = k$ et $\nu_p b \geqslant k + 1$. On note $\nu = \nu_p(a + b)$ et on suppose par l'absurde que $\nu \geqslant k + 1$. Alors p^{k+1} divise $(a + b) - b$. Contradiction.

Exercice 1 Montrer que les équations $x^2 = 2y^2$ et $x^4 + 3y^4 + 27z^4 = 9t^4$ n'ont pas de solutions non-triviales.

Solution de l'exercice 1 Pour $x^2 = 2y^2$, $\nu_2(x^2)$ est paire alors que $\nu_2(2y^2)$ est impaire. Pour la deuxième équation, les valuations $\nu_3(x^4)$, $\nu_3(3y^4)$ et $\nu_3(27z^4)$ ont des restes différents modulo 4, donc elles sont toutes distinctes. Par le point (ii) de la proposition précédente, $\nu_3(9t^4)$ est égale à la plus petite de ces valuations. Mais cela est impossible, $\nu_3(9t^4)$ est congrue à 2 modulo 4.

Ici, la première valuation à utiliser était claire, à la lecture de l'énoncé. Dans d'autre cas, il faut considérer un diviseur premier p qui divise un des côtés des équations à résoudre.

Exercice 2 Soient b et n deux entiers, $n > 1$, tels que pour tout entier k il existe un entier a_k tel que $a_k^n \equiv b \bmod k$. Montrer que b est une puissance n-ième.

Solution de l'exercice 2 On prend $k = b^2$. Alors

$$(a_k)^n = b + mb^2$$

pour un m entier. Pour tout diviseur premier p de b la valuation du membre droit vaut $\nu_p(b)$. D'autre part, la valuation du membre gauche est $n\nu_p(a_k)$ donc $\nu_p(b) \equiv 0 \bmod n$. Ainsi b est une puissance n-ième.

Exercice 3 a) Soient un nombre naturel N et un premier p. Alors on a

$$\nu_p(N!) = \sum_{i=1}^{\infty} \left\lfloor \frac{N}{p^i} \right\rfloor .$$

b) On désigne par $\binom{N}{k}$ le nombre de choix de k éléments parmi N. Si $N = p^n$ et $N \geqslant k$ on a

$$v_p\left(\binom{N}{k}\right) = v_p(N) - v_p(k).$$

Exercice 4 Soit $P(x) = \sum_{i=0}^{d} a_i x^i$ un polynôme à coefficients entiers et p un nombre premier. Montrer de deux manières différentes que $P(x)^p \equiv P(x^p) \mod p$.

Exercice 5 (Théorème de Pépin) Pour $n > 0$, le n-ième nombre de Fermat $F_n = 2^{2^n} + 1$ est premier si et seulement si

$$3^{(F_n-1)/2} \equiv -1 \mod F_n. \tag{II.5}$$

Exercice 6 (Shortlist 2010) Montrer que l'équation suivante n'a qu'un nombre fini de solutions avec (m, n) entiers non-négatifs :

$$m^2 + 2 \cdot 3^n = m(2^{n+1} - 1).$$

Exercice 7 (Shortlist 2010) Pour tout couple d'entiers relatifs (a, b) on pose $f(k) = ak^3 + bk$. On dit qu'un couple (a, b) est n-bon si pour tout couple (m, k) d'entiers relatifs on a

$$\text{si } n \mid f(k) - f(m) \text{ alors } n \mid (k - m).$$

Si un couple est n-bon pour une infinité de valeurs de n, alors on dit qu'il est très bon. Trouver un couple (a, b) qui est 51-bon mais pas très bon. Montrer que si un couple est 2013-bon alors il est très bon.

Exercice 8 (Shortlist 2009) On dit qu'un nombre entier N est équilibré si $N = 1$ ou si N s'écrit comme produit d'un nombre pair de facteurs premiers, pas nécessairement distincts. Etant donné deux entiers positifs a et b on considère le polynôme $P(x) = (x + a)(x + b)$.

a) Montrez qu'il existe des entiers distincts a et b tels que $P(1), \ldots, P(50)$ sont équilibrés.

b) Si $P(n)$ est équilibré pour tout n, alors $a = b$.

Exercice 9 Si a et b sont deux nombres impairs alors

$$\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}} \left(\frac{b}{a}\right). \tag{II.6}$$

Exercice 10 Soit a un nombre entier impair qui n'est pas un carré parfait. Montrer qu'il existe une infinité de nombres premiers p tels que a est un non-résidu quadratique modulo p.

- Solutions des exercices -

Solution de l'exercice 3 a) On écrit les nombres de 1 à N dans une liste. Pour tout i de 1 à $\nu_p(N)$ on met un point à tous les multiples de p^i. Le nombre total de points est le membre droit de l'égalité que l'on doit montrer. D'autre part, tout nombre $k \in [1, N]$ à reçu exactement $\nu_p(k)$ points. Ainsi le nombre total de points est aussi égal au membre gauche de l'équation.

b) On applique le résultat précédent pour évaluer $\nu_p(N!)$ et $\nu_p(k!(N-k)!)$. Pour tout $i \in [1, \nu_p(k)]$ on a $\lfloor \frac{N}{p^i} \rfloor = \lfloor \frac{k}{p^i} \rfloor + \lfloor \frac{N-k}{p^i} \rfloor$. Pour $i \in [\nu_p(k)+1, \nu_p(N)]$ la différence $\lfloor \frac{N}{p^i} \rfloor = \lfloor \frac{k}{p^i} \rfloor + \lfloor \frac{N-k}{p^i} \rfloor$ vaut 1.

Solution de l'exercice 4 Soit d'abord $A(x)$ et $B(x)$ deux polynômes à coefficients entiers. Alors $(A(x)+B(x))^p = a^p + b^p + \sum_{k=1}^{p} \binom{p}{k} a^k b^{p-k}$. Comme tous les coefficients binomiaux qui apparaissent dans la somme de droite sont divisibles par p on obtient $(A(x)+B(x))^p \equiv A(x)^p + B(x)^p \mod p$.

Par récurrence on obtient que la somme de n'importe quel nombre de polynômes élevée à la puissance p-ième est égale à la somme des puissances p-ième. Quand on applique ce résultat aux monômes a_0, $a_1 x$, …, $a_d x^d$ de $P(x)$ on trouve

$$P(x)^p \equiv a_0^p + a_1^p x^p + \cdots + a_d^p (x^p)^d \mod p.$$

D'après le petit théorème de Fermat on a $a_i^p \equiv a_i \mod p$ pour tout $i \in [0, d]$, ce qui permet de conclure.

Remarque : L'application $P(x) \mapsto P(x)^p$ s'appelle morphisme de Frobenius et joue un rôle important dans l'étude des ensembles $\mathbb{Z}/p\mathbb{Z}$.

Solution de l'exercice 5

Implication $\Leftarrow$. On suppose que $3^{(F_n-1)/2} \equiv -1 \mod F_n$. Remarquez qu'il suffit de montrer que l'ordre multiplicatif de 3, ord(3), vaut $F_n - 1$. En effet, cela permet de conclure car, comme ord(3) divise $\varphi(F_n)$ on déduit $\varphi(F_n) = F_n - 1$, donc F_n est premier.

Comme $3^{(F_n-1)/2} \not\equiv 1 \mod F_n$, ord(3) ne divise pas $(F_n-1)/2 = 2^{2^n-1}$. D'autre part, en élevant l'équation (II.5) au carré on a $3^{F_n-1} \equiv 1 \mod F_n$. Alors ord(3) divise $F_n - 1 = 2^{2^n}$, donc $\text{ord}(3) = F_n - 1$.

Implication $\Rightarrow$. Supposons que F_n est premier. Rappelons l'identité

$$(X^{(F_n-1)/2} - 1)(X^{(F_n+1)/2} + 1) = X^{F_n-1} - 1 \equiv \prod_{a=0}^{F_n-1} (X - a) \mod F_n.$$

Ainsi, exactement la moitié des valeurs de a, résidu non-nul modulo F_n, vérifient $a^{(F_n-1)/2} \equiv 1 \mod F_n$. Comme, tous les restes quadratiques ont cette propriété, on déduit que $3^{(F_n-1)/2} \equiv -1 \mod F_n$ si et seulement si 3 est un non-résidu quadratique.

Par la loi de réciprocité quadratiue, on a

$$\left(\frac{3}{F_n}\right) = (-1)^{\frac{F_n-1}{2}\cdot\frac{3-1}{2}} \left(\frac{F_n}{3}\right).$$

Comme $F_n \equiv 4^{2^{n-1}} + 1 \equiv 2 \mod 3$, et comme 2 est un non-résidu modulo 3, on a $\left(\frac{F_n}{3}\right) = -1$. Donc 3 est un non-résidu modulo F_n et alors $3^{(F_n-1)/2} \equiv -1 \mod F_n$.

Solution de l'exercice 6 L'idée de base de l'exercice est que, si a et b sont deux nombres réels positifs et $a < b$ alors, pour deux nombres réels fixés c et d, l'ensemble d'entiers positifs n tels que $a^n > c \cdot b^n - d$ est fini.

On regarde l'équation de l'exercice comme une equation de deuxième degré en m pour laquelle n est un paramètre. Son déterminant doit être le carré d'un entier d : $(2^{n+1}-1)^2 - 8\cdot 3^n = d^2$. On obtient

$$(2^{n+1}-1-d)(2^{n+1}-1+d) = 8\cdot 3^n. \tag{II.7}$$

Les deux parenthèses ci-dessus ont la même parité, donc d est impair, notons le $d = 2d'+1$. On a deux cas : soit $2^n - d' = 2\cdot 3^p$ et $2^n - d' - 1 = 3^q$ avec $p+q = n$, soit $2^n - d' = 3^q$ et $2^n - d' - 1 = 2\cdot 3^p$ avec $p+q=n$. Dans les deux cas on a :

$$2^{n+1} - 1 = 3^q + 2\cdot 3^p, \tag{II.8}$$

avec $p+q = n$. En particulier on a $2^n > \frac{1}{2}3^{\max(p,q)}$. Comme $2 < 3^{2/3}$, pour tout n sauf un ensemble fini on a

$$\max(p,q) < \frac{2}{3}n. \tag{II.9}$$

En particulier, pour $n > 6$, on a $\min(p,q) \geqslant 2$, donc le membre droit dans l'Equation (II.8) est divisible par 9. Comme le membre gauche doit aussi être divisible par 9, on a $\mathrm{ord}_9(2) \mid (n+1)$. Ainsi, $n = 6n' + 5$ pour un entier n'. En utilisant l'identité $x^3 - 1 = (x-1)(x^2+x+1)$, l'Equation (II.8) devient

$$(4^{2n'} + 4^{n'} + 1)(4^{n'} - 1) = 2\cdot 3^p + 3^q. \tag{II.10}$$

On écrit $(4^{2n'} + 4^{n'} + 1)$ comme $(4^{n'}-1)^2 + 3\cdot 4^{n'}$. Puisque $4^{n'} \equiv 1 \bmod 3$, on déduit que 9 ne divise pas $(4^{2n'} + 4^{n'} + 1)$. Donc $3^{\min(p,q)-1}$ divise $4^{n'} - 1$. On a donc

$$3^{n/3-1} \leqslant 3^{\min(p,q)-1} \leqslant 4^{n'} - 1 = 2^{(n-5)/3} - 1. \tag{II.11}$$

De nouveau le fait énoncé en début de preuve pour $a = 2$ et $b = 3$ montre qu'il n'y a qu'un nombre fini de valeurs de n qui vérifie cette inégalité.

Solution de l'exercice 7 Montrons que le couple $(1, -51^2)$ est 51-bon mais pas très bon. Si (k,m) est un couple tel que $k^3 - 51^2 k \equiv m^3 - 51^2 m \bmod 51$, alors $(km^{-1})^3 \equiv 1 \bmod 17$ et $(km^{-1})^3 \equiv 1 \bmod 3$. Puisque 3 est relativement premier avec $\#(\mathbb{Z}/17\mathbb{Z})^*$ et respectivement $\#(\mathbb{Z}/3\mathbb{Z})^*$, on doit avoir $k \equiv m \bmod 51$. Soit maintenant n tel que $(1, -51^2)$ est très bon. En prenant $k = 51$ et $m = 0$ on voit que n divise $0 = f(51) - f(0)$. Alors n divise 51, donc on a un nombre fini de valeurs possibles.

Pour la dexième partie de l'exercice on procède en trois étapes :

1. Soit p et q deux nombres premiers entre eux. Si un couple est pq-bon alors il est p-bon.
2. Si un couple est 61-bon alors a est divisible par 61 et b ne l'est pas.
3. Si a est divisible par 61 et b ne l'est pas, alors (a,b) est 61^i-bon pour tout $i \in \mathbb{N}$.

1. Soit (a,b) un couple pq-bon. Soit (k,m) un couple tel que $f(k) - f(m) \equiv 0 \bmod p$. D'après le théorème chinois, il existe K et M tels que $K \equiv k \bmod p$ et $K \equiv M \equiv 0 \bmod q$. Alors pq divise $f(k) - f(m)$ donc pq divise $(K - M)$. En particulier p divise $K - M$, donc p divise $(k - m)$.

2. Supposons par l'absurde que (a,b) est 61-bon mais $a \not\equiv 0 \bmod 61$. D'abord on élimine le cas $b \equiv 0 \bmod 61$. En effet, comme 3 divise $61 - 1$, l'équation $w^3 \equiv 1 \bmod 61$ a deux solutions différentes de 1. En prenant $(k,m) = (w, 1)$ on voit que 61 divise $ak^3 - am^3$ mais pas $(k - m)$.

Supposons par l'absurde que a n'est pas un multiple de 61. Comme 7 est un non-résidu quadratique modulo 61 exactement une des équations suivantes a solution modulo 61 :

$$\begin{aligned} u^2 &\equiv ba^{-1} \bmod 61 \\ 7v^2 &\equiv ba^{-1} \bmod 61. \end{aligned}$$

Dans le premier cas on pose $(k, m) = (u, 0)$. On a $f(k)-f(m) \equiv (k-m)a(u^2-ba^{-1}) \equiv 0 \bmod 61$ et $k - m = u$. Comme $b \not\equiv 0 \bmod 61$, $u \not\equiv 0 \bmod 61$, ce qui contredit le fait que (a, b) est 61-bon. Dans le deuxième cas on pose $(k, m) = (2v, v)$. Alors $f(k)-f(m) \equiv (k-m)a(7v^2-ba^{-1}) \equiv 0 \bmod 61$. Comme (a, b) est 61-bon, on doit avoir $k - m = v \equiv 0 \bmod 61$, mais cela contredit le fait que $a \not\equiv 0 \bmod 61$.

3. Soit $i \in \mathbb{N}$, $i \geqslant 1$ et soit (a, b) un couple qui est 61-bon. Soit (k, m) tel que 61^i divise $f(k) - f(m)$. Alors 61^i divise $(k - m)(ak^2 + akm + am^2 - b)$. Comme a est divisible par 61 et b ne l'est pas, la deuxième parenthèse est relativement première avec 61. Donc $(k - m)$ est divisible par 61^i. On conclut que (a, b) est 61^i-bon.

Solution de l'exercice 8 **a)** On définit $f : \mathbb{N}^* \to \{0, 1\}$ en mettant $f(n) = 1$ si n a un nombre impair de diviseurs premiers non-distincts et 0 sinon. Ensuite on définit $F : \mathbb{N}^* \to \{0, 1\}^{50}$ par $F(a) = (f(a + 1), f(a + 2), \ldots, f(a + 50))$. Comme F ne peut prendre qu'un nombre fini de valeurs, elle prend forcément deux fois la même valeur, disons $F(a) = F(b)$. Alors on voit que $P(x) = (x + a)(x + b)$ convient.

b) On procède par l'absurde. L'idée est de chercher des valeurs de x où l'expression de $P(x)$ se simplifie. Comme $(x + a) - (x + b) = a - b$ on essaye de diviser les deux parenthèses par $(a-b)$. On prend $k \in \mathbb{N}$, $k > a/|a-b|$ et on pose $x = k(a-b)-a$. Alors $P(x) = (a-b)^2k(k+1)$. Comme $f(P(x)) = 1$, on a $f(k) = f(k + 1)$. Comme k est arbitraire, f est constante à partir d'un certain k. Cela est impossible car $f(p) = 1$ pour tout premier p et $f(c) = 0$ pour tout carré c.

Solution de l'exercice 9 Soient $a = \prod_{i\in I} a_i$ et $b = \prod_{j\in J} b_j$ les décompositions en facteurs premiers de a et b. Alors on a

$$\begin{aligned} \left(\frac{a}{b}\right) &= \prod_{i\in I, j\in J} \left(\frac{a_i}{b_j}\right) \\ \left(\frac{b}{a}\right) &= \prod_{i\in I, j\in J} \left(\frac{b_j}{a_i}\right). \end{aligned}$$

D'après la Loi de réciprocité quadratique, pour tous i et j on a $\left(\frac{a_i}{b_j}\right) = (-1)^{(a_i-1)(b_j-1)/4} \left(\frac{b_j}{a_i}\right)$. Il reste donc à montrer que $\left(\left(\prod_{i\in I} a_i\right) - 1\right) \left(\left(\prod_{j\in J} b_j\right) - 1\right)/4 \equiv \sum_{i\in I, j\in J} (a_i - 1)(b_j - 1)/4 \bmod 2$.

On remarque que pour deux nombres impairs x et y, $(x-1)(y-1)/4$ est pair si et seulement si au moins un des nombres x et y est congruent à 1 modulo 4. Ainsi le membre droit est égal à la parité de $\#\{i \in I \mid a_i \equiv 3 \bmod 4\} \cdot \#\{j \in J \mid b_j \equiv 3 \bmod 4\}$. Ce nombre est impair si et seulement si $a \equiv 3 \bmod 4$ et $b \equiv 3 \bmod 4$. Or, dans ce cas le membre gauche est aussi impair.

Solution de l'exercice 10 On montre le résultat par récurrence ; on suppose qu'on a déjà trouvé k nombre premiers $p_1, \ldots, p_k$ qui conviennent. On considère ℓ un facteur premier de a qui a une valuation impaire dans a et on pose $a' = \frac{a}{\ell^{v_\ell(a)}}$. Soit s un non-résidu quadratique modulo ℓ. Comme $v_\ell(a)$ est impair, s est un non-résidu quadritique modulo $l^{v_\ell(a)}$.

D'après le théorème chinois il existe un entier b tel que :

$$\begin{aligned} b &\equiv 1 \mod 4 \\ b &\equiv 1 \mod (p_1 p_2 \dots p_k) a' \\ b &\equiv s \mod \ell^{v_\ell(a)}. \end{aligned}$$

Puisque b est congruent à 1 modulo 4 on a $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ et $\left(\frac{b}{a'}\right) = \left(\frac{1}{a'}\right)$ car $b \equiv 1 \mod a'$. Or on a

$$\left(\frac{b}{a}\right) = \left(\frac{b}{a'}\right) \cdot \left(\frac{b}{\ell^{v_\ell(a)}}\right) = \left(\frac{1}{a'}\right) \cdot \left(\frac{s}{\ell^{v_\ell(a)}}\right) = -1.$$

Ainsi a est un non-résidu modulo b et, en particulier, modulo un de ses facteurs premiers. Comme b est relativement premier avec le produit $(p_1 \cdots p_k)$, ce nouveau nombre premier est distinct de $p_1, \dots, p_k$.

III. Deuxième période

Contenu de cette partie

1 Groupe A : algèbre

1 Cours d'algèbre : développements, factorisations, combinatoire

- Introduction -

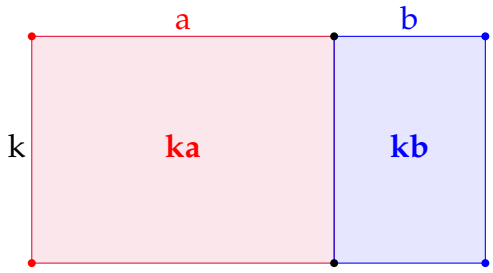
Le mot *algèbre* vient de l'arabe *al-djabr* qui signifie "restauration" au sens de "la réunion de ce qui a été cassé". Ce mot est apparu pour la première fois dans l'ouvrage *Ilm al djabr w'al muqàbalah* en 830 par un astronome arabe, Al-Khwarizmi (v. 780 - v. 850). La restauration (*al djabr*) et la confrontation (*al muqàbalah*) dont il s'agit sont des "rééquilibrages" des deux membres d'une équation, comme pour une balance.

Ce cours portera donc sur les façons de modifier des expressions littérales, en utilisant développement, factorisation et identités remarquables.

On notera $(a, b) \in \mathbb{R}^2$ et $(k, n) \in \mathbb{N}^2$.

- Développement / factorisation -

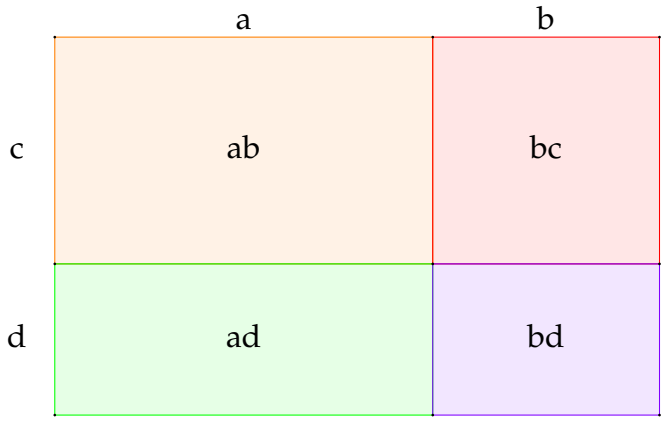
Proposition 1.1 (La factorisation simple)**.** $k \times (a + b) = k \times a + k \times b$



Démonstration.

□

Proposition 1.2 (La factorisation du rectangle)**.** $(a + b) \times (c + d) = ac + ad + bc + bd$



Démonstration.

□

Exercice 1 Touver toutes les solutions de l'équation $ab - a - b = 1$ avec $a > b > 0$ entiers.

Solution de l'exercice 1 On factorise avec $(a-1)(b-1) = ab-a-b+1$ qui donne $(a-1)(b-1) = 2$ d'où l'unique solution $(3,2)$.

Exercice 2 Trouver les solutions entières de $a^2b^2 = a^2 + b^2$.

Solution de l'exercice 2 Toujours avec la factorisation du rectangle, l'équation devient

$$(a^2-1)(b^2-1) = 1.$$

Or 2 n'est pas un carré, la seule solution est donc $(0,0)$.

Exercice 3 Soient a et b deux nombres vérifiant

$$\frac{a}{1+b} + \frac{b}{1+a} = 1.$$

Montrer que $a^3 + b^3 = a + b$.

Solution de l'exercice 3 On met sur le même dénominateur, ce qui donne $a(1+a) + b(1+b) = (1+a)(1+b)$ donc en simplifiant $a^2 + b^2 = 1 + ab$. En multipliant par $(a+b)$ de chaque côté on obtient l'égalité voulue.

Exercice 4 Trouver k tel que $(a+b)(b+c)(c+a) = (a+b+c)(ab+bc+ca) + k\,abc$.

Solution de l'exercice 4 Il suffit de développer les deux membres : $(a+b)(b+c)(c+a) = (ab+ac+b^2+bc)(c+a) = a^2b+a^2c+ab^2+ac^2+b^2c+bc^2+2abc$, $(a+b+c)(ab+bc+ca)+kabc = a^2b + a^2c + ab^2 + ac^2 + b^2c + bc^2 + 3abc + kabc$ donc $k = -1$.

- Identités remarquables de degré 2 -

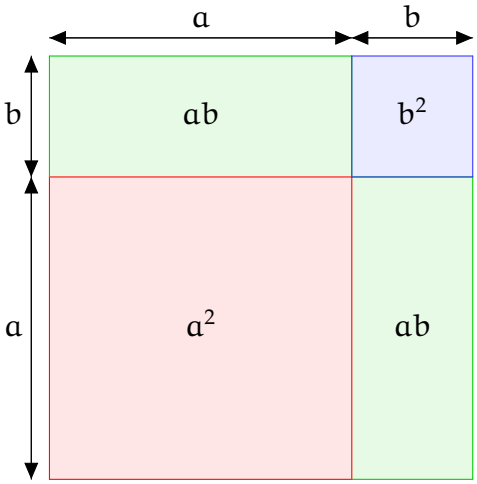
Proposition 1.3 (Identités remarquables de degré 2)**.**

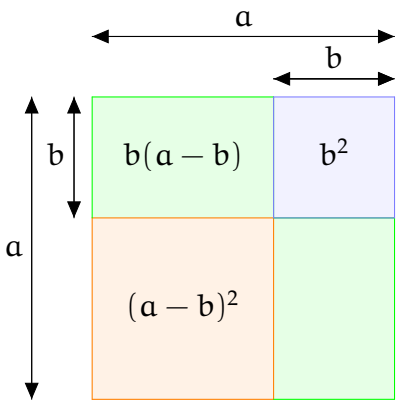
$$(a+b)^2 = a^2 + 2ab + b^2$$

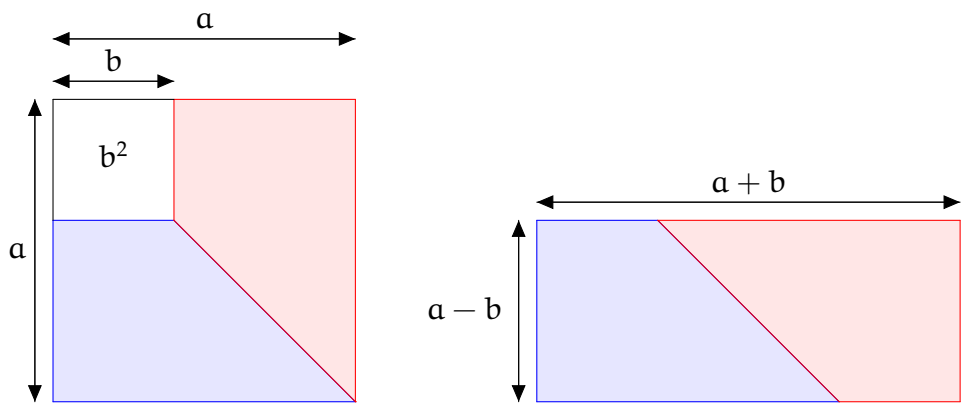
$$(a-b)^2 = a^2 - 2ab + b^2$$

$$a^2 - b^2 = (a+b)(a-b)$$

Démonstration.







□

Exercice 5 Trouver des entiers k tel que $4n^2 + kn + 9$ soit un carré pour tout n.

Solution de l'exercice 5 $(2n+3)^2 = 2n^2 + 6n + 9$, $(2n-3)^2 = 2n^2 - 6n + 9$ donc k peut valoir -12 ou 12 (et on pourrait même prouver que nulle autre valeur de k ne convient).

Exercice 6 Calculer (sans calculatrice) $1001^2 - 999^2$.

Solution de l'exercice 6 $1001^2 - 999^2 = (1001 + 999) * (1001 - 999) = 2 * 2000 = 4000$.

Exercice 7 Soient a et b deux nombres positifs tels que $\frac{a}{1+a} + \frac{b}{1+b} = 1$.

Montrer que $\frac{a}{1+b^2} - \frac{b}{1+a^2} = a - b$.

Solution de l'exercice 7 L'égalité donne $ab = 1$. Alors, en multipliant le numérateur et dénominateur de $\frac{a}{1+b^2}$ par a, et en simplifiant, on a $\frac{a}{1+b^2} = \frac{a^2}{a+b}$ et de même en multipliant le numérateur et dénominateur de $\frac{b}{1+a^2}$ par b, et en simplifiant, on a $\frac{b}{1+a^2} = \frac{b^2}{a+b}$. D'où $\frac{a}{1+b^2} - \frac{b}{1+a^2} = \frac{a^2-b^2}{a+b} = a - b$.

Exercice 8 Montrer que $n^4 + 4$ n'est jamais un nombre premier (pour $n \geqslant 2$).

Solution de l'exercice 8 $n^4 + 4 = (n^2+2)^2 - (2n)^2 = (n^2 + 2 + 2n)(n^2 + 2 - 2n)$

- Identités remarquables de degré 3 -

Proposition 1.4 (Identités remarquables de degré 3)**.**

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$
$$(a-b)^3 = a^3 - 3a^2b + 3ab^2 - b^3$$
$$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$$
$$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$$

Exercice 9 Soient a et b deux réels. On pose $s = a + b$ et $p = ab$. Exprimer $a^3 + b^3$ en fonction de s et p.

Solution de l'exercice 9 $(a+b)^3 = a^3 + b^3 + 3a^2b + 3ab^2 = a^3 + b^3 + 3ab(a+b)$ donc $a^3 + b^3 = s^3 - 3sp$.

- Degré n -

On cherche à généraliser les résultats précédents pour un degré n quelconque.

Remarque 1.5 ($a^n - b^n$)**.** On a vu :

$$a^2 - b^2 = (a - b)(a + b)$$

$$a^3 - b^3 = (a - b)(a^2 + ab + b^2)$$

En calculant $a^4-b^4 = (a^2-b^2)(a^2+b^2) = (a-b)(a+b)(a^2+b^2) = (a-b)(a^3+a^2b+ab^2+b^3)$, on peut intuiter la généralisation :

Proposition 1.6. $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b^{n-3} + ab^{n-2} + b^{n-1})$

Démonstration. On développe le membre de droite et on obtient :

$$\begin{aligned} &a^n + a^{n-1}b + a^{n-2}b + \ldots + a^2b^{n-2} + ab^{n-1} - a^{n-1}b - a^{n-2}b^2 - \ldots - ab^{n-1} - b^n \\ &= a^n + a^{n-2}b + \ldots + a^2b^{n-2} + ab^{n-1} - a^{n-2}b^2 - \ldots - ab^{n-1} - b^n \\ &\vdots \\ &= a^n - b^n \end{aligned}$$

□

Remarque 1.7 ($(a + b)^n$)**.** On a :

$$(a + b)^1 = a + b$$

$$(a + b)^2 = a^2 + 2ab + b^2$$

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

On voit apparaître des coefficients qui sont symétriques. De plus tous les termes sont homogènes. Cherchons comment obtenir ces coefficients.

Examinons de plus près le cas $n = 4$. Écrivons $(a + b)^4 = (a + b)(a + b)(a + b)(a + b)$. Un terme du développement s'obtient en sélectionnant dans chacune des parenthèses soit "a" soit "b".

- Par exemple, "a^4" s'obtient en sélectionnant à chaque fois "a".
- Mais si on veut obtenir "ab^3", il faut choisir un "a" puis sélectionner "b" dans les autres parenthèses. On a quatre possibilités pour choisir le "a" : le coefficient devant "ab^3" est donc 4.
- De même, pour obtenir "a^2b^2", il faut choisir deux "a" et sélectionner "b" dans les deux autres parenthèses. En explicitant à la main les différentes configurations, on trouve qu'il y a six façons de choisir deux "a" parmi les quatre : le coefficient devant "a^2b^2" est 6.

Pour pouvoir généraliser, il va donc falloir calculer le nombre de façons de choisir k "a" parmi n, d'où la nécessité d'introduire les bases de la combinatoire.

- Combinatoire : apprendre à compter -

Exercice 10 Combien existe-t-il de mots de 5 lettres ?

Solution de l'exercice 10 Il y a 26 lettres dans l'alphabet, donc 26 choix possibles pour la première lettre du mot, puis 26 pour la seconde, etc... D'où 26^5 mots différents.

Proposition 1.8. Soit A un ensemble à n éléments. Il existe n^k combinaisons de k éléments de A ordonnés.

Définition 1.9. On définit la factorielle d'un entier naturel n, notée $n\,!$ (lire "factorielle n"), comme le produit des nombres entiers strictement positifs inférieurs ou égaux à n.

En d'autres termes : $n\,! = 1 \times 2 \times 3 \times \ldots \times (n-1) \times n$.

Exercice 11 Combien existe-t-il de nombres formés avec les chiffres de 1 à 4, dont tous les chiffres sont différents ?

Solution de l'exercice 11 On distingue les nombres à 1, 2, 3 ou 4 chiffres. S'il y a 1 seul chiffre, on a 4 possibilités. S'il y en a deux, on a 4 possibilités pour le premier chiffre et 3 pour le deuxième puisque les chiffres doivent être différents, donc 12 possibilités au total. De même s'il y a trois chiffres, on a $4 \times 3 \times 2$ possibilités et $4\,!$ s'il y en a quatre.

Finalement il y a $4 + 12 + 24 + 24 = 64$ nombres.

Proposition 1.10. Il existe $n\,!$ façons d'ordonner n éléments différents.

Démonstration. On choisit tout d'abord l'objet qui sera placé au rang 1, ensuite celui qui sera au rang 2, etc... Lorsque l'on choisit celui qui aura le rang 1, on dispose de n objets : on a donc n choix. Au rang 2, il nous reste $n-1$ objets donc $n-1$ choix et ainsi de suite jusqu'au rang n où il ne nous reste plus qu'un seul objet, donc un seul choix. Ainsi, le nombre de possibilités est $n \times (n-1) \times (n-2) \times \ldots \times 2 \times 1 = n\,!$ □

Proposition 1.11 (Arrangements)**.** Il existe $\dfrac{n\,!}{(n-k)\,!}$ façons de choisir k éléments ordonnés parmi n.

Démonstration. On dispose de n objets et on les choisit un par un jusqu'à en avoir k. De façon similaire à la démonstration précédente : on a n choix pour le premier objet, $n-1$ pour le deuxième et lorsqu'on veut choisir le k^e, il reste $n-k+1$ objets donc $n-k+1$ choix. Ainsi le nombre de possibilités est $n \times (n-1) \times (n-2) \times \ldots \times (n-k+1) = \dfrac{n\,!}{(n-k)\,!}$. □

Exercice 12 Quelle est la probabilité que deux stagiaires soient nés le même jour (pas nécessairement la même année) ? Rappel : Il y a 62 stagiaires.

Solution de l'exercice 12 On va déterminer la probabilité du contraire, donc la probabilité qu'on ne puisse trouver deux personnes nées le même jour. Dans ce cas, on doit choisir 62 jours différents parmi les 365 du calendrier, avec ordre puisque deux stagiaires ne sont pas interchangeables : c'est un arrangement. Il y a donc $\frac{365\,!}{(365-62)\,!}$ cas dans lesquel on ne peut trouver deux stagiaires étant nés le même jour. Le nombre de possibilités total est de 365^{62}. Ainsi la probabilité que deux stagiaires soient nés le même jour est de $1 - \frac{1}{365^{62}} \times \frac{365\,!}{(365-62)\,!} = 99.59095749\%$.

Proposition 1.12. Il existe $\frac{n!}{k!(n-k)!}$ façons de choisir k éléments parmi n sans tenir compte de l'ordre. On note $\binom{n}{k}$ cette quantité.

Démonstration. On sait qu'il y a $k!$ façons d'ordonner les k éléments choisis. Donc lorsqu'on compte le nombre de façons de choisir k éléments parmi n avec ordre, on en compte $k!$ fois trop. Ainsi il faut diviser $\frac{n!}{(n-k)!}$ par $k!$ et on obtient bien $\frac{n!}{k!(n-k)!} = \binom{n}{k}$. □

Proposition 1.13 (Binôme de Newton)**.**

$$(a+b)^n = \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{k}a^{n-k}b^k + \ldots + \binom{n}{n}a^0 b^n$$

Exercice 13

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{k} + \ldots + \binom{n}{n} = ?$$

Solution de l'exercice 13 On reconnaît un binôme de Newton pour lequel $a = 1$ et $b = 1$. La réponse est donc 2^n.

Exercice 14

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^k\binom{n}{k} + \ldots + (-1)^n\binom{n}{n} = ?$$

Solution de l'exercice 14 Comme pour l'exercice précédent, il s'agit de reconnaître un binôme de Newton mais cette fois avec $a = 1$ et $b = -1$. On trouve donc $(1-1)^n = 0$.

Corollaire 1.14.

$$\binom{n}{k} = \binom{n}{n-k}$$

Proposition 1.15 (Formule de Pascal)**.**

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Démonstration. On veut choisir k éléments parmi n. On isole un élément. Soit cet élément fait partie des choisis, soit il n'en fait pas partie. Dans le premier cas, il faut encore choisir $k-1$ éléments parmi les $n-1$ restants, dans le deuxième cas, on doit choisir k éléments parmi les $n-1$ restants. Ainsi,

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

□

Corollaire 1.16. Pour trouver la valeur de $\binom{n}{k}$ pour des petits n on écrit le triangle de Pascal :

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

Il suffit d'écrire des "1" sur les côtés du triangle, puis chaque nombre est égal à la somme des deux nombres au dessus, d'après la proposition précédents. On trouve ainsi facilement les valeurs des coefficients binomiaux.

2 TD d'algèbre

- Combinatoire -

Exercice 1 Exprimer le nombre de diagonales d'un n-gône convexe.

Solution de l'exercice 1 Chaque sommet est relié par une diagonale à tous les autres, sauf 3 (ses deux voisins et lui-même). Donc il y a $\frac{n(n-3)}{2}$ diagonales.

En combinatoire, on est souvent amené à compter des configurations dont certaines sont considérées équivalentes. On compte alors le nombre total de combinaisons possibles en considérant qu'elles sont différentes, puis on divise par le nombre de combinaisons qui sont équivalentes. Par exemple pour compter ses moutons, un berger compte le nombre total de pattes puis divise par 4, car en considérant que deux pattes sont équivalentes si elles appartiennent au même animal, alors chaque patte est équivalente à 3 autres, donc on les groupe par 4.

Exercice 2 On colorie chaque face d'un cube d'une couleur différente choisie parmi 6. Combien y a-t-il de coloriages distincts ?

Solution de l'exercice 2 Si l'on considère que le cube est dans une position fixée, il y a $6! = 720$ façons de le colorier. Or, un cube colorié peut être dans 24 positions (6 choix de la face du bas, 4 rotations possibles). Donc il existe $\frac{720}{24} = 32$ coloriages différents.

Exercice 3 n personnes ($\geqslant 3$) sont assises autour d'une table circulaire. Combien y a-t-il de dispositions distinctes ? On considérera que deux positions sont identiques si chaque convive a les mêmes voisins dans les deux positions.

Solution de l'exercice 3 Il y a $n!$ façons de positionner n personnes autour d'une table. Or une table peut être disposée de $2n$ façons différentes : n rotations et une symétrie sont possibles. Donc il existe $\frac{n!}{2n}$ dispositions de tables possibles.

Un deuxième principe important de la combinatoire consiste à compter la même quantité de deux manières différentes. On parle de *double comptage*.

Exercice 4 Montrer que $k\binom{n}{k} = n\binom{n-1}{k-1}$.

Solution de l'exercice 4 Une première solution calculatoire consistant à utiliser la formule des coefficients binomiaux ne sera pas détaillée ici. Voici une solution combinatoire alternative : soit un groupe de n personnes. k personnes fondent une association et choisissent un président. Il y a donc $\binom{n}{k}$ façons de choisir les membres, puis k chefs possibles. Mais on peut

d'abord choisir le président (n choix), puis les $n-1$ membres restants, soit $\binom{n}{(n-1)}$ cas. D'où l'égalité par double comptage.

Exercice 5 Montrer que $\sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k}=\binom{2n}{n}$.

Solution de l'exercice 5 Comme ci-dessus, une première solution calculatoire consiste à utiliser la formule des coefficients binomiaux, et ne sera pas détaillée ici. Voici une solution combinatoire : soit un groupe de $2n$ personnes, parmi lesquelles n filles et n garçons. Comptons le nombre de possibilités de former un club avec n membres. C'est $\binom{2n}{n}$. Mais si l'on sait qu'il y a k garçons dans le club, il y a $\binom{n}{k}$ façons de choisir ces k garçons parmi les n, puis il faut completer avec $n-k$ filles. Donc il y a $\binom{n}{k}\binom{n}{n-k}$ façons de faire un club de n personnes avec k garçons. En sommant pour k de 0 à n on obtient bien l'égalité par double comptage.

- Inégalités : un carré est toujours positif ! -

Une des inégalités les plus simples est la suivante : $\forall x\in\mathbb{R}, x^2\geqslant 0$. En remplacant x par une expression plus intéressante puis en développant, on peut obtenir de nombreuses inégalités, dont voici quelques exemples.

Dans les exercices qui suivent, a et b sont des réels strictement positifs.

Exercice 6 (Inégalité arithmético-géométrique)
Montrer que $\frac{a+b}{2}\geqslant\sqrt{ab}$.

Solution de l'exercice 6 On développe $(\sqrt{a}-\sqrt{b})^2\geqslant 0$ qui donne $a+b\geqslant 2\sqrt{ab}$.

Exercice 7 Montrer que pour tout $x>0$, $x+\frac{1}{x}\geqslant 2$.

Solution de l'exercice 7 On développe $(\sqrt{x}-\sqrt{\frac{1}{x}})^2\geqslant 0$, qui donne $x+\frac{1}{x}\geqslant 2$, ou on applique directement l'exercice précédent avec x et $\frac{1}{x}$.

Exercice 8 Soient x, y et z trois réels strictement positifs. Montrer que

$$\frac{x}{y}+\frac{y}{z}+\frac{z}{x}+\frac{x}{z}+\frac{z}{y}+\frac{y}{x}\geqslant 6.$$

Solution de l'exercice 8 On regroupe un terme et son inverse, et on applique l'exercice précédent, pour obtenir $\frac{x}{y}+\frac{y}{x}+\frac{z}{x}+\frac{x}{z}+\frac{z}{y}+\frac{y}{z}\geqslant 2+2+2=6$

Exercice 9 Montrer que $\sqrt{\frac{a^2+b^2}{2}}\geqslant\frac{a+b}{2}$.

Solution de l'exercice 9 On montre le carré de cette inégalité, c'est-à-dire $\frac{a^2+b^2}{2}\geqslant\frac{a^2+b^2+2ab}{4}$. Comme $(a-b)^2\geqslant 0$, on a aussi $2a^2+2b^2\geqslant a^2+b^2+2ab$ en ajoutant a^2+b^2 et en passant $-2ab$ dans le membre de droite. On en déduit l'inégalité ci-dessus en divisant par 4. Comme chaque membre est positif, on peut prendre la racine de l'inégalité, et on obtient $\sqrt{\frac{a^2+b^2}{2}}\geqslant\frac{a+b}{2}$.

Exercice 10 Montrer que $\sqrt{ab}\geqslant\frac{2}{\frac{1}{a}+\frac{1}{b}}$.

Solution de l'exercice 10 On développe $(\frac{1}{\sqrt{a}}+\frac{1}{\sqrt{b}})^2\geqslant 0$, qui donne $\frac{1}{a}+\frac{1}{b}\geqslant\frac{2}{\sqrt{ab}}$ donc l'inégalité cherchée.

En mettant bout à bout toutes ces inégalités, on a :

$$\min(a,b) \leqslant \frac{2}{\frac{1}{a}+\frac{1}{b}} \leqslant \sqrt{ab} \leqslant \frac{a+b}{2} \leqslant \sqrt{\frac{a^2+b^2}{2}} \leqslant \max(a,b)$$

On parle respectivement de moyenne harmonique, géométrique, arithmétique et quadratique.

2 Groupe B : algèbre

1 Cours d'algèbre : techniques de calcul, coefficients binomiaux, inégalités

- Techniques de calcul et de factorisation -

Identités remarquables Rappelons les trois identités connues depuis le collège :

$$(a+b)^2 = a^2 + 2ab + b^2, \quad (a-b)^2 = a^2 - 2ab + b^2, \quad a^2 - b^2 = (a-b)(a+b).$$

L'identité suivante généralise la troisième identité :

Proposition 2.1. Soient a, b des réels. Alors pour tout entier $n \geqslant 1$,

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}) = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$$

Démonstration. Il suffit de développer le côté droit :

$$(a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k = \sum_{k=0}^{n-1} a^{n-k}b^k - \sum_{k=0}^{n-1} a^{n-1-k}b^{k+1}.$$

Dans la deuxième somme on effectue le changement de variable $l = k+1$. On obtient

$$a^n + \sum_{k=1}^{n-1} a^{n-k}b^k - \sum_{l=1}^{n} a^{n-l}b^l = a^n - b^n.$$

□

Exemple 2.2. Soit une suite géométrique de premier terme x_0 et de raison r. Alors la somme de ses n premiers termes se calcule à l'aide de l'identité ci-dessus appliquée à $a = 1$ et $b = r$:

$$x_0 + x_0 r + x_0 r^2 + \ldots + x_0 r^{n-1} = x_0 \frac{1-r^n}{1-r}.$$

Existe-t-il une identité analogue pour $a^n + b^n$? Lorsque n est pair, pas vraiment. Par contre, si n est impair, on a

$$a^n + b^n = a^n - (-b^n) = a^n - (-b)^n,$$

et d'après l'identité précédente, cela donne

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1}) = (a+b)\sum_{k=0}^{n-1} a^{n-1-k}(-b)^k.$$

Exercice 1 Si $a + b = 2$ et $a^2 + b^2 = 2$, combien vaut $a^3 + b^3$? Et $a^4 + b^4$?

Exercice 2 Soient a et b des réels positifs tels que $\frac{a}{1+a} + \frac{b}{1+b} = 1$. Montrer qu'alors

$$\frac{a}{1+b^2} - \frac{b}{1+a^2} = a - b.$$

Binôme de Newton : Généralisons maintenant les deux autres identités. Soient n et $k \leqslant n$ des entiers naturels. On note $\binom{n}{k}$ (et on prononce "k parmi n") le nombre de manières de choisir un sous-ensemble à k éléments dans un ensemble à n éléments. Ce sont les coefficients qui vont intervenir dans le développement de $(a+b)^n$. Plus précisément,

Proposition 2.3. (Binôme de Newton) Pour tous a, b, on a

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

En effet, chaque terme dans le développement de $(a+b)^n$ s'obtient en choisissant a dans certains facteurs et b dans tous les autres. Chaque terme est donc bien de la forme $a^k b^{n-k}$ pour un certain k. À k fixé, on obtient un terme $a^k b^{n-k}$ autant de fois qu'il y a de manières de choisir k fois a parmi les n facteurs, donc $\binom{n}{k}$. Le coefficient devant $a^k b^{n-k}$ est donc bien $\binom{n}{k}$.

Cependant, tant qu'on n'a pas donné de formule pour $\binom{n}{k}$, ce résultat ne dit pas grand chose. On a en fait la formule suivante :

Proposition 2.4. Soit n un entier naturel, et k un entier naturel inférieur à n. Alors

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}.$$

Démonstration. Nous allons prouver la deuxième formule (qui est clairement équivalente à la première). Le numérateur $n(n-1)\dots(n-k+1)$ correspond au fait de choisir un premier élément, pour lequel il y a n choix, ensuite un deuxième parmi les $n-1$ restants (ce qui fait $(n-1)$ choix), et cætera jusqu'au k-ième, pour lequel il y a $n-(k-1) = n-k+1$ choix. Maintenant, le sous-ensemble obtenu ne dépend pas de l'ordre dans lequel on a choisi ses éléments. Il faut donc diviser par le nombre de permutations d'un ensemble de k éléments, à savoir $k!$. □

Exemple 2.5. Vérifier que $\binom{n}{0} = 1$, que $\binom{n}{1} = n$, et que pour tout k, $\binom{n}{k} = \binom{n}{n-k}$, d'abord en utilisant la définition de $\binom{n}{k}$, puis en utilisant la formule. Cela signifie que le développement de $(a+b)^n$ commencera toujours par $a^n + na^{n-1}b$ et sera symétrique. En plus du cas $n=2$ ci-dessus, il est bon de connaître les cas $n=3$ et $n=4$:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3, \quad (a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

Exercice 3 Montrer que pour tout entier naturel n,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \text{ et } \sum_{k=0}^{n} \binom{n}{k}(-1)^k = 0.$$

Sommes télescopiques : Parfois on peut faire apparaître dans un calcul une somme de la forme

$$(a_0 - a_1) + (a_2 - a_2) + \dots + (a_{n-1} - a_n) + (a_n - a_{n+1}).$$

Alors tous les termes au milieu se simplifient (on dit parfois en jargon mathématique qu'ils se "télescopent") et on se retrouve simplement avec $a_0 - a_{n+1}$.

Exercice 4 Calculer

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\ldots+\frac{1}{2013\times 2014}.$$

- Inégalités -

Pour les inégalités usuelles, voir les polycopiés des stages précédents, ainsi que le cours d'Animath rédigé par Pierre Bornsztein.

Exercice 5 Montrer l'inégalité de Nesbitt : pour tous les réels $a, b, c > 0$, on a

$$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}\geqslant\frac{3}{2}.$$

Trouver également le cas d'égalité.

Exercice 6 Soient $a_1, \ldots, a_n \geqslant 0$ des réels. Montrer que

$$n(a_1^3+\ldots+a_n^3)\geqslant(a_1+\ldots+a_n)(a_1^2+\ldots+a_n^2).$$

Exercice 7 Soient $a_1, \ldots, a_n > 0$ tels que $a_1 \ldots a_n = 1$. Montrer que

$$\prod_{i=1}^{n}(2+a_i)\geqslant 3^n.$$

Exercice 8 Montrer que pour tous réels x et y, on a

$$x^2+y^2+1>x\sqrt{y^2+1}+y\sqrt{x^2+1}.$$

Exercice 9 Montrer que pour tous $a, b, c > 0$

$$\frac{(a+2b+3c)^2}{a^2+2b^2+3c^2}\leqslant 6.$$

- Solutions des exercices -

Solution de l'exercice 1 D'après l'identité ci-dessus, on a $a^3+b^3=(a+b)(a^2-ab+b^2)=2(2-ab)$. Il suffit donc d'évaluer ab. On a $4=(a+b)^2=a^2+b^2+2ab=2+2ab$, d'où $ab=1$, et $a^3+b^3=2$. Ensuite, $4=(a^2+b^2)^2=a^4+b^4+2a^2b^2=a^4+b^4+2$, d'où $a^4+b^4=2$.

Solution de l'exercice 2 La première chose à faire est d'exploiter un peu mieux la condition qui nous est donnée. Une manière simple de le faire est de tout mettre au même dénominateur et de multiplier par $(1+a)(1+b)$. On obtient

$$a(1+b)+b(1+a)=(1+a)(1+b),$$

c'est-à-dire, en développant et en simplifiant, $ab = 1$. Ainsi, la condition de l'énoncé n'est qu'une manière déguisée de dire que a et b sont inverses l'un de l'autre ! En remplaçant b par $\frac{1}{a}$ dans le premier terme du côté gauche de l'expression cherchée, on obtient :

$$\frac{a}{1+b^2} - \frac{b}{1+a^2} = \frac{a}{1+\frac{1}{a^2}} - \frac{b}{1+a^2} = \frac{a^3-b}{1+a^2}.$$

Afin de faire disparaître le dénominateur, on va introduit artificiellement des facteurs $(1+a^2)$ au numérateur et on utilise encore $ab = 1$:

$$\frac{a^3-b}{1+a^2} = \frac{a^3+a-a+a^2b-a^2b-b}{1+a^2} = \frac{a(a^2+1)-a+a-b(1+a^2)}{1+a^2} = a-b.$$

Solution de l'exercice 3 On applique simplement la formule du binôme à $a = b = 1$ et à $a = 1, b = -1$.

Solution de l'exercice 4 L'astuce est de remarquer que pour tout entier strictement positif k, $\frac{1}{k(k+1)} = \frac{k+1-k}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$. Par télescopage, la somme cherchée vaut donc $1 - \frac{1}{2014} = \frac{2013}{2014}$.

Solution de l'exercice 5 Appelons I le côté gauche de l'inégalité, et $J = a(b+c) + b(c+a) + c(a+b)$. Alors par Cauchy-Schwarz, $IJ \geqslant (a+b+c)^2$. On se ramène donc à montrer

$$\frac{(a+b+c)^2}{2(ab+bc+ca)} \geqslant \frac{3}{2},$$

ce qui est équivalent à

$$2(a^2+b^2+c^2) \geqslant 2(ab+bc+ca),$$

vrai car équivalent à

$$(a-b)^2 + (b-c)^2 + (c-a)^2 \geqslant 0.$$

On voit grâce à cette dernière inégalité aussi que l'égalité n'a lieu que lorsque $a = b = c$.

Solution de l'exercice 6 Par symétrie, on peut supposer $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$ et on applique l'inégalité de Tchebychev.

Solution de l'exercice 7 On applique l'IAG à chaque facteur : $2 + a_i = 1 + 1 + a_i \geqslant 3\sqrt[3]{a_i}$, d'où l'inégalité grâce à la condition sur les a_i. L'égalité n'a lieu que lorsque tous les a_i valent 1.

Solution de l'exercice 8 Remarquons qu'il suffit de prouver l'inégalité lorsque x et y sont positifs. Dans ce cas, en appliquant l'IAG à chacun des termes du côté droit , on a

$$x\sqrt{y^2+1} + y\sqrt{x^2+1} \leqslant \frac{1}{2}(x^2+y^2+1) + \frac{1}{2}(y^2+x^2+1) = x^2+y^2+1.$$

Il suffit donc de montrer que l'inégalité est en fait stricte, c'est-à-dire que le cas d'égalité n'a jamais lieu. Or d'après le cas d'égalité de l'IAG, pour qu'il y ait égalité il faut et il suffit que $x = \sqrt{y^2+1}$ et $y = \sqrt{x^2+1}$ simultanément, ce qui, en mettant au carré, donne bien deux conditions contradictoires.

Solution de l'exercice 9 On applique Cauchy-Schwarz :

$$(1\times a + 1\times b + 1\times b + 1\times c + 1\times c + 1\times c)^2 \leqslant 6\times(a^2+2b^2+3c^2).$$

Une autre possibilité est

$$(1\times a + \sqrt{2}\times\sqrt{2}b + \sqrt{3}\times\sqrt{3}c)^2 \leqslant (1^2+\sqrt{2}^2+\sqrt{3}^2)(a^2+(\sqrt{2}b)^2+(\sqrt{3}c)^2).$$

2 TD d'algèbre

- Suites -

Définition 2.6. On appelle $u_0, \cdots, u_n \cdots$, où $u_k \in \mathbb{K}$ pour tout $k \in \mathbb{N}$ une suite à valeurs dans $\mathbb{K}$, notée (u_n) ou $(u_n)_{n\in\mathbb{N}}$. On peut en fait définir une suite $(u_n)_{n\in I}$ où I est inclus dans $\mathbb{N}$, éventuellement fini, mais c'est plus rare.

La méthode de résolution d'un exercice portant sur les suites est en général assez junglesque, mais il y a quelques idées à connaître. Il importe de chercher si :
• la suite étudiée est croissante ou décroissante,
• la suite à une **limite** : u_n se rapproche a d'une valeur l, éventuellement infinie, lorsque n tend vers l'infini (si $l \in \mathbb{R}$, on dit alors que (u_n) converge vers l),
• la suite est **périodique** : il existe $p \in \mathbb{N}$ tel que pour tout entier naturel n, $u_{n+p} = u_n$. Parfois, cette propriété n'est vraie qu'à partir d'un certain rang, et la suite est alors dite ultimement périodique. Une suite (ultimement) périodique de période 1 est dite **stationnaire**.
On dispose de quelques propriétés :

Proposition 2.7. Toute suite croissante majorée est convergente.
Toute suite décroissante minorée est convergente.
Toute suite périodique convergente est stationnaire.

Il existe de plus quelques types de suites assez particuliers :

Définition 2.8. Une suite de la forme $u_n = an + b$ avec $a, b \in \mathbb{R}$ est dite **arithmétique** de raison a.
Une suite de la forme $u_n = b \times a^n$ avec $a, b \in \mathbb{R}$ est dite **géométrique** de raison a.

Et il convient de noter quelques propriétés sommatoires :

Proposition 2.9. Soit $u_n := an + b$ pour tout $n \in \mathbb{N}$. On a $\sum_{n=0}^{N-1} u_n = a\frac{N(N-1)}{2} + Nb$.
Soit $u_n := ba^n$ pour tout $n \in \mathbb{N}$. On a $\sum_{n=0}^{N-1} u_n = b\frac{1-a^N}{1-a}$.

La démonstration, purement calculatoire, est laissée au bon plasir du lecteur.
On peut même envisager une sorte de mélange entre ces deux types de suites, abordé dans la rubrique suivante.

Suites et récurrence

On peut souvent démontrer une propriété voulue sur une suite, voire même trouver l'expression du terme général, en utilisant une récurrence. Cette récurrence s'exprime la plupart du temps sous forme de deux types d'équations. Le premier est une équation de la forme

$$u_{n+1} = f(u_n).$$

f est presque toujours continue, auquel cas

Proposition 2.10. si l est la limite de la suite (u_n) (qui n'en a pas forcément !), alors

$$f(l) = l$$

Exercice 1 Étudier la suite définie par $u_0 = 0$ et $u_{n+1} = \sqrt{12 + u_n}$ pour tout $n \in \mathbb{N}$.

Concernant le second type d'équations :

Définition 2.11. Soit (u_n) une suite réelle, on dit qu'elle satisfait une **équation de récurrence d'ordre k** (linéaire) lorsqu'il existe $k \in \mathbb{N}^*$ et des réels $a_0, \cdots, a_{k-1}$ tels que pour tout entier naturel n,

$$u_{n+k} + a_{k-1}u_{n+k-1} + \cdots + a_0 u_n = 0$$

Définition 2.12. L'équation $X^k + a_{k-1}X^{k-1} + \cdots + a_0 = 0$ est appelée **équation caractéristique**.

Exemple 2.13. Pour une suite arithmétique de raison a, $u_{n+1} - u_n = u_{n+2} - u_{n+1} = a$, donc $u_{n+2} - 2u_{n+1} + u_n = 0$ est une équation de récurrence vérifiée par u_n.
Pour une suite géométrique de raison a, $u_{n+1} - au_n = 0$.
Une suite **arithmético-géométrique** vérifie une relation de la forme : $u_{n+1} = au_n + b$, et on obtient l'équation de récurrence $u_{n+2} - (a+1)u_{n+1} + au_n = 0$

La résolution générale d'une telle équation de récurrence (dont la démonstration est inutile et fastidieuse dans notre cadre) utilise la notion de polynôme, abordée dans la section suivante. Contentons-nous des ordres 1 et 2 ici.

Proposition 2.14. Si pour tout $n \in \mathbb{N}$, $u_{n+1} - au_n = 0$, alors $u_n = u_0 a^n$.

Proposition 2.15. Si pour tout $n \in \mathbb{N}$, $u_{n+2} + a_1 u_{n+1} + a_0 u_n = 0$, on résout l'équation caractéristique du second degré $X^2 + a_1 X + a_0 = 0$.
• Si elle a deux solutions distinctes r_1 et r_2, alors : $u_n = c_1 r_1^n + c_2 r_2^n$, où c_1 et c_2 sont déterminées avec, par exemple, les valeurs de u_0 et u_1.
• Si elle a une racine double r, alors : $u_n = (an + b)r^n$, et encore une fois u_0 et u_1 permettent de déterminer a et b.

Sauriez-vous retrouver dans la propriété précédente où se cachent les suites arithmétiques, géométriques, et arithmético-géométriques ?

Exemple 2.16. Une suite géométrique correspond à une équation de récurrence d'ordre 1.
Une suite arithmétique correspond à une équation de récurrence d'ordre 2 ayant 1 pour racine double.
Une suite arithmético-géométrique de raison a correspond à une équation de récurrence d'ordre 2 dont les solutions sont 1 et a.

Tant de théorie prometteuse n'en appelle qu'avec plus de force des exercices permettant d'appliquer victorieusement ces nouvelles connaissances.
Exercice 2 Évariste doit monter un escalier de $n \geqslant 1$ marches. Pour ne pas trop se fatiguer, il décide à chaque pas de monter une ou deux marches à la fois, pas plus. De combien de manières différentes peut-il monter l'escalier ?

Les exercices suivants ne se rapportent pas nécessairement à un paragraphe précis du cours.

Exercice 3 Existe-t-il une suite d'entiers $(u_n)_{n\in\mathbb{N}^*}$ strictement croissante telle que pour tous entiers naturels n, m, on ait $u_{nm} = u_n + u_m$? Et simplement croissante ?

Exercice 4 On définit la suite (a_n) par $a_0 > 0$ et $a_{n+1} = \sqrt{a_n + 1}$ pour tout $n \in \mathbb{N}^*$. Montrer que la suite a au moins un terme irrationnel.

Et un petit classique pour la route :

Exercice 5 Soit (u_n) la suite définie par $u_0 = 5$ et $u_{n+1} = u_n + \frac{1}{u_n}$ pour $n \in \mathbb{N}$. Montrer que $u_{1000} > 45$.

- Polynômes -

Définition 2.17. • Soit $n \in N$, et $a_0, \cdots, a_n \in \mathbb{K}$, l'expression $P(X) = a_0 + \cdots + a_n X^n$ est un polynôme à coefficients dans $\mathbb{K}$. Si $a_n \neq 0$, condition presque systématiquement supposée réalisée dans la suite du cours, on dit que le polynôme est de degré n, ce qui s'écrit souvent $degP = n$.
• On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.
• Le coefficient a_n est appelé **coefficient dominant**. Si $a_n = 1$, le polynôme est dit **unitaire**.
• Le coefficient a_0 est souvent appelé "terme constant".
• Le terme $a_k X^k$ est appelé **monôme de degré k**.

Remarque 2.18. Une fonction polynôme associe à x (généralement un **réel** , on ne s'étendra pas ici au cas complexe) l'expression $P(x)$. Par la suite, on confondra classiquement et sans scrupules "polynôme" et "fonction polynôme".

Remarque 2.19. On a $P(0) = a_0$, petite relation très souvent utile. A noter aussi qu'en l'infini, le terme de coefficient dominant "écrase" tous les autres, d'où son nom (?) : le monôme $a_n x^n$ est arbitrairement plus grand que les autres.

Le fait que le terme dominant "écrase" les autres à l'infini et qu'un polynôme non constant diverge en $+\infty$ ou $-\infty$ permet d'établir le théorème essentiel suivant :

Théorème 2.20. L'écriture d'un polynôme est unique ! Si on a deux expressions pour un même polynôme, alors on peut identifier coefficient par coefficient.

On s'aperçoit qu'en additionnant ou multipliant des polynômes, on obtient encore des polynômes. Et,

Proposition 2.21. Soit $P, Q \in \mathbb{K}[X]$. On a $deg(P + Q) \leqslant max(degP, degQ)$ et $deg(PQ) = degP + degQ$.

Division euclidienne

Tout comme les entiers naturels, les polynômes de $\mathbb{K}[X]$ forment un ensemble (un algébriste dirait un anneau) muni d'une division euclidienne, donc avec un reste :

Proposition 2.22. Si $P, Q \in \mathbb{K}[X]$, il existe $S, R \in \mathbb{K}[X]$ tels que

$$P = SQ + R$$

et $\deg R < \deg Q$. Et bien sûr, si $R = 0$, on dit que Q divise P.

Remarques 2.23. Ici, c'est donc le degré du polynôme qui joue plus ou moins le rôle de l'entier naturel de la division euclidienne habituelle.
Les polynômes de degré 0 sont les fonctions constantes, excepté $P = 0$, le polynôme nul, qui est de degré $-\infty$.

L'exercice suivant permet de se familiariser avec l'application de la division euclidienne : si $\deg P < \deg Q$, $S = 0$ et $R = P$, sinon, si $P = a_p X^p + \cdots + a_0$ et $Q = b_q X^q + \cdots + b_0$, le premier terme de S est $\frac{a_p}{b_q} X^{p-q}$, et on continue en divisant $P - \frac{a_p}{b_q} X^{p-q} Q$ par Q.

Exercice 6 Effectuer la division euclidienne de $2X^3 + 5X^2 + 6X + 1$ par $X^2 - 3X + 2$.

Racines d'un polynôme

On s'aperçoit qu'une expression factorisée de la forme $a_n(X - r_1) \cdots (X - r_n)$ constitue également un polynôme (on verra ultérieurement comment relier les r_i aux coefficients a_i dudit polynôme). Elle a **l'avantage d'être très maniable** : on identifie notamment les points où elle s'annule, qui sont alors les r_i.

Définition 2.24. On appelle **racine** (réelle) d'un polynôme P un réel r tel que $P(r) = 0$. Leur recherche est quasi-obsessionnelle lorsqu'on étudie un polynôme.

Remarque 2.25. On exclura dans les énoncés suivants le cas du polynôme nul, dont tout réel est racine.

Notons le théorème fondamental suivant :

Théorème 2.26. Soit P un polynôme de degré n. Il admet exactement n racines complexes (non nécessairement distinctes), donc au plus n racines réelles.

La démonstration est hors de notre propos, l'intérêt est de majorer le nombre de racines éventuelles. Parfois, on peut au contraire le minorer :
Exercice 7 Montrer qu'un polynôme de degré impair a au moins une racine réelle.

On peut voir ce théorème différement :

Proposition 2.27. Un polynôme de degré au plus n ayant au moins $n + 1$ racines est le polynôme nul (tous ses coefficients sont nuls).

La propriété suivante est d'une grande utilité :

Proposition 2.28. Soit P un polynôme dont a est une racine. Il existe un polynôme Q tel que $P = (X - a)Q$.

Ceci se démontre en divisant euclidiennement P par $X - a$. Obtenir des racines d'un polynôme permet ainsi de le factoriser. Certaines racines peuvent "plus" diviser le polynôme que d'autres :

Définition 2.29. Soit P un polynôme, on appelle racine k-ième de P un réel a tel que $(X-a)^k$ divise P, mais pas $(X-a)^{k+1}$. On dit que la **multiplicité** de ladite racine est k.

Exemple 2.30. Pour le degré 2, si $P(X) = aX^2 + bX + c$, on distingue 3 cas :
-si le discriminant $\Delta := b^2 - 4ac < 0$, il n'y a pas de racine réelle.
-si $\Delta = 0$, il y a une racine réelle double.
-si $\Delta > 0$, il y a deux racines réelles simples.

Exercice 8 Soit P un polynôme de degré 2008 tel que pour tout entier $k \in \{1, \cdots 2009\}$, $P(k) = \frac{1}{k}$. Calculer $P(0)$.

Polynômes symétriques élémentaires

On aborde ici la relation évoquée entre les coefficients et les racines d'un polynôme : on considère le polynôme

$$P(X) = a_n X^n + \cdots + a_0 = a_n(X - r_1)\cdots(X - r_n)$$

Définition 2.31. Le k-ème polynôme symétrique élémentaire est défini par

$$\sigma_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} r_{i_1} \cdots r_{i_k}$$

Théorème 2.32. Formule de Viète Pour $0 \leqslant k \leqslant n$,

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Démonstration. On développe l'expression factorisée de P et on regroupe les termes faisant intervenir X^{n-k}. □

Remarque 2.33. Une fois les racines fixées, les polynômes symétriques élémentaires sont uniques. Réciproquement, une fois les polynômes symétriques fixés, les racines sont déterminées à permutations près. On a ainsi un autre moyen de manipuler les racines d'un polynôme.

Exemple 2.34. Pour le degré 2, si $P(X) = ax^2+bx+c = a(x-r_1)(x-r_2)$, alors $\sigma_1 = r_1+r_2 = -\frac{b}{a}$ et $\sigma_2 = r_1 r_2 = \frac{c}{a}$.

À présent, exerçons-nous !
Exercice 9 Exprimer $x^3+y^3+z^3-3xyz$ en fonction des polynômes symétriques élémentaires.

Exercice 10 Soit $A = \sqrt[3]{5-2\sqrt{13}} + \sqrt[3]{5+2\sqrt{13}}$. Simplifier cette expression.

Factorisation des polynômes

On a vu que, pour factoriser un polynôme, on pouvait en chercher ses racines. Ce n'est pas toujours possible ; de plus, ces racines ne sont pas forcément dans l'ensemble de départ considéré ($\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, etc.). Dans certains cas, aucune factorisation (à multiplication par un terme constant près) n'est envisageable !

Définition 2.35. On dit que $P \in \mathbb{K}[X]$ est irréductible sur $\mathbb{K}$ lorsque toute expression de P sous la forme $Q \times R$ avec $Q, R \in \mathbb{K}[X]$ entraîne que Q ou R soit de degré 0.

Exemple 2.36. Le polynôme X^2+1 est irréductible sur $\mathbb{R}$: sinon, il s'écrirait $(X-a)(X-b)$ avec a, b réels. Ceci n'est pas possible, car ses racines i et $-i$ sont complexes mais non pas réelles.

Remarque 2.37. Si $\mathbb{K} \subset \mathbb{L}$, il est clair que tout polynôme réductible sur $\mathbb{K}$ l'est sur $\mathbb{L}$, mais la réciproque n'est pas toujours vraie, comme en atteste l'exemple suivant.

Exemple 2.38. Le polynôme X^2-2 est irréductible sur $\mathbb{Z}$ et $\mathbb{Q}$, mais pas sur $\mathbb{R}$, ses racines étant $\pm\sqrt{2}$.

On peut conjecturer que **pour un polynôme à coefficients entiers** la réductibilité est la même sur $\mathbb{Z}$ ou sur $\mathbb{Q}$, et en effet,

Théorème 2.39. Tout polynôme de $\mathbb{Z}[X]$ est réductible sur $\mathbb{Z}$ si et seulement s'il l'est sur $\mathbb{Q}$.

Démonstration. Soit $P \in \mathbb{Z}[X]$. S'il est réductible sur $\mathbb{Z}$, il l'est sur $\mathbb{Q}$. Réciproquement, supposons que l'on aie $P = RS$ avec $R, S \in \mathbb{Q}[X]$. Soit $a, b \in \mathbb{Z}$ tels que $aR, bS \in \mathbb{Z}[X]$.
Pour tout polynôme $p \in \mathbb{Z}[X]$, on note $c(p)$ le pgcd de ses coefficients : le lecteur pourra vérifier que $c(pq) = c(p)c(q)$.
Alors $c(aR)c(bS) = c(abP) = ab \times c(P)$. Donc $P = R'S'$ avec $R' = c(P)\frac{aR}{c(aR)}$ et $S' = \frac{bS}{c(bS)}$, qui sont bien sûr des polynômes à coefficients entiers. □

Pour tester la réductibilité sur $\mathbb{Z}$, on dispose d'un critère incomplet :

Théorème 2.40. Critère d'Eisenstein : Soit $P = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$, s'il existe un nombre premier p divisant tous les a_i sauf a_n, et tel que p^2 ne divise pas a_0, alors P est irréductible sur $\mathbb{Z}$.

Démonstration. Supposons par l'absurde que $P = QR$ avec $Q = b_qX^q + \cdots + b_0$ et $R = c_rX^r + \cdots + c_0$, $q, r > 1$. Sans perte de généralité, comme p, et non pas p^2, divise $a_0 = b_0c_0$: p divise b_0 et pas c_0. Et, $a_n = b_qc_r$ donc p ne divise pas b_q.
Soit alors i_0 le plus grand indice tel que si $i \leqslant i_0$, $p|b_i$. On a :

$$a_{i_0+1} = b_0c_{i_0+1} + \cdots + b_{i_0+1}c_0$$

et $p|a_{i_0+1}$ donc $p|c_0$: contradiction. □
Une petite application astucieuse, qui demande de (modestes) connaissances arithmétiques :
Exercice 11 Soit p un nombre premier, montrer que le polynôme $1 + X + \cdots + X^{p-1}$ est irréductible sur $\mathbb{Z}$.

Exercice 12 Soit $n \in \mathbb{N}^*$ et $a_1, \cdots, a_n$ des entiers relatifs distincts. Montrer que le polynôme

$$P(X) = 1 + \prod_{i=1}^{n} (X - a_i)$$

est irréductible sur $\mathbb{Z}$.

- Solutions des exercices -

Suites

Solution de l'exercice 1

On constate, par une récurrence rapide, que la suite est bornée par 4. On montre de même par récurrence sur n que $u_{n+1} > u_n$: l'initialisation se vérifie avec $u_1 = \sqrt{12} > 0 = u_0$. Si on suppose $a_{n+1} > a_n$, il vient $a_{n+2} = \sqrt{12 + a_{n+1}} >= a_{n+1}$, ce qui clôt la récurrence.
La suite est croissante et majorée, elle admet donc une limite l. La fonction $x \to \sqrt{12+x}$ est continue donc $l = \sqrt{12+l}$, soit $l^2 - l - 12 = 0$. L'unique solution positive de cette équation est 4, qui est donc la limite de la suite.

Solution de l'exercice 2

On note u_n le nombre de manières différentes de monter un escalier de n marches. Si $n \geqslant 3$, pour la première marche, soit on la franchit seule, ce qui laisse u_{n-1} possibilités, soit on en monte 2 à la fois, ce qui laisse u_{n-2} autres possibilités. L'équation de récurrence obtenue est donc

$$u_{n+2} - u_{n+1} - u_n = 0$$

pour tout $n \in \mathbb{N}^*$. L'équation caractéristique associée $X^2 - X - 1 = 0$ a pour solutions $\Phi = \frac{1+\sqrt{5}}{2}$ et $\varphi = \frac{1-\sqrt{5}}{2}$, donc pour $n \in \mathbb{N}^*$,

$$u_n = A\Phi^n + B\varphi^n.$$

Avec $u_1 = 1$ et $u_2 = 2$, on trouve : $A = \frac{1+\sqrt{5}}{2\sqrt{5}}$ et $B = \frac{\sqrt{5}-1}{2\sqrt{5}}$.

Solution de l'exercice 3

• Si (u_n) est strictement croissante, on a pour tout $n \geqslant 1$: $u_{n+1} \geqslant u_n + 1$ donc $u_2 = u_{2n} - u_n \geqslant n$, ce qui est absurde pour $n > u_2$. Donc une telle suite n'existe pas.
• Si (u_n) est simplement croissante, c'est plus délicat. La suite nulle est clairement solution. Pour montrer que c'est la seule solution, on raisonne de nouveau par l'absurde et on suppose $u_k > 0$ pour un certain k. On sait que la suite ne peut être strictement croissante, donc il existe $m \in \mathbb{N}^*$ tel que $u_m = u_{m+1}$. Le lecteur prouvera par récurrence sur $j \geqslant 1$ que

$$u_{n^j} = j \times u_n.$$

De ceci résulte que pour tout $j \in \mathbb{N}^*$, $u_{m^j} = u_{(m+1)^j}$.
Or, $\frac{m+1}{m} > 1$, donc pour un certain $i \in \mathbb{N}^*$, $(m+1)^i \geqslant m^i \times k$ et, par croissance de la suite,

$$u_{(m+1)^i} \geqslant u_{m^i} + u_k > u_{m^i},$$

d'où une contradiction.

Solution de l'exercice 4
Supposons par l'absurde que pour tout $n \in \mathbb{N}$, a_n est rationnel, ce que l'on écrit $a_n = \frac{p_n}{q_n}$ avec $p_n \in \mathbb{Z}$, $q_n \in \mathbb{Z}^*$ premiers entre eux. On a :

$$\frac{p_{n+1}^2}{q_{n+1}^2} = \frac{p_n + q_n}{q_n}$$

et $p_n + q_n$ et q_n sont premiers entre eux, et p_{n+1}^2 et q_{n+1}^2 aussi, donc on peut identifier le numérateur et le dénominateur des deux fractions (au signe près). Il en résulte que $|\sqrt{q_n}| = |q_{n+1}|$ et finalement : $|q_n| = \sqrt[1/2n]{|q_0|} \in \mathbb{N}^*$ pour tout entier naturel n. On en déduit que $|q_0| = 1 = |q_n|$ autrement dit, la suite est constituée d'entiers, qui sont alors positifs (car racines carrées de réels). Or $a_1 > 1$ donc $a_n > 1$ par récurrence, soit $a_n \geqslant 2$, auquel cas on vérifie que $a_n > \sqrt{1 + a_n} = a_{n+1}$. Donc (a_n) est une suite infinie décroissante d'entiers strictement positifs, ce qui est impossible.
Conclusion : la suite admet un terme irrationnel.

Solution de l'exercice 5 La suite (u_n) étant clairement à termes positifs, il suffit de montrer que $u_{1000}^2 > 2025$. Or,

$$u_{n+1}^2 = u_n^2 + 2 + \frac{1}{u_n^2} > u_n^2 + 2$$

Donc $u_{1000}^2 > 1000 \times 2 + u_0 = 2025$.
Il est naturel d'être frustré et bluffé par une telle solution. Pour ceux qui voudraient un petit peu plus de réflexion et de calcul, on peut explorer les cas $u_0 = 4, 3$, etc.

Polynômes

Solution de l'exercice 6
Avec les notations du cours : $S = 2X + 11$ et $R = 35X - 21$.

Solution de l'exercice 7
En $+\infty$ et $-\infty$, le polynôme a des limites infinies (car non constant) et de signes opposés (car c'est le terme dominant qui l'emporte à l'infini, et c'est une puissance impaire). D'après le théorème des valeurs intermédiaires, un polynôme étant continu, le polynôme a une racine réelle.

Solution de l'exercice 8
On cherche un polynôme proche de P que l'on puisse déterminer en utilisant ses racines. Si $1 \leqslant k \leqslant 2009$, on a :

$$kP(k) - 1 = 0,$$

donc si on pose $Q(X) = XP(X) - 1$, Q est de degré 2009, donc on a trouvé toutes ses racines et il existe $A \in \mathbb{R}$ tel que

$$Q(X) = A(X-1)\cdots(X-2009).$$

En faisant $X = 0$ on trouve $-1 = A \times (-1)^{2009} \times 2009!$, donc $A = \frac{1}{2009!}$. On a donc

$$P(X) = \frac{2009! + (X-1) + \cdots (X-2009)}{2009!X}$$

(pour avoir un polynôme, on a bien pris soin par le choix de A que le dénominateur divise le numérateur !). On cherche $P(0)$ qui est le terme constant, donc on cherche le terme de degré 1 dans le numérateur. En développant, il vient :

$$P(0) = \frac{2009!/2009 + 2009!/2008 + \cdots + 2009!/1}{2009!}$$

donc $P(0) = \sum_{k=1}^{2009} \frac{1}{k}$.

Solution de l'exercice 9
On obtient $x^3 + y^3 + z^3 = \sigma_1(\sigma_1^2 - \sigma_2)$.

Solution de l'exercice 10
On pose $a = \sqrt[3]{5 - 2\sqrt{13}}$ et $b = \sqrt[3]{5 + 2\sqrt{13}}$. On a

$$\begin{aligned} A^3 &= a^3 + b^3 + 3ab(a + b) \\ A^3 &= 10 + 3\sqrt[3]{25 - 52}A \\ A^3 &= 10 - 9A \\ A^3 + 9A - 10 &= 0 \end{aligned}$$

On a affaire à un polynôme de degré 3 dont 1 est racine évidente. On factorise :

$$A^3 + 9A - 10 = (A - 1)(A^2 + A + 10)$$

Le polynôme de degré 2 ci-dessus n'a pas de racine réelle, on en déduit $A = 1$.

Solution de l'exercice 11
Selon la subtile suggestion de l'enchaînement du cours, l'application du critère d'Eisenstein avec le nombre premier p permet de résoudre le problème. Notons déjà que l'on peut écrire $P(X) = \frac{X^p - 1}{X - 1}$ puisqu'il s'agit d'une somme géométrique. Pour faire apparaître p, on procède (astuce suprême) à un petit changement de variable en posant $Y = X - 1$ et en développant avec le binôme de Newton :

$$P(Y) = \frac{(Y + 1)^n - 1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}$$

On vérifie aisément que $P(Y)$ se factorise dans $\mathbb{Z}[Y]$ si et seulement si $P(X)$ se factorise dans $\mathbb{Z}[X]$. Notons donc, pour $0 \leqslant k \leqslant p - 1$, $c_k = \binom{p}{k+1}$. On a $c_0 = p$, donc il est divisible par p, et pas par p^2. $c_{p-1} = 1$ qui n'est pas multiple de p. Il reste donc à prouver que pour $2 \leqslant k \leqslant p-1$, $p | \binom{p}{k}$. Or,

$$p! = \binom{p}{k} \times ((p - k)!k!).$$

Or p, premier, divise $p!$ et non pas $(p - k)!k!$, donc par le lemme d'Euclide, $p | \binom{p}{k}$, ce qui (par)achève la démonstration.

Solution de l'exercice 12
Remarquons que sans perte de généralité, quitte à permuter les a_i, on peut supposer que

$$a_1 < \cdots < a_n.$$

Une fois n'est pas coutume, on raisonne par l'absurde. Supposons que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$. P étant de degré n, Q et R sont de degré au plus $n-1$. Pour tout i, $Q(a_i)R(a_i) = 1$, donc $Q(a_i) = R(a_i) = \pm 1$. Autrement dit, le polynôme $R - Q$ a au moins n racines distinctes, or il est de de degré au plus $n-1$ (car c'est le cas de R et Q). Donc $R - Q = 0$, donc $P = R^2 + 1$. Il en découle que pour tout réel x :

$$P(x) - 1 = R^2(x) \geqslant 0.$$

Or $P - 1$ change de signe (sans s'annuler) entre $]-\infty, a_1[$ et $]a_1, a_2[$: contradiction. Donc P est irréductible sur $\mathbb{Z}$.
Remarque : on a supposé à la fin du raisonnement que $n \geqslant 2$, mais si $n = 1$, un polynôme de degré 1 est toujours irréductible.

3 Groupe C : polynômes

1 Cours de polynômes

- Opérations sur les polynômes -

On commence par définir la notion de polynôme et voir quelques propriétés.

Définition 3.1. Une fonction P de $\mathbb{R}$ dans $\mathbb{R}$ est appelée polynôme à coefficient réels (abrégé en polynôme dans ce qui suit) s'il existe des nombres réels $a_0, \dots, a_n$ tels que pour tout $x \in \mathbb{R}$:

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Si $a_n \neq 0$, on dit que le degré de P, noté $\deg P$, vaut n. On décrète que le degré du polynôme nul est $-\infty$. Dans ce cas, a_n est appelé le coefficient dominant de P. Si le coefficient dominant de P vaut 1, on dit que ce polynôme est unitaire. On note $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients réels. De même, on note $\mathbb{Q}[X]$ l'ensemble des polynômes à coefficients rationnels et $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients entiers.

Dans ce qui suit, nous ne ferons pas de distinction entre polynôme et fonction polynômiale associée. Il faudrait la faire en toute rigueur, mais plutôt que de rendre l'exposition abstraite, nous préférons insister sur les idées sous-jacentes. Voir l'appendice situé à la fin du cours pour plus de détails.

On notera indifféremment $P(x)$ ou $P(X)$ ou encore P.

Exemple 3.2. La fonction $P(x) = \sqrt{2} - 2x + \pi x^2$ est un polynôme de degré 2 de coefficient dominant π. La fonction $Q(x) = |x|$ n'est pas un polynôme (pourquoi ?).

Remarque 3.3. Par convention, le degré du polynôme nul est $-\infty$. Ainsi, les polynômes de degré zéro sont exactement les fonctions constantes non nulles.

Proposition 3.4. Soient P, Q deux polynômes. Alors $P + Q$ et $P \times Q$ sont également deux polynômes.

Démonstration. Pour $P + Q$ il suffit d'utiliser le fait que $\alpha x^i + \beta x^i = (\alpha + \beta) x^i$ pour un nombre réel x, et pour $P(x) \times Q(x)$, il suffit de développer le produit. □

Exemple 3.5. Pour tout réel a et tout entier positif n, $P(x) = (x - a)^n$ est un polynôme de degré n.

Proposition 3.6. Soient P, Q deux polynômes. Alors $\deg(P + Q) \leqslant \max(\deg P, \deg Q)$ et $\deg(P \times Q) = \deg P + \deg Q$ (avec la convention $-\infty + \alpha = -\infty$ pour que cet énoncé soit valable si l'un des deux polynômes est nul).

Démonstration. On vérifie aisément que $\deg(P + Q) = \deg P$ si $\deg P > \deg Q$, que $\deg(P + Q) = \deg Q$ si $\deg Q > \deg P$ et que si $\deg P = \deg Q$, alors $\deg(P + Q) \leqslant \deg P$. Il peut cependant ne pas y avoir égalité (prendre par exemple $P(x) = x^2$ et $Q(x) = -x^2$).

La deuxième partie de la proposition découle du fait que si a_n est le coefficient dominant de P et b_m est le coefficient dominant de Q, alors $a_n b_m$ est le coefficient dominant de PQ. □

Exemple 3.7. Soit E un ensemble fini et $f : E \to \mathbb{N}$ une application. Alors

$$P(x) = \sum_{\alpha \in E} x^{f(\alpha)}$$

est un polynôme à coefficients entiers. Si k_n désigne le nombre nombre d'éléments $\alpha \in E$ tels que $f(\alpha) = n$, alors le coefficient devant x^n est égal à k_n. Le polynôme P est appelé fonction génératrice associée à f. Ce genre de polynômes apparaissent fréquemment en combinatoire, où il arrive qu'on ne connaisse pas de formule explicite pour k_n, bien que le polynôme P se calcule aisément (voir exercice 30). L'intérêt d'introduire cette fonction génératrice est que la connaissance du polynôme P nous permet alors d'accéder à certaines informations (par exemple des formules de récurrence ou un comportement asymptotique).

- Division euclidienne et racines -

Dans cette partie, notre but est d'expliquer en quoi la connaissance des racines d'un polynôme P, c'est-à-dire des éléments x tels que $P(x) = 0$, donne des informations sur P. On commence par montrer qu'il existe une notion de division euclidienne de polynômes très similaire à celle des entiers.

Division euclidienne de polynômes Ici, et dans tout ce qui suit, $\mathbb{K}$ désigne $\mathbb{Q}$ ou $\mathbb{R}$.

Théorème 3.8. Soient $P, U \in \mathbb{K}[X]$ avec $\deg U \geqslant 1$. Alors il existe un unique couple de polynômes $Q, R \in \mathbb{K}[X]$ tels que :

$$P = QU + R \qquad \text{et} \qquad \deg(R) \leqslant \deg(U) - 1.$$

Démonstration. Pour l'existence, on applique l'algorithme vu en cours en abaissant à chaque étape le degré de P. Plus précisément, on pose $P_0 = P$ et $Q_0 = 0$. On commence à l'étape 0 et voici ce qu'on fait à l'étape k : notons d_k degré de P_k et c_k son coefficient dominant. Notons également n le degré de U et u_n son coefficient dominant. Si $\deg(P_k) \leqslant \deg(U) - 1$, on arrête l'algorithme en prenant $Q = Q_k$ et $R = P_k$. Sinon, on pose :

$$P_{k+1} = P_k - \frac{c_k}{u_n} X^{d_k - n} U \qquad \text{et} \qquad Q_{k+1} = Q_k + \frac{c_k}{u_n} X^{d_k - n}.$$

On passe ensuite à l'étape $k+1$. L'algorithme se termine bien car le degré de P_k est au plus $\deg P - k$, et les polynômes Q et R donnés par l'algorithme vérifient les conditions requises.

Pour l'unicité, supposons par l'absurde qu'il existe deux tels couples Q, R et Q', R'. Alors $QU + R = Q'U + R'$. En particulier, $Q \neq Q'$, car sinon on a aussi $R = R'$. Cela implique également :

$$U(Q - Q') = R' - R.$$

Or, d'après la proposition 3.6, le degré du terme de gauche et supérieur ou égal à celui de U et celui de droite est inférieur ou égal à $\deg(U) - 1$, ce qui est contradictoire et conclut la démonstration. □

Exemple 3.9. La division euclidienne de $X^5 - 3X + 2X + 1$ par $X^3 + 3X^2 - 2X - 1$ est :

$$X^5 - 3X^3 + 2X + 1 = (X^2 - 3X + 8)(X^3 + 3X^2 - 2X - 1) + \left(-29X^2 + 15X + 9\right).$$

Remarque 3.10. La division euclidienne telle quelle est fausse pour des polynômes à coefficients entiers. Par exemple, il n'existe pas de $Q \in \mathbb{Z}[X]$ tel que $3x^2+1 = Q(x)(2x+1)$ (comparer les coefficients dominants). En revanche, en reproduisant la démonstration précédente, si $P, U \in \mathbb{Z}[X]$ **et que le coefficient dominant de** U **est** 1, alors si $\deg U \geqslant 1$, il existe il existe un unique couple de polynômes $Q, R \in \mathbb{K}[X]$ tels que :

$$P = QU + R \qquad \text{et} \qquad \deg(R) \leqslant \deg(U) - 1.$$

En effet, dans la preuve précédente, il a fallu diviser par « u_n ». Or, lorsqu'on divise par des éléments de $\mathbb{Z}$, on ne reste pas dans $\mathbb{Z}$. Ceci explique un peu d'ailleurs pourquoi la théorie des polynômes à plusieurs variables est plus compliquée que celle des polynômes à une variable. En effet, on peut par exemple voir les polynômes réels à deux variables comme les polynômes en y à coefficients dans $\mathbb{R}[X]$. Mais, de même que dans $\mathbb{Z}$, tous les éléments de $\mathbb{R}[X]$ ne sont pas inversibles.

Définition 3.11. Soient $P, Q \in \mathbb{K}[X]$ avec P non nul. On dit que P divise Q s'il existe $R \in \mathbb{K}[X]$ tel que $Q = PR$.

Ainsi, P divise Q si le reste de la division euclidienne de Q par P vaut 0.

Exemple 3.12. Trouvons le reste de la division euclidienne de $A(x) = x^{2013} + 2013$ par $B(x) = x - 1$. Par division euclidienne, on écrit $A(x) = Q(x)B(x) + R(x)$ avec $R(x)$ un polynôme de degré au plus 0. Ainsi R est un polynôme constant qu'on notera c. Autrement dit, $A(x) = Q(x)B(x) + c$ et il nous reste à trouver la valeur de c. Prenons $x = 1$: $A(1) = Q(1)B(1) + c$. Or, $B(1) = 0$. On en déduit que $c = A(1) = 2014$.

Exercice 1 Trouver le reste de la division euclidienne de $x^{100} - 2x^{51} + 1$ par $x^2 - 1$.

Racines et factorisation de polynômes Nous voyons ici que la connaissance des racines d'un polynôme permet de le factoriser. Rappelons que $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{Q}$.

Définition 3.13. Un élément $x \in \mathbb{K}$ est appelé *racine* d'un polynôme $P \in \mathbb{K}[X]$ si $P(x) = 0$.

Exemple 3.14. Le polynôme réel $X^2 - 1$ a deux racines réelles, qui sont 1 et -1. Le polynôme X^2+1 n'a pas de racine réelle. Le polynôme réel X^2-2 a deux racines réelles, mais le polynôme à coefficients rationnels $X^2 - 2$ n'a pas de racines rationnelles car $\sqrt{2}$ est irrationnel. Si $a \in \mathbb{K}$, le polynôme $(X-1)^{2012}$ est de degré 2012 mais n'a qu'une seule racine qui est 1.

Le théorème suivant est très important et doit être connu.

Théorème 3.15. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Les deux propositions suivantes sont équivalentes :

1. a est racine de P, autrement dit $P(a) = 0$.
2. Il existe un polynôme $Q \in \mathbb{K}[X]$ tel que :

$$P(x) = Q(x)(x - a).$$

Démonstration. Il est clair que le deuxième point implique le premier. Quant à la réciproque, le point clé est d'utiliser la division euclidienne. En effet, supposons que $P(a) = 0$. Écrivons alors la division euclidienne de P par $X - a$ sous la forme $P(x) = Q(x)(x - a) + R(x)$ avec R un polynôme de degré au plus $1 - 1 = 0$. Ainsi, R est un nombre réel, noté c. Bref, $P(x) = Q(x)(x - a) + c$. Évaluons cette quantité en $x = a$: $0 = P(a) = Q(a)(a - a) + c$. Donc $c = 0$, ce qu'on voulait démontrer. □

Théorème 3.16. Un polynôme de degré n a au plus n racines différentes.

Démonstration. Par l'absurde, soit $P \in \mathbb{R}[X]$ de degré n ayant au moins $n+1$ racines différentes, notées $r_1, \ldots, r_{n+1}$. D'après le théorème précédent, il existe un polynôme Q tel que $P(x) = Q(x)(x - r_1)$. Mais alors, pour $2 \leqslant i \leqslant n + 1$, $0 = P(r_i) = Q(r_i)(r_i - r_1)$. Comme $r_i - r_1 \neq 0$, ceci impose $Q(r_i) = 0$. On recommence ce raisonnement avec Q pour finalement obtenir l'existence d'un polynôme T tel que $P(x) = T(x)(x - r_1) \cdots (x - r_{n+1})$. Alors d'après la proposition 3.6 :

$$n = \deg(P) = \deg T + n + 1 > n,$$

ce qui est absurde. □

Remarque 3.17. Il existe des polynômes qui n'ont pas de racines réelles, par exemple $P(x) = x^4 + 1$.

Ce théorème important implique quelques corollaires donnant une information concernant le polynôme sachant quelque chose sur ses racines.

Corollaire 3.18. Soit $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polynôme de degré n. On suppose qu'il a n racines différentes $r_1, \ldots, r_n$. Alors :

$$P(x) = a_n(x - r_1) \cdots (x - r_n).$$

Démonstration. En reprenant la démonstration précédente, on voit qu'il existe un polynôme T tel que $P(x) = T(x)(x - r_1) \cdots (x - r_n)$. En comparant les degrés des termes de gauche et de droite, il vient que T est de degré nul, donc un nombre réel. En regardant le coefficient dominant des deux côtés de l'égalité, on trouve que $T(x) = a_n$. □

Corollaire 3.19. Un polynôme de degré au plus n ayant $n + 1$ racines est nul. Ainsi, un polynôme ayant une infinité de racines est forcément le polynôme nul.

Exercice 2 En utilisant le corollaire précédent, retrouver le fait que $Q(x) = |x|$ n'est pas un polynôme.

On en déduit le résultat important suivant.

Proposition 3.20. Soient $a_0, a_1, \ldots, a_n$ et $b_0, b_1, \ldots, b_m$ des nombres réels. On suppose que pour tout nombre réel x :

$$a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n = b_0 + b_1 x + \cdots + b_m x^m.$$

Alors $m = n$ et pour tout i entre 0 et n on a $a_i = b_i$.

Démonstration. Soit $P(x) = a_0 + a_1x + a_2x^2 + \cdots a_nx^n - (b_0 + b_1x + \cdots + b_mx^m)$, qui est un polynôme à coefficients réels. Par hypothèse, ce polynôme a une infinité de racines ; il est donc nul ! □

Exemple 3.21. Soit P un polynôme de degré 2013 vérifiant $P(k) = k$ pour $k = 1, 2, \ldots, 2013$ et $P(0) = 1$. Trouvons $P(-1)$.

Le polynôme $P(x) - x$ est de degré 2013 et admet 2013 racines qui sont $k = 1, 2, \ldots, 2013$. On a donc forcément

$$P(x) - x = c \cdot (x-1)(x-2)\cdots(x-2013)$$

avec c un nombre réel. En évaluant en $x = 0$, il vient $1 = P(0) = -c \cdot 2013!$, de sorte que $c = -1/2013!$. D'où

$$P(-1) = -1 + \frac{2014!}{2013!} = 2013.$$

Pour conclure cette partie, prouvons la propriété utile suivante en identifiant les coefficients.

Proposition 3.22. Soit P un polynôme tel que $P(x)^2$ soit un polynôme en x^2 (c'est-à-dire qu'il existe un polynôme R tel que $P(x)^2 = R(x^2)$. Alors il en est de même de $P(x)$ ou de $P(x)/x$ (c'est-à-dire qu'il existe un polynôme Q tel que soit $P(x) = Q(x^2)$, soit $P(x) = xQ(x^2)$).

Démonstration. Écrivons $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ avec $a_n \neq 0$. Comme $P(x)^2 = R(x^2)$, le coefficient devant x^{2n-1} dans $P(x)^2$, à savoir $2a_na_{n-1}$, est nul. On en déduit que $a_{n-1} = 0$. De même, le coefficient devant x^{2n-3} dans $P(x)^2$, à savoir $2a_na_{n-3}$, est nul. On en déduit que $a_{n-3} = 0$. De même, on obtient que $a_{n-2k-1} = 0$ pour $n-2k-1 \geqslant 0$. Le résultat en découle. □

Pour illustrer cette propriété, on pourra chercher l'exercice suivant.

Exercice 3 Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que $16P(x^2) = P(2x)^2$.

Racines multiples et polynôme dérivé Doit-on dire que le polynôme $P(x) = (x-1)^n$ a une seule racine, ou bien n racines qui sont les mêmes ? Pour ne pas faire de confusion, nous traitons le cas des racines multiples.

Définition 3.23. Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et un entier $m \in \mathbb{N}^*$. On dit que α est racine de multiplicité m de P s'il existe $Q \in \mathbb{K}[X]$ tel que $P(x) = (x-\alpha)^mQ(x)$ et s'il n'existe pas $Q \in \mathbb{K}[X]$ tel que $P(x) = (x-\alpha)^{m+1}Q(x)$. On dit que α est une racine multiple si $m \geqslant 2$.

Il se trouve qu'on dispose d'un critère assez pratique permettant de reconnaître une racine multiple.

Définition 3.24. Soit $P = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{K}[X]$. On définit le polynôme dérivé P' par $P'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$.

La proposition suivante, réminiscente des propriétés de l'opérateur de dérivation sur les fonctions réelles dérivables, est fondamentale.

Proposition 3.25. Pour $P, Q \in \mathbb{K}[X]$, on a :

$$(PQ)' = PQ' + P'Q.$$

Proposition 3.26. Soient $a \in \mathbb{K}$ et $n \geqslant 1$ un entier. Soit $P(x) = (x-a)^n$. La dérivée de P est $P'(x) = n(x-a)^{n-1}$.

Démonstration. Prouvons cela par récurrence sur n. Pour $n = 1$, le polynôme dérivé de $x - a$ est bien 1. Supposons le résultat acquis au rang n, montrons-le au rang $n+1$. Soit $Q(x) = (x-a)^{n+1}$. En écrivant $(x-a)^{n+1} = (x-a)(x-a)^n$, on obtient

$$Q'(x) = (x-a)^n + (x-a)\left((x-a)^n\right)'.$$

Donc par hypothèse de récurrence, $Q'(x) = (x-a)^n + (x-a)\cdot(n-1)(x-a)^n = n(x-a)^n$. Ceci conclut la récurrence et la preuve de la proposition. □

Théorème 3.27. Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$. Alors α est une racine multiple de P si, et seulement si, $P'(\alpha) = 0$.

Démonstration. Dans le sens direct, écrivons $P(x) = (x-\alpha)^m Q(x)$ avec $m \geqslant 2$ et $Q \in \mathbb{K}[X]$. En dérivant cette expression, il vient $P'(x) = m(x-\alpha)^{m-1}Q(x) + (x-\alpha)^m Q'(x)$. En prenant $x = \alpha$, on conclut que $P'(\alpha) = 0$.

Pour la réciproque, supposons que $P'(\alpha) = 0$ et raisonnons par l'absurde en supposant que α soit une racine non multiple de P. Alors P s'écrit $P(x) = (x-\alpha)Q(x)$ avec $Q(\alpha) \neq 0$ (si $Q(\alpha) = 0$, d'après le théorème 3.15, on pourrait écrire $P(x) = (x-\alpha)^2 R(X)$). En dérivant cette expression, il vient $P'(x) = Q(x) + (x-\alpha)Q'(x)$. En prenant $x = \alpha$, il vient $P'(\alpha) = Q(\alpha) \neq 0$, ce qui est absurde. □

Exemple 3.28. Soit $n \geqslant 1$ un entier et montrons que $(X+1)^2$ divise $P(X) = X^{4n+2} + 2X^{2n+1} + 1$. D'après le théorème 3.15, il suffit que -1 est racine double de P. Ceci découle aisément du fait que $P(-1) = 0$ et $P'(-1) = 0$.

Remarque 3.29. Si $P'(\alpha) = 0$, cela n'implique pas que α soit racine multiple (ou racine tout court !) de P. Il faut en effet s'assurer que $P(\alpha) = 0$ pour utiliser le corollaire précédent. Par exemple, si $P(x) = x^2 - 2$, on a $P'(x) = 2x$, mais 0, bien que racine de P', n'est pas racine de P.

Remarque 3.30. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Pour un entier $k \geqslant 1$, notons $P^{(k)}$ le polynôme P dérivé k fois. Soit $n \geqslant 1$ un entier. Plus généralement, on peut démontrer par récurrence sur n l'équivalence

$$P(a) = 0, P'(a) = 0, \ldots, P^{(n)}(a) = 0 \Leftrightarrow (x-a)^n \text{ divise } P.$$

Exercices d'application **Exercice 4** Trouver les réels a, b tels que $(x-1)^2$ divise $ax^4 + bx^3 + 1$.

Exercice 5 Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que pour tous réels x, $P(2x) = P'(x)P''(x)$.

Exercice 6 Soit $P(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[X]$ qui possède n racines réelles différentes. Montrer que pour tout x réel, $P(x)P''(x) \leqslant P'(x)^2$. En déduire que pour $1 \leqslant k \leqslant n-1$, $a_{k-1}a_{k+1} \leqslant a_k^2$.

Exercice 7 (Oral ENS 2009) Soit $P \in \mathbb{R}[X]$ de degré $n \geqslant 1$. On suppose que toutes les racines de P sont réelles. Montrer que $(n-1)\left(P'(x)\right)^2 \geqslant nP(x)P''(x)$ et déterminer les cas d'égalité.

Interpolation Étant donnés un nombre fini de points du plan, existe-t-il un polynôme tel que que sa courbe représentative passe par ces points ? Trouver un tel polynôme, c'est résoudre un problème d'interpolation.

Théorème 3.31. Soient $a_1, \dots a_n$ et $b_1, \dots, b_n$ des nombres réels (avec les a_i deux à deux distincts). Alors il existe un unique polynôme P de degré au plus $n-1$ tel que pour tout i, $P(a_i) = b_i$.

Démonstration. Montrons d'abord l'unicité en considérant P, Q deux polynômes vérifiant les conditions de l'énoncé du théorème. $P - Q$ est alors un polynôme de degré au plus $n-1$, qui admet au moins n racines différentes, à savoir $a_1, \dots, a_n$. Il est donc nécessairement nul.

Quant à l'existence, pour $1 \leqslant i \leqslant n$, introduisons les polynômes suivants, appelés polynômes d'interpolation de Lagrange :

$$L_i(x) = \prod_{j=1, j\neq i}^{n} \frac{x - a_j}{a_i - a_j}.$$

L'intérêt est que pour tout j différent de i, $L_i(a_j) = 0$, alors que $L_i(a_i) = 1$. On en déduit aisément que le polynôme :

$$P(x) = \sum_{i=1}^{n} b_i L_i(x)$$

convient. □

Ainsi, un polynôme de degré n est complètement déterminé par les images de $n+1$ points distincts.

Exercice 8 Soient $a_1, \dots a_n$ et $b_1, \dots, b_n$ des éléments de $\mathbb{K}$ (avec les a_i deux à deux distincts). Trouver tous les polynômes $P \in \mathbb{K}[X]$ tels que $P(a_i) = b_i$.

Exercice 9 Trouver tous les polynômes à coefficients complexes P tels que pour tout rationnel q, $P(q)$ est rationnel.

Exercice 10 On définit les polynômes de Hermite comme suit : $H_0 = 1$ et pour $n \geqslant 1$, $H_n(x) = \frac{1}{n!}\prod_{k=0}^{n-1}(X-k)$.

1. Vérifier que pour tout $k \in \mathbb{Z}$, $H_n(k) \in \mathbb{Z}$.
2. Trouver tous les polynômes $P \in \mathbb{C}[X]$ tels que, pour tout $k \in \mathbb{N}$, $P(k) \in \mathbb{Z}$.
3. i Calculer, pour des entiers $j \leqslant k$ la somme :

$$\sum_{i=j}^{k} (-1)^{k-i} \binom{k}{i} \binom{i}{j}.$$

Indication. On pourra écrire $X^k = (X + 1 - 1)^k$.

ii Soit (u_j) une suite de nombres réels. Montrer que les deux conditions suivantes sont équivalentes :

i. Il existe $P \in \mathbb{R}[X]$ tel que, pour tout $j \in \mathbb{N}$, on a $u_j = P(j)$.

ii. Il existe un entier positif n tel que, pour tout entier $i \geqslant n+1$:

$$\sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} u_j = 0.$$

Cas des polynômes à petit degré Nous maintenant quelques applications des résultats précédents, parfois sous la forme d'exercice corrigé.

Proposition 3.32. Soient b, c deux nombres réels. On souhaite connaître le nombre de réels x tels que $x^2 + bc + c = 0$. Soit $\Delta = b^2 - 4c$, appelé le discriminant. Alors :

1. Si $\Delta < 0$, il n'y a pas de solution.
2. Si $\Delta = 0$, il y a une seule solution qui est $-\frac{b}{2}$.
3. Si $\Delta > 0$, il y a exactement deux solutions, qui sont :

$$\frac{-b + \sqrt{b^2 - 4c}}{2} \qquad \text{et} \qquad \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Démonstration. L'idée est de se ramener au cas $b = 0$ en écrivant $x^2 + bx + c$ sous la forme suivante, dite forme canonique :

$$x^2 + bx + c = (x + \frac{b}{2})^2 + c - \frac{b^2}{4}.$$

L'intérêt réside dans le fait que x n'intervient qu'une fois dans la nouvelle expression. Cette forme rend très souvent de précieux services et est à retenir. Ainsi, $x^2 + bx + c = 0$ si, et seulement si, $(x + \frac{b}{2})^2 = \frac{b^2}{4} - c$. Ainsi, un carré étant positif, si $\frac{b^2}{4} - c = \Delta/4 < 0$, il n'y a pas de solution, d'où le premier point. D'un autre côté, si $\Delta \geqslant 0$, alors $(x + \frac{b}{2})^2 = \frac{b^2}{4} - c$ si, et seulement si :

$$x + \frac{b}{2} = \sqrt{\frac{b^2}{4} - c} \qquad \text{ou} \qquad x + \frac{b}{2} = -\sqrt{\frac{b^2}{4} - c}.$$

On en déduit les points 2. et 3. □

Exemple 3.33. Le polynôme $P(x) = x^2 + x + 1$ a un discriminant égal à -3, et n'a donc pas de racine réelle.

Exercice 11 Soient $a, b, c \in \mathbb{R}$, avec $a \neq 0$, et considérons le graphe de la fonction $P(x) = ax^2 + bx + c$. Montrer qu'en faisant une homothétie et une translation, on peut obtenir le graphe de la fonction $Q(x) = x^2$.

Remarque 3.34. Il s'ensuit qu'étant donné un polynôme de degré 2, on peut aisément dire s'il a des racines réelles, et le cas échéant donner leur expression. Ceci est tout à fait remarquable : on peut montrer qu'il existe des polynômes de degré 5 dont les racines réelles ne s'expriment pas en utilisant des racines carrées, cubiques, etc. Cependant, si $P(x)$ est un polynôme de degré 3 et si on trouve une racine évidente a (par exemple $a = 1, 2, -1, -2, ...$), alors on peut effectuer la division euclidienne de P par $x - a$. On en déduit qu'il existe Q, un polynôme de degré 2, tel que $P(x) = Q(x)(x - a)$. Mais Q est de degré 2, et ce qui précède s'applique. La moralité de ceci est que si on trouve une racine évidente d'un polynôme de degré 3, alors on arrivera à connaître toutes ses racines. À titre d'illustration, on pourra chercher l'exercice suivant.

Exercice 12 Trouver tous les nombres réels x, y, z vérifiant :

$$\begin{cases} (x+1)yz = 12 \\ (y+1)zx = 4 \\ (z+1)xy = 4. \end{cases}$$

- Polynômes symétriques élémentaires -

Dans cette partie, nous nous intéressons aux liens unissant les coefficients d'un polynôme à ses racines.

Relations de Viète

Proposition 3.35 (Relations de Viète)**.** Soit $P(x) = ax^2 + bx + c$ un polynôme réel de degré 2 (avec $a \neq 0$) ayant z_1 et z_2 comme racines réelles. Alors $z_1 z_2 = \frac{c}{a}$ et $z_1 + z_2 = -\frac{b}{a}$.

Démonstration. D'après le corollaire 3.18, on a $P(x) = a(x - z_1)(x - z_2)$. En développant le terme de droite, on trouve les égalités annoncées. □

Ces relations sont utiles car elles expriment les coefficients du polynôme en fonction des racines. À ce titre, on cherchera l'exercice suivant.
Exercice 13 Trouvez toutes les valeurs du paramètre a pour que l'équation

$$ax^2 - (a+3)x + 2 = 0$$

admette deux racines réelles de signes opposés.

Proposition 3.36 (Relations de Viète dans le cas général)**.** Soit $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{K}[X]$ avec $a_n \neq 0$. Si $\alpha_1, \ldots, \alpha_n$ sont les racines de P, alors, en notant, pour $1 \leqslant k \leqslant n$,

$$\sigma_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \alpha_{i_1} \cdots \alpha_{i_k},$$

on a :

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

Par exemple :

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}, \sum_{1 \leqslant i < j \leqslant n} \alpha_i \alpha_j = -\frac{a_{n-2}}{a_n}, \ldots, \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}.$$

Remarque 3.37. Les $\sigma_1, \ldots, \sigma_n$ sont appelés *fonctions symétriques élémentaires des* α_i. *Symétriques*, parce qu'une permutation des α_i laisse les σ_k invariants. *Élémentaires*, parce qu'on peut montrer que toute expression symétrique en n variables peut s'exprimer polynômialement à l'aide de ces fonctions symétriques élémentaires. Plus précisément, si $P(x_1, \ldots, x_n)$ est un polynôme à n variables (on laisse le lecteur imaginer ce que c'est) tel que pour toute permutation σ de $\{1, \ldots, n\}$ on ait $P(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, alors il existe un polynôme à n variables R tel que $P(x_1, \ldots, x_n) = R(\alpha_1, \ldots, \alpha_n)$.

Exemple 3.38. En notant $\alpha_1 = x_1 + x_2 + x_3$, $\alpha_2 = x_1x_2 + x_1x_3 + x_2x_3$ et $\alpha_3 = x_1x_2x_3$, on a :

$$x_1^3 + x_2^3 + x_3^3 = \alpha_1^3 - 3\alpha_1\alpha_2 + 3\alpha_3.$$

Bref, lorsqu'on a affaire à des quantités symétriques, il peut être parfois judicieux de faire intervenir les fonctions symétriques élémentaires associées.

Exercice 14 Soit $P \in \mathbb{R}[X]$ non nul. Montrer que les sommes des racines complexes de P, P', …, $P^{(n-1)}$ (où $P^{(n-1)}$ désigne le polynôme P dérivé $n-1$ fois) forment une suite arithmétique.

Exercice 15 Trouver tous les réels x, y vérifiant $x^5 + y^5 = 33$ et $x + y = 3$.

Relations de Newton Nous allons voir que des sommes symétriques particulières (sommes des puissances k-ièmes) peuvent s'exprimer assez simplement grâce aux fonctions symétriques élémentaires.

Théorème 3.39 (Relations de Newton)**.** Soit $n \geqslant 1$, et notons $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires des α_i. Notons $S_k = \alpha_1^k + \cdots + \alpha_n^k$ pour $k \geqslant 0$. Alors, pour tout entier $k \geqslant 1$,

$$\sum_{r=0}^{k-1} (-1)^r \sigma_r S_{k-r} + (-1)^k k\sigma_k = 0, \tag{III.1}$$

avec la convention $\sigma_0 = 1$ et $\sigma_r = 0$ quand $r > n$.

Ainsi, à titre d'illustration, pour $r = 1, 2, \ldots, n$:

$$\begin{aligned} S_1 - \sigma_1 &= 0 \\ S_2 - \sigma_1 S_1 + 2\sigma_2 &= 0 \\ S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 &= 0 \\ &\vdots \\ S_n - \sigma_1 S_{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1} S_1 + (-1)^n n\sigma_n &= 0 \end{aligned}$$

et pour $r > n$:

$$S_r - \sigma_1 S_{r-1} + \sigma_2 S_{r-2} + \cdots + (-1)^n \sigma_n S_{r-n} = 0.$$

Remarque 3.40. Si $\alpha_1, \ldots, \alpha_n$ sont les racines du polynôme $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, alors pour tout entier $k \geqslant 0$:

$$a_n S_{k+n} + a_{n-1} S_{k+n-1} + a_{n-2} S_{k+n-2} + \cdots + a_0 S_k = 0.$$

En effet, il suffit d'écrire que $x^k P(\alpha_1) + \cdots x^k P(\alpha_n) = 0$. Les formules de Newton sont donc très facilement établies lorsque $k \geqslant n$.

Par ailleurs, en réécrivant le polynôme P sous la forme $P(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n$ (attention aux indices !), les relations de Viète donnent $b_j = (-1)^j \sigma_j$, de sorte que les relations de Newton s'écrivent aussi, pour tout entier $k \geqslant 1$,

$$\sum_{r=0}^{k-1} b_r S_{k-r} + k b_k = 0.$$

Preuve des relations de Newton, qui peut être sautée en première lecture. Nous avons déjà traité le cas $k \geqslant n$ plus haut et pouvons donc supposer que $k < n$. La preuve qui suit est due à Doron Zeilberger. Considérons $\mathcal{A} = \mathcal{A}(n,k)$ l'ensemble des couples $(A, j^{(l)})$, où :

(i) A est un sous-ensemble de $\{1,2,\dots,n\}$,

(ii) j appartient à $\{1,2,\dots,n\}$,

(iii) $|A| + l = k$, où $|A|$ est le nombre d'éléments de A,

(iv) $l \geqslant 0$, et si $l = 0$ alors $j \in A$.

On définit ensuite le poids $w(A, j^{(l)})$ de $(A, j^{(l)})$ par la formule

$$w(A, j^{(l)}) = (-1)^{|A|} \left(\prod_{a \in A} \alpha_a \right) \alpha_j^l.$$

Par exemple, $w(\{1,3,5\}, 2^{(3)}) = (-1)^3 \alpha_1\alpha_3\alpha_5 \cdot \alpha_2^3 = -\alpha_1\alpha_2^3\alpha_3\alpha_5$. On voit aisément que la somme des poids de tous les éléments de $\mathcal{A}$ est égale au terme de gauche de (III.1).

Prouvons maintenant que cette somme est nulle. À cet effet, considérons l'application $T : \mathcal{A} \to \mathcal{A}$ définie par :

$$T(A, j^{(l)}) = \begin{cases} (A \backslash \{j\}, j^{(l+1)}), & j \in A, \\ (A \cup \{j\}, j^{(l-1)}), & j \notin A. \end{cases}$$

Cette application vérifie $w(T(A, j^{(l)})) = -w(A, j^{(l)})$ et est une involution (i.e. T composé avec elle-même donne l'identité). On peut donc assembler tous les poids par paires de sorte que chaque paire contienne un poids et son opposé. La somme de tous les poids est donc bien nulle, ce qui conclut la preuve.

Mentionnons qu'il est également possible de procéder par récurrence sur $n-k$ pour prouver les relations de Newton. □

Exemple 3.41. Soient x, y, z des nombres réels tels que $x + y + z = 1$, $x^2 + y^2 + z^2 = 3$ et $x^3 + y^3 + z^3 = 7$. Trouvons la valeur de $x^5 + y^5 + z^5$.

À cet effet, notons S_k et σ_k respectivement les sommes des puissances k-ièmes et la k-ième fonction symétrique élémentaire de x, y, z. Les relations de Newton donnent

$$S_1 - \sigma_1 = 0, \qquad S_2 - \sigma_1 S_1 + 2\sigma_2 = 0, \qquad S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 = 0.$$

On en tire que $\sigma_1 = 1$, $\sigma_2 = -1$ et $\sigma_3 = 1$. D'après les relations de Viète, x, y, z sont donc les solutions de $t^3 - t^2 - t - 1 = 0$. Ainsi, d'après la Remarque 3.40, nous avons

$$S_{k+3} = S_{k+2} + S_{k+1} + S_k$$

pour $k \geqslant 0$. Il s'ensuit que $S_4 = 1 + 3 + 7 = 11$ puis que $S_5 = 3 + 7 + 11 = 21$.

Exercice 16 Soient x et y deux nombres non nuls tels que $x^2 + xy + y^2 = 0$ (x et y sont des nombres complexes, mais ce n'est pas trop grave). Trouver la valeur de

$$\left(\frac{x}{x+y}\right)^{2013} + \left(\frac{y}{x+y}\right)^{2013}.$$

Exercice 17 Trouver tous les nombres réels x, y, z tels que

$$x + y + z = 3, \qquad x^2 + y^2 + z^2 = 3, \qquad x^3 + y^3 + z^3 = 3.$$

- Polynômes à coefficients entiers -

Nous présentons maintenant quelques spécificités des polynômes à coefficients entiers :

- ⋆ Nous avons déjà vu que si $P, Q \in \mathbb{Z}[X]$ et que $\deg Q \geqslant 1$, on peut toujours effectuer la division euclidienne de P par Q à condition que le coefficient dominant de Q soit égal à 1.
- ⋆ Une propriété extrêmement utile est que si $P \in \mathbb{Z}[X]$, alors pour tous entiers $a \neq b$, $a - b$ divise $P(a) - P(b)$. Ceci est une simple conséquence du fait que $a - b$ divise $a^n - b^n$ pour $n \geqslant 1$.
- ⋆ Si $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$, et si p/q est une racine rationnelle de P sous forme irréductible, alors p divise a_0 et q divise a_n. Ce simple fait permet de restreindre la recherche des racines rationnelles d'un polynôme à coefficients entiers.
- ⋆ Un polynôme $P \in \mathbb{Q}[X]$ vérifie $P(k) \in \mathbb{Z}$ pour tout $k \in \mathbb{Z}$ si et seulement si il existe des entiers $a_0, a_1, \ldots a_n$ tels que

$$P(x) = a_0 \binom{x}{0} + a_1 \binom{x}{1} + \cdots + a_n \binom{x}{n},$$

où on note $\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$ si $k \neq 0$ et $\binom{x}{0} = 1$. Cette propriété découle de l'Exercice 10 (2).

Exemple 3.42. Cherchons tous les nombres réels x, y, z tels que

$$x + y + z = 17, \qquad xy + yz + xz = 94, \qquad xyz = 168.$$

D'après les relations de Viète, x, y, z sont racines de $P(x) = x^3 - 17x^2 + 94x - 168 = 0$. Cherchons des racines "évidentes" de P. Il est naturel de d'abord chercher des racines entières, qui sont forcément des diviseurs de 168 (pour tester si par exemple 2 est racine, on effectue la division euclidienne de P pa $x - 2$ et on regarde si le reste est nul). On remarque que $x = 4$ est racine, et sans difficulté on trouve que $x = 6$ et $x = 7$ sont racines du polynôme $P(x)/(x - 4)$. Ainsi, les solutions (x, y, z) sont les six permutations possibles de $(4, 6, 7)$.

Exercice 18 Soient a, b, c des entiers différents. Montrer qu'il n'existe pas de polynôme P à coefficients entiers tel que $P(a) = b$, $P(b) = c$ et $P(c) = a$.

La factorisation par $a - b$ du polynôme $P(a) - P(b)$ peut être utile dans d'autres cas également, voir par exemple l'exercice suivant.

Exercice 19 Soient $P, Q \in \mathbb{R}[X]$ deux polynômes unitaires tels que $P(P(x)) = Q(Q(x))$ pour tout réel x. Prouver que $P(x) = Q(x)$.

- Interlude : un peu de topologie -

Nous considérons dans cette partie des polynômes à coefficients réels et voyons comment des résultats de la théorie de l'analyse réelle s'appliquent dans notre cas. Nous utiliserons la propriété suivante :

Proposition 3.43. Soit $P \in \mathbb{R}[x]$ un polynôme, et a, α, b, β des réels tels que $a < b$, $P(a) = \alpha$ et $P(b) = \beta$. Alors pour tout réel γ compris entre α et β, il existe un réel c tel que $a \leqslant c \leqslant b$ et $P(c) = \gamma$.

En particulier, si $a < b$ sont tels que $P(a) < 0$ et $P(b) > 0$, alors il existe au moins une racine réelle de P dans l'intervalle $]a, b[$.

La proposition précédent est un cas particulier du théorème des valeurs intermédiaires, valable plus généralement pour toute fonction *continue* à valeurs réelles.

On en déduit le résultat intéressant suivant :

Proposition 3.44. Soit $P \in \mathbb{R}[X]$ un polynôme de degré impair. Alors P admet au moins une racine réelle.

Démonstration. Écrivons $P(x) = a_n x^n + \cdots + a_1 x + a_0$ avec $a_n \neq 0$ et $n \geqslant 1$. Supposons en premier lieu que $a_n > 0$ et rouvons tout d'abord que $P(x) \to \infty$, lorsque $x \to \infty$, c'est-à-dire que pour tout $M > 0$, il existe x_0 tel que pour tout $x > x_0$ on ait $P(x) > M$. À cet effet, écrivons

$$P(x) = a_n x^n \left(1 + \frac{a_{n-1}}{a_n} \cdot \frac{1}{x} + \cdots + \frac{a_0}{a_n} \cdot \frac{1}{x^n}\right).$$

La somme à l'intérieur de la parenthèse converge vers 1 lorsque $x \to \infty$, et le terme $a_n x^n$ diverge vers $+\infty$ lorque $x \to \infty$. Le résultat en découle. Lorsque $x \to \infty$, on prouve de même que $P(x) \to -\infty$. On en déduit qu'il existe $a < 0 < b$ tels que $P(a) < 0$ et $P(b) > 0$. Le résultat en découle d'aprs la proposition 3.43.

Si $a_n < 0$, le raisonnement est similaire, mais cette fois-ci $P(x) \to -\infty$ quand $x \to \infty$ et $P(x) \to \infty$ lorsque $x \to -\infty$. □

Exercice 20 Trouver tous les polynômes P à coefficients réels tels que pour tout réel $x > 0$ on ait :

$$\left|P(x)P\left(\frac{1}{x}\right)\right| \leqslant 1.$$

- Nombres complexes et théorème de d'Alembert-Gauss -

Nombres complexes Nous avons vu qu'il existait des polynômes de $\mathbb{R}[X]$ qui ne possédaient pas de racines réelles. Un des intérêts de l'introduction des nombres complexes (et c'est dans cette optique qu'ils ont été introduits au XVIè siècle) est de pallier cette difficulté via le théorème de d'Alembert-Gauss (énoncé par d'Alembert et démontré par Gauss).

Définition 3.45. Notons $\mathbb{C}$ l'ensemble des couples de nombres réels (a, b) munis :

1. de l'addition suivante : $(a, b) + (c, d) = (a + c, b + d)$,
2. des multiplications suivantes : $(a, b) \times (c, d) = (ac - bd, ad + bc)$ et pour λ réel, $\lambda(a, b) = (\lambda a, \lambda b)$.

Nous voyons l'ensemble des nombres réels plongés dans l'ensemble des nombres complexes : à chaque réel a, on peut associer le nombre complexe $(a, 0)$. Notons enfin i le nombre complexe $(0, 1)$. Ainsi, nous pouvons représenter chaque nombre complexe (a, b) sous la forme $(a, b) = a(1, 0) + b(0, 1) = a + ib$.

Remarque 3.46. Avec les règles de multiplication précédentes, on voit que $i^2 = -1$, et que $(a + bi)(c + di) = ac - bd + (ad + bc)i$. Ainsi, tout se passe comme si i était un « nombre » tel que $i^2 = -1$ dans toutes les manipulations. En particulier, i est racine du polynôme $X^2 + 1 = 0$.

Remarque 3.47. Tout élément non nul de $\mathbb{C}$ possédant un inverse, les résultats des sections précédentes sont aussi valables pour $\mathbb{K} = \mathbb{C}$.

Exercice 21 Pour quels entiers $n \geqslant 1$ le polynôme $1 + x^2 + x^4 + \cdots + x^{2n-2}$ est-il divisible par le polynôme $1 + x + x^2 + \cdots + x^{n-1}$?

Théorème de d'Alembert-Gauss Nous admettons le théorème (qu'on appelle aussi théorème fondamental de l'algèbre) suivant :

Théorème 3.48. Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine. On dit que $\mathbb{C}$ est algébriquement clos.

Par une récurrence sur le degré, on en déduit :

Corollaire 3.49. Soit $P \in \mathbb{C}[X]$. Alors P peut s'écrire sous la forme :

$$P(x) = c(x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k},$$

où $c, \alpha_1, \ldots, \alpha_k$ sont des nombres complexes et $m_1, \ldots, m_k$ sont des entiers strictement positifs.

Nous définissons finalement la conjugaison complexe, qui sera utile lorsque nous voudrons déterminer les polynômes irréductibles de $\mathbb{R}[X]$.

Définition 3.50. Soit $z = a + bi \in \mathbb{C}$. On définit son *conjugué* $\overline{z}$ par $\overline{z} = a - bi$.

Proposition 3.51. Pour tous $w, z \in \mathbb{C}$, on a $\overline{wz} = \overline{w} \cdot \overline{z}$.

Démonstration. Exercice. □

- Arithmétique de $\mathbb{K}[X]$ -

De même que dans le cas des nombres entiers, la division euclidienne entre polynômes permet de démontrer le théorème de Bézout, et par voie de conséquence de définir la notion de PGCD et d'avoir accès au lemme de Gauss. Les démonstrations étant similaires au cas des entiers, nous ne les reproduisons pas. Dans tout ce qui suit, $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

Théorème de Bézout dans $\mathbb{K}[X]$

Définition 3.52. Soient $P, Q \in \mathbb{K}[X]$. Lorsque P est non nul, on rappelle que P divise Q s'il existe $R \in \mathbb{K}[X]$ tel que $Q = PR$. On dit que P et Q sont premiers entre eux s'ils n'ont comme diviseurs communs (dans $\mathbb{K}[X]$) que les constantes non nulles. Nous utilisons aussi ces définitions dans le cas de $\mathbb{Z}[X]$.

Remarque 3.53. La définition précédente laisse penser que la notion de primalité entre deux polynômes dépend de l'ensemble choisi pour ses coeffecients : ainsi, a priori, rien n'empêche que deux polynômes à coefficients entiers soient premiers entre eux lorsqu'ils sont vus comme éléments de $\mathbb{Q}[X]$, mais qu'ils ne le soient plus lorsqu'on les voit comme éléments de $\mathbb{C}[X]$.

Théorème 3.54 (Bézout)**.** Soient $P, Q \in \mathbb{K}[X]$. Alors P et Q sont premiers entre eux si, et seulement si, il existe $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1$.

Exercice 22 Soit $x \in \mathbb{R}$. Les énoncés suivants sont-ils vrais ou faux ?

a. Si x^7 et x^{12} sont rationnels, alors x est rationnel.

b. Si x^9 et x^{12} sont rationnels, alors x est rationnel.

Corollaire 3.55. Si $P, Q \in \mathbb{Q}[X]$ sont premiers entre eux, alors, vus comme éléments de $\mathbb{R}[X]$, ils sont premiers entre eux.

Démonstration. D'après le théorème de Bézout, il existe $U, V \in \mathbb{Q}[X]$ tels que $PU + QV = 1$. A fortiori, $U, V \in \mathbb{R}[X]$, donc, d'après la réciproque du théorème de Bézout, P et Q sont premiers entre eux vus comme éléments de $\mathbb{R}[X]$. □

Du théorème de Bézout on déduit le théorème de Gauss.

Théorème 3.56. Si $P, Q, R \in \mathbb{K}[X]$ sont tels que P soit premier avec Q et P divise QR, alors P divise R.

Polynômes irréductibles de $\mathbb{K}[X]$ Les polynômes irréductibles jouent le rôle des nombres premiers : ce sont en quelque sorte les briques de base lorsqu'on souhaite factoriser des polynômes.

Définition 3.57. Un polynôme $P \in \mathbb{K}[X]$ est dit *irréductible* dans $\mathbb{K}[X]$ si P n'est pas constant et si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes et les polynômes proportionnels à P non nuls, ou, de manière équivalente, s'il n'existe pas $Q, R \in \mathbb{K}[X]$ tels que $P = QR$ avec $\deg Q \geqslant 1$ et $\deg R \geqslant 1$.

On en déduit l'équivalent du théorème de factorisation en nombre premiers.

Théorème 3.58. Tout polynôme de $\mathbb{K}[X]$ se décompose de manière unique, à l'ordre des facteurs près, sous la forme :

$$P = cP_1^{k_1}P_2^{k_2}\cdots P_k^{\alpha_k},$$

où $c \in \mathbb{K}^*, k_i \in \mathbb{N}^*$ et les P_i sont des polynômes distincts unitaires et irréductibles dans $\mathbb{K}[X]$.

À titre d'exercice nous laissons la preuve de ce théorème (très proche de son équivalent pour les nombres entiers).

Le théorème précédent nous invite à chercher les polynômes irréductibles de $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$. Nous commençons par une proposition générale.

Proposition 3.59. Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 est irréductible si, et seulement si, il n'a pas de racine.

Démonstration. Exercice. □

Proposition 3.60. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de premier degré.

Démonstration. Il est clair que ces polynômes sont bien irréductibles. Réciproquement, si $P \in \mathbb{C}[X]$ de degré au moins 2 est irréductible, d'après le théorème de d'Alembert-Gauss, il peut s'écrire $P(x) = (x-\alpha)Q(x)$, se qui contredit son irréductibilité. □

Passons maintenant à l'étude des polynômes à coefficients réels.

Proposition 3.61. Tout polynôme $P \in \mathbb{R}[X]$ se décompose sous la forme :

$$P(x) = c\prod_{i=1}^{r}(x-\alpha_i)\prod_{i=1}^{s}(x^2+a_ix+b_i).$$

En conséquence, les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de premier degré et ceux du second degré à discriminant négatif.

Démonstration. D'après le corollaire 3.49, on peut écrire $P(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, où les α_i sont complexes. En utilisant la proposition 3.51, on voit que si α est racine de P, alors $\overline{\alpha}$ est également racine de P. En effet, si $P(x) = a_0 + a_1x + \cdots + a_nx^n$ avec les a_i réels, on a $0 = \overline{P(\alpha)} = \overline{a_0 + a_1\alpha + \cdots + a_n\alpha^n} = \overline{a_0} + \overline{a_1\alpha} + \cdots + \overline{a_n\alpha^n} = a_0 + a_1\overline{\alpha} + \cdots + a_n\overline{\alpha}^n$. Dans l'expression donnant P sous forme factorisée, on regroupe alors par paires les racines complexes (non réelles) avec leurs conjugués. En remarquant que pour un nombre complexe z, $(x-z)(x-\overline{z}) = x^2 + ax + b$, avec $a, b \in \mathbb{R}$ tels que $a^2 - 4b \leqslant 0$, on conclut.

Le raisonnement précédent montre qu'un polynôme irréductible de $\mathbb{R}[X]$ est un polynôme de premier degré ou du second degré à discriminant négatif. Réciproquement, de tels polynômes sont irréductibles en vertu de la proposition 3.59. □

Exercice 23 Soient $P, Q \in \mathbb{R}[X]$ deux polynômes non nuls tels que pour tout réel x, $P(x^2+x+1) = P(x)Q(x)$. Montrer que P est de degré pair. Peut-on trouver de tels polynômes ?

Exercice 24 Soit P un polynôme à coefficients réels tel que $P(x) \geqslant 0$ pour tout réel x. Montrer qu'il existe deux polynômes $Q, R \in \mathbb{R}[X]$ tels que $P = Q^2 + R^2$.

Polynômes irréductibles à coefficients entiers ou rationnels Dans le cas de $\mathbb{Q}[X]$, il n'y a pas de caractérisation satisfaisante des polynômes irréductibles (essentiellement parce que des propriétés arithmétiques de $\mathbb{Z}$ rentrent en jeu). On peut toutefois donner quelques méthodes de recherche de racines et des critères d'irréductibilité.

Proposition 3.62. Soit $P(x) \in \mathbb{Q}[X]$ et cherchons ses racines rationnelles. Quitte à multiplier P par le ppcm des dénominateurs de ses coefficients, on peut supposer que $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[X]$. Soit p/q une racine rationnelle de P. Alors p divise a_0 et q divise a_n.

Démonstration. Il suffit d'écrire $P(p/q) = 0$, de réduire au même dénominateur et d'utiliser le lemme de Gauss pour les entiers. □

Venons-on à l'irréductibilité.

Remarque 3.63. En vertu de la remarque 3.59, on peut en pratique vérifier si un polynôme de degré 2 ou 3 à coefficients entiers ou rationnels est irréductible.

Exemple 3.64. Le polynôme $x^3 + x^2 - 2x - 1$ est irréductible dans $\mathbb{Q}[X]$ puisqu'il est sans racine dans $\mathbb{Q}$.

On commence par introduire le contenu d'un polynôme afin de montrer que les irréductibles de $\mathbb{Z}[X]$ sont irréductibles dans $\mathbb{Q}[X]$, ce qui n'est pas évident a priori.

Définition 3.65. Soit $P \in \mathbb{Z}[X]$ non nul. On appelle contenu de P et on note $c(P)$ le pgcd de ses coefficients (au signe près).

Exemple 3.66. Par exemple, $c(-6x^6 + 3x^5 + 27x - 90) = 3$.

Lemme 3.67. Pour $P, Q \in \mathbb{Z}[X]$ non nuls, $c(PQ) = c(P)c(Q)$ au signe près.

Démonstration. Montrons d'abord le résultat lorsque $c(P) = c(Q) = 1$. Raisonnons par l'absurde que $c(PQ) \neq 1$ en considérant un nombre premier p divisant $c(PQ)$. Écrivons $P(x) = \sum_i a_i x^i$, $Q(x) = \sum_i b_i x^i$, $P(x)Q(x) = \sum_i c_i x^i$. Comme $c(P) = c(Q) = 1$, il existe $i_0, j_0 \in \mathbb{N}$ tels que :

$$\begin{aligned} &\forall i < i_0, \quad p | a_i \text{ mais } p \not| a_{i_0} \\ &\forall j < j_0, \quad p | b_j \text{ mais } p \not| b_{j_0}. \end{aligned}$$

Par hypothèse, on a :

$$p | c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_i = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j.$$

Mais alors p divise $a_{i_0} b_{j_0}$, ce qui est absurde.

Dans le cas général, notons $P' = P/c(P), Q' = Q/c(Q)$ de sorte que $c(P') = c(Q') = 1$. Ainsi, $c(P'Q') = 1$. Or $c(P'Q') = c(PQ)/c(P)c(Q)$, d'où le résultat. □

On en déduit également le résultat suivant.

Proposition 3.68. Soit $P \in \mathbb{Z}[X]$. Alors P est irréductible dans $\mathbb{Z}[X]$ si, et seulement, si P est irréductible dans $\mathbb{Q}[X]$ et $c(P) = 1$.

Démonstration. Si P est irréductible dans $\mathbb{Q}[X]$ et $c(P) = 1$, il est clair qu'il l'est dans $\mathbb{Z}[X]$. Réciproquement, supposons P irréductible dans $\mathbb{Z}[X]$ (ce qui implique $c(P) = 1$) et par l'absurde supposons qu'il n'est pas irréductible dans $\mathbb{Q}[X]$. Écrivons alors $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ unitaires de degré au moins 1. Écrivons $Q(x) = \frac{a}{b}Q'(x)$ avec $Q' \in \mathbb{Z}[X]$, $c(q') = 1$ et a, b entiers premiers entre eux. De même, écrivons $R(x) = \frac{c}{d}R'(x)$ avec $R' \in \mathbb{Z}[X]$, $c(R') = 1$ et c, d entiers premiers entre eux. Alors $bdP(x) = acQ'(x)R'(x)$. Comme $c(P) = 1$, il vient $bd = c(bdP(x)) = c(acQ'R') = ac$ (au signe près). Ainsi, $P = QR = \frac{ac}{bd}Q'R' = Q'R'$ (au signe près) avec $Q', R' \in \mathbb{Z}[X]$. Ceci contredit l'irréductibilité de P dans $\mathbb{Z}[X]$. □

De manière un peu similaire, on démontre la proposition suivante, parfois utile.

Proposition 3.69. Soit $P, Q \in \mathbb{Q}[X]$ unitaires tels que $R = PQ \in \mathbb{Z}[X]$. Alors P et Q sont à coefficients entiers.

Démonstration. Notons u (resp. v) le ppcm des dénominateurs des coefficients de P (resp. Q). Alors $uvR = uvPQ = (uP)(vQ)$. Donc $c(uvR) = c(uP)c(vQ)$ d'après le lemme précédent. Or, comme P et Q sont unitaires, $c(uP) = c(vQ) = 1$ et $c(uvR) \geqslant uv$. On en déduit que $u = v = 1$ et donc que $P, Q \in \mathbb{Z}[X]$. □

Exercice 25 Soit $P(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}[X]$ avec ad impair et bc pair. On suppose que P a toutes ses racines réelles. Montrer qu'au moins une racine de P est un nombre réel irrationnel.

Remarque 3.70. Ainsi, l'étude de l'irréductibilité d'un polynôme à coefficients entiers sur $\mathbb{Q}[X]$ se réduit à l'étude de l'irréductibilité de $\mathbb{Z}[X]$, qui est a priori plus facile.

Voici un exemple (important) d'application de ceci.

Théorème 3.71. Soit $P(x) = a_n x^n + \cdots + a_1 x + a_0$ un polynôme de $\mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que :

1. p divise $a_0, a_1, \ldots, a_{n-1}$,
2. p ne divise pas a_n,
3. p^2 ne divise pas a_0.

Alors P est irréductible dans $\mathbb{Q}[X]$.

Démonstration. D'après la proposition précédente, il suffit de montrer que P est irréductible dans $\mathbb{Z}[X]$. Supposons donc par l'absurde que $P(x) = Q(x)R(x)$ avec Q, R deux polynômes non constants de $\mathbb{Z}[X]$ avec $Q(x) = q_k x^k + \cdots q_0$ et $R(x) = r_l x^l + \cdots + r_0$. Alors $a_0 = q_0 r_0$. Par suite, d'après le point 3., p divise q_0 ou r_0, mais pas les deux à la fois. Sans perte de généralité, supposons que p divise q_0 mais pas r_0. D'autre part, p ne divise pas q_k, car sinon il diviserait a_n, ce qui est exclu. Soit donc i_0 le plus petit indice i ($1 \leqslant i \leqslant k$) tel que p ne divise par q_i. Alors :

$$a_{i_0} = q_{i_0} r_0 + q_{i_0-1} r_1 + \cdots + q_o r_{i_0}.$$

Comme $i_0 \leqslant k < n$, p divise a_{i_0} et donc p divise $q_{i_0} r_0$, et donc p divise r_0, ce qui est absurde. □

Exemple 3.72. Soit p un nombre premier et $P(x) = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[X]$. En appliquant le critère d'Eisenstein au polynôme $Q(x) = P(x+1)$, on voit que P est irréductible dans $\mathbb{Q}[X]$.

Exercice 26 (IMO 93, exercice 1) Soit $n \geqslant 2$ un entier. Montrer que le polynôme $P(x) = x^n + 5x^{n-1} + 3$ est irréductible sur $\mathbb{Z}[X]$.

- Quelques exercices -

Exercice 27 (Canada 1970) Soit P un polynôme à coefficients entiers. On suppose qu'il existe des entiers deux à deux distincts a, b, c, d tels que $P(a) = P(b) = P(c) = P(d) = 5$. Montrer qu'il n'existe pas d'entier k tel que $P(k) = 8$.

Exercice 28 (Benelux 2010) Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que pour tous réels a, b, c on ait :

$$p(a+b-2c) + p(b+c-2a) + p(c+a-2b) = 3p(a-b) + 3p(b-c) + 3p(c-a).$$

Exercice 29 (IMO 2004, exercice 2) Trouver tous les polynômes P à coefficients réels qui vérifient, pour tous a, b, c réels tels que $ab + bc + ca = 0$:

$$P(a-b) + P(b-c) + P(c-a) = 2P(a+b+c).$$

Exercice 30 Soit $n \geqslant 1$ un entier. On note $\mathfrak{S}_n$ l'ensemble des permutations de l'ensemble $\{1, 2, \ldots, n\}$. Pour $\sigma \in \mathfrak{S}_n$, on note aussi $\mathrm{cyc}(\sigma)$ le nombre de cycles de σ. Soit $P_n(x)$ le polynôme suivant :

$$P_n(x) = \sum_{\sigma \in \mathfrak{S}_n} x^{\mathrm{cyc}(\sigma)}.$$

Montrer que P_n a toutes ses racines réelles et que ce sont des entiers négatifs.

Exercice 31 (Test de sélection Chine 2008) Soient m, n des entiers strictement positifs et $P \in \mathbb{Z}[X]$ un polynôme de degré n tel que tous ses coefficients soient impairs. On suppose que $(x-1)^m$ divise P. Montrer que si $m \geqslant 2^k$ (avec $k \geqslant 2$ entier), alors $n \geqslant 2^{k+1} - 1$.

- Quelques motivations -

Pourquoi étudie-t-on les polynômes ? Voici quelques éléments de réponse donnés sans démonstration.

Théorème 3.73. Soit f une fonction réelle infiniment dérivable (si vous ne savez pas ce que ça veut dire, imaginez qu'elle est très gentille). Soit $x_0 \in \mathbb{R}$. Alors pour tout entier n, pour tout $\epsilon > 0$, il existe $\eta > 0$ et des réels $a_0, \ldots, a_n$ tels que pour tout $x \in [x_0 - \eta, x_0 + \eta]$:

$$|f(x - x_0) - a_0 - a_1(x - x_0) - \cdots - a_n(x - x_0)^n| \leqslant \epsilon |(x - x_0)^n|.$$

Ainsi, au voisinage de tout point, la fonction « ressemble » à un polynôme.

Théorème 3.74. Soit $f : [0, 1] \to \mathbb{R}$ une fonction continue. Alors il existe une suite de polynômes $P_1(x), P_2(x), \cdots$ telle que pour tout $\epsilon > 0$, il existe $N > 0$ tel que pour tout $n \geqslant N$:

$$\text{pour tout } x \in [0, 1] \qquad |f(x) - P_n(x)| \leqslant \epsilon.$$

Ainsi, toute fonction continue sur $[0, 1]$ peut être approchée sur tout $[0, 1]$ par des polynômes.

Signalons finalement que l'étude de l'ensemble des zéros communs de plusieurs polynômes à n variables, appelé variété algébrique, est centrale en géométrie algébrique.

- Distinction entre polynôme et fonction polynômiale -

Ici, nous expliquons pourquoi il est nécessaire de faire cette distinction en commençant par définir d'une autre manière un polynôme. Ici, $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ou bien $\mathbb{Z}/p\mathbb{Z}$ muni des lois d'addition et de multiplication usuelles.

Définition 3.75. Un polynôme à coefficients dans $\mathbb{K}$ est une suite infinie d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang.

Exemple 3.76. Par exemple, $(0, 1, 2, 3, 0, 0, \ldots, 0, \ldots)$ et $(0, 0, \ldots, 0, \ldots)$ sont tous deux des polynômes. Par contre, $(1, 1, \ldots, 1, \ldots)$ n'en est pas un.

Définition 3.77. Soit $P = (u_n)_n$ et $Q = (v_n)_n$ deux polynômes. On définit le polynôme $P + Q$ par la suite $w_n = u_n + v_n$ (qui est bien nulle à partir d'un certain rang) et le polynôme $P \times Q$ par la suite (z_n), où $z_n = \sum_{i+j=n} u_n v_n$ (vérifier que (z_n) est nulle à partir d'un certain rang). On identifie les éléments de $\mathbb{K}$ avec les polynômes constants via l'application qui à un élément $\lambda \in \mathbb{K}$ associe le polynôme $(\lambda, 0, 0, \ldots, 0, \ldots)$. Remarquons que ceci est cohérent avec la notion de multiplication intuitive d'un polynôme par un élément de $\mathbb{K}$: si (u_n) est un polynôme et $\lambda \in \mathbb{K}$, alors le polynôme $\lambda \times (u_n)$ est le polynôme (λu_n).

Nous introduisons maintenant l'indéterminée X.

Définition 3.78. Notons X le polynôme $(0, 1, 0, 0, \ldots)$.

Proposition 3.79. Tout polynôme P s'exprime sous la forme $P = \sum_{i=0}^{n} a_n X^n$. On note indifféremment P ou $P(X)$ pour rappeler qu'on note X l'indéterminée (on pourrait très bien la noter Y !).

Démonstration. Si $P = (a_0, a_1, a_2, \ldots)$, notons N un entier tel que $i \geqslant N$ implique $a_i = 0$. Alors $P(X) = a_0 + a_1 X + \cdots + a_N x^N$. Ceci est une conséquence immédiate de la définition de X et de la multiplication entre polynômes. □

Voici maintenant le lien entre polynôme et fonction polynômiale associée. Rappelons que, pour l'instant, un polynôme est juste une suite de nombres qui est nulle à partir d'un certain rang et n'est pas vu comme une application.

Proposition 3.80. Soit $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ un polynôme. On note $\widetilde{P}$ l'application définie par $\widetilde{P}(x) = a_0 + a_1 x + \cdots + a_n x^n$ pour $x \in \mathbb{K}$, qu'on appelle application polynômiale associée à P. L'application $P \mapsto \widetilde{P}$ est injective si $\mathbb{K}$ est infini. Si $\mathbb{K}$ est fini, cette application n'est pas nécessairement injective.

Démonstration. Plaçons nous d'abord dans le cas où $\mathbb{K}$ est infini. Soient $P, Q \in \mathbb{K}[X]$ tels que $\widetilde{P} = \widetilde{Q}$. Écrivons $P(X) = \sum_i a_i X^i$ et $Q(X) = \sum_i b_i X^i$. Alors le polynôme $P(x) - Q(x)$, au sens des sections précédentes, a une infinité de racines, donc est nul. Donc $a_i = b_i$ pour tout i.

Par contre, dans le cas où $\mathbb{K}$ est fini, le raisonnement précédent ne s'applique pas. Exhibons d'ailleurs un contre-exemple. Considérons $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ et $P(X) = X^p - X$. D'après le petit théorème de Fermat, pour tout $x \in \mathbb{K}$, on a $P(x) = 0$. Ainsi, P n'est pas le polynôme nul, mais les deux fonctions polynômiales associées sont les mêmes. □

En d'autres termes, lorsque $\mathbb{K}$ est infini (par exemple $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, ce qui explique que nous n'avons pas perdu de généralité dans les premières sections), nous pouvons parler sans distinction de polynôme ou de fonction polynômiale associée. En revanche, dans les autres cas, il faut faire très attention !

- Éléménts de réponse aux exercices -

Solution de l'exercice 1 On cherche le reste sous la forme $R(X) = aX + b$. On a $R(1) = P(1)$, $R(-1) = P(-1)$, ce qui permet de calculer $R(X) = -2X + 2$.

Solution de l'exercice 2 Si $Q(x)$ était un polynôme, alors $Q(x) - x$ serait un polynôme avec une infinité de racines, donc serait de degré nul, c'est absurde.

Solution de l'exercice 3 Comme $P(x)^2 = 16P(x^2/4)$ est un polynôme en x^2, on peut appliquer la proposition 3.22. Dans le premier cas, s'il existe un polynôme Q tel que $P(x) = Q(x^2)$, on obtient $16Q(x^4) = 16P(x^2) = P(2x)^2 = Q(4x^2)^2$, et donc $16Q(x^2) = Q(4x)^2$. Dans le deuxième cas, s'il existe un polynôme Q tel que $P(x) = Q(x^2)$, on obtient similairement que $4Q(x^2) = Q(4x)^2$.

On peut donc réappliquer la proposition 3.22 à Q, et de même on obtient que, pour tout entier $k \geqslant 0$, il existe un entier $0 \leqslant i \leqslant 2^k$ et un polynôme R_k tel que $P(x) = x^i R_k(x^{2^k})$.

En choisissant k tel que $2^k > \deg P$, il s'ensuit que R_k est forcément constant et donc que $P(x) = c \cdot x^i$. En réinjectant dans l'équation de départ, on obtient $P(x) = 16(x/4)^i$ pour un certain entier $i \geqslant 0$ (et toutes ces solutions conviennent bien, réciproquement).

Solution de l'exercice 4 1 doit être racine double de P. Cela nous donne deux équations : $P(1) = 0$ et $P'(1) = 0$, qui permettent de trouver $a = 3$ et $b = -4$.

Solution de l'exercice 5 On note n le degré de P. En passant l'équation aux degrés, on obtient $n = (n-1)+(n-2) = 2n-3$, donc $n = 3$. On peut facilement calculer le coefficient dominant, on laisse le soin au lecteur de terminer les calculs.

Solution de l'exercice 6 On remarque que la dérivée de $\frac{P'}{P}$ est $\frac{P''-P'^2}{P^2}$ qui est du même signe que $P'' - P'^2$. Or on voit facilement que $\frac{P'(x)}{P(x)} = \sum \frac{1}{x-\alpha_i}$ donc $(\frac{P'(x)}{P(x)})' = \sum \frac{-1}{(x-\alpha_i)^2} < 0$ d'où le résultat. Pour obtenir l'inégalité sur les coefficients on procède de la manière suivante. Pour $k = 1$, l'inégalité provient de $P(0)P''(0) \leqslant P'(0)^2$. Ensuite on applique l'inégalité aux polynômes $P^{(k-1)}$: $P^{(k-1)}P^{(k+1)} \leqslant \left(P^{(k)}\right)^2$ d'où $a_{k-1}(k-1)! \times a_{k+1}(k+1)! \leqslant a_k^2 \times k!^2$ or $\frac{k!^2}{(k-1)!(k+1)!} = \frac{k}{k+1} \leqslant 1$ d'où le résultat.

Solution de l'exercice 7 Notons $\alpha_1, \ldots, \alpha_n$ les n racines de P. On écrit :

$$\frac{P''(x)P(x) - P'(x)^2}{P(x)^2} = \left(\frac{P'(x)}{P(x)}\right)' = \sum_{i=1}^{n} \frac{-1}{(x-\alpha_i)^2}.$$

Ainsi,

$$\begin{aligned}(n-1)P'(x)^2 - nP(x)P''(x) &= P(x)^2 \cdot \frac{n(P'(x)^2 - P(x)P''(x)) - P'(x)^2}{P(x)^2} \\ &= P(x)^2 \left(\sum_{i=1}^{n} \frac{n}{(x-\alpha_i)^2} - \left(\sum_{i=1}^{n} \frac{1}{(x-\alpha_i)}\right)^2\right),\end{aligned}$$

qui est positif d'après l'inégalité de Cauchy–Scwharz. Le cas d'égalité s'obtient lorsque tous les α_i sont égaux, i.e. lorsque $P(x)$ est de la forme $P(x) = c(X-a)^n$.

Solution de l'exercice 8 On a déja résolu le problème lorsque le degré de P est au plus $n-1$ grâce aux interpolateurs de Lagrange. Si le degré de P est supérieur ou égal à n, notons L le polynôme interpolateur associé aux a_i et b_i. Le polynôme $P-L$ s'annule en $a_1, \dots, a_n$. On a donc

$$P(X) = c_1 \sum_{i=1}^{n} b_i \prod_{j=1, j\neq i}^{n} \frac{X-a_j}{a_i-a_j} + c_2(X-a_1)(X-a_2)\cdots(X-a_n).$$

Solution de l'exercice 9 Un polynôme à coefficients rationnels est clairement solution. Réciproquement, si P est un polynôme de degré n vérifiant cette propriété, alors en interpolant en $n+1$ points rationnels, on remarque que P est à coefficients rationnels.

Solution de l'exercice 10

1. Soit $i \geqslant n$. Alors
$$\frac{1}{n!}\prod_{k=0}^{n-1}(i-k) = \binom{i}{n} \in \mathbb{Z}.$$
On traite similairement le cas $i < 0$.
2. On remarque que $H_n(n) = 1$ et $H_n(i) = 0$ pour des entiers $0 \leqslant i \leqslant n-1$. Si $P \in \mathbb{C}[X]$ est tel que $P(k) \in \mathbb{Z}$ pour tout $k \in \mathbb{N}$, notons n le degré de P et soit
$$Q(X) = P(X) - \sum_{i=0}^{n} P(i)H_i(X).$$
Le polynôme Q est de degré n et possède $n+1$ racines $0, 1, \dots, n$. On en déduit que Q est nul. Les polynômes cherches sont donc des combinaisons linéaires entières des polynômes de Hermite.
3. (i) On a
$$\begin{aligned} X^k = (X+1-1)^k &= \sum_{i=0}^{k}\binom{k}{i}(X+1)^i(-1)^{k-i} = \sum_{i=0}^{k}\binom{k}{i}\left(\sum_{j=0}^{i}\binom{i}{j}X^j\right)(-1)^{k-i} \\ &= \sum_{j=0}^{k}\left(\sum_{i=j}^{k}(-1)^{k-i}\binom{k}{i}\binom{i}{j}\right)X^j. \end{aligned}$$
Ainsi, en identifiant les coefficients, la somme cherchée est nulle pour $0 \leqslant j \leqslant k-1$ et vaut 1 pour $j = k$.

(ii) Pour prouver que 1. implique 2., si P est de degré n, on peut écrire
$$P(X) = \sum_{i=0}^{n} P(i)H_i(X).$$
On a alors pour tout entier $j \geqslant 0$.
$$P(j) = \sum_{k=0}^{n}\binom{j}{k}P(k)$$

et

$$\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}u_j = \sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}P(j) = \sum_{j=0}^{i}\sum_{k=0}^{n}(-1)^{i-j}\binom{i}{j}\binom{j}{k}P(k).$$

D'après ce qui précède, cette somme est nulle pour $i \geqslant n+1$.
Pour montrer que 2. implique 1., on voit que le polynôme

$$P(X) = \sum_{i=0}^{n} u_i H_i(X)$$

convient en utilisant un raisonnement similaire.

Solution de l'exercice 11 On met P sous forme canonique : $P = a(x-b)^2 + c$. On translate de b selon l'axe des abscisses, de $-c$ selon l'axe des ordonnées, et on applique une homothétie de rapport $\frac{1}{\sqrt{a}}$.

Solution de l'exercice 12 Soit (x, y, z) une solution. Visiblement, aucun de ces nombres n'est nul. En retranchant la troisième équation à la deuxième équation, on en déduit que $zx = xy$, puis, en simplifiant par x (qui est non nul), on obtient que $z = y$. En retranchant la troisième équation à la première équation, on obtient : $y^2 - xy = 8$, ou encore $xy = y^2 - 8$. La deuxième équation se réécrit $y^2x + xy = 4$. Il vient donc :

$$y(y^2-8) + y^2 - 8 = 4,$$

ou encore $y^3 + y^2 - 8y - 12 = 0$. On remarque que $y = 3$ est une solution. En effectuant la division euclidienne de $y^3 + y^2 - 8y + 12$ par $y - 3$, on trouve :

$$y^3 + y^2 - 8y - 12 = (y-3)(y^2+4y+4) = (y-3)(y+2)^2.$$

On en déduit que $y = z = 3$ ou $y = z = -2$. Dans le premier cas, $x = \frac{1}{3}$ et dans le deuxième cas, $x = 2$. Réciproquement, les triplets $(2,-2,-2)$ et $(\frac{1}{3},3,3)$ sont solution et ce sont donc les seules.

Solution de l'exercice 13 Supposons que $ax^2 - (a+3)x + 2 = 0$ admette deux racines de signe opposé, notées z_1, z_2. Alors d'après les relations de Viète, $z_1z_2 = 2/a$. Or z_1 et z_2 sont de signe opposés si, et seulement si, $z_1z_2 < 0$. On en déduit que $a < 0$. Réciproquement, si a<0, alors le discriminant de l'équation vaut $a^2 - 2a + 9$. Pour montrer qu'il est positif, utilisons la forme canonique en écrivant $a^2 - 2a + 9 = (a-1)^2 + 8 \geqslant 0$. Ainsi, lorsque $a < 0$, il y a deux solutions réelles notées z_1, z_2. D'après les relations de Viète, $z_1z_2 = 2/a < 0$, de sorte que z_1 et z_2 sont de signe opposés.

Remarquons que dans la preuve de la réciproque, il a d'abord fallu montrer que le polynôme avait deux racines réelles avant d'utiliser les relations de Viète.

Solution de l'exercice 14 On pose $P = \sum a_k X^k$, et on appelle n le degré de P. La somme des racines de $P^{(k)}$ vaut $\frac{a_{n-1}(n-1)(n-2)\ldots(n-k)}{a_n n(n-1)\ldots(n-k+1)} = \frac{a_{n-1}(n-k)}{a_n n}$. La suite est donc arithmétique, de raison $\frac{-a_{n-1}}{n a_n}$.

Solution de l'exercice 15 Indication : introduire $\sigma_1 = x + y$ et $\sigma_2 = xy$, puis écrire les équations correspondantes pour σ_1 et σ_2, puis les résoudre.

Solution de l'exercice 16 On a clairement $x/(x+y)+y/(x+y)=1$ et

$$\frac{x}{x+y}\cdot\frac{y}{x+y}=\frac{xy}{x^2+2xy+y^2}=1.$$

Ainsi, $x/(x+y)$ et $y/(x+y)$ sont les racines de $t^2-t+1=0$, de sorte que les sommes $S_k=(x/(x+y))^k+(y/(x+y))^k$ vérifient $S_0=2$, $S_1=1$ et

$$S_{k+2}=S_{k+1}-S_k$$

pour $k\geqslant 0$. On en déduit que la suite (S_k) est période de période 6, ses valeurs étant successivement $2,1,-1,-2,-1,1,2,1,-1,\ldots$. On en déduit que $S_{2013}=-2$.

Solution de l'exercice 17 On écrit les relations de Newton :

$$S_1-\sigma_1=0,\qquad S_2-\sigma_1S_1+2\sigma_2=0,\qquad S_3-\sigma_1S_2+\sigma_2S_1-3\sigma_3=0.$$

Ainsi, $\sigma_1=3$, $\sigma_2=3$, $\sigma_3=1$. On en tire que x,y,z sont racines de $t^3-3t^2+3t-1=0$. Or $t^3-3t^2+3t-1=(t-1)^3$. Donc $x=y=z=1$.

Solution de l'exercice 18 Voir le TD.

Solution de l'exercice 19 Écrivons

$$P(P(x))-Q(Q(x))=(Q(P(x))-Q(Q(x)))+S(P(x)),$$

où $S(x)=P(x)-Q(x)$. Suppsons que $S\neq 0$. Soient k le degré de S et n le degré de Q. On voit aisément que le degré de $Q(P(x))-Q(Q(x))$ est n^2-n+k et que le degré de $R(P(x))$ est kn.

Si $k\geqslant 1$, on a $kn<n^2-n+k$, et donc le degré de $P(P(x))-Q(Q(x))$ est n^n-n+k, absurde.

Si $k=0$, S est constant. Écrivons $S=c$. On obtient alors que $Q(Q(x)+c)=Q(Q(x)-c)$. Ainsi, $Q(z+c)=Q(z)-c$ pour une infinité de réels z, et donc $Q(x+c)=Q(x)-c$. Donc $Q(kc)=Q(0)-kc$ pour tout entier k, et donc $Q(x)=Q(0)-x$. Ceci contredit le fait que Q est unitaire.

Solution de l'exercice 20 Écrivons $P(x)=x^nQ(x)$ pour un certain entier $n\geqslant 0$ et $Q(x)$ un polynôme tel que $Q(0)\neq 0$. Alors Q vérifie la propriété de l'énoncé. Si Q n'est pas constant, en faisant tendre x vers l'infini, on voit que forcément $Q(0)=0$, absurde. Donc Q est constant est P est de la forme $P(x)=cx^n$ avec $c\in\mathbb{R}$ et $n\geqslant 0$. Réciproquement, on vérifie que les polynômes de la forme $P(x)=cx^n$ avec $|c|\leqslant 1$ et $n\geqslant 0$ conviennent.

Solution de l'exercice 21 Soit $P(x)=1+x+\cdots+x^{n-1}=(1-x^n)/(1-x)$. Ainsi, $P(x)$ divise $P(x^2)$ si et seulement si il existe un polynôme $Q(x)$ tel que

$$\frac{1-x^{2n}}{1-x^2}=Q(x)\frac{1-x^n}{1-x},$$

ou encore

$$(1+x^n)=Q(x)(1+x).$$

Ainsi, $P(X)$ divise $P(X^2)$ si et seulement si -1 est racine de $1+X^n$, autrement dit si et seulement si n est impair.

Solution de l'exercice 22 La première assertion est vraie (utiliser le théorème de Bézout pour les nombres entiers avec 7 et 12). La seconde assertion est fausse (prendre $x = 2^{1/3}$).

Solution de l'exercice 23 Supposons par l'absurde que P admette une racine réelle, α. Alors $\alpha^2 + \alpha + 1$ est une autre racine du polynôme, strictement supérieure à la précédente. On construit ainsi une infinité de racines distinctes, contradiction. Donc toutes les racines de P sont complexes, donc P est de degré pair.

En outre, il existe bien de tels polynômes P. Ainsi, pour tout entier naturel k, le polynôme $P_k(X) = (X^2+1)^k = (X+i)^k(X-i)^k$ est bien tel que $P_k(X^2+1) = (X^2+X+1-i)^k(X^2+X+1+i)^k = (X+1+i)^k(X+1-i)^k(X-i)^k(X+i)^k = (X^2+2X+2)^k(X^2+1)^k$ est soit divisible par $P_k(X)$.

Solution de l'exercice 24 On écrit P comme produit de polynômes irréductibles dans $\mathbb{R}$. P est le produit de polynômes de degrés 2 de discriminant négatifs et de polynômes de la forme $(x-a)^{2k}$ (en effet si la multiplicité d'une racine était impaire, au voisinage de cette racine on pourrait rendre P négatif). Pour exprimer la partie complexe comme somme de carrés, on la sépare en deux termes conjugués l'un de l'autre (en séparant les termes $(X-z)$ des $(X-\bar{z})$). Cela termine, car $(P-iQ)(P+iQ) = P^2+Q^2$.

Solution de l'exercice 25 On démarre par diviser P par son contenu, ce qui ne modifie pas les hypothèses (car ce contenu est impair). Supposons par l'absurde que P a toutes ces racines rationnelles. Comme $c(P) = 1$, ces racines sont entières. Comme d est impair, ces trois racines sont impaires, et les relations coefficients racines montrent que b et c sont impairs, ce qui est absurde.

Solution de l'exercice 26 Supposons qu'il existe deux polynômes g et h, à coefficients entiers, tels que $f = gh$. Comme $f(0) = 3$, on peut supposer, sans perte de généralité que $|g(0)| = 3$ et on écrit : $g(x) = x^k + a_{k-1}x^{k-1} + ... + a_0$ ($a_0 = \pm 3$). On s'inspire maintenant de la démonstration du critère d'Eisenstein : soit j le plus petit indice tel que a_j ne soit pas divisible par 3. On pose $h(x) = x^p + b_{p-1}x^{p-1} + ... + b_0$ et $f(x) = x^n + c_{n-1}x^{n-1} + ... + c_0$, il apparaît que le coefficient $c_j = a_j b_0 + a_{j-1}c_1 + ...$ n'est pas divisible par 3 car $b_0 a_0 = 3$ et $a_0 = \pm 3$. Compte tenu de l'expression de f,$j \geqslant n-1$, donc $k \geqslant n-1$ donc $p \leqslant 1$ donc le polynôme h s'écrit $\pm x \pm 1$, ce qui est absurde car $f(\pm 1) = 0$.

Solution de l'exercice 27 On écrit P sous la forme $P(X) = Q(X)(X-a)(X-b)(X-c)(X-d)+5$, et on suppose par l'absurde que $P(k) = 8$. Alors $Q(k)(k-a)(k-b)(k-c)(k-d) = 1$. Or, $(k-a)$, $(k-b)$, $(k-c)$ et $(k-d)$ sont des entiers distincts, et comme 3 est premier, il ne peut pas être écrit comme produit de 4 entiers distincts : il y a là une contradiction.

Solution de l'exercice 28 En injectant $a = b = c = 0$, on trouve $P(0) = 0$. En prenant $b = c = 0$, on obtient $P(-2a) = 3P(-a) + P(a)$, et ce pour tout a. On suppose P de degré n. En examinant les coefficients dominants, on obtient $2^n = (-1)^n + 3$, donc n vaut 1 ou 2, et P est de la forme $aX^2 + bX$. On vérifie réciproquement que ces polynômes conviennent.

Solution de l'exercice 29 On remarque tout d'abord, en prenant $b = c = 0$, que P est pair, et ne contient donc que des termes de degré pair. En évaluant en zéro, on trouve que le terme constant doit être nul. On essaie ensuite $a = 6x$, $b = 3x$ et $c = -2x$. Cela donne $P(3x) + P(5x) + P(-8x) = 2P(7x)$. On note n le degré de P. En comparant les coefficients dominants, on trouve $3^n + 5^n + (-8)^n = 2 \cdot 7^n$. C'est impossible pour $n \geqslant 5$. P est donc de la forme $aX^4 + bX^2$. On vérifie réciproquement que ces polynômes conviennent.

Solution de l'exercice 30 Soit $c_n(k)$ le nombre de permutations de longueur n. Pour résoudre l'exercice, établissons une relation de récurrence sur les $c_n(k)$. Nous allons, pour cela, dénombrer les permutations $\sigma \in \mathfrak{S}_n$ tel que $\mathrm{cyc}(\sigma) = k$ en les comptant séparément selon la valeur de $\sigma(n)$. Si $\sigma(n) = n$, on remarque que se donner une telle permutation revient simplement à se donner une permutation de $\{1, \dots, n-1\}$ ayant $(k-1)$ cycles (puisque n est tout seul dans son cycle). Il y a donc $c_{n-1}(k-1)$ permutations qui relèvent de ce cas.

Examinons maintenant le cas où $\sigma(n)$ est un entier m fixé strictement inférieur à n. L'entier n apparaît alors dans un cycle de σ qui est de longueur au moins 2 (puisqu'il contient au moins n et m) et on peut construire une permutation τ de $\{1, \dots, n-1\}$ simplement en retirant n de ce cycle et en laissant les autres cycles inchangés. Par construction, il est évident que τ a encore k cycles. Par ailleurs, on peut reconstruire σ à partir de τ et l'entier m comme suit : on regarde le cycle de τ qui contient m et, dans ce cycle, on insère l'entier n juste avant m. On déduit de cela qu'il y a $c_{n-1}(k)$ permutations à k cycles telles $\sigma(n)$ est égal à un entier $m < n$ fixé.

En mettant ensemble les deux raisonnements précédents, on aboutit à $c_n(k) = c_{n-1}(k-1) + (n-1)c_{n-1}(k)$. En tenant compte du fait que $c_{n-1}(0) = c_{n-1}(n) = 0$ trivialement, et en sommant l'égalité précédente pour k variant de 1 à n, il vient :

$$P_n(x) = \sum_{k=1}^{n} c_n(k)x^k = \sum_{k=1}^{n-1} c_{n-1}(k)x^{k+1} + (n-1) \cdot \sum_{k=1}^{n-1} c_{n-1}(k)x^k = (x+n-1) \cdot P_{n-1}(x),$$

ce qui permet de conclure l'exercice.

Solution de l'exercice 31 PREMIÈRE SOLUTION. Si $n < 2^{k+1}$, soit A un polynôme à coefficients entiers tel que $P = 2A + \sum_{i=1}^{n} X^i$. Pour tout polynôme $Q(X) \in \mathbb{Z}[X]$, on sait que $Q(X)^2 - Q(X^2) \in 2\mathbb{Z}[X]$: il suffit, pour s'en convaincre, de développer $Q(X)^2$ et de considérer tous les coefficients dans $\mathbb{Z}/2\mathbb{Z}$, annulant ainsi les doubles produits. Un récurrence montre alors qu'il existe un polynôme $B \in \mathbb{Z}[X]$ tel que $(X-1)^{2^k} = X^{2^k} + 1 + 2B(X)$.

Or, si $(X-1)^m$ divise P et si $m \geqslant 2^k$, c'est qu'il existe deux polynômes C et D, où C a ses coefficients dans $\{0, 1\}$, tels que $P = (X-1)^{2^k}(C + 2D)$. En développant, on trouve $2A + \sum_{i=1}^{n} X^i = (X^{2^k}+1)C + 2((X-1)^{2^k}D + BC + 2BD)$. En outre, puisque $n < 2^{k+1}$, alors $\deg(C + 2D) < 2^k$, donc $\deg C < 2^k$. En particulier, $(X^{2^k} + 1)$ a ses coefficients dans $\{0, 1\}$. Ainsi, le polynôme $\sum_{i=1}^{n} X^i - (X^{2^k} + 1)C$ a des coefficients pairs et appartenant à $\{-1, 0, 1\}$: ils sont tous nuls. Puisque $n \geqslant 2^k$, on en déduit que $\deg C \geqslant 2^k - 1$, donc que $\deg C = 2^k - 1$ et que $n = 2^k + \deg C = 2^{k+1} - 1$.

DEUXIÈME SOLUTION. Cette solution fait appel à des notions a priori plus avancées, mais apparaît alors comme plus naturelle : c'est d'ailleurs d'une telle solution que l'on peut « humainement » trouver une solution telle que la première solution.

L'énoncé suggère de se placer à la fois modulo 2 (les coefficients de A sont impairs) et modulo $(X-1)^{2^k}$ (on veut tester une divisibilité par $(X-1)^m$ avec $m \geqslant 2^k$) : qu'à cela ne tienne, faisons les deux à la fois ! Tout d'abord, on remarque, comme dans la première solution, que, sitôt qu'on se place dans $\mathbb{F}_2[X]$ ($\mathbb{F}_2$ désigne le corps à 2 éléments, c'est-à-dire $\mathbb{Z}/2\mathbb{Z}$), on sait que $(a+b)^2 \equiv a^2 + 2ab + b^2 \equiv a^2 + b^2$. Une simple récurrence montre alors que $Q(X^2) \equiv Q(X)^2$ puis que $(X-1)^{2^k} \equiv X^{2^k} + 1$.

Ensuite, notons que $A \equiv \sum_{i=0}^{n} X^i \equiv \frac{X^{n+1}+1}{X+1} \pmod 2$. On en profite pour se rappeler que $n = \deg A \geqslant m \geqslant 2^k$, de sorte que $n + 1 > 2^k$. Alors $X^{2^k} + 1$ divise $(X+1)A = X^{n+1} + 1$ dans $\mathbb{F}_2[X]$. Or, si on écrit $n + 1 = q2^k + r$ avec $q \in \mathbb{N}$ et $0 \leqslant r < 2^k$, on sait que $X^{n+1} + 1 \equiv$

$X^r + 1 \pmod{2, X^{2^k+1}}$. Donc $X^{2^k} + 1$ divise aussi $X^r + 1$ dans $\mathbb{F}_2[X]$, de sorte que $r = 0$. Ainsi, 2^k divise $n + 1 > 2^k$, donc $n + 1 \geqslant 2^{k+1}$, ce qui conclut.

2 TD de polynômes

- Énoncés des exercices -

Exercice 1 Soit P un polynôme à coefficients entiers. Montrez que pour tous entiers a et b, $(a - b)$ divise $(P(a) - P(b))$.

Exercice 2 Trouver tous les polynômes réels P tels que $P(0) = 0$ et $P(X^2 + 1) = P(X)^2 + 1$.

Exercice 3 Soient a, b, c, d les quatre racines de $X^4 - X^3 - X^2 - 1$. Calculer $P(a) + P(b) + P(c) + P(d)$, où $P(X) = X^6 - X^5 - X^4 - X^3 - X$.

Exercice 4 Soit P un polynôme réel. Le reste de la division euclidienne de $P(X)$ par $X - 1$ est 2 est le reste de la division euclidienne par $X - 2$ est 1. Quel est le reste de la division euclidienne de $P(X)$ par $X^2 - 3X + 2$?

Exercice 5 Trouver tous les triplets x, y, z tels que

$$\begin{aligned} x + y + z &= 5 \\ x^2 + y^2 + z^2 &= 19 \\ x^3 + y^3 + z^3 &= 53 \end{aligned}$$

Exercice 6 Le produit de deux des quatre racines du polynôme

$$P(X) = X^4 - 18X^3 + kX^2 + 200X - 1984$$

est égal à -32. Trouvez k.

Exercice 7 Soit P un polynôme réel qui vérifie $P(x) \geqslant 0$ pour tout $x \in \mathbb{R}$. Montrez qu'il existe deux polynômes Q et R tels que

$$P(X) = Q(X)^2 + R(X)^2.$$

Exercice 8

1. Trouvez tous les polynômes réels P tels que $P(X^2) = P(X)^2$.
2. Trouvez tous les polynômes réels P tels que $P(X^2) = P(X)P(X + 1)$.
3. Trouvez tous les polynômes réels P tels que $P(X + 1) + P(X - 1) = 2P(X)$.

Exercice 9 Soit P un polynôme réel qui vérifie $P(\cos x) = P(\sin x)$. Montrer qu'il existe un polynôme Q tel que

$$P(X) = Q(X^4 - X^2).$$

Exercice 10 Soit P un polynôme à coefficients entiers de degré $n \geqslant 2$. Soit k un entier et Q le polynôme

$$Q(X) = P(P(\cdots(P(X))\cdots)),$$

où P est écrit k fois. Montrez qu'il y a au plus n entiers a tels que $Q(a) = a$.

Exercice 11 Trouver tous les couples de polynômes réels P et Q tels que

$$P(Q(X)) = (X-1)(X-2)\ldots(X-15).$$

Exercice 12 Soit P un polynôme à coefficients entiers. Soit n un entier impair et $x_1, x_2, \ldots, x_n$ une famille de n entiers tels que $P(x_1) = x_2$, $P(x_2) = x_3$, …, $P(x_n) = x_1$. Montrez que tous les x_i sont égaux.

- Solutions des exercices -

Solution de l'exercice 1 Écrivons P sous la forme $P(X) = \sum_{i=0}^{n} p_i X^i$. En utilisant la relation $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$, on trouve la factorisation

$$P(a) - P(b) = (a-b)\left(\sum_{i=0}^{n} p_i \sum_{j=0}^{i-1} a^j b^{i-1-j}\right),$$

d'où l'on tire la relation de divisibilité demandée.

Solution de l'exercice 2 Soit (u_n) la suite réelle telle que $u_0 = 0$ et $u_{n+1} = u_n^2 + 1$. Une récurrence immédiate montre que $P(u_n) = u_n$. La suite (u_n) étant strictement croissante, le polynôme $P(X) - X$ a une infinité de racines, ce qui prouve que $P(X) = X$, qui est effectivement une solution du problème.

Solution de l'exercice 3 Tout d'abord, remarquons que $P(X) = X^2(X^4 - X^3 - X^2 - 1) - X^3 + X^2 - X$. En utilisant la formule de récurrence sur les polynômes symétriques, il nous suffit de calculer $-S_3 + S_2 - S_1$. Or, $\sigma_1 = 1$, $\sigma_2 = -1$ et $\sigma_3 = 0$. Donc $S_1 = \sigma_1 = 1$, $S_2 = \sigma_1 S_1 - 2\sigma_2 = 3$ et $S_3 = \sigma_1 S_2 - \sigma_2 S_1 + 3\sigma_3 = 4$, et la somme recherchée est -2.

Solution de l'exercice 4 La clé est d'utiliser le théorème des restes chinois pour les polynômes : en l'occurrence, on introduit le polynôme $Q(X) = -X + 3$. Alors $P(X)$ et $Q(X)$ ont même reste dans les divisions euclidiennes par $X-1$ et $X-2$, ce qui signifie que $P(X) - Q(X)$ est divisible à la fois par les polynômes $X-1$ et $X-2$ premiers entre eux, donc par leur produit $X^2 - 3X + 2$. En particulier, le reste recherché est $Q(X) = -X + 3$.

Solution de l'exercice 5 On utilise une fois de plus la formule de récurrence sur les polynômes symétriques : ici $S_1 = 5$, $S_2 = 19$ et $S_3 = 53$, donc $\sigma_1 = S_1 = 5$, $\sigma_2 = \frac{1}{2}(\sigma_1 S_1 - S_2) = 3$ et $\sigma_3 = \frac{1}{3}(S_3 - \sigma_1 S_2 + \sigma_2 S_1) = -9$. Les réels x, y, z recherchés sont donc les racines du polynôme $X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3 = X^3 - 5X^2 + 3X + 9 = (-3+X)^2(1+X)$. À symétrie des variables x, y et z près, nous recherchions donc le triplet $(-1, \sqrt{3}i, -\sqrt{3}i)$.

Solution de l'exercice 6 Notons a et a' les racines de P donc le produit vaut -32, b et b' les deux autres racines de P. On sait que $aa'bb' = -1984$, donc $bb' = \frac{-1984}{-32} = 62$. Ainsi, $a' = -\frac{32}{a}$ et $b' = \frac{62}{b}$. En outre, $a + a' + b + b' = a - \frac{32}{a} + b + \frac{62}{b} = 18$, tandis que $aa'bb'\left(\frac{1}{a} + \frac{1}{a'} + \frac{1}{b} + \frac{1}{b'}\right) =$

$-1984\left(\frac{1}{a}-\frac{a}{32}+\frac{1}{b}+\frac{b}{62}\right)=-200$, ou encore $-\frac{a+a'}{32}+\frac{b+b'}{62}=-\frac{200}{1984}$. Ces deux égalités nous indiquent donc que $a+a'=4$ et $b+b'=14$. Puisque $k=aa'+bb'+(a+a')(b+b')$, il s'ensuit que $k=86$, qui, réciproquement, convient bien.

Solution de l'exercice 7 Il s'agit en fait de l'exercice 24 prévu en cours, mais non traité durant la séance et donc reporté à la séance de TD.

Solution de l'exercice 8

1. Si $x=r\exp(i\theta)$ est une racine de P et $y=\sqrt{r}\exp(i\theta/2)$ une racine carrée de x (avec $0\leqslant r$ et $0<\theta\leqslant 2\pi$), alors ρ est aussi une racine de P. Ce faisant, si P admet une racine non nulle, alors il admet des racines ayant une infinité d'arguments différents, et donc $P=0$. On peut ainsi chercher P de la forme $P(X)=cX^n$, qui convient si et seulement si $x\in\{0,1\}$.
2. Si x est une racine de P, alors x^2 et $(x-1)^2$ aussi : si P est non nul, alors $|x|\in\{0,1\}$, donc $|x-1|\in\{0,1\}$, de sorte que $x\in\{0,1,\omega,\overline{\omega}\}$, où $\omega=\exp(\frac{i\pi}{6})$. Ainsi, ni $(\omega-1)^2$ ni $(\overline{\omega}-1^2)$ n'est racine de P, d'où $x\in\{0,1\}$: $P(X)=cX^a(X-1)^b$. L'équation devient alors $cX^{2a}(X-1)^b(X+1)^b=c^2(X-1)^bX^{a+b}(X+1)^a$: les solutions sont donc les polynômes dela forme $cX^n(X-1)^n$, où $x\in\{0,1\}$.
3. Posons tout d'abord $a=P(1)-P(0)$ et $b=P(0)$. L'équaiton donne $P(X+1)-P(X)=P(X)-P(X-1)$, donc $P(n+1)-P(n)=a$ pour tout entier $n\in\mathbb{N}$. En particulier, le polynôme $P(X+1)-P(X)-a$ est donc nul, et on sait que $P(n)=b+na$ pour tout entier $n\in\mathbb{N}$, de sorte que le polynôme $P(X)-aX-b$ est lui aussi nul. Ainsi, P est un polynôme affine, et alors il convient en effet.

Solution de l'exercice 9 Soit $r\in[-1,1]$ un réel, et $x=\arcsin(r)$. Alors $P(r)=P(\sin x)=P(\cos x)=P(\cos(-x))=P(\sin(-x))=P(-r)$, de sorte que P est pair et que l'on peut écrire $P(X)=R(X^2)$. L'équation devient alors : $R(r^2)=P(r)=P(\sin x)=P(\cos x)=P(\sqrt{1-\sin^2 x})=R(1-\sin^2 x)=R(1-r^2)$. Tout réel $r^2\in[0,1]$ est donc racine du polynôme $R(X)-R(1-X)$, de sorte que $R(X)=R(1-X)$: en posant $S(X)=R(X+1/2)$, il vient $S(X)=R(X+1/2)=R(1/2-X)=S(-X)$, donc S est pair et l'on peut écrire $S(X)=T(X^2)$. Enfin, en posant $Q(X)=T(X+1/4)$, il s'ensuit que $P(X)=R(X^2)=S(X^2-1/2)=T(X^4-X^2+1/4)=Q(X^4-X^2)$.

Solution de l'exercice 10 Supposons que l'entier a soit un point fixe de Q. On définit la suite (a_i) par a_0 et $a_{i+1}=P(a_i)$. Alors on sait que $a_0=a_k$, et que chaque $a_{i+1}-a_i$ divise $P(a_{i+1})-P(a_i)=a_{i+2}-a_{i+1}$. La suite (a_i) est cyclique, et la suite des différences de deux termes consécutifs croît (en valeur absolue), de sorte que $a_2=a_0$ et que a est point fixe de $P(P(X))$ et décrit, sous l'action de P, une orbite de cardinal 1 ou 2 (cela veut dire que la suite (a_i) prend une ou deux valeurs distinctes).

S'il n'existe aucune telle orbite de cardinal 2, alors a est nécessairement point fixe de $P(X)$ et, puisque $P(X)-X$ est de degré n, il existe au plus n tels points. S'il existe deux entiers $a<b$ tels que $P(a)=b$ et $P(b)=a$, soit c un point fixe de $P(P(X))$, et $d=P(c)$, tels que $c\leqslant d$. Alors $c-a$ divise $d-b$, qui lui-même divise $c-a$, donc $|c-a|=|d-b|$; de même, $c-b$ divise $d-a$, qui lui-meme divise $c-b$, de sorte que $|c-b|=|d-a|$. Cela montre que $a+b=c+d$, de sorte que c est nécessairement une racine du polynôme $X+P(X)-a-b$, dont le degré est n : ainsi, même dans ce cas, $P(P(X))$ a au plus n points fixes entiers.

Solution de l'exercice 11 Posons $R(X) = \prod_{k=1}^{15}(X-k)$, ainsi que $m = \deg P$ et $n = \deg Q$. Notons que, si $a \neq 0$, alors remplacer $P(X)$ et $Q(X)$ par $P(\frac{X-b}{a})$ et $aQ(X)+b$ ne change rien au problème, de sorte que l'on suppose tout d'abord que Q est unitaire et que $Q(1) = 0 : 0$ est alors racine de P, qui se trouve lui aussi être unitaire.

En outre, $15 = \deg R = mn$, donc $(m,n) \in \{(1,15),(3,5),(5,3),(15,1)\}$. Si $m = 1$, alors nécessairement $Q(X) = X-1$ et $P(X) = R(X)+15$!. Si $m = 15$, alors nécessairement $Q(X) = R(X)$ et $P(X) = X$. Il nous reste donc à nous intéresser au cas où $m = 3$ ou bien $m = 5$.

Dans ces deux cas, soit λ_i les racines de P (avec $1 \leqslant i \leqslant m$) et $\mu_{i,j}$ les racines de $Q-\lambda_i$ (avec $1 \leqslant j \leqslant n$). On sait que $\{\mu_{i,j} : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\} = \{1,2,\dots,15\}$: les n familles de racines $(\mu_{i,j})_{1\leqslant j\leqslant m}$ ont les mêmes polynômes symétriques $\sigma_1,\dots,\sigma_{m-1}$, donc les mêmes polynômes de Newton $S_1,\dots,S_{m-1}$ (avec $S_k = \sum_{j=1}^{m}\mu_{i,j}^k$). En particulier, $S_k = \frac{1}{n}\sum_{t=1}^{15} t^k$ pour $1 \leqslant k < m$; et, puisque les $\mu_{i,j}$ sont entiers, S_k est entier également.

Or, pour $m = 5$, on remarque que l'on doit avoir $\sum_{t=1}^{15} t^2 \equiv 1 \pmod 3$, de sorte que S_2 ne peut être entier : cette situation est impossible. Il nous reste à étudier le cas $m = 3$, où l'on peut écrire $Q(X) = (X-1)(X-\mu_{1,2})(X-\mu_{1,3})$, en choisissant $\lambda_1 = 0$. Alors $\mu_{1,2}+\mu_{1,3} = S_1 - 1 = 23$ et $\mu_{1,2}^2+\mu_{1,3}^2 = S_2 - 1 = 247$, de sorte que $\mu_{1,2}\mu_{1,3} = \frac{23^2-247}{2} = 141$; 141 est un nombre premier, donc une telle factorisation n'existe pas.

Les polynômes P et Q recherchés sont donc les polynômes $P(X) = R(\frac{X-b}{a})$ et $Q(X) = aX+b$, ou bien $P(X) = \frac{X-b}{a}$ et $Q(X) = aR(X)+b$, où $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$.

Solution de l'exercice 12 D'après l'exercice 1, on sait que x_2-x_1 divise x_3-x_2, qui divise x_4-x_3, etc, jusqu'à x_n-x_{n-1}, qui divise x_1-x_n. Les $|x_{i+1}-x_i|$ sont donc deux à deux égaux (en notant $x_1 = x_{n+1}$), de sorte que l'on peut écrire $x_{i+1} = x_i + a\varepsilon_i$, avec $a = |x_2-x_1|$ et $\varepsilon_i \in \{-1,1\}$. En particulier, $0 = x_{n+1}-x_1 = a\sum_{i=1}^{n}\varepsilon_i$: le facteur de droite est un nombre impair, donc non nul, de sorte que $a = 0$, c'est-à-dire que $x_1 = x_2 = \cdots = x_n$.

4 Groupe D : géométrie

1 Cours/TD de géométrie : inversions

Le but de cette séance est de vous présenter une transformation géométrique très puissante, et potentiellement utile pour la résolution de problèmes olympiques : l'inversion.

Dans toute cette partie, tous les angles sont orientés et considérés modulo 2π.

- Inversion : définition et action sur les angles -

Soit $\mathcal{E}$ le plan euclidien usuel.

Définition 4.1. Soit O un point du plan $\mathcal{E}$, et p un réel non nul. On appelle *inversion* de *pôle* O et de *puissance* p la transformation de $\mathcal{E}\backslash\{O\}$ dans lui-même envoyant le point M sur le point M' de (OM) tel que $\overline{OM'} \cdot \overline{OM} = p$. (Autrement dit, M' est le point de (OM) tel que $\overrightarrow{OM'} = \frac{p}{OM^2}\overrightarrow{OM}$). Nous la noterons $I_{O,p}$.

Remarques 4.2.
- Clairement, $I_{O,p}(I_{O,p}(M)) = M$: l'inversion est une involution. En particulier, elle est bijective.
- Soit r la racine carrée de $|p|$. Notons $\mathcal{C}_{O,r}$ le cercle de centre O et de rayon r. Alors $I_{O,p}$ échange intérieur et extérieur de $\mathcal{C}_{O,r}$, agit comme la symétrie de centre O sur $\mathcal{C}_{O,r}$ si p est négatif, et stabilise $\mathcal{C}_{O,r}$ si p est positif. On appelle souvent I_{O,r^2} l'inversion de cercle $\mathcal{C}_{O,r}$.
- Soit P un point non fixé par $I_{O,p}$. Alors la puissance de O par rapport à un cercle passant par P et P' est p, la puissance de l'inversion considérée.

Proposition 4.3. Soient P et Q dans $\mathcal{E}\backslash\{O\}$, et P' et Q' leurs images par $I_{O,p}$. Alors OPQ et $OQ'P'$ sont inversement semblables.

Démonstration. Clairement, $\widehat{POQ} = \widehat{P'OQ'}$. De plus, $\frac{OP}{OQ'} = \frac{|p|}{OP'} \cdot \frac{OQ}{|p|} = \frac{OQ}{OP'}$. □

Remarques 4.4. On en déduit deux propriétés importantes :
- une formule bien pratique sur l'effet de l'inversion sur les distances :

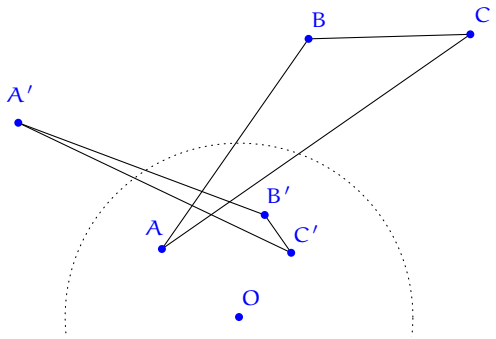
$$P'Q' = \frac{OQ'}{OP} \cdot PQ = \frac{|p|}{OP \cdot OQ} \cdot PQ,$$

- l'effet de l'inversion sur les angles issus du pôle : $\widehat{OPQ} = -\widehat{OQ'P'}$. En particulier, P, P', Q et Q' sont cocycliques.

Cela nous permet de déduire l'effet d'une inversion sur des angles plus généraux :

Proposition 4.5. Soient A, B et C des points distincts du pôle. On a alors $\widehat{ABC} = \widehat{C'B'A'} + \widehat{A'OC'}$.

Démonstration.



On a

$$\begin{aligned}\widehat{ABC} &= \widehat{ABO} + \widehat{OBC} \\ &= \widehat{OA'B'} + \widehat{B'C'O} \\ &= 2\pi + \widehat{A'OB'} + \widehat{OB'A'} + \widehat{C'B'O} + \widehat{B'OC'} \\ &= \widehat{C'B'A'} + \widehat{A'OC'}.\end{aligned}$$

□

Que se passe-t-il si A et C sont très proches de B ? Et bien, par continuité de l'inversion l'angle $\widehat{A'OC'}$ est très petit, et donc $\widehat{C'B'A'}$ est très proche de $\widehat{ABC}$. On dit que l'inversion renverse localement les angles. Voici un autre point de vue : considérons deux courbes suffisamment régulières s'intersectant en B. On les paramètre par deux fonctions ϕ et ψ de $\mathbb{R}$ dans $\mathcal{E}$ valant B en 0. Quand t est très petit, l'angle $\widehat{\phi(t)B\psi(t)}$ tend vers l'angle entre les tangentes en B des deux courbes, qui par définition est l'angle entre les deux courbes. De même, l'angle $\widehat{\phi(t)'B'\psi(t)'}$ tend vers l'angle entre les images de nos deux courbes par l'inversion. Enfin, l'angle $\widehat{\phi(t)'O\psi(t)'}$ tend vers 0. Nous avons montré que l'inversion inverse les angles entre courbes. Par exemple, les images de deux droites orthogonales par notre inversion seront deux courbes orthogonales.

- Images des droites et des cercles -

Cette section est justement dédiée à l'étude de l'image de certaines courbes par une inversion.

Proposition 4.6. L'inversion $I_{O,p}$ laisse globalement stable toute droite passant par O.

Proposition 4.7. L'inversion $I_{O,p}$ envoie un cercle ne passant pas par O sur un autre cercle ne passant pas par O.

Démonstration. On pourrait raisonner en regardant l'effet de l'inversion sur le théorème de l'angle inscrit, mais je préfère donner une preuve inspirée des remarques suivantes :

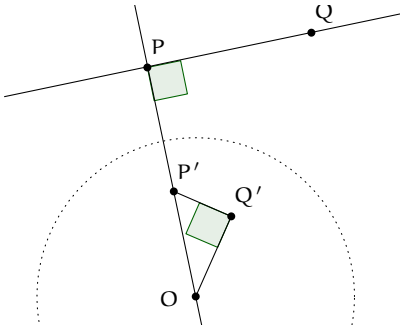
- L'inversion $I_{O,p}$ laisse globalement invariant tout cercle tel que O ait pour puissance p par rapport à ce cercle.
- Notons $h_{O,\lambda}$ l'homothétie de centre O et de rapport λ. Alors $h_{O,\lambda} \circ I_{O,p} = I_{O,\lambda p}$.

Considérons donc $\mathcal{C}$ un cercle ne passant pas par O. Notons p' la puissance de O par rapport à ce cercle (qui est non nulle). Alors $I_{O,p}(\mathcal{C}) = h_{O,\frac{p}{p'}} \circ I_{O,p'}(\mathcal{C})$ donc $I_{O,p}(\mathcal{C}) = h_{O,\frac{p}{p'}}(\mathcal{C})$ qui est de toute évidence un cercle ne passant pas par O. □

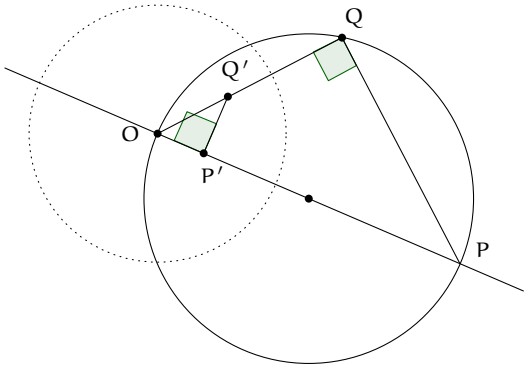
Notons que, par symétrie du problème par rapport à la droite reliant pôle et centre du cercle, le centre du cercle de départ, le centre de son image et le pôle sont alignés, un fait souvent bien utile. Autre fait utile que l'on pourrait déduire de cette preuve : si $\mathcal{C}$ et $\mathcal{C}'$ sont deux cercles et O un point, il existe une inversion centrée en O envoyant $\mathcal{C}$ sur $\mathcal{C}'$ si et seulement s'il existe une homothétie centrée en O envoyant $\mathcal{C}$ sur $\mathcal{C}'$.

Proposition 4.8. L'inversion $I_{O,p}$ envoie une droite ne passant pas par O sur un cercle passant par O et envoie un cercle passant par O sur une droite ne passant pas par O.

Démonstration. Soit D une droite ne passant pas par O. Soit P le projeté orthogonal de O sur D. Soit Q sur D. L'angle $\widehat{OPQ}$ est droit, donc l'angle $\widehat{OQ'P'}$ est droit, donc Q′ appartient au cercle de diamètre OP′.



Réciproquement, soit $\mathcal{C}$ un cercle passant par O, P le point de $\mathcal{C}$ diamétralement opposé à O. Soit Q sur $\mathcal{C}$. L'angle $\widehat{OQP}$ est droit, donc l'angle $\widehat{OP'Q'}$ est droit, donc Q′ est sur la droite orthogonale à OP′ passant par P′.



□

Voici une autre façon de formuler ces résultats. Rajoutons au plan un point à l'infini, que nous appelons ∞. Étendons l'inversion $I_{O,p}$ en une application de $\mathcal{E} \cup \{\infty\}$ dans lui-même, en décrétant que le pôle est envoyé à l'infini et que le point à l'infini est envoyé sur le pôle. La nouvelle inversion est elle aussi involutive. Disons enfin que, par convention, les droites sont les cercles passant par le point à l'infini. Alors les résultats de cette partie disent simplement que l'inversion envoie cercles sur cercles.

- L'inversion en pratique -

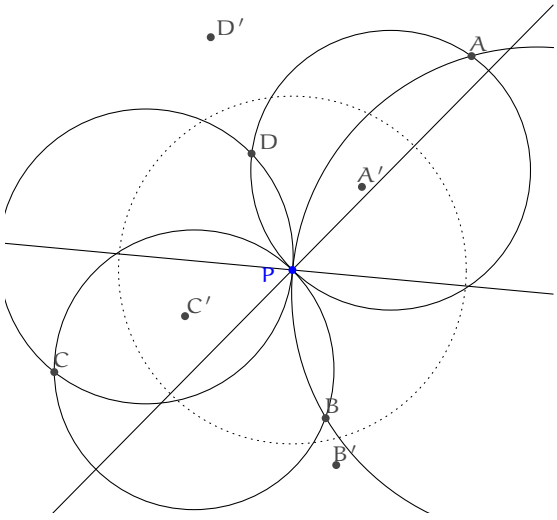
Maintenant, nous allons voir comment se servir de l'inversion pour résoudre des problèmes de type olympique. L'idée de base est la suivante : choisir une inversion, puis à l'aide des propriétés des inversions traduire les propriétés de la figure de départ en propriétés de la figure inversée. Si l'inversion est judicieuse, la figure inversée sera facile à étudier, on démontre donc des résultats sur cette figure inversée, puis on applique à nouveau l'inversion pour voir ce que ces résultats nous disent sur la figure de départ. Le point important est bien sûr le choix de l'inversion.

Une des forces de cette technique est qu'elle permet de se débarasser des cercles (en inversant par rapport à un des points du cercle), ce qui permet par exemple de transformer des problémes pénibles de tangences ou d'orthogonalité de cercles en des problèmes plus simples faisant intervenir des droites.

Exercice 1 Soit P un point, $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ et $\mathcal{C}_4$ quatre cercles tels que $\mathcal{C}_1$ et $\mathcal{C}_3$ soient extérieurement tangents en P, et que $\mathcal{C}_2$ et $\mathcal{C}_4$ soient extérieurement tangents en P. Supposons que $\mathcal{C}_1$ et $\mathcal{C}_2$, $\mathcal{C}_2$ et $\mathcal{C}_3$, $\mathcal{C}_3$ et $\mathcal{C}_4$ et $\mathcal{C}_4$ et $\mathcal{C}_1$ s'intersectent en des points A, B, C et D distincts de P. Prouver que

$$\frac{AB \cdot BC}{AD \cdot DC} = \frac{PB^2}{PD^2}.$$

Solution de l'exercice 1 Appliquons une inversion de centre P et de puissance p quelconque. Cette inversion transforme $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ et $\mathcal{C}_4$ en quatre droites D_1, D_2, D_3 et D_4 passant par P, telles que D_1 et D_3 soient parallèles, et D_2 et D_4 soient parallèles (en effet P, l'unique point d'intersection de $\mathcal{C}_1$ et $\mathcal{C}_3$, est envoyé à l'infini par l'inversion).



Ainsi, A', B', C' et D' sont les sommets d'un parallélogramme, donc $A'B' = C'D'$ et $B'C' = D'A'$.

Utilisons la formule sur les distances pour revenir aux distances de départ, on obtient

$$\frac{AB}{PA \cdot PB} = \frac{CD}{PC \cdot PD'}, \qquad \frac{BC}{PB \cdot PC} = \frac{DA}{PD \cdot PA'},$$

d'où le résultat recherché.

Une autre force de l'inversion est la relation $\widehat{OPQ} = -\widehat{OQ'P'}$, qui permet de changer le sommet d'un angle, et permet de simplifier grandement certaines relations faisant intervenir des sommes d'angles. Cette astuce permet notamment de trivialiser les exercices 2 des olympiades 1993 et 1996.

Exercice 2 Soit $ABCD$ un quadrilatère tel que $\widehat{DAB} + \widehat{BCD} = 90°$. Montrer que

$$AB^2 \cdot CD^2 + AD^2 \cdot BC^2 = AC^2 \cdot BD^2.$$

Solution de l'exercice 2 Appliquons une inversion de centre D et de puissance p quelconque. Alors

$$\begin{aligned} 90° &= \widehat{DAB} + \widehat{BCD} \\ &= \widehat{A'B'D} + \widehat{DB'C'} \\ &= \widehat{A'B'C'}. \end{aligned}$$

On en déduit que $A'B'^2 + B'C'^2 = A'C'^2$, donc que

$$\frac{p^2}{DA^2 \cdot DB^2} \cdot AB^2 + \frac{p^2}{DB^2 \cdot DC^2} \cdot BC^2 = \frac{p^2}{DA^2 \cdot DC^2} \cdot AC^2,$$

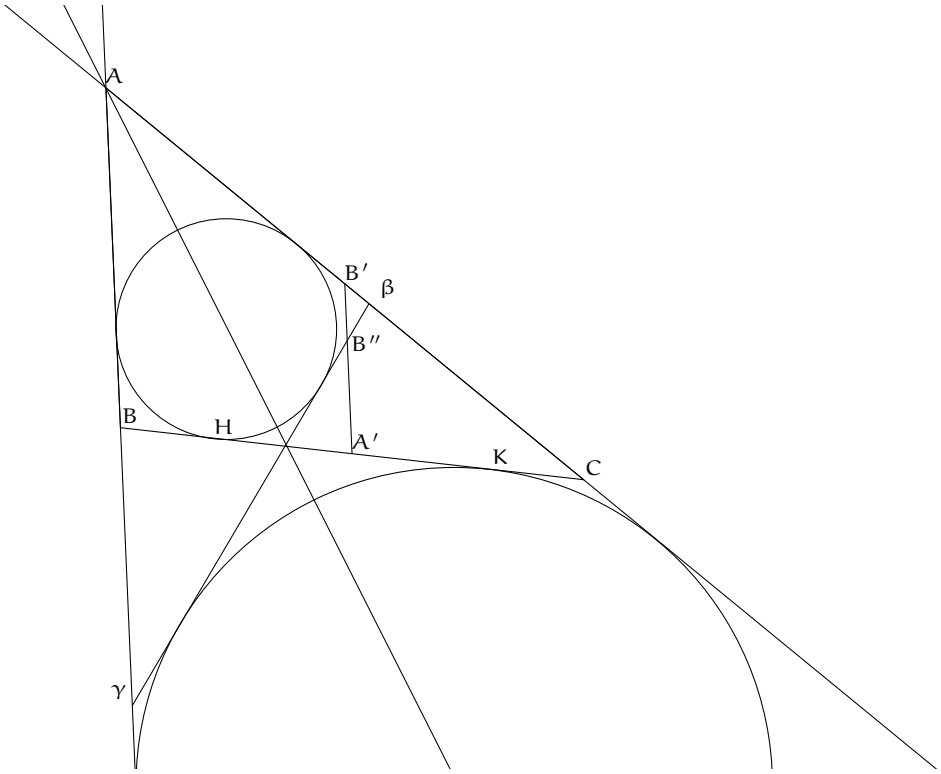
ce qu'il fallait démontrer.

Remarque 4.9. Je n'ai pas donné cet exo pendant la séance, traitant à la place l'exo 2 des OIM 1996, pas bien plus difficile. En effet je me suis rendu compte juste avant la séance que mon exercice était un cas particulier de l'exercice 98 de la muraille, et que cette preuve résolvait aussi l'exercice : l'égalité demandée est juste l'inversée de la formule d'Al-Kashi appliquée à $A'B'C'$. Je la laisse donc l'exercice ici comme preuve alternative de cet exercice.

Dans ces deux exemples, nous avons considéré la figure de base et son inversée indépendamment. Les cas plus compliqués obligent souvent à étudier les deux figures en même temps. il faut alors faire attention au choix de la puissance, afin que les deux figures se superposent agréablement.

Exercice 3 Prouver le théorème de Feuerbach, qui dit que le cercle d'Euler d'un triangle est tangent au cercle inscrit et aux trois cercles exinscrits.

Solution de l'exercice 3 Fixons quelques notations. Appelons ABC notre triangle, a, b et c les longueurs de ses côtés, p son demi-périmètre, A', B' et C' les milieux de ses côtés, $\mathcal{C}$ son cercle inscrit, et $\mathcal{C}_A$ le cercle exinscrit opposé au sommet A. Par symétrie, il suffit de montrer que $\mathcal{C}$ et $\mathcal{C}_A$ sont tangents au cercle d'Euler. Une idée est d'inverser par rapport à un point du cercle d'Euler, probablement A' : montrer qu'une droite est tangente à deux cercles semble plus simple que le problème d'origine. Le problème, c'est qu'une inversion complique le reste de la figure : AB et BC deviennent par exemple des cercles. Ce n'est pas très grave : ce qui est important, c'est que les images des deux cercles $\mathcal{C}$ et $\mathcal{C}_A$ soient faciles à contrôler.



Regardons donc la puissance de A' par rapport à $\mathcal{C}$ et $\mathcal{C}_A$. Appelons H et K les points de tangence de ces cercles avec BC. Déjà, si $c = b$, la figure est symétrique par rapport à la bissectrice intérieure du sommet A, et il est clair que $A' = H = K$, le théorème est donc vrai. Supposons maintenant que $b > c$. Il est bien connu que $CH = p - c$ et $BK = p - b$, et donc $A'H = A'K = \frac{b-c}{2}$. La puissance de A' par rapport aux deux cercles est donc $(\frac{b-c}{2})^2$, et l'inversion $I_{A',(\frac{b-c}{2})^2}$ les stabilise donc !

Il faut maintenant montrer que cette inversion envoie le cercle d'Euler sur une droite tangente aux deux cercles. Il n'y a pas le choix, il faut que cette droite soit le symétrique de BC par rapport à la bissectrice intérieure du sommet A. Introduisons donc β et γ les symétriques de B et C par rapport à cette bissectrice, et montrons que B' est envoyé par l'inversion sur un point de $\beta\gamma$. Appelons B'' l'intersection de $\beta\gamma$ avec $A'B'$. Par théorème de Thalès, on obtient $A'B' = \frac{c}{2}$,

$$B'B'' = A\gamma \cdot \frac{B'\beta}{A\beta} = b \cdot \frac{c - \frac{b}{2}}{c} = b - \frac{b^2}{2c},$$

puis $A'B'' \cdot A'B' = (A'B' - B'B'') \cdot A'B' = (\frac{b-c}{2})^2$. Ainsi, B'' est bien l'image de B' par notre inversion. Par des calculs similaires, C' est envoyé sur l'intersection C'' de $A'C'$ et de $\beta\gamma$. Ainsi, l'image du cercle d'Euler est une droite passant par deux points de $\beta\gamma$, c'est donc $\beta\gamma$, ce qui termine.

Pourquoi cette preuve marche-t-elle ? Car notre centre d'inversion, A', était sur le cercle clé du problème, mais aussi sur l'axe radical des deux autres cercles $\mathcal{C}$ et $\mathcal{C}_A$, ce qui nous a permit de conserver ces cercles. C'est une idée à retenir : les axes radicaux sont des candidats particulièrement intéressants pour des centres d'inversion.

Exercice 4 Soient A, B, C, D et E cinq points du plan en position générale (c'est-à-dire tels que trois d'entre eux ne soient jamais alignés, et tels que quatre d'entre eux ne soient jamais cocycliques). On appelle séparateur un cercle passant par trois de ces points, tel qu'un des

deux points restant soit situé à l'intérieur du cercle, et l'autre à l'extérieur. Combien y-a-t-il de séparateurs ?

Solution de l'exercice 4 On se rend vite compte que, si l'on essaie de traiter le problème naïvement, on va rapidement se retrouver avec des études de cas parfaitement sordides. On s'arrête donc une minute pour réfléchir à comment simplifier cette étude de cas au maximum. Pour cela, on aimererait bien se débarasser du plus grand nombre de cercles possibles, ce qui incite à inverser à travers un de nos points, disons A. Un autre façon de dire la même chose est de dire que ces questions de séparation seront plus simples avec un point à l'infini, car il sera toujours clair si ce point est séparé ou non des autres.

Dans toute la suite, j'appelerai ABC le cercle passant par les trois points A, B et C, et de même pour les autres cercles. Regardons donc l'effet de notre inversion sur les séparateurs. On vérifie que l'inversion envoie un séparateur passant par A, disons ABC, sur une droite $B'C'$ séparant D' et E' : le segment DE, qui coupe ABC en exactement un point (distinct de A), est envoyé sur un arc de cercle coupant la droite $B'C'$ en exactement un point. Réciproquement, on vérifie de la même façon qu'une telle droite est renvoyée sur un séparateur.

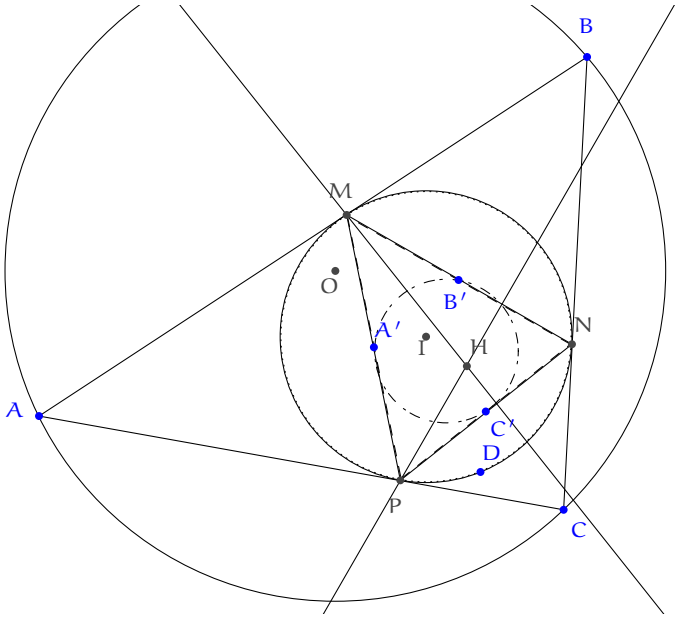
Le deuxième cas est celui des séparateurs ne passant pas par A. Supposons donc que BCD sépare A et E. Le segment AE coupe BCD en exactement un point (distint de A), donc l'image du segment, qui est une demi-droite issue de E, coupe le cercle $B'C'D'$ en exactement un point : E' est donc à l'intérieur de ce cercle (et ce, que E soit intérieur ou extérieur à BCD). Réciproquement, si $B'C'D'$ contient E', on vérifie de même que BCD est un séparateur.

On s'est donc ramené au problème suivant : on considère quatre points du plan en position générale, on cherche à compter le nombre de droites séparant deux de ces points, ainsi que le nombre de cercles passant par 3 points contenant le 4-ième. Il y a deux cas à traiter. Cas 1 : si un des points, disons D, est à l'intérieur du triangle ABC, alors il y a trois telles droites, AD, BD et CD, et un tel cercle, ABC (c'est le seul par un argument d'angle). Cas 2 : si les points sont les sommets d'un quadrilatère convexe. Alors il y a deux droites qui conviennent, les diagonales, et deux cercles : il y a forcément deux sommets, disons A' et C', tels que la somme des angles en ces deux sommets soit supérieure stricte à $180°$ (car les points sont non cocycliques), et par un argument d'angle les seuls cercles fonctionnant sont $A'B'D'$ et $C'B'D'$.

Bonus ! Un exercice non fait en cours, mais déjà tapé avant la séance, donc je le laisse ici.

Exercice 5 Soit ABC un triangle, M, N et P les points de tangence du cercle inscrit avec les segments AB, BC et CA. Montrer que le centre du cercle circonscrit de ABC, le centre du cercle inscrit de ABC, et l'orthocentre de MNP sont alignés.

Solution de l'exercice 5



Soit I et O les centres des cercles inscrit, et circonscrits à ABC. On remarque que IPAM, IMBN et INCP sont cocycliques, ce qui incite à se demander l'effet d'une inversion de cercle le cercle inscrit à ABC. Elle stabilise M, N et P et envoie A sur un point A' de la droite PM, et de plus IA est orthogonal au cercle passant par IPAM (c'est un diamètre), donc IA' doit être orthogonal à l'image du cercle par l'inversion : la droite PM. Ainsi, comme $IM = IP$, A' est le milieu de PM, et $A'B'C'$ est le triangle des milieux de de PMN. Ce type de configuration sert souvent, et est à retenir, pour pouvoir les repérer rapidement.

Le cercle circonscrit à ABC est donc envoyé sur le cercle d'Euler de MNP. Or on a dit dans le cours que si une inversion envoie un cercle sur un autre, les centres de ces deux cercles sont aligés avec le pôle de l'inversion. Ainsi, O est sur la droite reliant I (le centre du cercle circonscrit à MNP) avec le centre du cercle d'Euler de MNP. Il est bien connu que cette droite est la droite d'Euler de MNP, qui contient en particulier l'orthocentre de MNP, ce qui conclut la preuve.

- Complément : inversion et géométrie projective complexe -

Cette partie n'a aucun intérêt pour la résolution de problèmes olympiques, et peut confortablement être sautée. Elle est destinée aux élèves connaissant un peu de géométrie projective complexe, qui ont certainement remarqué les nombreux points communs entre inversions et transformations projectives, et aimeraient savoir de quoi il retourne.

Les transformations projectives de la droite complexe sont les homographies, et admettent une écriture de la forme $z \mapsto \frac{az+b}{cz+d}$. Comment s'écrit une inversion en complexe ? On voit facilement que l'inversion $I_{O,p}$ admet l'écriture

$$z \mapsto o + \frac{p}{\overline{z} - \overline{o}} = \frac{o\overline{z} + p - o\overline{o}}{\overline{z} - \overline{o}},$$

où o désigne l'affixe du pôle O. Ainsi, une inversion est « presque » une homographie, plus précisément c'est la composition d'une homographie et de la symétrie axiale $z \mapsto \overline{z}$.

Ainsi, une inversion est, à peu de choses près, un cas particulier de transformation projective, et n'a donc que peu d'intérêt sur le plan théorique. Elle a par contre un réel intérêt pratique : l'inversion a été construite de façon à vérifier des propriétés géométriques agréables que n'ont pas les transformations projectives générales, et elles méritent donc d'être étudiées à part. Je pense en particulier à la dualité cercles passant par le pôle, droites ne passant pas par le pôle (qui est une propriété des involutions), fort confortable.

Les inversions sont tout de même des transformations très riches, on pourrait notamment montrer que toute transformation projective (et même toute transformation de $\mathcal{E} \cup \{\infty\}$ envoyant cercles sur cercles) s'écrit comme produit de réflexions et d'inversions. Ainsi, les inversions sont suffisamment riches pour récupérer toute la géométrie projective.

2 Cours de géométrie

- Exercices -

Exercice 1

Soit $ABCD$ un quadrilatère convexe inscrit dans un cercle de centre O. Les diagonales (AC) et (BD) se coupent en P. Les cercles circonscrits aux triangles ABP et CDP se recoupent en Q. Si O, P, Q sont distincts, prouver que (OQ) est perpendiculaire à (PQ).

Exercice 2 (formule de Brahmagupta)

Soit $ABCD$ un quadrilatère convexe inscriptible, a, b, c, d les longueurs de ses côtés AB, BC, CD, DA et p son demi-périmètre. Montrer que :

$$\text{aire}(ABCD) = \sqrt{(p-a)(p-b)(p-c)(p-d)}$$

Exercice 3

Existe-t-il un triangle dont les longueurs des côtés sont des nombres premiers et dont l'aire est entière non nulle ?

Exercice 4

Soit ABC un triangle, O et I les centres de ses cercles circonscrit (de rayon R) et inscrit (de rayon r). Calculer la puissance de I par rapport au cercle circonscrit à ABC. En déduire la formule d'Euler : $OI^2 = R^2 - 2Rr$.

Exercice 5

Montrer que si a, b, c sont les longueurs des côtés d'un triangle, $abc \geqslant (a+b-c)(a-b+c)(-a+b+c)$. En déduire que : $R \geqslant 2r$, R et r étant les rayons des cercles circonscrit et inscrit au triangle.

Exercice 6

Les diagonales AC et BD d'un quadrilatère inscriptible $ABCD$ se coupent en E. Prouver que si $\widehat{BAD} = \frac{\pi}{3}$ et $AE = 3 \cdot CE$, alors la somme de deux des côtés du quadrilatère est égale à la somme des deux autres.

Exercice 7

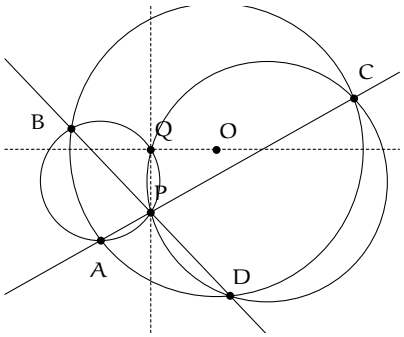
Soit $ABCDE$ un pentagone convexe vérifiant la propriété (P) : $aire(ABC) = aire(BCD) = aire(CDE) = aire(DEA) = aire(EAB) = 1$. Calculer l'aire du pentagone $ABCDE$. Ce pentagone est-il nécessairement régulier ?

- Solutions des exercices -

Solution de l'exercice 1

L'angle $\widehat{AQD} = \widehat{AQP} + \widehat{PQD} = \widehat{ABP} + \widehat{PCD} = \widehat{AOD}$ car les angles inscrits $\widehat{ABD} = \widehat{ACD}$ sont égaux chacun à la moitié de l'angle au centre $\widehat{AOD}$. On en déduit que A, D, O, Q sont cocycliques, donc $\widehat{OQD} = \widehat{OAD}$. Dès lors, $\widehat{OQP} = \widehat{OQD} + \widehat{DQP} = \widehat{OAD} + \widehat{DCA} = 90°$ car l'angle inscrit $\widehat{DCA}$ est égal à l'angle de (AD) à la tangente en A au cercle de centre O, et cette tangente est perpendiculaire à (OA).

Solution de l'exercice 2



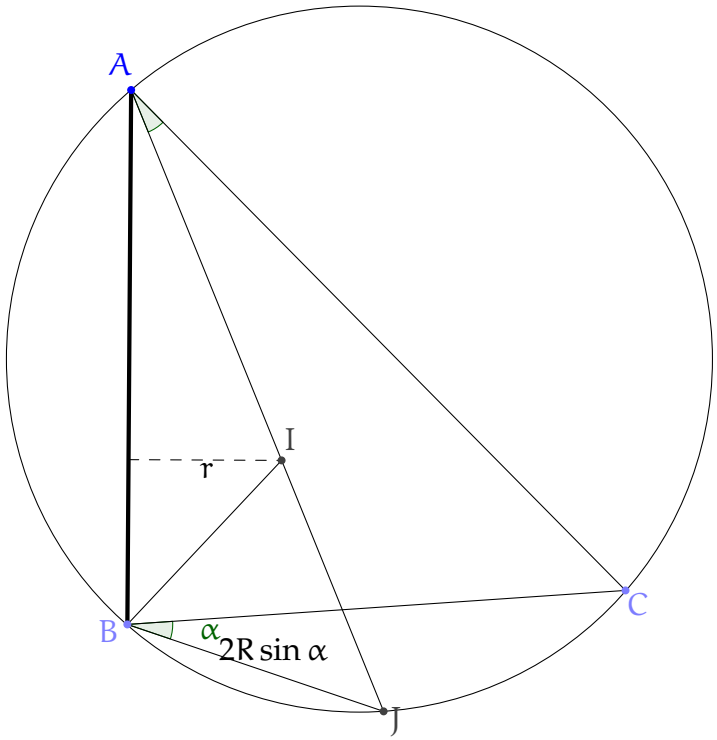
Le quadrilatère $ABCD$ étant convexe, son aire S est la somme des aires des triangles ABC et CDA, soit : $\frac{1}{2}(ab\sin\widehat{B} + cd\sin\widehat{D})$ en appelant $\widehat{A}, \widehat{B}, \widehat{C}, \widehat{D}$ les angles du quadrilatère. Pour faire disparaître ces sinus, il faut utiliser des cosinus : $16S^2 + (2ab\cos\widehat{B} - 2cd\cos\widehat{D})^2 = 4a^2b^2 + 4c^2d^2 - 8abcd\cos(\widehat{B}+\widehat{D})$. Comme $ABCD$ est inscriptible, $\widehat{B}+\widehat{D} = \pi$, d'où : $16S^2 + (2ab\cos\widehat{B} - 2cd\cos\widehat{D})^2 = (2ab+2cd)^2$. Or les cosinus s'obtiennent par la formule d'Al Kashi : $AC^2 = a^2 + b^2 - 2ab\cos\widehat{B} = c^2 + d^2 - 2cd\cos\widehat{D}$, d'où $2ab\cos\widehat{B} - 2cd\cos\widehat{D} = a^2 + b^2 - c^2 - d^2$ et finalement : $16S^2 = (2ab + 2cd)^2 - (a^2 + b^2 - c^2 - d^2)^2 = \left((a+b)^2 - (c-d)^2\right)\left((c+d)^2 - (a-b)^2\right) = (a+b+c-d)(a+b-c+d)(a-b+c+d)(-a+b+c+d) = 16(p-d)(p-c)(p-b)(p-a)$ ce qui achève la démonstration.

On notera que pour $d = 0$, soit $D = A$, on retrouve la formule bien connue de Héron : $aire(ABC) = \sqrt{p(p-a)(p-b)(p-c)}$. Par ailleurs, la démonstration ci-dessus montre que si $\widehat{B} + \widehat{D} \neq \pi$, alors l'aire est inférieure à $\sqrt{(p-a)(p-b)(p-c)(p-d)}$: un quadrilatère de côtés a, b, c, d a une aire maximale lorsqu'il est inscriptible.

Solution de l'exercice 3

Si l'on appelle a, b, c les longueurs des côtés du triangle et S son aire, la formule de Héron peut s'écrire : $16S^2 = (a+b+c)(-a+b+c)(a-b+c)(a+b-c)$. Or les quatre facteurs sont entiers de même parité, ils sont obligatoirement tous pairs. Ce qui signifie que soit un soit trois des nombres a, b, c sont pairs. Ces trois nombres étant premiers, un ou trois d'entre eux est égal à 2. Si tous les trois sont égaux à 2, alors la formule de Héron donne $S^2 = 3$ et S n'est pas entier. Si un seul est égal à 2, soit p le plus petit des deux autres : d'après l'inégalité triangulaire (stricte car le triangle est d'aire non nulle), le plus grand sera strictement inférieur à $p+2$, donc égal à p car lui aussi doit être premier. On trouve alors $S^2 = p^2 - 1$, qui ne peut pas être un carré parfait. Donc un tel triangle n'existe pas.

Solution de l'exercice 4

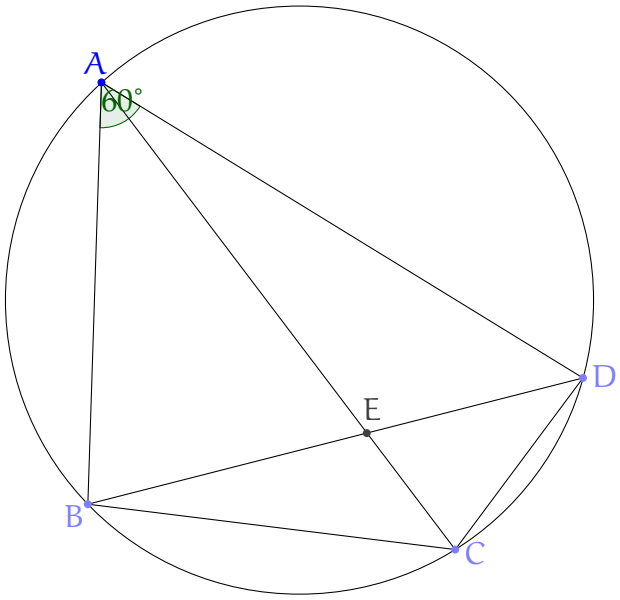


Posons $\alpha = \widehat{BAI} = \widehat{IAC}$, et $\beta = \widehat{CBI} = \widehat{IBA}$, et appelons J le point où (AI) recoupe le cercle circonscrit. Dans le triangle BIA, $\widehat{BIJ} = \widehat{BAI} + \widehat{IBA} = \alpha + \beta$, mais comme l'angle inscrit $\widehat{JBC} = \widehat{JAC} = \alpha$, $\widehat{JBI}$ vaut lui aussi $\alpha + \beta$, donc le triangle JBI est isocèle : $JI = JB = 2R\sin\alpha$ (corde interceptée par un angle inscrit de mesure α). Or $AI\sin\alpha = r$ (r est la distance de I au côté AB de l'angle $\widehat{ABI} = \alpha$). Donc en valeur absolue, $IA \cdot IJ = 2Rr$ et comme I est intérieur au cercle circonscrit, sa puissance par rapport audit cercle est $-2Rr$. Par ailleurs la puissance d'un point par rapport à un cercle est le carré de sa distance au centre moins le carré du rayon du cercle. On en déduit : $OI^2 = R^2 - 2Rr$.

Solution de l'exercice 5

Remarquons d'abord que d'après l'inégalité triangulaire, chacun des trois nombres $a+b-c$, $a-b+c$, $-a+b+c$ est positif ou nul. Or : $(a+b-c)(a-b+c) = a^2-(b-c)^2 \leqslant a^2$, tout comme $(a-b+c)(-a+b+c) \leqslant c^2$ et $(-a+b+c)(a+b-c) \leqslant b^2$. En multipliant ces trois inégalités, toutes entre termes positifs, on obtient : $(a+b-c)^2(a-b+c)^2(-a+b+c)^2 \leqslant a^2b^2c^2$, d'où l'inégalité cherchée sachant que chacun des membres est positif ou nul. Or d'après la formule de Héron, $(a+b-c)(a-b+c)(-a+b+c) = \frac{8S^2}{p}$, en appelant classiquement S l'aire du triangle et $p = \frac{a+b+c}{2}$ son demi-périmètre. Et $abc = 4RS$ car $S = \frac{1}{2}ab\sin\widehat{C}$ et $c = 2R\sin\widehat{C}$. Donc $R \geqslant \frac{2S}{p} = 2r$, la formule $S = rp$ résultant classiquement de $S = aire(ABI)+aire(BCI)+aire(CAI)$.

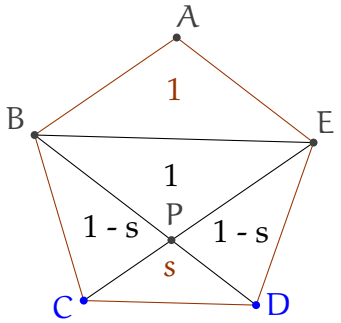
Solution de l'exercice 6



Pour utiliser l'hypothèse $\widehat{BAD} = \frac{\pi}{3}$ il faut faire intervenir l'aire du triangle BAD, égale à $\frac{1}{2}AB \cdot AD \cdot \sin\frac{\pi}{3}$, soit la formule d'Al Kashi : $BD^2 = AB^2 + AD^2 - 2 \cdot AB \cdot AD \cdot \cos\frac{\pi}{3} = AB^2+AD^2-AB\cdot AD$. Pareillement, comme les angles $\widehat{BAD}$ et $\widehat{BCD}$ du quadrilatère inscriptible ABCD sont supplémentaires : $BD^2 = CB^2 + CD^2 - 2 \cdot CB \cdot CD \cdot \sin\frac{2\pi}{3} = CB^2 + CD^2 + CB \cdot CD$. Or la deuxième relation de l'hypothèse permet de comparer les aires de DAB et BCA : $aire(DAE) = 3 \cdot aire(DCE)$ et $aire(BAE) = 3 \cdot aire(BCE)$, donc $aire(DAB) = 3 \cdot aire(DCB) = 3\cdot CD\cdot CB \sin\frac{2\pi}{3}$. Comme $\sin\frac{2\pi}{3} = \sin\frac{\pi}{3}$, on en déduit : $AB\cdot AD = 3\cdot CB\cdot CD$. Donc $(AB-AD)^2 = BD^2-AB\cdot AD = BD^2-3\cdot CB\cdot CD = (CB-CD)^2$, d'où l'on déduit : ou bien $AB-AD = CB-CD$, soit $AB + CD = AD + BC$, ou bien $AB - AD = -(CB - CD)$, soit $AB + BC = CD + DA$.

Solution de l'exercice 7

Les triangles BCD et CDE, de même aire, ont même base CD donc même hauteur relative à CD, d'où (BE) parallèle à (CD). On démontre pareillement que, par exemple, (CE) parallèle à (AB) et (BD) à (AE). Si l'on appelle P l'intersection des diagonales BD et CE, ABPE est un parallélogramme. Par symétrie par rapport au centre du parallélogramme, $aire(BPE) = aire(EAB) = 1$. Reste à déterminer l'aire s de PCD, car $aire(PCB) = aire(PDE) = 1 - s$ d'où $aire(ABCDE) = 4 - s$. Or $\frac{aire(PCB)}{aire(PCD} = \frac{PB}{PD} = \frac{aire(EPB)}{aire(EPD)}$ peut s'écrire : $\frac{1-s}{s} = \frac{1}{1-s}$, soit : $1-3s+s^2 = 0$, dont la seule racine comprise entre 0 et 1 est : $\frac{3-\sqrt{5}}{2}$. D'où $aire(ABCDE) = \frac{5+\sqrt{5}}{2}$.



Le pentagone n'est pas nécessairement régulier. Considérons en effet un pentagone régulier, et choisissons un repère orthonormé dans lequel les sommets A, B, C, D, E ont pour coordonnées respectives ; $(a, a'), (b, b'), (c, c'), (d, d'), (e, e')$. Considérons un autre repère, ni orthogonal ni normé, et traçons dans cet autre repère les points de mêmes coordonnées. Toutes les aires du premier repère seront multipliées par la même constante dans le second repère, donc dans ce second repère les cinq triangles auront également la même aire. Pourtant le pentagone ne sera plus du tout régulier.

Utilisation des nombres complexes en géométrie

Pour conclure, voici deux exemples d'utilisation des nombres complexes en géométrie, un classique et facile, un autre non classique et plus difficile.

Rappelons que les nombres complexes sont les nombres de la forme $x + iy$, où i vérifie $i^2 = (-i)^2 = -1$. À chaque nombre complexe $x + iy$ on peut associer le point de coordonnées (x, y) ou le vecteur de composantes (x, y). $x + iy$ est appelé l'affixe du point ou du vecteur. On peut ainsi quotienter deux vecteurs en calculant le quotient de leurs affixes : ce quotient $x + iy$ a pour module $\rho = \sqrt{x^2 + y^2}$ le rapport des modules des vecteurs et pour argument θ (tel que $x + iy = \rho(\cos\theta + i\sin\theta)$ l'angle entre le vecteur dénominateur et le vecteur numérateur. Les deux complexes $x + iy$ et $x - iy$ sont dits conjugués, et si un complexe est de module $1 = \sqrt{x^2 + y^2}$ son conjugué est égal à son inverse.

Exercice 8

Sur les côtés d'un quadrilatère convexe $ABCD$, à l'extérieur du quadrilatère, on construit quatre triangles rectangles isocèles AMB, BNC, CPD, DQA, rectangles en M, N, P, Q respectivement. Montrer que MP et NQ sont perpendiculaires et de même longueur.

Solution de l'exercice 8

Dire que MA et MB sont perpendiculaires et de même longueur signifie : $MB = i \cdot MA$ ou $MB = -i \cdot MA$. Supposons que les sommets A, B, C, D soient positionnés de telle sorte que $MB = i \cdot MA$, appelons a, b, c, d les affixes de A, B, C, D et m, n, p, q ceux de M, N, P, Q. $b - m = i(a - m)$, d'où $(1 - i)m = b - ia$. On obtient pareillement : $(1 - i)n = c - ib$, $(1 - i)p = d - ic$ et $(1 - i)q = a - id$, donc l'affixe de MP, $p - m = \frac{ia - b - ic + d}{1 - i} = i\frac{a + ib - c - id}{1 - i} = i(q - n)$ a même module que l'affixe de NQ, leurs arguments diffèrent de $\frac{\pi}{2}$, ce qui suffit à prouver que les segments sont perpendiculaires et de même longueur.

Exercice 9

Théorème de Morley

Montrer que les points d'intersection des trissectrices d'un triangle forment un triangle équilatéral.

Ce théorème, historiquement important, se démontre de plusieurs manières. L'une d'elles, due à Alain Connes, a fait l'objet d'un problème d'agrégation. En voici une utilisant les nombres complexes :

Solution de l'exercice 9

Soient α, β, γ les affixes des sommets A, B, C d'un triangle, inscrit dans un cercle de centre O (d'affixe 0) et de rayon R. Considérons trois complexes a, b, c, de module 1, tels que : $\beta = \alpha c^6, \gamma = \beta a^6, \alpha = \gamma b^6$ et $a^2b^2c^2 = j = \frac{-1 + i\sqrt{3}}{2}$, racine cubique de l'unité. Comme $(\alpha\beta\gamma)a^6b^{12} = \alpha\beta\gamma\left(\frac{\gamma}{\beta}\right)\left(\frac{\alpha^2}{\gamma^2}\right) = \alpha^3$, l'une des racines cubiques de $\alpha\beta\gamma$, m, vérifie :

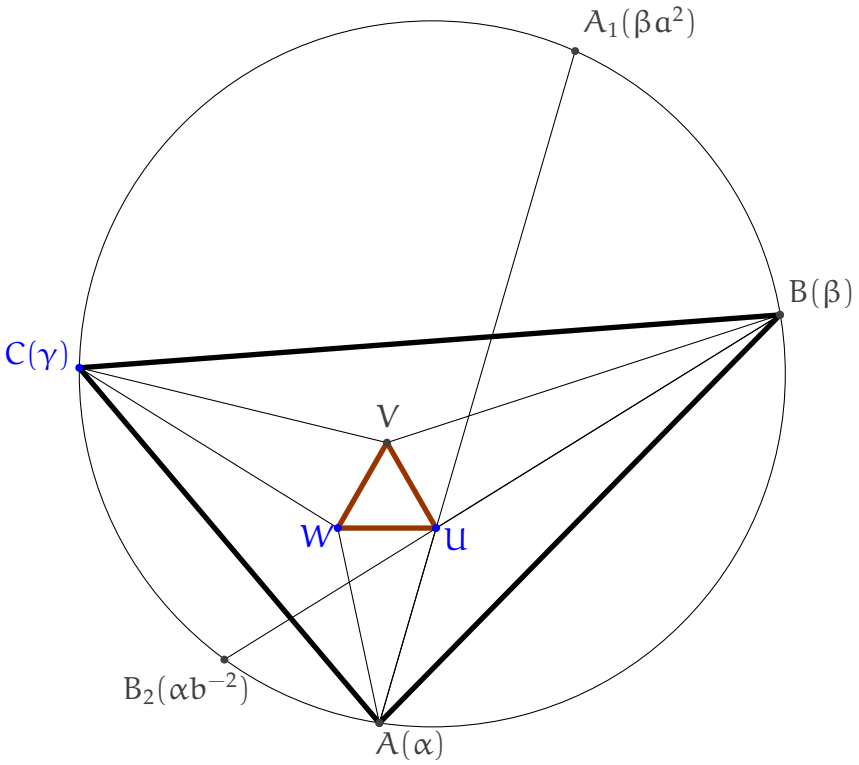
$$\alpha = ma^2b^4 = mj^2c^{-4}a^{-2}$$

$$\beta = \alpha c^6 = mjb^2c^4 = ma^{-4}b^{-2}$$

$$\gamma = mj^2c^2a^4 = mjb^{-4}c^{-2}$$

Or, de manière très générale, si z et z' sont deux complexes de même module non nul, pour tout $m \neq 0$, $m(z^2 - z'^2)$ est perpendiculaire à mzz', puisque $\frac{z}{z'}$ et $\frac{z'}{z}$ sont conjugués.

Il en résulte que la trisectrice issue de A, d'affixe $\alpha = ma^2b^4$, et passant par A_1, d'affixe $\beta a^2 = ma^{-2}b^{-2}$, est perpendiculaire à mb, donc parallèle à $mb(a-a^{-1})(ab+a^{-1}b^{-1})$, puisque $(a-a^{-1})$ est imaginaire pur et $(ab+a^{-1}b^{-1})$ est réel. Dès lors, le point d'affixe : $u = ma^{-2}b^{-2} + mb(a - a^{-1})(ab + a^{-1}b^{-1}) = m\left(a^{-2}b^{-2} + (a^2b^2 - b^2) + (1 - a^{-2})\right)$ appartient à la trisectrice AA_1.



La trisectrice issue de B, d'affixe $\beta = ma^{-4}b^{-2}$, et passant par B_2, d'affixe $\alpha b^{-2} = ma^2b^2$, est, quant à elle, perpendiculaire à ma^{-1}, donc parallèle à $ma^{-1}(b - b^{-1})(ab + a^{-1}b^{-1})$, et elle passe par le point $u' = ma^2b^2 - ma^{-1}(b - b^{-1})(ab + a^{-1}b^{-1})$.

Il se trouve que

$$u = u' = m(1 + jc^{-2} + j^2c^2 - a^{-2} - b^2)$$

Le point d'affixe $u = u'$ est donc l'intersection des trisectrices AA_1 et BB_2.

Une simple permutation suffit pour déterminer les affixes des deux autres intersections :

$$v = mj(1 + ja^{-2} + j^2a^2 - b^{-2} - c^2)$$

$$w = mj^2(1 + jb^{-2} + j^2b^2 - c^{-2} - a^2)$$

et il est clair que : $u + jv + j^2w = 0$, soit : $j(v - u) = -j^2(w - u)$, ce qui entraîne que u, v et w sont les affixes des sommets d'un triangle équilatéral.

3 Géométrie projective

Ce texte n'est qu'une introduction à la géometrie projective bidimensionnelle réelle, contenant les premiers résultats, sûrement les plus spectaculaires. Il n'y a pas réellement de références canoniques en géometrie projective, même si les ouvrages de Yaglom « Geometric Transformations » sont incontournables pour les transformations en tous genres...

- Plan projectif, birapport et harmonicité -

L'un des buts de la géométrie projective est faire en sorte que deux droites distinctes quelconques se coupent en exactement un point. Pour ce faire, on rajoute au plan une droite à l'infini, où chaque point correspond au point d'intersection d'une famille de droites parallèles. On ne distinguera plus fondamentalement deux droites concourantes et deux droites parallèles : ces dernières ont juste leur point d'intersection qui est sur la droite à l'infini.

L'objet probablement le plus intéressant en géometrie projective, celui qu'on cherchera à conserver en définissant les transformations projectives, est le birapport :

Définition 4.10. Soit A, B, C, D quatre points alignés. On définit leur birapport (réel) :

$$b_{A,B,C,D} = \frac{\overline{CA}}{\overline{CB}} : \frac{\overline{DA}}{\overline{DB}}$$

où $\frac{\overline{CA}}{\overline{CB}}$ désigne le rapport algébrique.

Remarques 4.11.

- On remarquera que le birapport ne peut valoir 1 que dans certains cas dégénérés.
- On peut tout à fait prendre des points à l'infini dans le calcul du birapport, avec la convention (naturelle en termes de limites) que $\frac{\infty}{\infty} = 1$.
- On a un certain nombre d'identités algébriques sur le birapport que le lecteur est invité à explorer. On utilisera par exemple à de multiples reprises des identités de la forme $b_{A,B,C,D} = b^{-1}_{B,A,C,D}$. Une autre identité intéressante est $b_{A,B,C,D} + b_{A,C,B,D} = 1$, qui, dans le cas complexe, est exactement le théorème de Ptolémée (exercice !).
- On peut facilement vérifier que la connaissance du birapport et de la position de trois des points permet d'identifier uniquement le dernier point. Ce fait sera régulièrement utilisé.
- On peut remarquer que le birapport est un cas particulier des produits cycliques de rapports (de la forme $\frac{\overline{X_1Y_1}}{\overline{X_2Y_1}} \cdot \frac{\overline{X_2Y_2}}{\overline{X_3Y_2}} \cdot ... \cdot \frac{\overline{X_nY_n}}{\overline{X_1Y_n}}$ avec $Y_i \in (X_iX_{i+1})$ pour tout i). De manière générale, le lecteur attentif pourra remarquer que la plupart des propriétés intéressantes du birapport (notamment en termes de projection) restent vrai pour les produits cycliques de rapports, ce qui conduira en particulier à la démonstration du théorème de Ceva.

Définition 4.12. Soient A, B, C, D alignés. Ils sont dits harmoniques si leur birapport vaut -1.

L'exemple suivant est particulièrement important et récurrent :

Exemple 4.13. Si M est le milieu de [AB], alors A,B,M et le point à l'infini de la droite (AB) sont harmoniques.

Proposition 4.14. Si A, B, C et D sont harmoniques, on peut toujours supposer qu'ils sont de la forme -1, 1, x et $1/x$.

Démonstration. On peut toujours poser $A = -1$, $C = 1$, $B = x$. Il suffit ensuite par unicité du quatrième point harmonique de prouver que $b_{-1,1,x,1/x} = -1$, ce qui est un calcul aisé. □

Remarque 4.15. Le lecteur attentif aura remarqué le lien avec les inversions. Plus précisément, ce sont les involutions (transformations projectives complexes de la forme $z \mapsto 1/z$) qui sont ici pertinentes, en particulier dans $\mathbb{C}$ où cette propriété reste vérifiée.

Corollaire 4.16 (MacLaurin et Newton)**.** Soient A, B, C, D quatre points harmoniques et M le milieu de [AB].

Alors $MC \cdot MD = MB^2$ (identité de MacLaurin) et $DB \cdot DA = DC \cdot DM$ (identité de Newton).

Démonstration. C'est un simple calcul en utilisant la proposition précédente. □

Définition 4.17. Soient a, b, c, d quatre droites concourantes. On définit leur birapport :

$$b_{a,b,c,d} = \frac{\sin(c,a)}{\sin(c,b)} : \frac{\sin(d,a)}{\sin(d,b)}.$$

On définit comme pour les points la notion de droites harmoniques.

Proposition 4.18. Soit a, b, c, d concourantes en P et Δ une droite ne passant pas par P. Δ coupe a, b, c, d en A, B, C, D. (respectivement). On a $b_{a,b,c,d} = b_{A,B,C,D}$.

Démonstration. On exprime les sinus en termes d'aires algébriques que l'on simplifie ensuite en utilisant que la hauteur est la même pour tous les triangles :

$$b_{a,b,c,d} = \frac{\frac{|CPA|}{PA\cdot PC}\frac{|DPB|}{PB\cdot PD}}{\frac{|CPB|}{PB\cdot PC}\frac{|DPA|}{PA\cdot PD}} = \frac{\overline{CA}}{\overline{CB}} : \frac{\overline{DA}}{\overline{DB}}$$

□

Corollaire 4.19. Si Δ' est une autre droite ne passant pas par P, $b_{A',B',C',D'} = b_{A,B,C,D}$: le birapport est conservé par projection.

Remarque 4.20. Si les quatre droites sont concourantes sur la droite à l'infini (autrement dit parallèles), l'invariance du birapport par projection découle du théorème de Thalès.

Exemple 4.21. Soient d et d' deux droites, de bissectrices Δ et Δ'. Alors d, d' , Δ , Δ' sont harmoniques.

Démonstration. On peut soit faire un calcul direct, soit projeter sur une droite parallèle à Δ' et utiliser l'exemple 4.13. □

Remarque 4.22. On peut facilement utiliser l'unicité du birapport pour montrer toutes sortes de réciproques, par exemple si on a quatre droites harmoniques, voire une simple droite harmonique ou bien un angle droit.

Exercice 1 Soit ABC un triangle, H le pied de la hauteur issue de A, J celui de la bissectrice, M le milieu de $[BC]$ et E le point de tangence du cercle inscrit sur $[BC]$.

Montrer que $ME^2 = MJ \cdot MH$.

Solution de l'exercice 1 Soit I_A le centre du cercle exinscrit à A, et I le centre du cercle inscrit. Soit enfin A' le point de tangence du cercle exinscrit sur $[BC]$. Un calcul classique de chasse aux tangentes (exercice !) montre que M est le milieu de $[JA']$.

D'après l'exemple précédent, (BA), (BC), (BI) et (BI_A) sont harmoniques. Par conséquent, en projetant sur (AI) depuis B, les points A, J, I, I_A sont harmoniques. En projetant sur (BC) depuis le point à l'infini de (AH), on voit que H, J, E, A' sont harmoniques. La formule demandée n'est autre que celle de MacLaurin (après réordonnement idoine des points).

Théorème 4.23 (Quadrilatère complet)**.** Soit A,B, C, D quatre points, $E = (AC) \cap (BD)$, $F = (AB) \cap (DC)$, $G = (AD) \cap (BC)$, $X = (GE) \cap (AB)$ et $Y = (GE) \cap (DC)$.

Alors A, B, X et F sont harmoniques.

Démonstration. On peut raisonner très facilement avec Ceva et Mélénaus. Mais avant tout, il faut remarquer qu'une telle figure permet de projeter très facilement.

En projetant depuis G puis depuis E, $b_{A,B,X,F} = b_{D,C,Y,F} = b_{A,B,F,X} = b_{A,B,X,F}^{-1}$.

Comme $b_{A,B,X,F} \neq 1$, $b_{A,B,X,F} = -1$ d'où la conclusion. □

Remarque 4.24. Bien sûr, on peut trouver par projection ou par analogie de nombreux autres points/droites harmoniques. J'y ferai également référence sous le terme de théorème du quadrilatère complet. Il est important de savoir identifier immédiatement un tel diagramme.

Exercice 2 Soit ABC un triangle, D, E, F les points de tangence à (BC), (AC) et (AB) du cercle inscrit. Soit $\mathcal{C}$ un cercle tangent intérieurement au cercle inscrit, en D. Soient P et Q sur $\mathcal{C}$ tels que (BP) et (CQ) soient tangentes à $\mathcal{C}$. Montrer que (EF), (PQ) et (BC) sont concourantes.

Solution de l'exercice 2 Reformulons d'abord le problème. On a B, D, C alignés, un cercle tangent à (BC) en D, variable, et une intersection I, a priori propre au cercle (celle de (PQ) et (BC)), et il faut montrer que I est un point fixe. On a trois points fixes alignés : on peut espérer que I soit le quatrième point harmonique. C'est en fait le cas ici, comme on va le voir.

(BQ), (PC) et (MD) sont concourantes (point de Gergonne, par exemple d'après Ceva). On a donc un quadrilatère complet et I, D, B et C sont bien harmoniques.

On peut de plus définir un birapport sur le cercle (et sur n'importe quelle conique de manière générale, même si l'indépendance de P est alors moins immédiate) :

Définition 4.25. Soit A, B, C, D quatre points sur un cercle $\mathcal{C}$. On définit leur birapport :

$$b_{A,B,C,D} = b_{(PA),(PB),(PC),(PD)}$$

pour n'importe quel point P sur le cercle.

Cette définition est bien indépendante du point P considéré (théorème de l'angle inscrit et quelques considérations de signes).

Remarque 4.26. On peut vérifier que le birapport ainsi défini correspond au birapport complexe $\frac{(c-a)}{(c-b)} : \frac{(d-a)}{(d-b)}$ (qui est ici réel d'après le théorème de l'angle inscrit) grâce à la loi des sinus. C'est faux pour une conique quelconque (le birapport complexe n'étant même pas réel).

On définit comme d'habitude l'harmonicité de quatre points sur un cercle.

Il faut être extrêmement prudent sur le fait qu'on NE peut PAS utiliser la définition précédente pour P qui n'est pas sur $\mathcal{C}$. On a néanmoins la proposition suivante :

Proposition 4.27. Soit A, B, C, D, A′, B′, C′, D′ des points sur un cercle, tels que (AA′), (BB′), (CC′) et (DD′) soient concourantes.

Alors, $b_{A',B',C',D'} = b_{A,B,C,D}$.

Démonstration. Ce résultat peut se montrer directement de manière fort horrible. Ce que j'invite le lecteur courageux à faire. La méthode la plus efficace est de prendre de l'avance sur ce cours, d'utiliser une transformation projective qui envoie le cercle sur un cercle et le point de concourance soit à l'infini (auquel cas c'est clair par symétrie axiale) soit au centre du cercle (auquel cas c'est clair par symétrie centrale). □

Proposition 4.28. Soit P en dehors d'un cercle $\mathcal{C}$, A et B sur $\mathcal{C}$ de sorte à ce que (PA) et (PB) soit tangentes à $\mathcal{C}$ et C et D sur le cercle afin que P, C et D soient alignés.

Alors, A, B, C, D sont harmoniques.

Démonstration. On peut bien sûr encore utiliser une transformation projective, mais il y a ici une autre solution élégante.

On applique la propriété précédente aux points A, B, C, D et au point P : $b_{A,B,C,D} = b_{A,B,D,C} = b_{A,B,C,D}^{-1}$, d'où, comme $b_{A,B,C,D} \neq 1$, $b_{A,B,C,D} = -1$ et la conclusion. □

Remarque 4.29. Comme toujours, par unicité, on a la réciproque. C'est donc bien la configuration canonique des point harmoniques sur un cercle.

Exercice 3 Soit A, B et C sur un cercle et D l'intersection (éventuellement à l'infini des tangentes en B et C).

Montrer que (AD) est la symédiane (issue de A) dans ABC, c'est-à-dire la symétrique de la médiane par rapport à la bissectrice.

Solution de l'exercice 3 Soit E la deuxième intersection de (AD) avec le cercle. A,E,C,B sont harmoniques, donc la tangente en A, (AD), (AC), et (AB) le sont, ainsi que les symétriques de ces droites (respectivement (AM), (AB), (AC) et d) par rapport à la bissectrice de $\hat{A}$ (dans ABC).

d est parallèle à (BC) car l'angle entre d et (AC) est le même que celui entre la tangente en A et (AB), qui vaut l'angle en C par théorème des angle inscrit. On a donc deux angles alternes-internes égaux. On projette alors sur (BC) et on obtient que M est le milieu de [BC].

Exercice 4 Soient Γ_1 et Γ_2 deux cercles s'intersectant en A et B, K l'intersection des tangentes à Γ_1 en A et B. Si M est sur Γ_1, on pose P l'intersection de (MA) avec Γ_2, C l'intersection de (MK) avec Γ_1 et Q l'intersection de (AC) avec Γ_2.

Montrer que (PQ) a un point fixe quand M varie sur Γ_1.

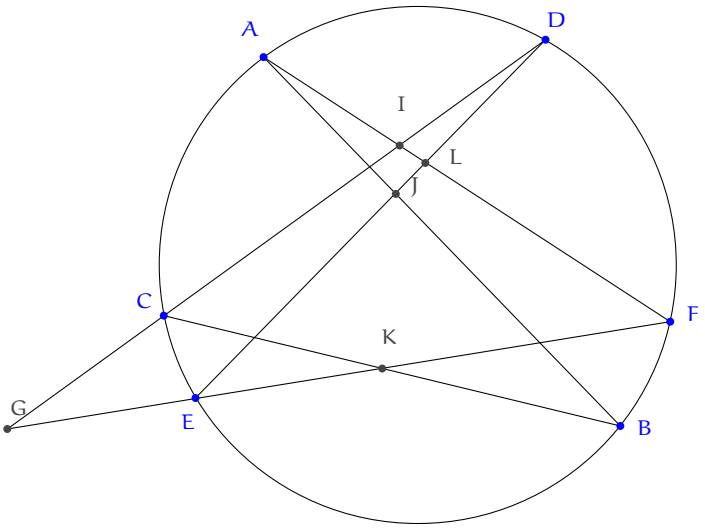
Solution de l'exercice 4 B, A, C et M sont harmoniques. En projetant depuis A, on trouve B, A′, Q, P harmoniques avec A′ le deuxième point d'intersection de (AK) et Γ_2.

Soit I l'intersection des tangentes à Γ_2 en B et A′. Alors (QP) passe par I, qui est le point fixe cherché.

Théorème 4.30 (Pascal)**.** Soit ABCDEF un hexagone (pas forcément convexe) inscrit dans un cercle. Soient I, J, K les intersections respectives de (AF) et (CD), (AB) et (DE), (BC) et (EF).

Alors I, J et K sont alignés.

Démonstration.



On appelle J′ l'intersection de (IK) et de (DE). On considère le birapport de E, L, J, D. Comme souvent, l'idée est de projeter pour trouver des quadruplets de même birapport, jusqu'à tomber sur E, L, J′ ,D. On en déduira J = J′, soit I, J et K alignés.

En projetant par rapport à A puis C puis I, on trouve que $b_{E,L,J,D} = b_{E,B,F,D} = b_{E,F,K,P} = b_{E,L,J',D}$, d'où la conclusion.

□

Remarque 4.31. Notre démonstration marche tout aussi bien avec une conique quelconque. De plus, une transformation projective permet aussi de justifier que cette généralisation est équivalente au Pascal de base.

Le théorème de Pascal est très utilisé, que ce soit en géométrie élémentaire ou en géométrie projective. L'exercice suivant est un exemple d'application parmi plein d'autres.

Exercice 5 Soit ABC un triangle et Γ son cercle circonscrit. Soit M un point de la bissectrice issue de A et A_1, B_1, C_1 les deuxièmes points d'intersections de Γ avec (AM), (BM) et (CM) respectivement. On note $P = (AB) \cap (A_1C_1)$ et $Q = (AC) \cap (A_1B_1)$.

Montrer que (PQ) est parallèle à (BC).

Solution de l'exercice 5 Cette situation a clairement un air de Pascal. On l'applique dans un premier temps naturellement à l'hexagone CA_1B_1BAC pour obtenir que P, M et Q sont alignés. Cela permet de simplifier la figure en enlevant B_1 et Q.

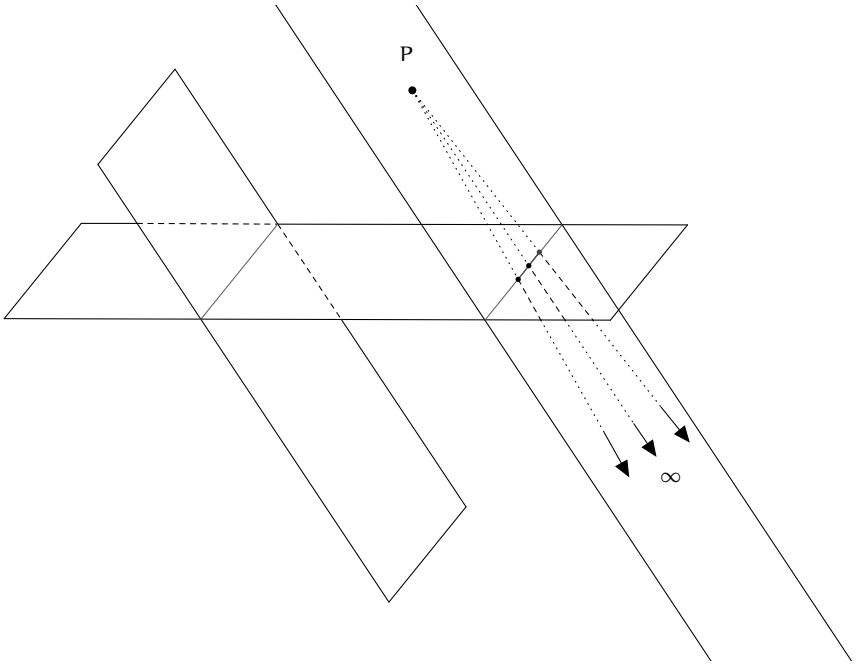
Pour prouver le parallélisme, on introduit le point Ω à l'infini de la droite (BC). Comment trouver un hexagone dont l'intersection de deux côtés opposés soit Ω ? (BC) s'impose de lui-même et la tangente en A_1 (théorème du pôle Sud...) vient ensuite naturellement. On considère alors (pour obtenir les points P et M également) l'hexagone dégénéré $A_1A_1C_1CBA$, qui montre que P, M et Ω sont alignés, d'où la conclusion.

- Transformations projectives -

Dans cette partie, nous nous intéresserons aux transformations projectives bidimensionnelles réelles, c'est-à dire les transformations du plan projectif qui conservent le birapport. Elles sont clairement stables par composition. On peut prouver que toutes ces transformations sont de la forme suivante :

Définition 4.32. On se place en dimension 3. On appelle transformation projective toute transformation qui consiste à projeter un plan $\mathcal{P}_1$ sur un autre plan $\mathcal{P}_2$ depuis un point P (en identifiant ensuite les deux plans comme le plan projectif).

Remarque 4.33. On voit là tout l'intérêt de la droite à l'infini : la droite D de $\mathcal{P}_1$ telle que le plan formé par P et D soit parallèle à $\mathcal{P}_2$ est envoyée sur la droite à l'infini. Le lecteur studieux se demandera sur quoi est envoyée la droite à l'infini de $\mathcal{P}_2$...



Clairement, ces transformations conservent l'alignement. La propriété 4.19 permet de plus d'affirmer qu'elles conservent le birapport de quatre points. En utilisant la propriété 4.18, on peut de plus remarquer qu'elles conservent le birapport de quatre droites et donc, par définition, celui de quatre points sur un cercle.

Toutefois, il faut faire très attention : les transformations projectives ne conservent ni les longueurs, ni les rapports de longueurs, ni les angles, ni les cercles qui sont envoyés en général sur des coniques (preuve ?).

En contrepartie de cette mauvaise conservation des propriétés, les transformations projectives laissent énormément de liberté. Quelles sont les possibilités qu'elles nous offrent ?

Théorème 4.34. En projetant on peut :
- envoyer un point/une droite à l'infini
- envoyer n'importe quels quatre points en position générale sur n'importe quels quatre points (un carré par exemple).

Démonstration. Le premier point est clair d'après la remarque précédente. Intéressons-nous au deuxième point. Il suffit clairement de montrer que l'on peut envoyer n'importe quels quatre points sur un carré.

Pour ce faire on envoie les intersections des côtés opposés à l'infini de sorte qu'on a un parallélogramme, qu'on transforme en carré par une transformation affine (i.e. point de projection à l'infini). □

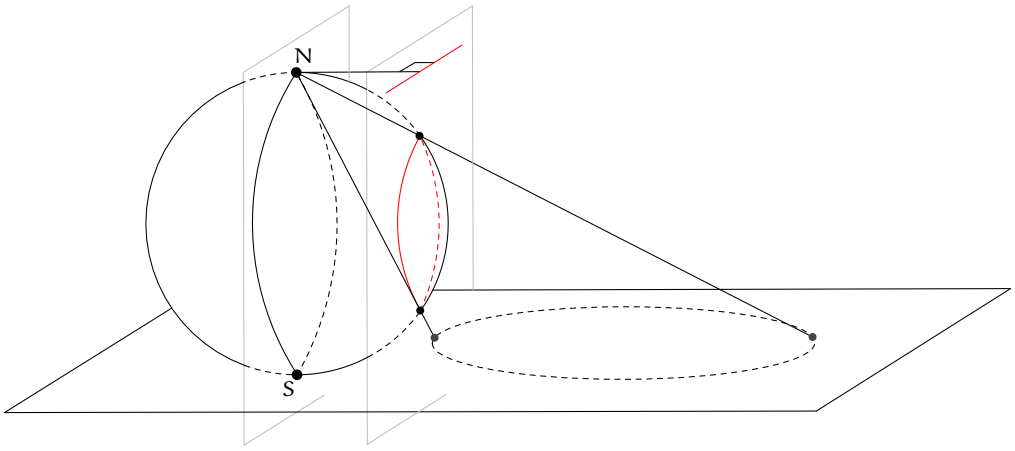
Remarque 4.35. Quatre points est bien la condition maximale. En effet, avec cinq points en position générale A, B, C, D et E on a déjà des birapports exprimables et qui devront être conservés. Par exemple $b_{A,B,(EC)\cap(AB),(ED)\cap(AB)}$.

Lemme 4.36. Considérons une sphère, son pôle Nord N et son pôle Sud S ainsi qu'un plan $\mathcal{P}$ tangent en S à la sphère. Alors, la projection stéréographique qui a un point P de la sphère associe $(PN) \cap \mathcal{P}$ conserve les cercles.

Démonstration. Ce n'est pas le plus intéressant et c'est un calvaire de faire cette démonstration sur un papier 2-dimensionnel. Le lecteur se référera donc au très bon film "Dimensions". L'idée est de regarder un cône autour du cercle que l'on souhaite projeter et d'utiliser Thalès ou des triangles semblables. □

Remarque 4.37. La projection stéréographique serait stricto sensu plus du domaine de la géométrie projective unidimensionnelle complexe car le point N est envoyé sur un unique point à l'infini. Mais il faut en fait voir ici cette projection comme une simple astuce de calcul.

Théorème 4.38. En projetant on peut envoyer un cercle donné sur un cercle et une droite disjointe de ce cercle sur la droite à l'infini.



Démonstration. Pour le voir, on prend une sphère dont l'intersection avec notre plan est le cercle, de rayon la distance du centre du cercle à la droite. Il y a alors un et un seul diamètre de la sphère parallèle au plan et perpendiculaire à la droite. On l'appelle axe des pôles. L'extrémité qui fait face à la droite est dite pôle Nord, l'autre pôle Sud. On projette notre plan sur le plan tangent au pôle Sud, depuis le pôle Nord. □

Théorème 4.39. En projetant, on peut envoyer un cercle donné sur un cercle et un point à l'intérieur (strictement) en son centre.

Démonstration. Il est également possible de montrer cette affirmation en manipulant intelligemment la géométrie de l'espace. Mais le plus simple est ici de loin de se référer au chapitre suivant en affirmant qu'il suffit d'envoyer le cercle sur un cercle et la polaire du point considéré sur la droite à l'infini, ce que l'on peut faire d'après le théorème précédent. □

Ces théorèmes peuvent s'appliquer dans énormément de situations, tant qu'il n'y a pas trop de longueurs, de cercles ou d'angles. Le lecteur est invité à reprendre les preuves de la première partie en utilisant maintenant des transformations projectives.

Théorème 4.40 (Ceva)**.** Soit A, B, C un triangle et X, Y et Z des points sur (BC), (CA) et (AB) respectivement.

Alors (AX), (BY) et (CZ) sont concourantes si et seulement si $\frac{\overline{AZ}}{\overline{BZ}} \cdot \frac{\overline{BX}}{\overline{CX}} \cdot \frac{\overline{CY}}{\overline{AY}} = -1$.

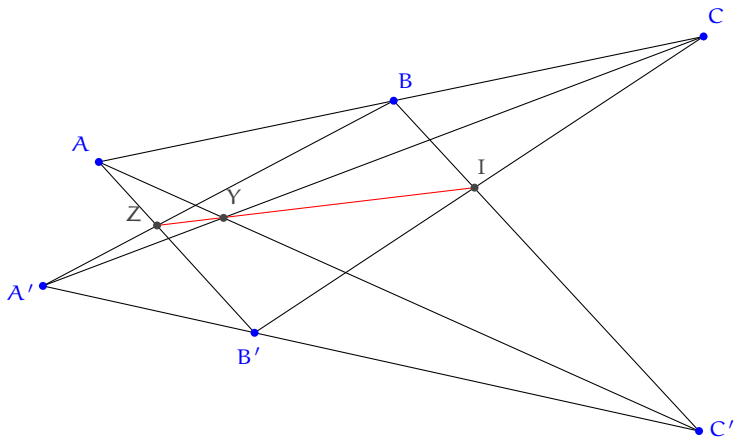
Démonstration. On nomme $O = (AX) \cap (BY)$.

$\frac{\overline{AZ}}{\overline{BZ}} \cdot \frac{\overline{BX}}{\overline{CX}} \cdot \frac{\overline{CY}}{\overline{AY}}$ est un produit cyclique de rapports. Il est donc conservé par transformation projective (voire remarque 4.11).

On peut donc envoyer A, B, C et O sur un triangle équilatéral et son centre. Auquel cas le théorème est trivial. □

Théorème 4.41 (Pappus)**.** Soit A, B, C trois points alignés et A', B', C' trois autres points alignés. On pose $X = (AB') \cap (A'B)$ $Y = (AC') \cap (A'C)$ et $Z = (BC') \cap (B'C)$.

Alors X, Y et Z sont alignés.



Démonstration.

On envoie X et Y sur la droite à l'infini. Dans la nouvelle figure, $(AB') \parallel (A'B)$ et $(AC') \parallel (A'C)$, d'où d'après Thalès, en notant P l'intersection des deux droites portant A, B, C et A', B', C' (si elles sont parallèles, c'est encore plus simple), $\frac{PA}{PB'} = \frac{PA'}{PB}$ et $\frac{PA}{PC'} = \frac{PA'}{PC}$, d'où $\frac{PB}{PC'} = \frac{PB'}{PC}$ et donc $(BC') \parallel (B'C)$ d'après Thalès. Z est donc sur la droite à l'infini, et en particulier il est aligné avec X et Y, d'où la conclusion. □

Remarque 4.42. Une autre preuve consisterait à remarquer que le théorème de Pappus est exactement le théorème de Pascal dans le cas d'une conique dégénérée en deux doites. On peut donc le prouver par continuité à partir de Pascal en prenant la limite d'une suite d'hyperbole tendant vers ces deux droites.

Théorème 4.43 (Desargues)**.** Soit ABC et $A'B'C'$ deux triangles perspectifs, i.e. tels que (AA'), (BB'), (CC') soient concourantes. On pose $X = (AC) \cap (A'C')$, $Y = (BC) \cap (B'C')$ et $Z = (AB) \cap (A'B')$.

Alors, X, Y et Z sont alignés.

Démonstration. On envoie (YZ) sur la droite à l'infini. (AB) est maintenant parallèle à $(A'B')$, (BC) à $(B'C')$. Les deux triangles sont donc des agrandissements l'un de l'autre, d'où $(AC) \parallel (A'C')$, i.e. X sur la droite à l'infini et donc aligné avec Y et Z. D'où la conclusion. □

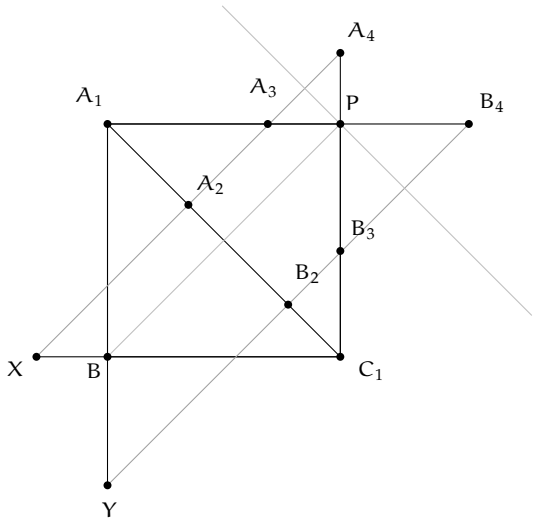
Exercice 6 Soit ABC un triangle et P un point en son intérieur. Soit A_1, B_1 et C_1 les intersections de (AP), (BP) et (CP) avec les côtés respectifs du triangle. Soit A_2 et C_2 sur (A_1C_1) tels que (AA_1) coupe $[B_1A_2]$ en son milieu et (CC_1) coupe $[B_1C_2]$ en son milieu. Soit $A_3 = (A_2B_1) \cap (CC_1)$ et $C_3 = (C_2B_1) \cap (AA_1)$.

Montrer que $(A_3C_3) \parallel (AC)$.

Solution de l'exercice 6 Une idée naturelle est d'envoyer la droite (AC) à l'infini. On obtiendra plein de droites parallèles et les milieux ne poseront pas de problèmes puisqu'ils s'exprimeront en termes de birapports.

Mais tant qu'à faire, autant profiter pleinement du degré de libreté, autant simplifier encore davantage la figure : on peut envoyer BC_1PA_1 sur un carré ! Notons X le point à l'infini de (B_1A_2), Y celui de (B_1C_2), A_4 le milieu de A_2B_1 et C_4 le milieu de C_2B_1.

Ces conditions s'écrivent $b_{B_1,A_2,A_4,X} = -1$, i.e. dans la figure projetée où B_1 est à l'infini, A_2 milieu de $[A_4X]$. De même, B_2 est milieu de $[B_4Y]$. Or, ces segments sont parallèles à la diagonale du carré donc X et Y sont sur les côtés du carrés. Finalement, on obtient que (A_3B_3) est obtenu de (A_2B_2) par la symétrie par rapport à (A_1C_1) puis par rapport à la bissectrice extérieure de C_1PA_1, donc par translation (par parallélisme des axes). D'où $(XY) \parallel (A_3B_3)$, i.e. (XY), (A_3B_3) et (AC) concourantes. Ce qui est exactement le résultat souhaité une fois revenu dans la figure de départ.



- Pôles et polaires -

Définition 4.44. Soit $\mathcal{C}$ un cercle et P un point. La polaire de P est l'ensemble des points Q tels que, si (PQ) coupe $\mathcal{C}$ en X et Y, P, Q, X et Y sont harmoniques.

Théorème 4.45. La polaire est une droite.

Démonstration. Tout est projectif, il suffit donc d'envoyer le cercle sur un cercle et le pôle soit à l'infini, soit au centre du cercle. □

Remarque 4.46. Stricto sensu, la polaire est une portion de droite dans le cas où le pôle est à l'extérieur. Mais on la prolonge à la droite entière par convention (et c'est justifié après rajout de quelques dimensions).

Théorème 4.47. La polaire d'un point P à l'extérieur de $\mathcal{C}$ est la droite passant par les deux points de tangences des tangentes passant par P.

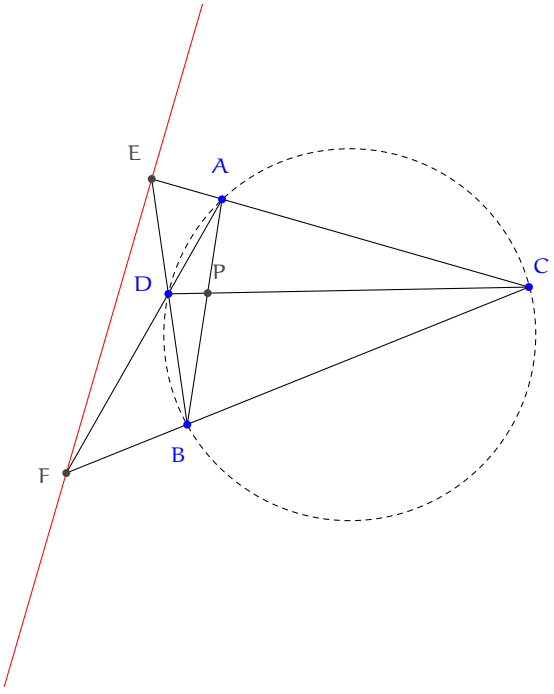
Démonstration. Trivial en prenant une corde tendant vers la tangente. □

On a un moyen général classique de construire la polaire, qu'il faut apprendre à reconnaître dans les figures :

Théorème 4.48. Soit A, B, C et D sur le cercle de manière à avoir A, B, P et C, D, P alignés. Soit $E = (AC) \cap (BD)$ et $F = (AD) \cap (BC)$.

Alors EF est la polaire de P.

Démonstration.



On peut soit, comme précédemment, utiliser une transformation projective envoyant le cercle sur un cercle et P à l'infini / sur le centre, auquel cas c'est clair par symétrie, soit utiliser le théorème du quadrilatère complet. □

Finalement, la polaire a deux propriétés simples mais souvent essentielles :

Proposition 4.49. Soit P un point et $\mathcal{C}$ un cercle de centre O. Alors (OP) est perpendiculaire à la polaire de P.

Démonstration. C'est clair par symétrie. □

Proposition 4.50. P est sur la polaire de Q si et seulement si Q est sur la polaire de P.

Démonstration. C'est clair par définition si (PQ) coupe le cercle (harmonicité avec les points d'intersection). Si ce n'est pas le cas, on peut raisonner de plusieurs manières. Soit dire qu'analytiquement c'est des fonctions polynômiales donc que l'avoir montré pour ce cas suffit à généraliser, soit pratiquer une involution / inversion pour rentrer les points dans le cercle. □

Exercice 7 Redémontrer la propriété 4.28 à l'aide des pôles et polaires.

Solution de l'exercice 7 Soit $X = (AB) \cap (CD)$. (AB) est la polaire de P donc X est sur la polaire de P donc P, X, D et C sont harmoniques. On obtient le résultat en projetant sur le cercle à partir de A ou de B.

Exercice 8 Soit ABC un triangle, A′, B′ et C′ les points de contact du cercle inscrit ω, D le pied de la hauteur issue de A, M le milieu de [AD]. Soit N le deuxième point d'intersection de (A′M) avec ω.

Montrer que le cercle circonscrit à BNC est tangent en N à ω.

Solution de l'exercice 8 Le cercle inscrit invite à considérer des pôles / polaires. Dans cet esprit, il est naturel d'introduire $A'' = (B'C') \cap (BC)$. A″ est sur la polaire (B′C′) de A et sur celle (BC) de A′, donc sa polaire est (AA′). En particulier, en notant I le centre du cercle inscrit, $(IA'') \perp (AA')$.

On a ainsi exhibé, puisque $(AD) \perp (BC)$, des points cocyliques, d'où on déduit $\widehat{DAA'} = \widehat{IA''A'}$ et $IA'A'' \sim A'DA$. Cela permet de faire entrer le point M en jeu : en notant M′ le milieu de [AA″], $IA'M' \sim A'DM$. En particulier, en faisant le raisonnement inverse, $(IM') \perp (A'M)$.

Or, A′ est déjà sur la polaire de M′ qui est donc (A′M). En particulier, (M′N) est tangente à ω en N. On souhaiterait maintenant montrer qu'elle est aussi tangente à l'autre cercle. Par puissance d'un point, il suffit de montrer que $M'N^2 = M'B \cdot M'C$, i.e. $M'A'^2 = M'D \cdot M'C$. C'est la formule de MacLaurin. Il suffit donc de prouver que A″, A′, B et C sont harmoniques, ce qui est vrai grâce au théorème du quadrilatère complet dans la configuration du point de Gergonne.

Exercice 9 Soit ABCD un quadrilatère cyclique. $E = (AD) \cap (BC)$ avec C entre B et E. Les diagonales s'intersectent en F. On considère le milieu M de [CD] et N sur le cercle circonscrit à ABM tel que $AN/BN = AM/CM$.

Montrer que E, F et N sont colinéaires.

Solution de l'exercice 9 La condition signifie clairement que M, N, A et B sont harmoniques (le birapport est réel, son module est 1 et ce n'est pas un cas dégénéré).

Soit $P = (AB) \cap (CD)$. Par la construction classique, (EF) est la polaire de P. On peut déjà faire disparaître la moitié de la figure.

Montrons que (après l'avoir conjecturé sur les dessins) le point d'intersection K de la polaire de P et de (DC) est sur le cercle circonscrit à ABM.

Dans un premier temps, par définition de la polaire, P, K, D et C sont harmoniques. Donc d'après la relation de Newton, $PD \cdot PC = PK \cdot PM$. D'où, en utilisant la puissance de P par rapport au cercle, $PK \cdot PM = PA \cdot PB$, ce qui prouve bien que A, B, K et M sont cocycliques.

Enfin, soit N' le second point d'intersection de la polaire avec ce cercle et X l'intersection de la polaire et de (AB). En projetant sur le cercle circonscrit à $ABKM$ à partir de K les points harmoniques P, X, A et B, on montre que les points M, N', A et B sont harmoniques, ce qui, par unicité du quatrième point harmonique montre que $N = N'$. D'où la conclusion.

- Dualité -

La géométrie projective bidimensionnelle réelle a une caractéristique intéressante : on peut y définir deux dualités.

Dans un premier temps, une dualité intrinsèque entre points et droites.

Définition 4.51. Considérons un énoncé projectif ne concernant que des points et des droites. On appelle énoncé dual l'énoncé où l'on remplace chaque occurence de « points » par un occurrence de « droites » et réciproquement, chaque occurence de « alignés » par « concourant » et réciproquement, chaque occurence de « la droite passant par P et Q » par « le point d'intersection de la droite p et de la droite q ».

Exemple 4.52. Le dual du théorème de Desargues est sa réciproque.

Théorème 4.53. Un énoncé projectif est vrai si et seulement si son dual est vrai.

Démonstration. Un argument est de dire que les axiomes de la géométrie projective sont fermés par passage au dual. Par exemple, on a un axiome "par tous deux points passe une unique droite" et son dual "toutes deux droites s'intersectent en un unique point".

Un autre argument est de regarder le plan projectif bidimensionnel réel comme l'ensemble des droites de $\mathbb{R}^3 \setminus \{(0;0;0)\}$ passant par l'origine et d'interpréter la dualité en associant à une telle droite (donc un point dans l'espace projectif) le plan (donc une droite dans l'espace projectif) perpendiculaire à la droite. Cette bijection vérifie effectivement les conditions de dualité.

Enfin, le dernier argument est que c'est une conséquence de la deuxième dualité, la dualité pôle / polaire, en choisissant un cercle arbitraire. □

La dualité est particulièrement intéressante parce qu'on a toujours deux résultats pour le prix d'un, sans avoir à faire la moindre démonstration supplémentaire.

Exercice 10 Soit a, b, c et a', b', c' deux triplets de droites concourantes. Soit x la droite joignant $a \cap b'$ et $b \cap a'$, y la droite joignant $a \cap c'$ et $c \cap a'$, z la droite joignant $b \cap c'$ et $c \cap b'$.

Montrer que x, y et z sont concourantes.

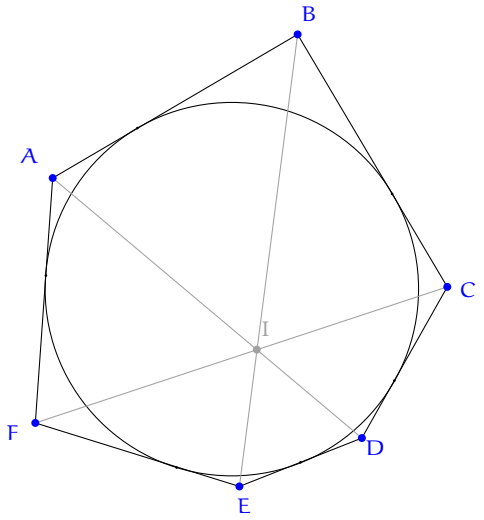
Solution de l'exercice 10 C'est le dual du théorème de Pappus.

Un cas particulier de cette dualité est la dualité pôle / polaire. Si on fixe un cercle et que l'on change une configuration en remplaçant chaque point par sa polaire et chaque droite par son pôle en écrivant l'énoncé dual, le cours sur les polaires nous assure que le problème est vrai si et seulement si le problème dualisé est vrai.

L'application type de ce principe est le théorème de Brianchon :

Théorème 4.54 (Brianchon)**.** Soit $\mathcal{C}$ un cercle inscrit dans un hexagone $ABCDEF$.

Montrer que (AD), (BE) et (CF) sont concourantes.



Démonstration.

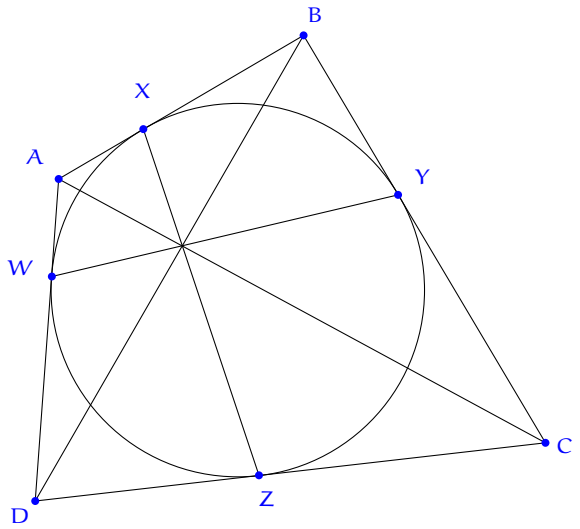
Dualisons par rapport à $\mathcal{C}$. On obtient le théorème de Pascal. D'où la conclusion. □

Le théorème de Brianchon est utile en lui-même, souvent dans des cas dégénérés.

Exercice 11 Soit $\mathcal{C}$ un cercle inscrit dans un quadrilatère $ABCD$. Soit X, Y, Z et W les points de tangence sur les côtés $[AB]$, $[BC]$, $[CD]$ et $[DA]$ respectivement.

Alors (XZ) et (YW) se coupent sur l'intersection des diagonales.

Solution de l'exercice 11



Utilisons Brianchon avec l'hexagone circonscriptible dégénéré $AXBCZD$. On obtient que (AC), (XZ) et (BD) sont concourantes.

D'où la conclusion après le raisonnement symétrique.

IV. Test de mi-parcours

Contenu de cette partie

1 Groupe A

1 Énoncés

Exercice 1 On écrit les 2013 nombres $1, 2, \ldots, 2013$ au tableau. À chaque étape, on a le droit de choisir deux nombres A et B, puis les effacer du tableau, puis ajouter sur le tableau le nombre $A - B$. On fait cela jusqu'à ce qu'il ne reste qu'un nombre au tableau. Peut-il rester le nombre 2 ?

Exercice 2 Montrer que $a^2 + b^2 + 2(a-1)(b-1) \geqslant 1$ pour tous nombres réels a et b.

Exercice 3 Montrer que

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

pour tout entier $n \geqslant 1$.

Exercice 4 Soit $n \geqslant 4$ un entier. On dessine toutes les diagonales d'un n-gône convexe. On suppose qu'il n'y a jamais trois diagonales qui se coupent en un même point. Quel est le nombre de parties en lequel le n-gône est divisé ?

On essayera de trouver la formule la plus simple possible.

2 Solutions

Solution de l'exercice 1 À chaque fois que l'on remplace A et B par $A - B$, la somme totale des nombres au tableau garde la même parité : c'est un invariant. La somme initiale est $\frac{2013\times 2014}{2} = 1007 \times 2013$, donc impaire. Ainsi, on ne peut obtenir 2 au bout des 2012 manipulations.

Solution de l'exercice 2 En développant, on voit que $a^2+b^2+2(a-1)(b-1) \geqslant 1$ si et seulement si $a^2 + b^2 + 2ab - 2a - 2b + 1 \geqslant 0$. Or,

$$a^2 + b^2 + 2ab - 2a - 2b + 1 = (a+b)^2 - 2(a+b) + 1 = (a+b-1)^2 \geqslant 0.$$

Solution de l'exercice 3 On montre la formule par récurrence sur $n \in \mathbb{N}^*$. On initialise à $n = 1$: les deux sommes valent alors 1.
Hérédité : on suppose que pour un certain $n \geqslant 1$, on a :

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Alors

$$\begin{aligned}\sum_{k=1}^{n+1} k^3 &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \\ &= \frac{n^2(n+1)^2}{4} + \frac{4(n+1)(n+1)^2}{4} \\ &= \frac{(n+1)^2(n^2+4n+4)}{4} \\ &= \frac{(n+1)^2(n+2)^2}{4} \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2\end{aligned}$$

La formule est donc bien vérifiée au rang $n+1$. Ceci clôt la récurrence.

Solution de l'exercice 4 Comptons les parties qui apparaissent au fur et à mesure que l'on ajoute des diagonales. Au départ, le n-gône sans diagonales constitue une seule partie. Puis, lorsque l'on trace une diagonale, on le divise en 2. On « crée »donc une nouvelle partie. Il faut donc rajouter $\frac{n(n-3)}{2} = \binom{n}{2} - n$ (le nombre total de diagonales) parties. Ceci est vrai lorsque la nouvelle diagonale tracée n'intersecte aucune ancienne diagonale. En revanche, lorsque deux diagonales s'intersectent, le nombre de parties supplémentaires "créées" est 2 et non 1. On a déjà compté une nouvelle partie pour ces diagonales, il reste à compter une partie supplémentaire à chaque fois que deux diagonales se croisent, ce qui arrive $\binom{n}{4}$ fois. En effet, à chaque quadruplet A, B, C, D de points sur le polygône correspond une unique intersection de diagonales : si les points A, B, C, D sont situés sur le polygône dans cet ordre, il s'agit des diagonales (AC) et (BD). On a donc un total de

$$1 + \frac{n(n-1)}{2} - n + \frac{n(n-1)(n-2)(n-3)}{24} = \frac{n^4 - 6n^3 + 23n^2 - 42n + 24}{24}$$

parties.

2 Groupe B

1 Énoncés

Exercice 1 On écrit les 2013 nombres $1, 2, \ldots, 2013$ au tableau. À chaque étape, on a le droit de choisir deux nombres A et B, puis les effacer du tableau, puis ajouter sur le tableau le nombre $A - B$. On fait cela jusqu'à ce qu'il ne reste qu'un nombre au tableau. Peut-il rester le nombre 2 ?

Exercice 2 Montrer que $a^2 + b^2 + 2(a-1)(b-1) \geqslant 1$ pour tous nombres réels a et b.

Exercice 3 Soit x un nombre réel non nul tel que $x + \frac{1}{x}$ est un nombre entier. Montrer que $x^n + \frac{1}{x^n}$ est un entier pour tout entier $n \geqslant 0$.

Exercice 4 Soit a, b, c, d des réels définis par

$$a = \sqrt{4 - \sqrt{5 - a}},\ b = \sqrt{4 + \sqrt{5 - b}},\ c = \sqrt{4 - \sqrt{5 + c}},\ d = \sqrt{4 + \sqrt{5 + d}}.$$

Calculer leur produit.

2 Solutions

Solution de l'exercice 1 À chaque fois que l'on remplace A et B par $A - B$, la somme totale des nombres au tableau garde la même parité : c'est un invariant. La somme initiale est $\frac{2013\times 2014}{2} = 1007 \times 2013$, donc impaire. Ainsi, on ne peut obtenir 2 au bout des 2012 manipulations.

Solution de l'exercice 2 PREMIÈRE SOLUTION. En développant, on voit que $a^2+b^2+2(a-1)(b-1) \geqslant 1$ si et seulement si $a^2 + b^2 + 2ab - 2a - 2b + 1 \geqslant 0$. Or

$$a^2 + b^2 + 2ab - 2a - 2b + 1 = (a + b)^2 - 2(a + b) + 1 = (a + b - 1)^2 \geqslant 0.$$

AUTRE SOLUTION. Pour un réel b fixé, voyons $a^2+b^2+2ab-2a-2b+1$ comme un polynôme de degré 2 en a et écrivons $a^2 + b^2 + 2ab - 2a - 2b + 1 = a^2 + a(2b-2) + b^2 - 2b + 1$. Posons $f(a) = a^2 + a(2b-2) + b^2 - 2b + 1$. Alors (rappelons que cela provient de l'écriture sous forme canonique) $f(a) \geqslant f(-(2b-2)/2)$. Ainsi

$$f(a) \geqslant f(1 - b) = (1 - b)^2 - 2(1 - b)^2 + (b - 1)^2 = 0,$$

d'où le résultat.

Solution de l'exercice 3 Montrons que la propriété suivante est vérifiée par récurrence sur n :

$$P_n : \qquad \text{« } \alpha^{n-1} + \frac{1}{\alpha^{n-1}} \in \mathbb{Z} \quad \text{et} \quad \alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z} \text{ ».}$$

- (Initialisation) P_1 est clairement vraie.
- (Hérédité) Soit $n \geqslant 1$ un entier et supposons que P_n est vraie. Remarquons que :

$$\alpha^{n+1} + \frac{1}{\alpha^{n+1}} = \left(\alpha + \frac{1}{\alpha}\right)\left(\alpha^n + \frac{1}{\alpha^n}\right) - \left(\alpha^{n-1} + \frac{1}{\alpha^{n-1}}\right),$$

qui est entier grâce à l'hypothèse de l'énonce et à l'hypothèse de récurrence P_n. Cela conclut.

Solution de l'exercice 4 Il serait merveilleux que les quatre réels a, b, c, d soient racines d'un même polynôme, dont le terme constant serait leur produit. Heureusement, c'est presque vrai. En effet, en élevant au carré deux fois chaque égalité (en prenant soin d'isoler la racine à chaque fois), on trouve que $a, b, -c, -d$ sont racines du polynôme $P(X) = X^4 - 8X^2 - X + 11$. Et, il est clair que $a, b > 0$ et $-c, -d < 0$ (les réels a, b, c, d sont non nuls, car $P(0) \neq 0$). De plus, si $a = b$, $\sqrt{4 - \sqrt{5 - a}} = \sqrt{4 + \sqrt{5 - a}}$ donc $5 - a = 0$, donc $5 = \sqrt{4 - 0} = 2$, ce qui est absurde. De même, on vérifie que $c \neq d$.
Ainsi P a quatre racines distinctes $a, b, -c, -d$, donc $abcd = 11$ par la formule de Viète.

3 Groupe C

1 Énoncés

Exercice 1 Trouver tous les réels a, b tels que le polynôme $(X-1)^2$ divise le polynôme $aX^4 + bX^3 + 1$.

Exercice 2

a) Soit T une similitude directe. Montrer qu'il existe une similitude directe de même centre envoyant tout point M sur le milieu de M et $T(M)$.

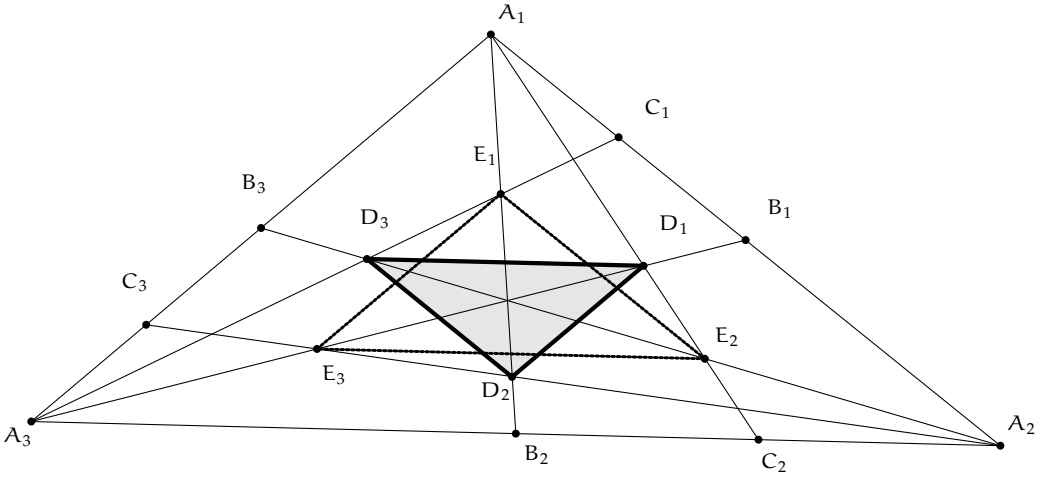
b) Soit $ABCD$ un quadrilatère, M et N les milieux de ses diagonales et P leur intersection. Soit O_1 et O_2 les centres des cercles circonscrits de ABP et CDP. Montrer que le milieu du segment $[O_1O_2]$ est le centre du cercle circonscrit de PMN.

Exercice 3 Trouver les tous les nombres réels x, y, z tels qu'on ait

$$x - y + z = 2 \qquad x^2 + y^2 + z^2 = 30 \qquad x^3 - y^3 + z^3 = 116.$$

Exercice 4 Soit $A_1A_2A_3$ un triangle. On construit les points suivants :
- B_1, B_2 et B_3 les milieux de A_1A_2, A_2A_3 et A_3A_1.
- C_1, C_2 et C_3 les milieux de A_1B_1, A_2B_2 et A_3B_3.
- D_1 l'intersection de (A_1C_2) et (B_1A_3), D_2 et D_3 définis de la même façon cycliquement.
- E_1 l'intersection de (A_1B_2) et (C_1A_3), E_2 et E_3 définis de la même façon cycliquement.

Calculer le quotient de l'aire de $D_1D_2D_3$ par l'aire de $E_1E_2E_3$.



2 Solutions

Solution de l'exercice 1 Soit $P(x) = ax^4 + bx^3 + 1$.

PREMIÈRE SOLUTION. On a vu que $(x-1)^2$ divise $P(x)$ si, et seulement si, $P(1) = 0$ et $P'(1) = 0$. Or, $P(1) = a + b + 1$ et $P'(1) = 4a + 3b$. La résolution de $a + b + 1 = 0$ et $4a + 3b = 0$ donne $b = -4$ et $a = 3$.

DEUXIÈME SOLUTION. On fait la division euclidienne de $ax^4 + bx^3 + 1$ par $(x-1)^2$. Après calculs, on trouve

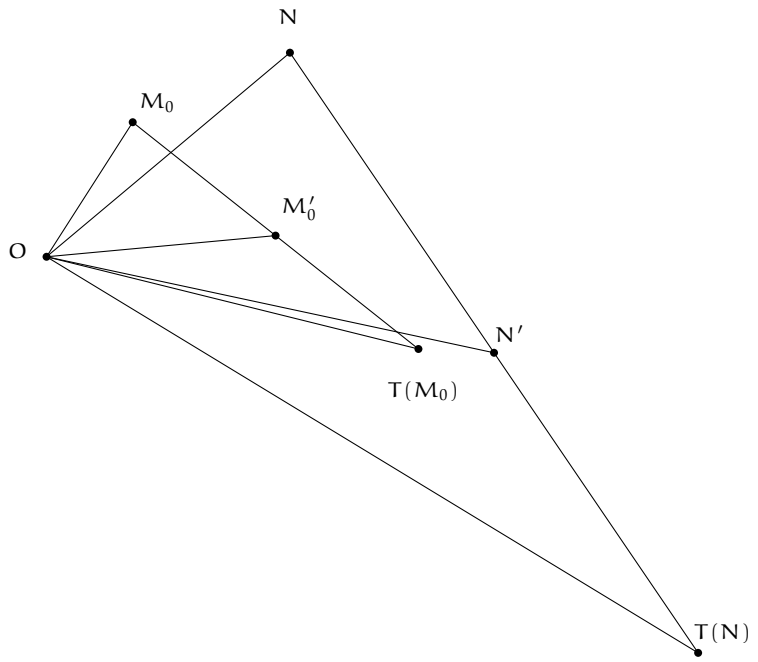
$$ax^4 + bx^3 + 1 = (x^2 - 2x + 1)(ax^2 + (b + 2a)x + 2b + 3a) + (3b + 4a)x + 1 - 2b - 3a.$$

Ainsi $(x-1)^2$ divise $ax^4 + bx^3 + 1$ si, et seulement si $3b + 4a = 0$ et $2b + 3a = 1$, c'est-à-dire si, et seulement si, $b = -4$ et $a = 3$.

TROISIÈME SOLUTION. Supposons que $ax^4 + bx^3 + 1 = (x-1)^2 P(x)$. Le polynôme $P(x)$ est unitaire de degré 2, et l'on peut ainsi écrire $P(x) = x^2 + ux + v$. En développant l'égalité $ax^4 + bx^3 + 1 = (x-1)^2(x^2 + ux + v)$, en identifiant les coefficients et en résolvant le système de deux équations, on trouve $b = -4$ et $a = 3$. Réciproquement, on vérifie que ces valeurs conviennent.

Solution de l'exercice 2

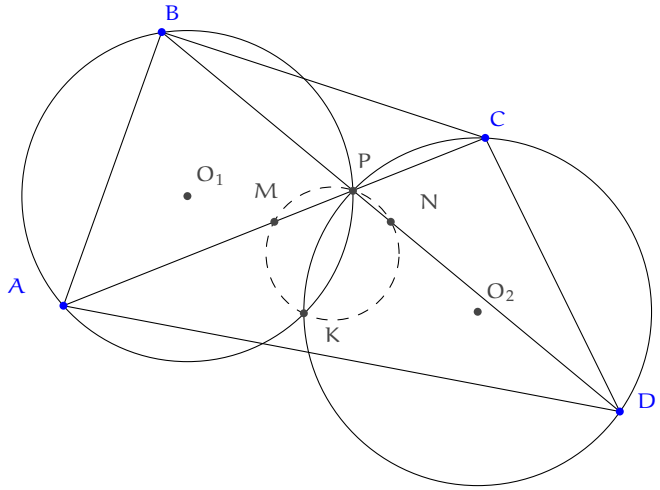
(i)



Soit O le centre de la similitude T. Pour un point M, notons M′ le milieu de M et de T(M). Fixons un point M_0 (différent de O) et considérons la similitude directe S de centre O qui envoie M_0 et M_0'. Soit N un autre point et montrons qu'elle envoie N sur N′. Les triangles $OM_0T(M_0)$ et ONT(N) étant semblables, les triangles OM_0M_0' et ONN′ sont semblables. Il existe donc une similitude directe de centre O notée S_2 envoyant M_0 sur M_0' et N sur N′. On en déduit que $S = S_2$, ce qui implique bien que S envoie N sur N′.

REMARQUE. Il est possible de résoudre facilement cette question en utilisant les nombres complexes. En effet, toute similitude directe f de centre O (où O est l'origine) est de la forme $f(z) = az$ avec $a \in \mathbb{C}$ deux nombres complexes. Pour résoudre la question, il suffit donc de vérfier que $(z + f(z))/2$ est de cette forme. Comme $(z + f(z))/2 = (1 + a)/2 \cdot z$, $z \mapsto (z + f(z))/2$ est une similitude directe de centre O qui vérifie les conditions de l'énoncé.

(ii) Soit K l'intersection des cercles circonscrits des triangles ABP et PCD.



On sait que K est le centre de la similitude directe T qui envoie [AC] sur [BD], et donc M sur N et O_1 sur O_2. On en déduit que M, P, N, K sont cocycliques. Considérons la nouvelle similitude S de centre K envoyant tout point U sur le milieu de [UT(U)] (qui existe par (i)). Elle envoie donc A sur M, B sur N et K sur K. Elle envoie donc le cercle circonscrit de ABP sur le cercle passant par M, P, N, K. Comme O_1 est envoyé sur le milieu de $[O_1O_2]$, on en déduit que le milieu de $[O_1O_2]$ est le centre du cercle passant par M, P, N, K.

Solution de l'exercice 3 L'énoncé fait penser à des sommes symétriques, à quelques changements de signe près. Pour y remédier, posons $t = -y$:
On veut résoudre :

$$\begin{aligned} x + z + t &= 2 \\ x^2 + z^2 + t^2 &= 30 \\ x^3 + z^3 + t^3 &= 116 \end{aligned}$$

On calcule donc les polynômes symétriques élémentaires σ_1, σ_2 et σ_3 en x, z et t :

$$\sigma_1 = S_1 = 2$$

$$\sigma_2 = \frac{1}{2}(S_1^2 - S_2) = -13$$

et, enfin, $S_3 = S_1S_2 - (S_1\sigma_2 - 3\sigma_3)$ donc :

$$\sigma_3 = \frac{1}{3}(S_3 - S_1S_2 + S_1\sigma_2) = \frac{1}{3}(116 - 60 - 26) = 10$$

x, z et t sont donc les racines de $P = X^3 - 2X^2 - 13X - 10$. On remarque que -1 est racine de P, ce qui permet de factoriser $P = (X+1)(X^2 - 3X - 10)$. On peut ensuite résoudre l'équation de degré 2 : les racines de P sont -1, -2 et 5 donc $\{x, z, t\} = \{-1, -2, 5\}$ donc les valeurs possibles de (x, y, z) sont $(-1, 2, 5)$, $(-1, -5, -2)$, $(-2, 1, 5)$, $(-2, -5, -1)$, $(5, 1, -2)$ et $(5, 2, -1)$.

Solution de l'exercice 4 Nous allons résoudre cet exercice avec les coordonnées barycentriques. On remarque que les deux triangles qui nous intéressent, $D_1D_2D_3$ et $E_1E_2E_3$, ont l'air de copies du grand triangle $A_1A_2A_3$, c'est-à-dire que ce sont les images du gros triangle par deux homtéties. Si on arrive à trouver les rapports de ces deux homotéties, on pourra en déduire le quotient des aires. Intéressons-nous tout d'abord au centre des homotéties : si $A_1 \to D_2$, $A_2 \to D_3$ et $A_3 \to D_1$, il faut que le centre soit sur l'intersection des trois droites (A_1D_2), (A_2D_3) et (A_3D_1), c'est-à-dire le centre de grabité G.

Calculons maintenant les coordonnées barycentriques de tous les points de la figure. Commençons par les points évidents :

$$A_1 : (1,0,0),\ A_2 : (0,1,0),\ A_3 : (0,0,0) \text{ et } G : (1,1,1).$$

Ensuite les B_i sont les milieux des segments donc

$$B_1 : (1,1,0),\ B_2 : (0,1,1),\ B_3 : (1,0,1),$$

et les C_i sont au quart des segments donc

$$C_1 : (3,1,0),\ C_2 : (0,3,1),\ C_3 : (1,0,3).$$

Regardons les D_i maintenant. Le point D_1 est l'intersection de (A_1C_2) avec (A_3B_1). Le cours sur les coordonnées barycentriques nous dit que les droites ont des equations du type $u\alpha + v\beta + w\gamma = 0$, avec (u,v,w) uniques à un coefficient multiplicatif près. Regardons la droite A_1C_2 : comme $A_1 : (1,0,0)$ est sur la droite, on en déduit $u = 0$, et comme $C_2 : (0,3,1)$ aussi on en déduit que $3v + w = 0$. L'équation de la droite est donc $\beta - 3\gamma = 0$. De la même manière on trouve que l'equation de (A_3B_1) est $\alpha - \beta = 0$. Le point D_1 est à l'intersection des deux droites, donc vérifie les deux equations, on résoud pour trouver que $D_1 : (3,3,1)$. Maintenant nous voulons trouver le rapport $\frac{GD_1}{GA_3}$. Le point G est sur la droite A_3D_1, donc G peut s'exprimer comme le barycentre de (A_3, λ) et de (D_1, μ), il suffit de trouver les poids λ, μ appropriés. La propriété sur les coordonnées barycentriques d'un barycentre dit que :

$$G : \left(\frac{3\mu}{7}, \frac{3\mu}{7}, \frac{\mu}{7} + \lambda\right),$$

on en déduit que $\mu = 7$ et $\lambda = 2$, et

$$\frac{GD_1}{GA_3} = \frac{-2}{7}.$$

La même démonstration donne le même résultat pour les points D_2 et D_3, donc le triangle $D_1D_2D_3$ est bien l'image du triangle $A_1A_2A_3$ par une homotétie de centre G et de rapport $\frac{-2}{7}$. Le rapport des aires vaut donc

$$\frac{[D_1D_2D_3]}{[A_1A_2A_3]} = \left(\frac{-2}{7}\right) = \frac{4}{49}.$$

Je vous laisse les résultats suivants : $E_1 : (3,1,1)$, et $\frac{GE_1}{GE_3} = \frac{2}{5}$ et

$$\frac{[E_1E_2E_3]}{[A_1A_2A_3]} = \frac{4}{25}.$$

Le quotient recherché est donc

$$\frac{[D_1D_2D_3]}{[E_1E_2E_3]} = \frac{25}{49}.$$

4 Groupe D

1 Énoncés

Exercice 1 Soit $ABCD$ un quadrilatère convexe inscrit dans un cercle Γ. Soit E l'intersection des diagonales, Δ une droite passant par E coupant les segments $[AB]$ et $[CD]$ en U et V et Γ en X et Y. Montrer que E est le milieu du segment $[XY]$ si et seulement si il est celui du segment $[UV]$.

Exercice 2 On pose $F_n = 2^{2^n} + 1$, $n \geqslant 2$ et on prend un facteur premier p de F_n. Montrer que :

a 2 est un reste quadratique modulo p ;

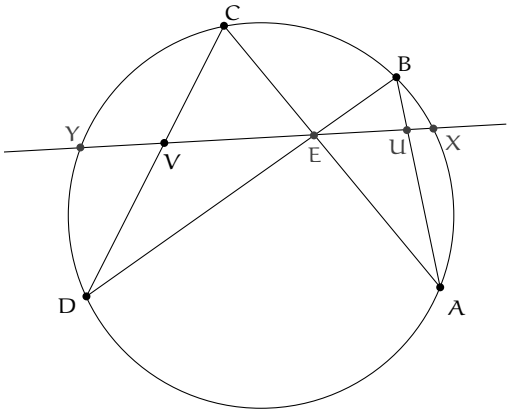
b $p \equiv 1 \pmod{2^{n+2}}$.

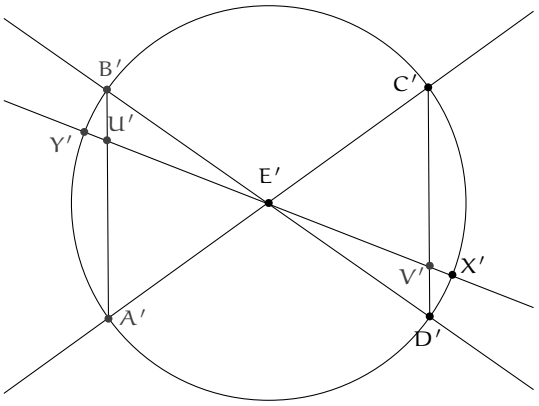
Exercice 3 Soit ABC un triangle, $\mathcal{C}_C$ et $\mathcal{C}_A$ ces cercle exinscrits opposés aux sommets A et C. Soit ω un cercle passant par B, tangent extérieurement à $\mathcal{C}_C$ et $\mathcal{C}_A$, et intersectant (AC) en deux points E et F. Montrer que $\widehat{ABE} = \widehat{FBC}$.

Exercice 4 Trouver tous les nombres premiers p, q, r tels que p divise $1 + q^r$, q divise $1 + r^p$ et r divise $1 + p^q$.

2 Solutions

Solution de l'exercice 1





On sait qu'il existe une transformation projective qui envoie le cercle sur un cercle et E sur son centre. On note A', B' etc... les images de A, B etc... et Z l'image du point à l'infini.
E est le milieu de $[XY]$ ssi X, Y, E et ∞ sont harmoniques ssi X', Y', E' et Z sont harmoniques et, de même, E est le milieu de $[UV]$ ssi U', V', E' et Z sont harmoniques.
Or, E' est le centre du cercle donc le milieu de $[X'Y']$, et c'est le milieu de $[U'V']$ d'après le théorème de Thalès, car $A'B'C'D'$ est un rectangle. On a donc X', Y', E', Z harmoniques ssi $Z = \infty$ et de même pour U', V', E', Z, d'où l'équivalence.

Remarque 4.1. Ce résultat est connu sous le doux nom de "théorème du papillon". Le lecteur intéressé pourra en consulter 17 preuves à l'adresse suivante :
http://www.cut-the-knot.org/pythagoras/Butterfly.shtml

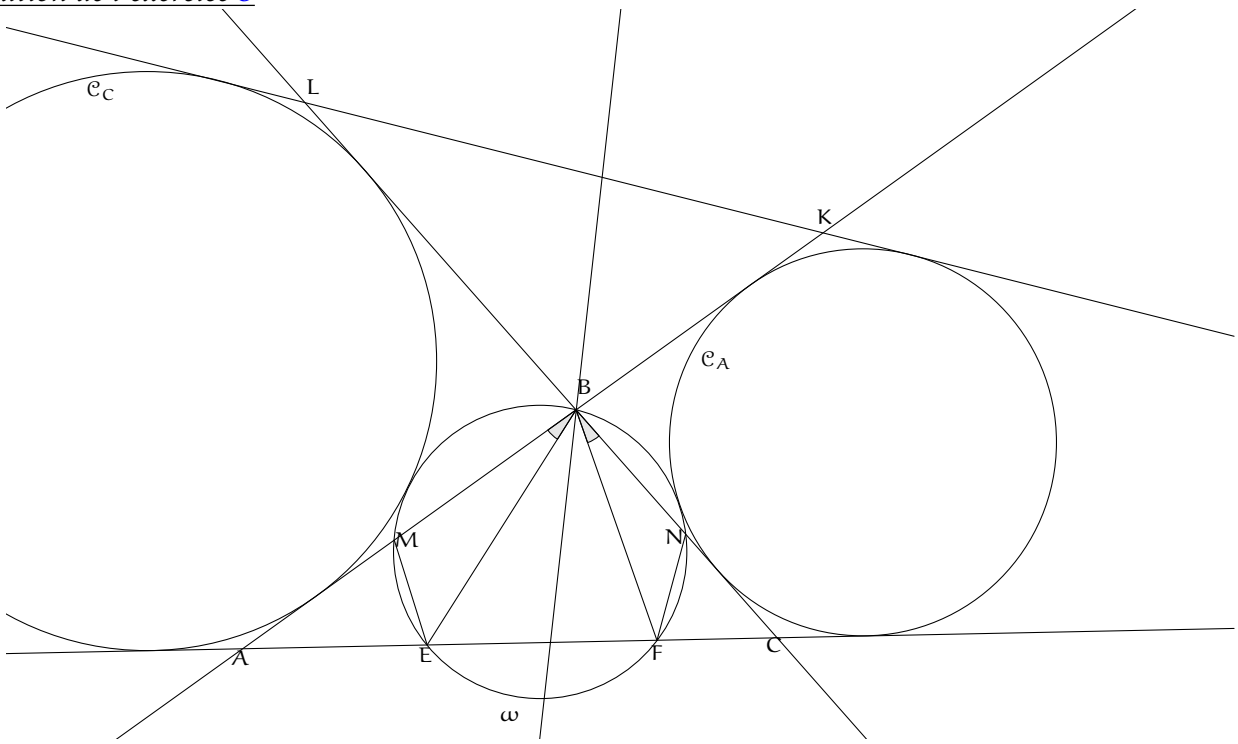
Solution de l'exercice 2

a On montre d'abord que $p \equiv 1 \bmod 2^{n+1}$. En effet, puisque $2^{2^{n+1}} \equiv 1 \bmod p$ on sait que $\mathrm{ord}_p(2)$ divise 2^{n+1}. D'autre part $2^{2^n} \not\equiv 1 \bmod p$, donc $\mathrm{ord}_p(2)$ ne divise pas 2^n. Maintenant, comme $\mathrm{ord}_p(2) = 2^{n+1}$ divise $p-1$, on trouve $p \equiv 1 \bmod 2^{n+1}$.
En particulier on a $p \equiv 1 \bmod 8$ et alors $p^2 - 1 = 16k + 1$ pour un entier k. Par la Loi de réciprocité quadratique on a $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = 1$.

b Soit a tel que $a^2 \equiv 2 \bmod p$. Alors $\mathrm{ord}_p(a) = 2\mathrm{ord}_p(2)$. Donc $\mathrm{ord}_p(a) = 2^{n+2}$. Comme cet ordre doit diviser $p-1$ on a le résultat.

Remarque : Si on cherche un diviseur de F_5 on arrive vite à tester $p = 5 \cdot 2^{5+2} + 1$. On a $F_5 \equiv 2^{32} + 1 \equiv 512^4 + 1 \equiv 0 \pmod{641}$, donc F_5 n'est pas premier.

Solution de l'exercice 3



Le problème parle d'angles, de cercles et de tangentes, il est donc tentant d'inverser. Il existe de plus un candidat intéréssant comme pôle d'inversion : B. En effet, il existe une homothétie centrée en B envoyant $\mathcal{C}_C$ sur $\mathcal{C}_A$, donc il existe une inversion centrée en B envoyant $\mathcal{C}_C$ sur $\mathcal{C}_A$ (si vous voulez le voir explicitement, introduisez les points P et Q de tangence de $\mathcal{C}_C$ avec AB (resp. de $\mathcal{C}_A$ avec BC), l'inversion en question est juste l'inversion de centre B et de puissance $-BP \cdot BQ$). Notons donc I cette inversion, p sa puissance.

Notre inversion I envoie ω sur une droite tangente à $\mathcal{C}_C$ et $\mathcal{C}_A$. On connaît déjà trois de leurs quatre tangentes communes : les côtés de ABC, et nécessairement ω est envoyé sur la quatrième que nous appelerons D. Introduisons M (resp. N) l'intersection de ω avec AB (resp. BC). Il sont respectivement envoyés sur les points K et L, intersections de D avec AB (resp. BC). Alors, $BK \cdot BM = |p| = BL \cdot BN$. Or, par symétrie de la figure par rapport à la droite joignant les centres de $\mathcal{C}_C$ et $\mathcal{C}_A$, $BA = BL$ et $BC = BK$. Ainsi, $BM/BA = BN/BC$, donc MN est parallèle à AC. Ainsi, les angles $\widehat{ABE}$ et $\widehat{FBC}$ interceptent des cordes de même longueur, donc sont égaux.

Solution de l'exercice 4 On commence par examiner la condition « p divise $1+q^r$ ». Elle se réecrit $q^r \equiv -1\,[p]$ et implique donc, en particulier, $q^{2r} \equiv 1\,[p]$. Ainsi l'ordre de q modulo p est un diviseur de $2r$. Comme r est supposé premier, c'est donc un élément de l'ensemble $\{1, 2, r, 2r\}$. Si on suppose en outre que $p \neq 2$, on a $q^r \not\equiv 1\,[p]$, et donc l'ordre de q modulo p est nécessairement 2 ou $2r$. Dans le premier cas, p divise $q^2-1=(q-1)(q+1)$, mais ne peut diviser $q-1$ (car $q^r \equiv -1\,[p]$) et par lemme de Gauss on obtient $q \equiv -1\,[p]$. Dans le deuxième cas, par théorème de Fermat on obtient que $2r$ divise $p-1$. En permutant les nombres p, q et r, on obtient bien sûr des conséquences analogues des deux autres conditions « q divise $1+r^p$ », et « r divise $1+p^q$ ».

On suppose maintenant que p, q et r sont tous les trois impairs, et pour commencer que l'on est dans le cas où $q \equiv -1\,[p]$. Le nombre premier p ne peut donc pas diviser $q-1$ (puisqu'il divise déjà $q+1$ et qu'il ne vaut pas 2). D'après les résultats du premier alinéa, la condition « q divise $1+r^p$ », implique donc que $r \equiv -1\,[q]$. En appliquant à nouveau le même argument, on trouve que $p \equiv -1\,[r]$. Or les trois congruences précédentes ne sont pas compatibles. Par exemple, elles impliquent $q \geqslant p-1$, $r \geqslant q-1$ et $p \geqslant r-1$, or deux de nos premiers ne peuvent être égaux, à cause de nos conditions « $q \equiv -1\,[p]$ », et si on suppose que p est maximal, nécessairement $q = p-1$, ce qui est impossible car p et q sont impairs. On en déduit que, toujours dans le cas où p, q et r sont supposés impairs, $2r$ divise $p-1$. En permutant circulairement les variables, on démontre de même que $2p$ divise $q-1$ et $2q$ divise $r-1$. Ainsi $8pqr$ divise $(p-1)(q-1)(r-1)$, ce qui n'est clairement pas possible étant donné que $8pqr > (p-1)(q-1)(r-1)$. Finalement, il n'y a pas de solution lorsque p, q et r sont tous les trois impairs.

On en vient à présent au cas où l'un de ces trois nombres est égal à 2. Quitte à permuter circulairement à nouveau p, q et r, on peut supposer que c'est p. Les conditions de l'énoncé disent alors que q est impair, que $r^2 \equiv -1\,[q]$ et que $2^q \equiv -1\,[r]$. Par ce qui a été fait dans le premier alinéa, cette dernière congruence entraîne que $r=3$ ou que $2q$ divise $r-1$. Le premier cas conduit à $9 \equiv -1\,[q]$, ce qui ne se produit que si $q=5$ puisque l'on a déjà écarté le cas $q=2$. On vérifie par ailleurs que le triplet $(2,5,3)$ est bien solution. Dans le second cas, maintenant, le produit $2q$ divise $r-1$, mais aussi $2(r^2+1)$ puisqu'on sait que $r^2 \equiv -1\,[q]$. Ainsi $2q$ divise $2(r^2+1)-2(r+1)(r-1)=4$, ce qui ne peut arriver.

En conclusion, il y a exactement trois solutions qui sont les triplets $(2,5,3)$, $(5,3,2)$ et $(3,2,5)$.

V. Troisième période

Contenu de cette partie

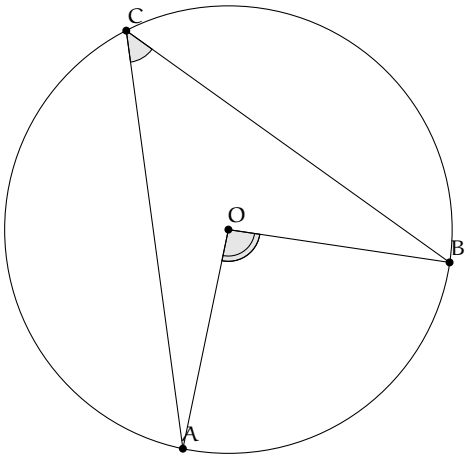
1 Groupe A : géométrie

1 Cours de géométrie : chasse aux angles, puissance d'un point

- La chasse aux angles -

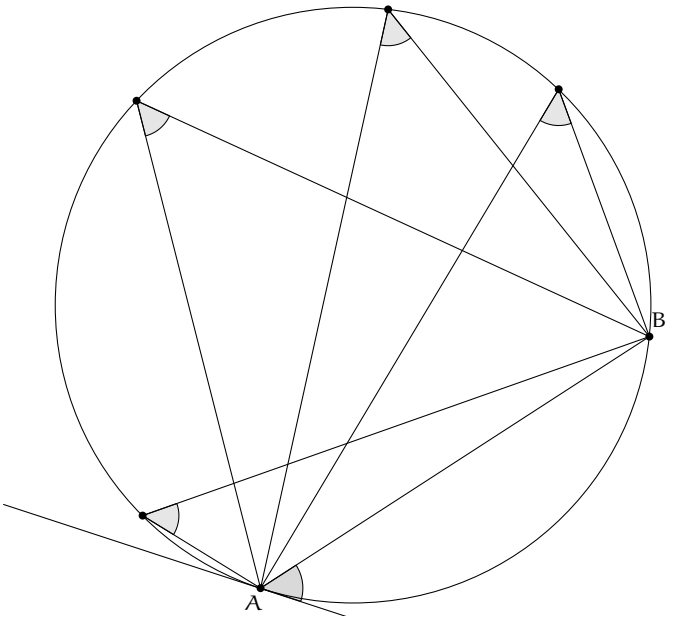
Il est bien souvent très pratique dans un problème de géométrie de savoir quels sont les angles égaux dans la figures, ou quelles sont les relations entre différents angles. Voici quelques techniques pour chasser les angles d'une figure.

Angle au centre - angle inscrit



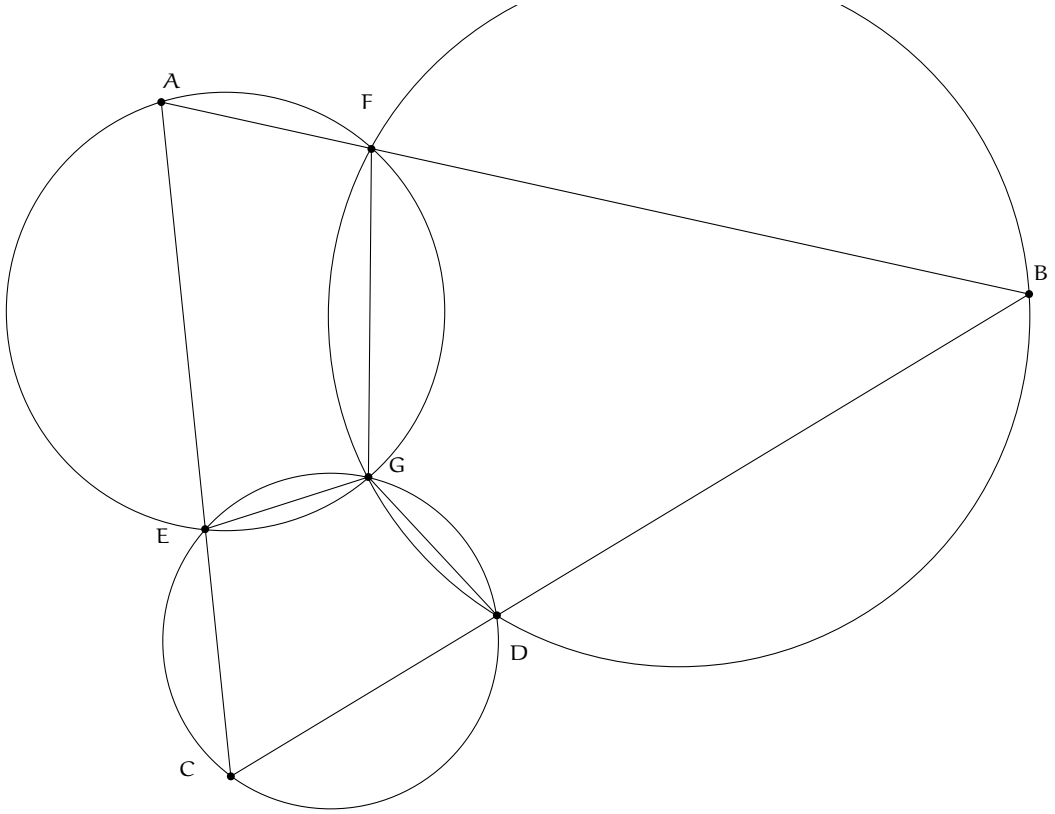
Théorème 1.1. $\widehat{ACB} = \frac{1}{2}\widehat{AOB}$, l'angle inscrit est la moitié de l'angle au centre.

Un corollaire très pratique est le suivant :



Corollaire 1.2. Tous les angles inscrits sont égaux, y compris l'angle inscrit "limite" : l'angle formé par la tangente.

Exercice 1 Montrer qu'un quadrilatère $ABCD$ est inscrit dans un cercle si et seulement si $\widehat{A} + \widehat{C} = \widehat{B} + \widehat{D} = 180°$.

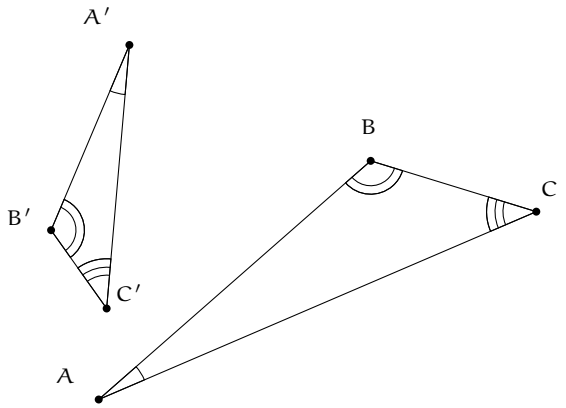


Exercice 2 (Théorème de Miquel) Soit ABC un triangle et D, E, F trois points sur les trois côtés du triangles. Montrer que les cercles circonscrits à AEF, BDF et CDE se coupent en un même point.

Exercice 3 Soit ABC un triangle, H son orthocentre et O le centre du cercle circonscrit. Montrer que $\widehat{BAO} = \widehat{CAH}$.

Exercice 4 (droite de Simson) Soit ABC un triangle et P un point. Soient P_1, P_2 et P_3 les projections de P sur les trois côtés du triangle. Montrer que P_1, P_2, P_3 alignés si et seulement si P est sur le cercle circonscrit.

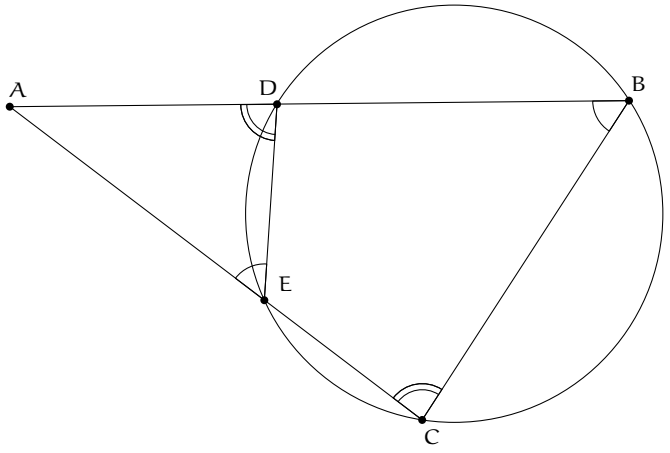
Triangles semblables On dit que deux triangles sont semblables lorsqu'ils ont la même forme.



Proposition 1.3. Les quatres propositions suivantes sont équivalentes :

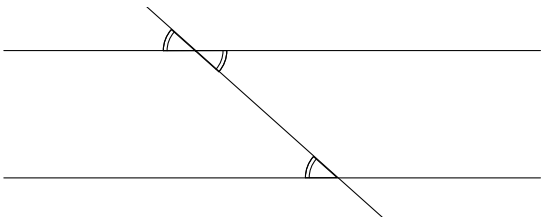
1. les triangles ABC et $A'B'C'$ sont semblables
2. $\widehat{A} = \widehat{A'}$, $\widehat{B} = \widehat{B'}$ et $\widehat{C} = \widehat{C'}$
3. $\frac{AB}{A'B'} = \frac{BC}{B'C'} = \frac{AC}{A'C'}$
4. $\widehat{A} = \widehat{A'}$ et $\frac{AB}{A'B'} = \frac{AC}{A'C'}$

Remarque 1.4. Dans la dernière propriété, les quotients concernent les deux côtés de l'angle $\widehat{A}$, et pas n'importe quels côtés.



Proposition 1.5. Les triangles ABC et AED ci-dessus sont semblables.

Droites parallèles



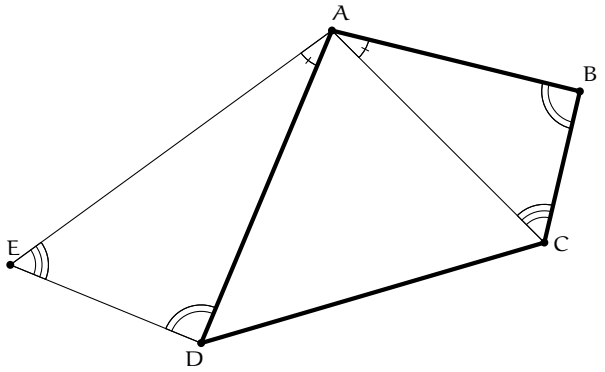
Lorsque deux droites sont parallèles, les angles alternes-internes et les angles correspondants sont égaux. Pour trouver des droites parallèles, n'oubliez pas que vous pouvez utiliser le théorème de Thalès.

- La géométrie du cercle -

Théorème de Ptolémée

Théorème 1.6. Soit $ABCD$ un quadrilatère. Alors $AC \cdot BD \leqslant AB \cdot BD + AD \cdot BC$, avec égalité ssi A, B, C, D cocycliques dans cet ordre.

Démonstration On commence la démonstration par construire le point E tel que le triangle ADE soit semblable au triangle ABC.



Les triangles ABC et ADE sont semblables, donc

$$\frac{AC}{AE} = \frac{AB}{AD} = \frac{BC}{DE}.$$

En prenant la seconde égalité on peut exprimer

$$DE = \frac{AD \cdot BC}{AB}.$$

Intéressons-nous maintenant aux triangles ABD et ACE. On se rend compte facilement que $\widehat{BAD} = \widehat{CAE}$, et en regardant la première égalité au-dessus on voit que $\frac{AB}{AC} = \frac{AD}{AE}$, donc les deux triangles sont semblables.

$$\frac{AB}{AC} = \frac{BD}{CE} \implies CE = \frac{AC \cdot BD}{AB}.$$

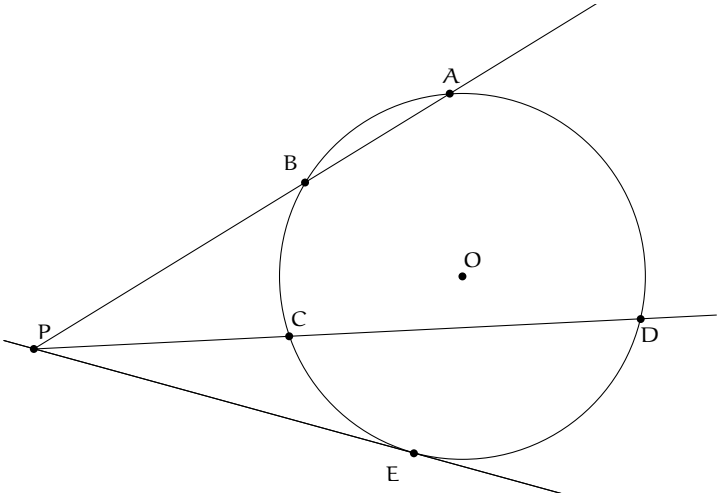
Ensuite on utilise simplement l'inégalité triangulaire :

$$CE \leqslant CD + DE \implies AC \cdot BD \leqslant AB \cdot BD + AD \cdot BC.$$

Ensuite regardons le cas d'égalité. L'inégalité triangulaire est une égalité ssi les points C, D, E sont alignés, ie ssi

$$\widehat{CDA} = 180° - \widehat{ADE} = 180° - \widehat{ABC} \iff A, B, C, D \text{ cocycliques.}$$

Puissance d'un point par rapport à un cercle Considérons un cercle Γ et un point P quelconque comme dans la figure suivante :

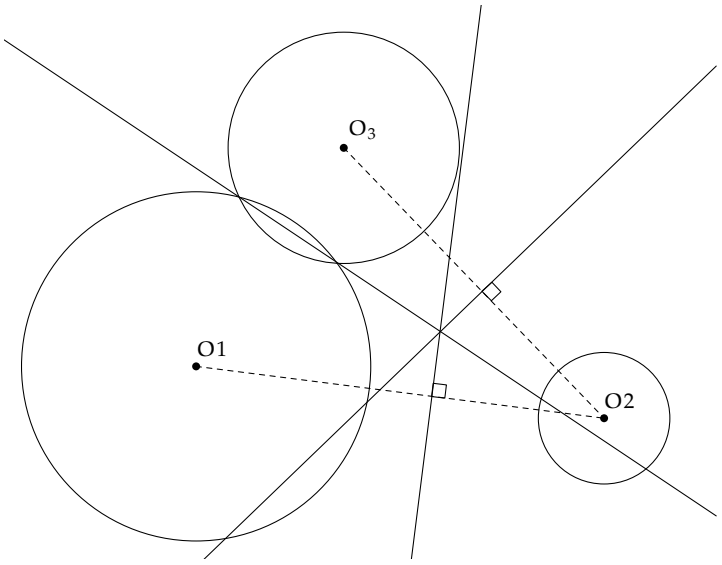


Proposition 1.7. $PA \cdot PB = PC \cdot PD = PE^2 = PO^2 - r^2$.

Démonstration Rappelez-vous que les triangles PAD et PCB sont semblables, donc $\frac{PA}{PC} = \frac{PD}{PB}$, ou encore $PA \cdot PB = PC \cdot PD$. Cette quantité ne dépend pas de quelle droite passant par P on utilise, si on utilise la tangente on trouve PE^2, si on utilise la droite passant par O on trouve $(PO - r)(PO + r) = PO^2 - r^2$.

Cette quantité est appelée la puissance du point P par rapport au cercle Γ, on la note $\mathcal{P}_\Gamma(P)$. Lorsqu'on calcule la puissance d'un point on considère des longueurs algébriques : $PA \cdot PB$ est positif si PA et PB sont dans le même sens (si P est à l'extérieur du cercle) et négatif s'ils sont dans des sens opposés (si P à l'intérieur).

Axe radical de deux cercles Il est intéressant de savoir, si on se donne deux cercles Γ_1 et Γ_2, quel est le lieu des point qui ont la même puissance par rapport à Γ_1 et à Γ_2. Je laisse au lecteur le soin de vérifié que ces points forment une droite Δ perpendiculaire à O_1O_2 appelée l'*axe radical* de Γ_1 et Γ_2.



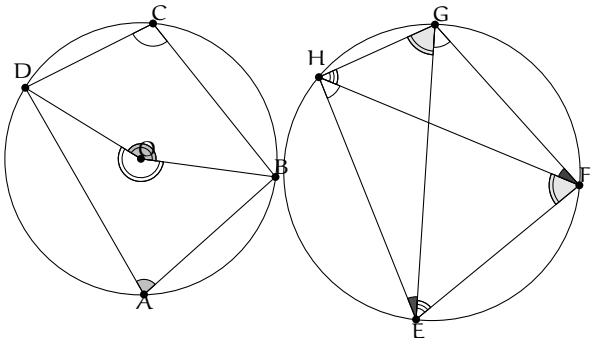
Proposition 1.8. Soient Γ_1, Γ_2 et Γ_3 trois cercles. Les axes radicaux Δ_{12}, Δ_{13} et Δ_{23} sont concourants.

Démonstration : Soit P le point d'intersection de Δ_{12} et Δ_{13}. Par définition, $\mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_2}(P)$ et $\mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_3}(P)$, donc $\mathcal{P}_{\Gamma_2}(P) = \mathcal{P}_{\Gamma_3}(P)$.

Exercice 5 Soient Γ_1 et Γ_2 deux cercles qui se coupent en A et B. On trace une tangente commune qui rencontre les cercles en C et D. Montrer que (AB) coupe $[CD]$ en son milieu.

- Solutions des exercices -

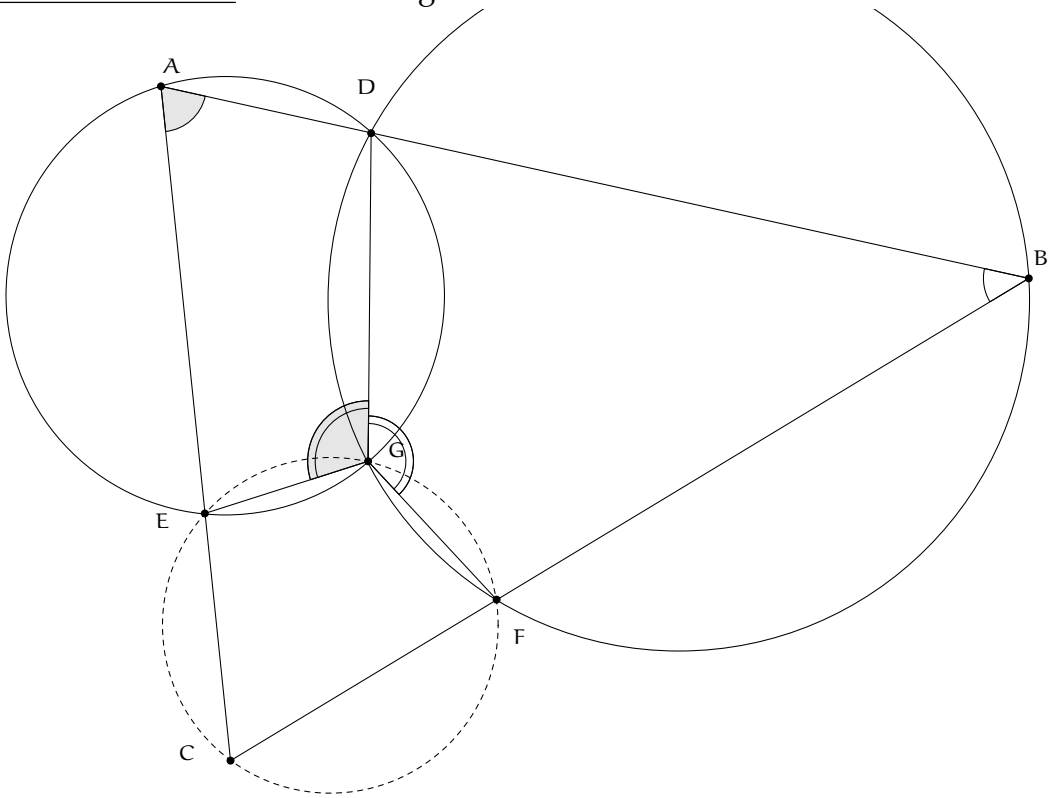
Solution de l'exercice 1 Nous allons exposer deux façons de résoudre ce problème.



Sur la figure de gauche, on voit que $\widehat{BOD} = 2\widehat{A}$ et $\widehat{DOB} = 2\widehat{C}$. Donc $\widehat{A} + \widehat{C} = \frac{\widehat{BOD}+\widehat{DOB}}{2} = 180°$.

Sur la figure de gauche, on peut trouver quatre couples d'angles inscrits. Donc $\widehat{F} + \widehat{H} = \widehat{GHF} + \widehat{HFG} + \widehat{FGE} + \widehat{EGH} = 180°$ puisque ce sont tous les angles du triangle FGH.

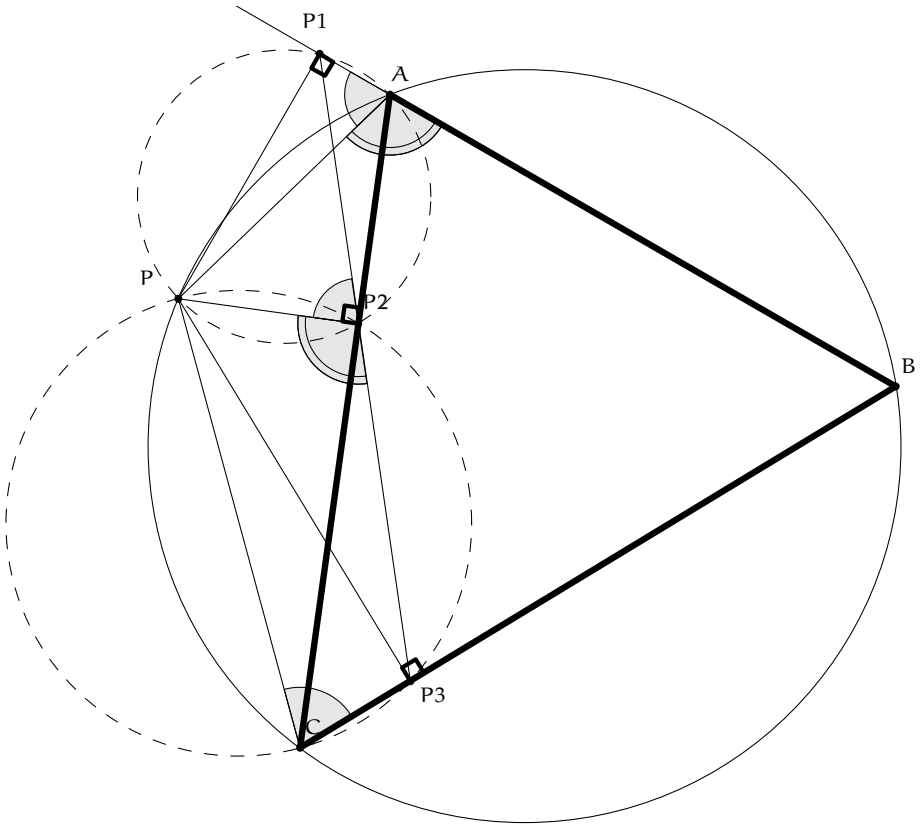
Solution de l'exercice 2 Faisons la figure :



Définissons G l'intersection des cercles circonscrits à ADE et à BDF, et nous montrerons que G est sur le cercle circonscrit de CEF. PSoient α, β et gamma les trois angles de ABC. Comme A, D, G, E cocycliques, $\widehat{DGE} = 180° - \alpha$. De même, $\widehat{EGF} = 180° - \beta$. Donc $\widehat{FGD} = 360°-(180°-\alpha)-180°-\beta)$ et donc $\widehat{FGD}+\gamma = 180\circ$. Les points C, D, G, F sont donc cocycliques.

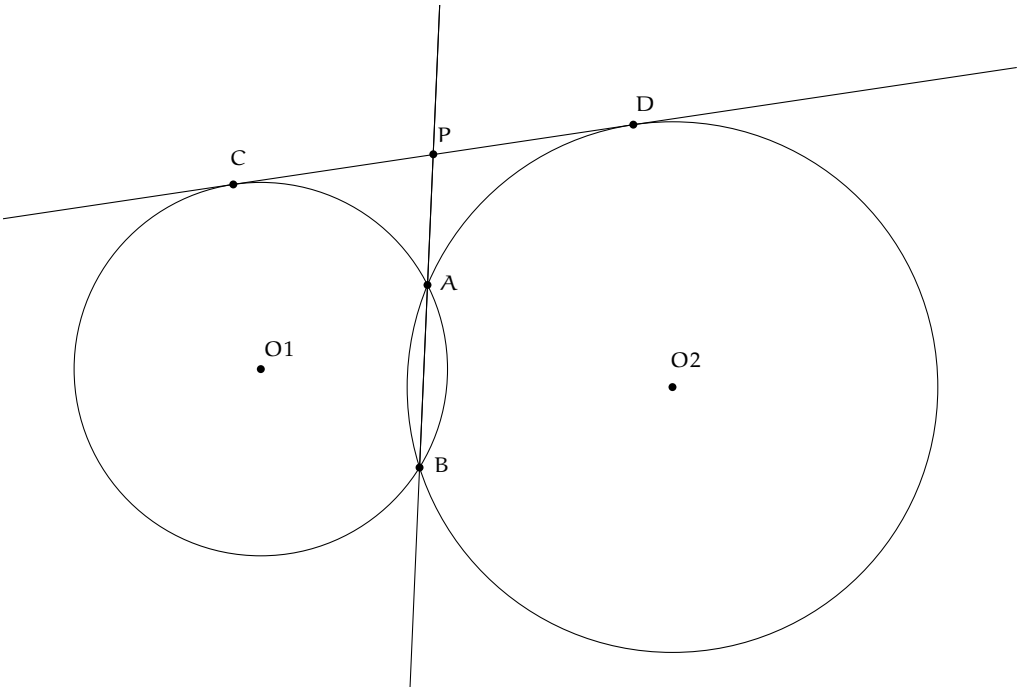
Solution de l'exercice 3 Définissons G l'intersection des cercles circonscrits à ADE et à BDF, et nous montrerons que G est sur le cercle circonscrit de CEF. PSoient α, β et γ les trois angles de ABC. Comme A, D, G, E cocycliques, $\widehat{DGE} = 180° - \alpha$. De même, $\widehat{EGF} = 180° - \beta$. Donc $\widehat{FGD} = 360° - (180° - \alpha) - 180° - \beta)$ et donc $\widehat{FGD} + \gamma = 180\circ$. Les points C, D, G, F sont donc cocycliques.

Solution de l'exercice 4 Commençons par faire la figure :



Comme il y a des angles droits en P_2 et P_1, le quadrilatère PP_1AP_2 est inscrit dans un cercle, donc $\widehat{P_1AP} = \widehat{P_1P_2P} = 180° - \widehat{PAB}$. Comme P est sur le cercle circonscrit de ABC, $\widehat{PCB} = 180° - \widehat{PAB} = \widehat{P_1P_2P}$. Enfin, comme P, P_2, P_3, C sont cocycliques, on a $\widehat{PP_2P_3} = 180° - \widehat{PCP_3} = 180° - \widehat{P_1P_2P}$. Donc $\widehat{P_1P_2P_3} = \widehat{P_1P_2P} + \widehat{PP_2P_3} = 180°$, les trois points sont alignés.

Solution de l'exercice 5 Voyons ce que donne la figure.



Comme A est sur l'intersection des deux cercles, il a une puissance nulle par rapport aux deux cercles, il est donc sur l'axe radical. De même pour B, donc AB est l'axe radical des deux cercles. Soit P le point d'intersection de (AB) avec $[CD]$.

$$PC^2 = \mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_1}(P) = PD^2.$$

2 TD de géométrie

- Énoncés-

Exercice 1 Soient Γ_1 et Γ_2 deux cercles s'intersectant en P et Q. On trace le segment $[PQ]$. On considère une droite d qui le coupe en un point intérieur au segment. On note A, B, C, D dans cet ordre ses 4 points d'intersection de d avec Γ_1 (pour A et C) et Γ_2 (pour B et D).

Prouver que $\widehat{APB} = \widehat{CQD}$.

Exercice 2 Soit Γ un cercle, BC une corde de Γ. Soit A le milieu de l'arc BC. Par A on mène deux cordes quelconques AD et AE qui coupent le segment $[BC]$ en F et G respectivement.

Montrer que le quadrilatère DFGE est inscriptible dans un cercle.

Exercice 3 Soient A, B, C et D quatre points cocycliques. On suppose que les droites (AB) et (CD) se coupent en E. Montrer que :

$$\frac{AC}{BC} \cdot \frac{AD}{BD} = \frac{AE}{BE}.$$

Exercice 4 Soit ABC un triangle rectangle en C. Sur la droite (AC) on place un point D tel que $CD = BC$, C étant situé entre A et D. La perpendiculaire à (AB) passant par D recoupe (BC) en E. Montrer que $AC = CE$.

Exercice 5 Le quadrilatère $ABCD$ est inscriptible dans un cercle de centre O. Les diagonales AC et BD sont perpendiculaires. Montrer que la distance de O à la droite (AD) est égale à la moitié de la longueur du segment $[BC]$.

Exercice 6 Soit ABC un triangle. Montrer que l'intersection de la bissectrice issue de $\widehat{B}$ et de la médiatrice de $[AC]$ appartient au cercle circonscrit de ABC.

Exercice 7 Soit ABC un triangle aux angles aigus d'orthocentre H. Montrer que les symétriques de H par rapport aux côtés du triangle appartiennent à son cercle circonscrit.

Exercice 8 On considère deux cercles tangents intérieurement en un point C et une corde $[AB]$ du grand cercle tangente au petit cercle en E. Montrer que la droite (CE) est la bissectrice de l'angle $\widehat{ACB}$.

Exercice 9 (Olympiades Balkaniques de Mathématiques 2012, exercice 1) Soient A, B, C trois points d'un cercle Γ de centre O. On suppose que $\widehat{ABC} > 90°$. Soit D l'intersection de la droite (AB) avec la perpendiculaire à (AC) passant par C. Soit l la droite passant par D perpendiculaire à (AO). Soit E l'intersection de la droite l avec (AC), et soit F l'intersection de Γ et de de l qui se situe entre D et E.

Prouver que les cercles circonscrits des triangles BFE et CFD sont tangents en F.

Exercice 10 Soient Γ_1, Γ_2 deux cercles qui se coupent en A et en B. Soit Δ une droite tangente aux deux cercles en M et en N. Montrer que (AB) coupe le segment $[MN]$ en son milieu.

Exercice 11 Soient $ABCD$ et $CDEF$ deux quadrilatères inscrits dans deux cercles Γ_1, Γ_2. On suppose que parmi les droites (AB), (CD) et (EF) il n'y en a pas deux qui soient parallèles. Alors les droites (AB), (CD) et (EF) sont concourantes si, et seulement si, les points A, B, E et F sont cocycliques.

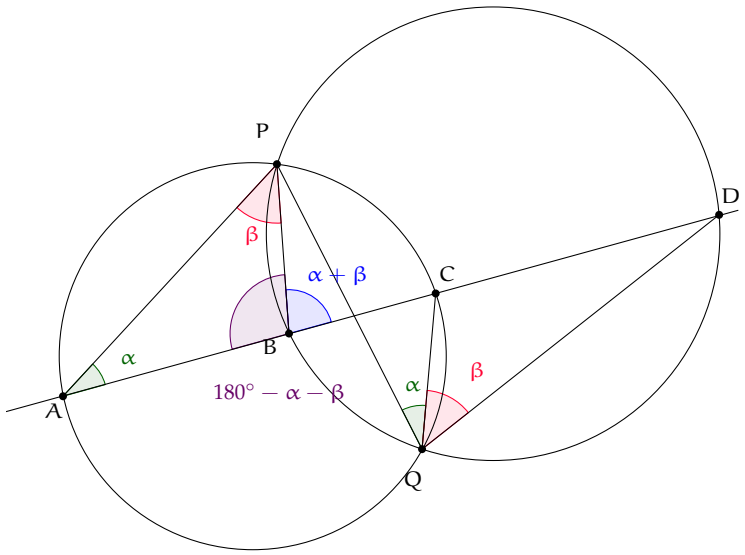
Exercice 12 Soit ABC un triangle, H son orthocentre. Soient M un point de $[AB]$ et N un point de $[AC]$. Les cercles de diamètre BN et CM se coupent en P et Q. Montrer que P, Q et H sont alignés.

Exercice 13 (Olympiades internationales de Mathématiques 2000, Exercice 1) Soient Ω_1 et Ω_2 deux cercles qui se coupent en M et en N. Soit Δ la tangente commune aux deux cercles, qui est plus proche de M que de N. Δ est tangente à Ω_1 en A et à Ω_2 en B. La droite passant par M et parallèle à Δ rencontre Ω_1 en C et Ω_2 en D. Soient E l'intersection des droites (CA) et (BD), P le point d'intersection de droites (AN) et (CD) et Q le point d'intersection des droites (BN) et (CD). Montrer que $EP = EQ$.

Exercice 14 Soit ABC un triangle acutangle. On note respectivement D, E, F les pieds des hauteurs sur les côtés $[BC]$, $[CA]$, $[AB]$. Soit P un point d'intersection de (EF) avec le cercle circonscrit à ABC. Soit Q le point d'intersection des droites (BP) et (DF). Montrer que $AP = AQ$.

- Solutions des exercices-

Solution de l'exercice 1 On commence par tracer une figure :

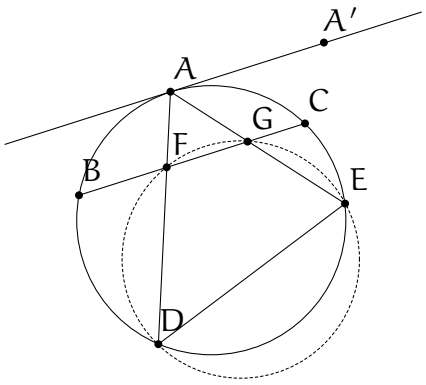


La présence de nombreux points cocycliques nous invite à chasser les angles : posons $\alpha = \widehat{PQC}$ et $\beta = \widehat{CQD}$. Les points P, B, Q, D sont cocycliques. Les angles $\widehat{PBD}$ et $\widehat{PQD}$ interceptent le même arc et sont donc égaux. Ainsi, $PBD = \alpha + \beta$, et donc $\widehat{ABP} = 180° - \alpha - \beta$.

D'autre part, les points P, A, Q, C sont cocycliques. Les angles $\widehat{PAC}$ et $\widehat{PQC}$ interceptent le même arc et sont donc égaux. Ainsi, $\widehat{PAB} = \alpha$.

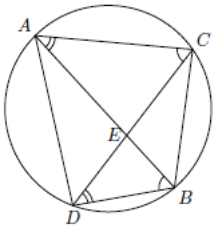
Nous avons de cette manière réussi à trouver deux des trois angles du triangle ABP. L'angle $\widehat{APB}$ vaut donc $180° - (\alpha + 180° - \alpha - \beta) = \beta$. On a bien $\widehat{CQD} = \widehat{APB}$, ce qu'il fallait démontrer.

Solution de l'exercice 2 Considérons la tangente a au cercle en A, et un point A' de a du même



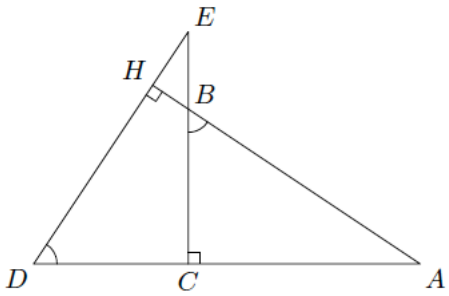
côté de (OA) que C. On a alors $\widehat{EDA} = \widehat{EAA'} = \widehat{EGC}$, la première égalité étant le cas tangent du théorème de l'angle inscrit, et la deuxième provenant du fait que a est parallèle à (BC). Donc $\widehat{EDF} = \widehat{EGC} = 180° - \widehat{EGF}$, ce qui prouve que EGFD est inscriptible.

Solution de l'exercice 3



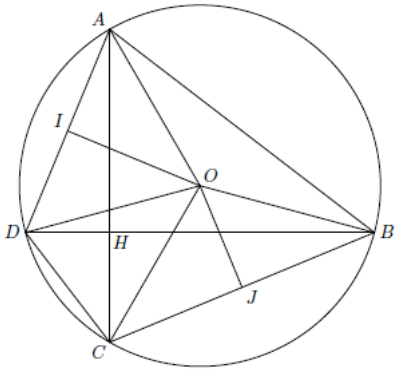
Les triangles EAC et EDB ont les mêmes angles donc sont semblables, d'où $\frac{AC}{BD} = \frac{EA}{ED}$. Le même raisonnement montre que les triangles EAD et ECB sont semblables, donc $\frac{AD}{BC} = \frac{ED}{EB}$. En faisant le produit, ED se simplifie, et il reste la relation cherchée.

Solution de l'exercice 4



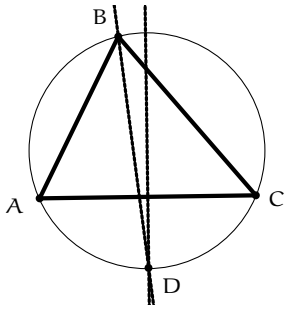
On a $\widehat{CBA} = \widehat{CDE}$, puisque (CB) est perpendiculaire à (CD) et (BA) à (DE). Il en résulte que les triangles CBA et CDE ont leurs angles égaux, ils sont semblables, et même égaux car CB = CD par hypothèse. Cela entraîne CA = CE.

Solution de l'exercice 5

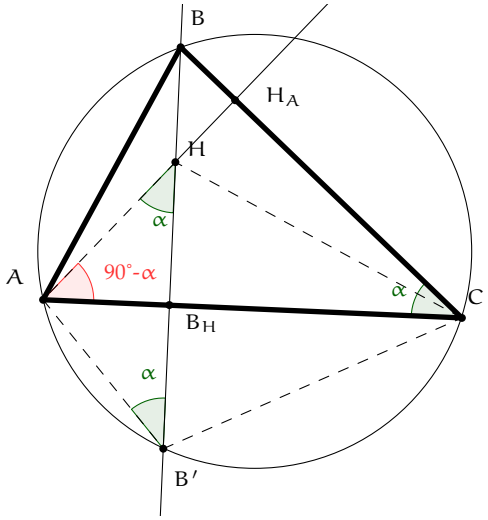


Par la propriété des angles inscrits, on a $\widehat{AOD} = 2\widehat{ABD}$ et donc $\widehat{IOA} = \widehat{ABD}$. De même $\widehat{COJ} = \widehat{CAB} = \frac{\pi}{2} - \widehat{ABD}$. On en déduit $\widehat{IOA} = \frac{\pi}{2} - \widehat{OJC} = \widehat{OCJ}$ puis que les triangles IOA et JCO sont semblables. Comme on a en outre OA = OC, ils sont isométriques et CJ = IO, ce qui permet de conclure.

Solution de l'exercice 6 Notons D l'intersection de la bissectrice issue de l'angle $\widehat{B}$ et du cercle circonscrit de ABC. Il faut et il suffit de montrer que D appartient à la médiatrice de [AC]. Comme les angles $\widehat{ABD}$ et $\widehat{DBC}$ sont égaux, ceci implique que les longueurs des arcs (AD) et (DC) sont égales, et donc que D appartient à la médiatrice de [AC].



Solution de l'exercice 7 Notons B_H le pied de la hauteur issue de B, B' son intersection avec le cercle circonscrit à ABC et A_H le pied de la hauteur issue de A (voir figure).



Il suffit de montrer que les angles $\widehat{AB'B_H}$ et $\widehat{AHB_H}$ sont égaux. En effet, dans ce cas, les triangles rectangles HAB_H et B_HAB' auraient trois angles identiques et un angle en commun et seraient alors égaux. Ceci implique $B'B_H = B_HH$ et donc que B' est le symétrique de H par rapport au côté (AC).

Montrons donc que $\widehat{AB'B_H} = \widehat{AHB_H}$. Notons $\alpha = \widehat{AB'B_H}$. Comme les angles $\widehat{AB'B_H}$ et $\widehat{ACB}$ interceptent le même arc, ils sont égaux. On en déduit que $\widehat{ACB} = \alpha$, puis $\widehat{H_AAC} = 90° - \alpha$ car AH_AC est rectangle en H_A. Mais alors, puisque AHB_H est rectangle en B_H, $\widehat{AHB_H} = 90° - \widehat{HAB_H} = \alpha$, ce qu'on voulait montrer.

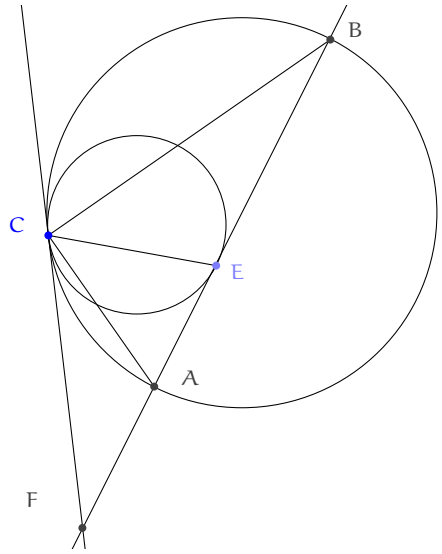
On démontre de même que les symétriques de H par rapport aux autres côtés appartiennent au cercle circonscrit.

Solution de l'exercice 8

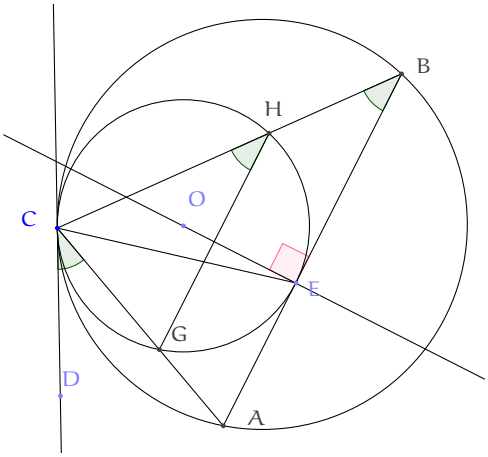
- (Première solution) Soit F le point d'intersection de la corde (AB) avec la tangente commune. Les triangles FAC et FCB sont semblables et $FC = FE$. Par suite :

$$\frac{CA}{CB} = \frac{FE}{FB} = \frac{FA}{FE} = \frac{FE - FA}{FB - FE} = \frac{AE}{EB},$$

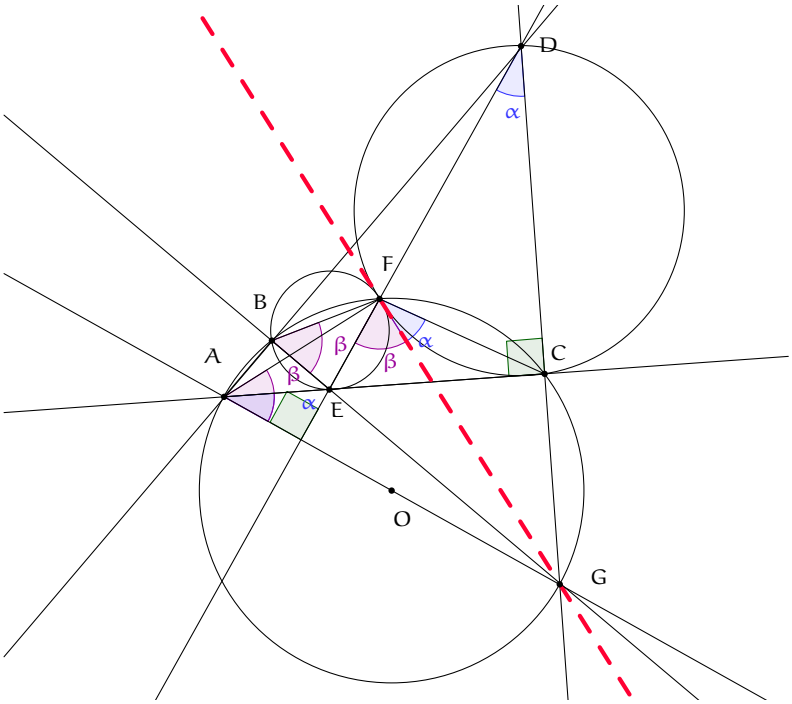
et la droite (CE) est la bissectrice de l'angle $\widehat{ACB}$.



- (Deuxième solution) Notons O le centre du petit cercle et soient G, H les points d'intersection de respectivement (CB) et (CA) avec le petit cercle. On introduit le point D comme sur la figure. On commence par faire une petite chasse aux angles pour montrer que (AB) et (GH) sont parallèles. On a $\widehat{ABC} = \widehat{ACD} = \widehat{GHC}$. Donc (AB) et (GH) sont parallèles. Or (OE) et (AB) sont perpendiculaires. Donc (OE) et (GH) sont perpendiculaires. Donc (OE) est la médiatrice de [GH]. Donc, d'après le premier exercice, (CE) est la bissectrice de $\widehat{ACB}$.



Solution de l'exercice 9 On commence par faire une figure soignée :



Cette figure suggère que les les droites (AO), (BE), la tangente commune cherchée et (DC) vont être concourantes. Notons ainsi G le point diamétralement opposé à A sur Γ.

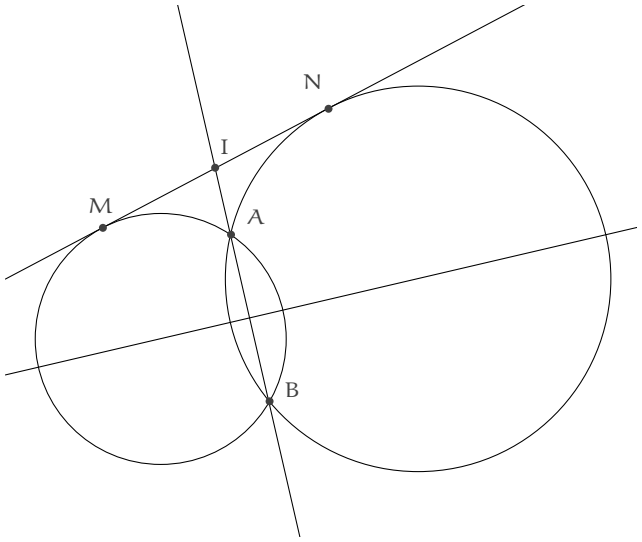
Première étape : (DC) passe par G. En effet, $[AG]$ étant un diamètre de Γ, ACG est rectangle en C, ce qui implique que les droites (DC) et (CG) sont les mêmes.

Deuxième étape : prouvons que (BE) passe par G. Pour cela, on remarque que E est l'orthocentre de ADG car E est l'intersection des deux hauteurs (AC) et (DE). Or ABG est rectangle en B, car $[AG]$ est un diamètre de Γ, ce qui implique que (BG) et (AD) sont perpendiculaires. Donc (BG) est la hauteur issue de G dans ADG, et donc l'orthocentre E appartient à (BG).

Troisième étape : posons $\alpha = \widehat{EDG}$. Pour montrer que (FG) est tangente au cercle circonscrit de FDC, montrons que $\widehat{GFC} = \alpha$. On a $\widehat{DEC} = 90° - \alpha$. Les droites (DE) et (AG) étant perpendiculaires, on en déduit que $\widehat{EAG} = \alpha$. Finalement, par cocyclicité de A,F,C,G, on en déduit que $\widehat{GFC} = \alpha$.

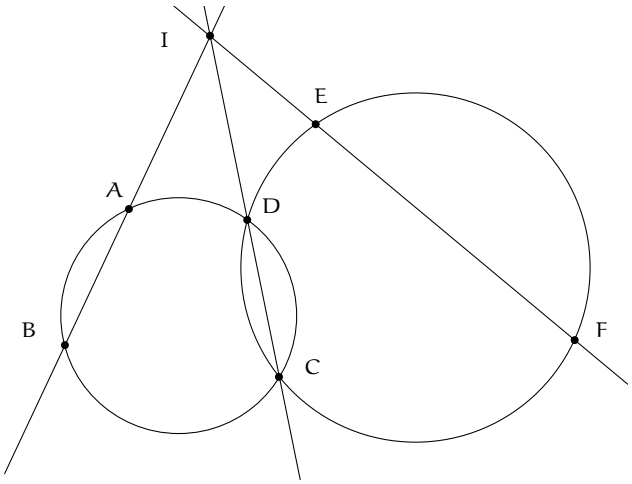
Posons $\beta = \widehat{EBF}$. Pour montrer que (FG) est tangente au cercle circonscrit de BEF, montrons que $\widehat{EFG} = \beta$. Par cocyclicité de A, B, F, G, on a $\widehat{FAG} = \beta$. Puis, en utilisant deux triangles rectangles, il vient $\widehat{AFE} = 90 - \beta$, puis $\widehat{EFG} = \beta$, ce qui conclut l'exercice.

Solution de l'exercice 10



La puissance de I par rapport au premier cercle vaut $IM^2 = IA \cdot IB$. La puissance de I par rapport au deuxième cercle vaut $IA \cdot IB = IN^2$. On en déduit que $IM^2 = IN^2$, d'où $IM = IN$.

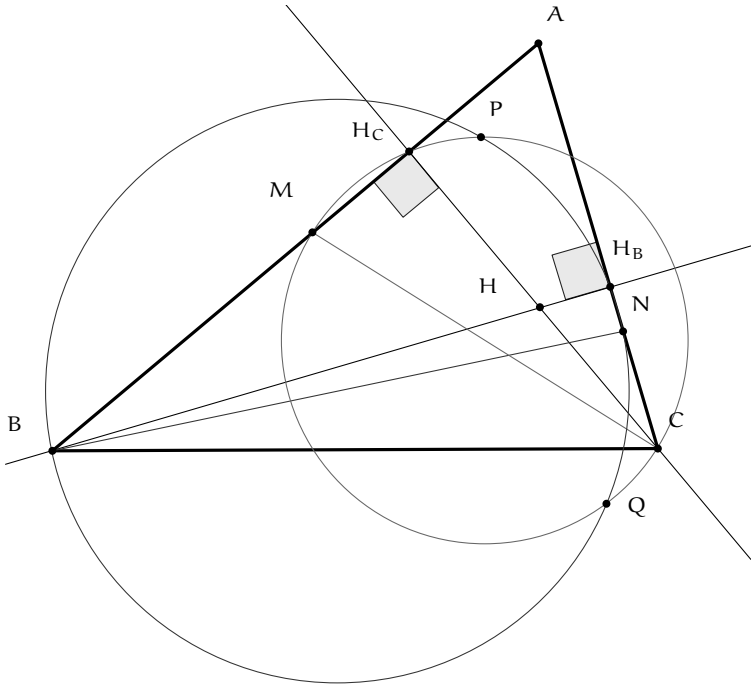
Solution de l'exercice 11



Supposons d'abord que les trois droites soient concourantes. Alors la puissance de I par rapport au cercle de gauche vaut $IA \cdot IB = ID \cdot IC$. La puissance de I par rapport au cercle de droite vaut $ID \cdot IC = IE \cdot IF$. On en déduit que $IA \cdot IB = IE \cdot IF$, et donc que A, B, F, E sont cocycliques.

Réciproquement, si A, B, F, E sont cocycliques, notons I le point d'intersection des droites (AB) et (EF). La puissance de I par rapport au cercle circonscrit à $ABFE$ vaut $IA \cdot IB = IE \cdot IF$. Donc I a même puissance par rapport aux deux cercles de la figure. I est donc sur leur axe radical, qui est (DC). Les trois droites (AB), (CD) et (EF) sont donc concourantes en I.

Solution de l'exercice 12

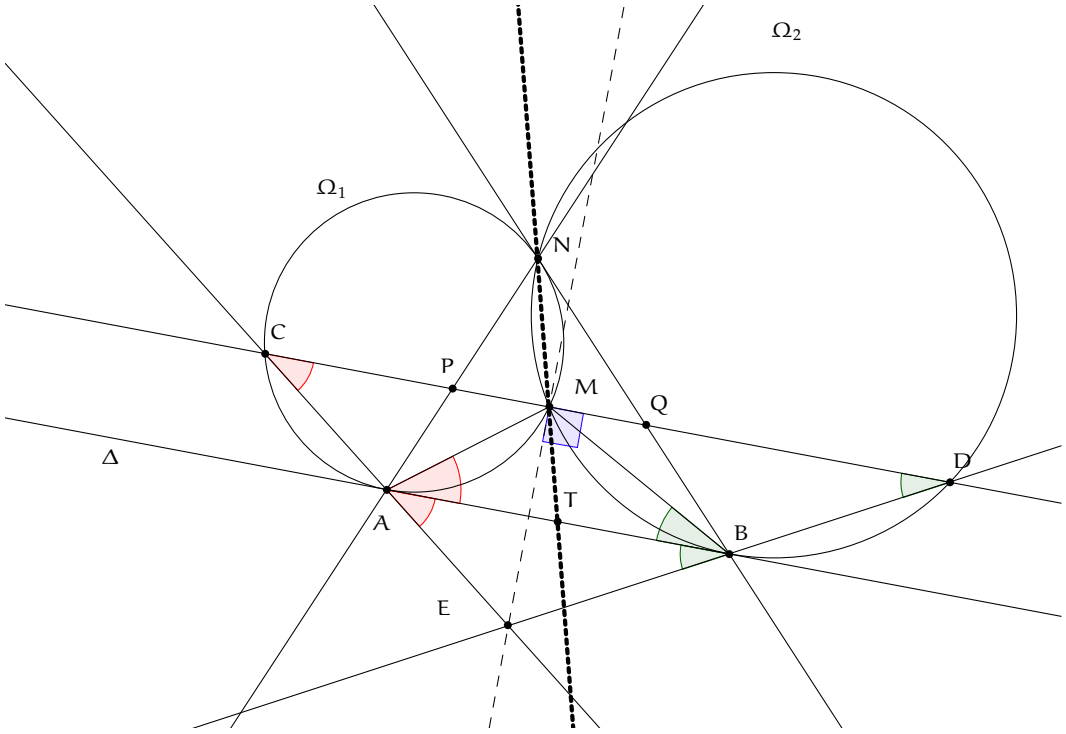


Nous allons montrer que H a la même puissance par rapport aux deux cercles de la figure, ce qui impliquera que H est sur leur axe radical, qui est (PQ).

Pour cela, comme $(BH_B) \perp (AC)$, H_B est sur le cercle de diamètre $[BN]$. La puissance de H par rapport au cercle de diamètre $[BN]$ vaut donc $-HB \cdot HH_B$. De même, la puissance de H par rapport au cercle de diamètre $[CM]$ vaut $-HC \cdot HH_C$.

Or les points B, H_C, H_B, C sont cocycliques : ces points sont situés sur le cercle de diamètre $[BC]$. On en déduit que $-HB \cdot HH_B = -HH_C \cdot HC$, ce qui conclut.

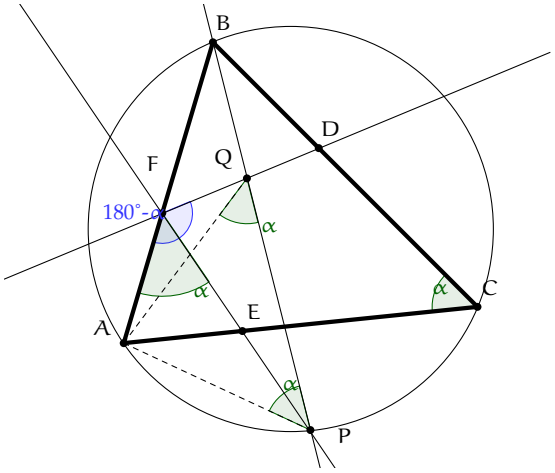
Solution de l'exercice 13



Il suffit d'être logique, qualité qui permet de résoudre nombre d'exercices de géométrie : une chasse aux angles s'impose, et montre que $\widehat{ABE} = \widehat{CDE} = \widehat{MBA}$, la dernière égalité étant d'une importance capitale. De même, $\widehat{BAE} = \widehat{MAB}$. Ces égalités impliquent que M et E sont images l'un de l'autre par la symétrie par rapport à la droite (AB). Les droites (ME) et (AB) sont orthogonales, puis les droites (ME) et (PQ) sont orthogonales.

Il faut également savoir reconnaître les situations classiques : ici, en notant T l'intersection des droites (MN) et (AB), il faut savoir que $TA = TB$ (voir exercice 5). Le théorème de Thalès montre alors que M est le milieu de $[PQ]$. En somme, (ME) est la médiatrice de $[PQ]$. E est donc bien équidistant de P et de Q.

Solution de l'exercice 14



Posons $\alpha = \widehat{APB}$. Par cocyclicité des points A, B, C, P, on a $\widehat{BCA} = \alpha$. Comme (AD) et (CF) sont des hauteurs, les points A, C, D, F sont cocycliques et donc $\widehat{AFD} = 180° - \alpha$. Donc $\widehat{AFD} + \widehat{APQ} = 180°$, ce qui implique que les points A, P, Q, F sont cocycliques.

On continue la chasse aux angles : $\widehat{AFE} = \widehat{BFD} = \widehat{BCA} = \alpha$ (pourquoi ?), et donc $\widehat{AQP} = \widehat{AFP} = \widehat{BCA}$. Le triangle APQ est donc isocèle, ce qui implique $AP = AQ$.

3 Cours/TD de géométrie : transformations

- Mémo -

Vecteurs

Définition 1.9. Un vecteur est un objet géométrique caractérisé par une direction, un sens et une longueur.

Proposition 1.10. $\overrightarrow{AB} = \overrightarrow{CD}$ si et seulement si ABDC est un parallélogramme.
$\overrightarrow{CD}$ peut s'écrire sous la forme $k\overrightarrow{AB}$ si et seulement si (AB) et (CD) sont parallèles. On dit alors que $\overrightarrow{AB}$ et $\overrightarrow{CD}$ sont colinéaires.

Proposition 1.11. (Relation de Chasles)

$$\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$$

Remarque 1.12. Cette relation s'utilise quand on cherche à avoir des informations sur un vecteur sans connaître les liens entre ses deux extrémités, mais que ces deux points "connaissent" un même point. Les exercices 1 et 2 en fournissent de bons exemples...

Proposition 1.13. M est le milieu de AB si et seulement si $\overrightarrow{AM} = \frac{1}{2}\overrightarrow{AB}$ ou, ce qui est équivalent, $\overrightarrow{CM} = \frac{1}{2}(\overrightarrow{CA} + \overrightarrow{CB})$ pour un point C quelconque.

Homothéties

Définition 1.14. Soient O un point du plan et k un réel non nul. L'homothétie de centre O et de rapport k est la transformation qui à un point M associe le point M′ tel que $\overrightarrow{OM'} = \overrightarrow{OM}$.

Proposition 1.15. Les homothéties conservent les angles, les droites, les cercles, les rapports de longueurs, etc. De plus, l'image d'une droite (Δ) par une homothétie est parallèle à Δ.

Proposition 1.16. La composée de deux homothéties h_1 et h_2 de rapports k_1 et k_2 est une translation si $k_1k_2 = 1$, et une homothétie de rapport k_1k_2 sinon. Dans ce cas, le centre de $h_1 \circ h_2$ est aligné avec ceux de h_1 et de h_2.

Proposition 1.17.

- Soient [AB] et [A′B′] deux segments supportés par des droites parallèles. Il existe une unique homothétie envoyant A sur A′ et B sur B′.
- Soient Γ_1 et Γ_2 deux cercles de rayons différents. Il existe exactement deux homothéties, une de rapport positif et une de rapport négatif, envoyant Γ_1 sur Γ_2.
  S'ils ont le même rayon, il existe exactement une homothétie et une translation envoyant l'un sur l'autre.
  De plus, si les cercles admettent des tangentes communes extérieures (resp. intérieures), alors leur intersection est le centre de l'homothétie positive (resp. négative) envoyant l'un sur l'autre.

Rotations

Définition 1.18. Soient O un point du plan et θ un angle. La rotation de centre O et d'angle θ est la transformation qui à un point M associe le point M′ tel que OM′ = OM et $\widehat{MOM'} = \theta$, les angles étant orientés.

Proposition 1.19. Les rotations conservent les longueurs, les angles, les droites, les cercles etc... De plus, si (Δ') est l'image d'une droite Δ par un rotation d'angle θ, alors l'angle entre les droites (Δ) et (Δ') vaut θ.

Proposition 1.20.

- La composée de deux rotations d'angles θ et θ' est une translation si $\theta+\theta'$ est un multiple de 2π, et une rotation sinon.
- Soient (Δ_1) et (Δ_2) deux droites se coupant en un point O et faisant entre elles un angle θ. On note s_1 et s_2 les symétries par rapport à (Δ_1) et (Δ_2). Alors $s_1 \circ s_2$ est la rotation de centre O et d'angle 2θ.

Proposition 1.21. Si $[AB]$ et $[A'B']$ sont deux segments non parallèles de même longueur, il existe une unique rotation envoyant A sur A' et B sur B'.

- Exercices -

Exercice 1 Redémontrer le théorème de la droite des milieux avec des vecteurs.

Solution de l'exercice 1 Soient ABC un triangle et M, N les milieux de $[AB]$ et $[AC]$. On a :

$$\overrightarrow{MN} = \overrightarrow{MA} + \overrightarrow{AN} = \frac{1}{2}(\overrightarrow{BA} + \overrightarrow{AC}) = \frac{1}{2}\overrightarrow{BC}$$

d'où le résultat.

Exercice 2 (Centre de gravité)
Montrer que les médianes d'un triangle sont concourantes en un point G vérifiant :

$$\overrightarrow{GA} + \overrightarrow{GB} + \overrightarrow{GC} = \overrightarrow{0}$$

Solution de l'exercice 2 Pour commencer, un point G vérifiant la condition vectorielle existe bien. Elle équivaut en effet, d'après la relation de Chasles, à :

$$3\overrightarrow{GA} + \overrightarrow{AB} + \overrightarrow{AC} = \overrightarrow{0}$$

soit $\overrightarrow{AG} = \frac{1}{3}(\overrightarrow{AB} + \overrightarrow{AC})$, et un unique point G vérifie cette propriété. Soit de plus M le milieu de BC. On a :

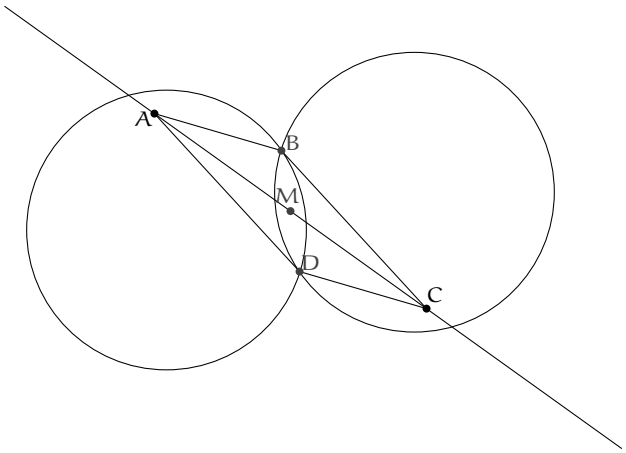
$$\overrightarrow{GM} = \frac{1}{2}(\overrightarrow{GB} + \overrightarrow{GC}) = -\frac{1}{2}\overrightarrow{GA}$$

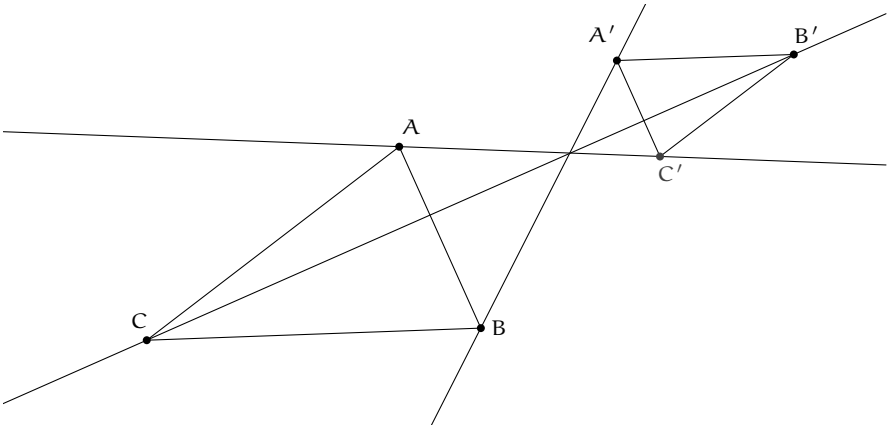
donc G, M et A sont alignés et G est sur la médiane issue de A, et de même pour les autres médianes.

Exercice 3 Etant donnés deux points A et C et un cercle Γ, construire deux points B et D sur Γ tels que ABCD soit un parallélogramme.

Solution de l'exercice 3 Soit M le milieu de $[AC]$: ABCD est un parallélogramme ssi M est le milieu de $[BD]$ ssi B est le symétrique de D par rapport à M. B doit donc être sur le symétrique Γ' de Γ par rapport à M, ce qui permet de le tracer. D est alors l'autre intersection des deux cercles.

Exercice 4 Soient ABC et $A'B'C'$ deux triangles tels que (AB) soit parallèle à $(A'B')$, (BC) à $(B'C')$ et (CA) à $(C'A')$.
Montrer que les droites (AA'), (BB') et (CC') sont parallèles ou concourantes.



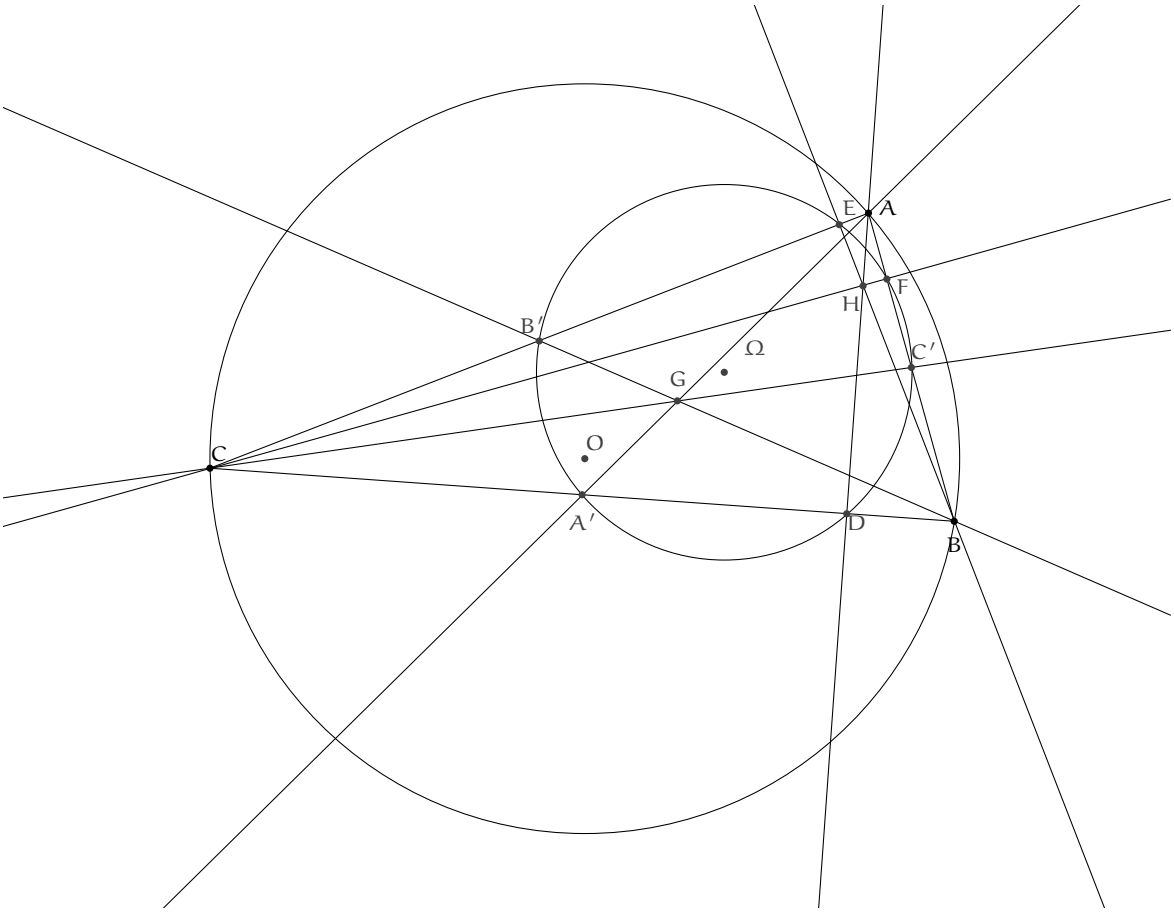


Solution de l'exercice 4 On note X le point d'intersection de (AA') et (BB') s'il existe. D'après le théorème de Thalès, on peut poser $k = \frac{XA'}{XA} = \frac{XB'}{XB}$. L'homothétie h de centre X et de rapport k envoie alors A sur A' et B sur B'. $h((AC))$ passe par A' et est parallèle à (AC) donc à $(A'C')$, d'où $h((AC)) = (A'C')$ et, de même $h((BC)) = (B'C')$. On a donc $h(C) = C'$, donc X, C et C' sont alignés, d'où le résultat. Si (AA') et (BB') sont parallèles, $ABB'A'$ est un parallélogramme donc il existe une translation t qui envoie A sur A' et B sur B' et, comme ci-dessus, on montre qu'elle envoie C sur C', donc (CC') est parallèle à (AA') et (BB').

Remarque 1.22. On a trouvé une condition nécessaire et suffisante sur deux triangles pour qu'il existe une homothétie envoyant l'un sur l'autre.

Exercice 5 (Droite et cercle d'Euler)
Soient ABC un triangle, O le centre de son cercle circonscrit, G son centre de gravité (i.e le point d'intersection de ses médianes) et H son orthocentre (i.e le point d'intersection de ses hauteurs). On note A', B' et C' les milieux de $[BC]$, $[CA]$ et $[AB]$ et D, E, F les pieds des hauteurs issues de A, B et C.

- Montrer que $A'B'C'$ est l'image de ABC par une homothétie bien choisie de centre G.
- En déduire que O, G et H son alignés.
- En utilisant la même homothétie, montrer que les points A', B', C', D, E et F sont cocycliques.



Solution de l'exercice 5

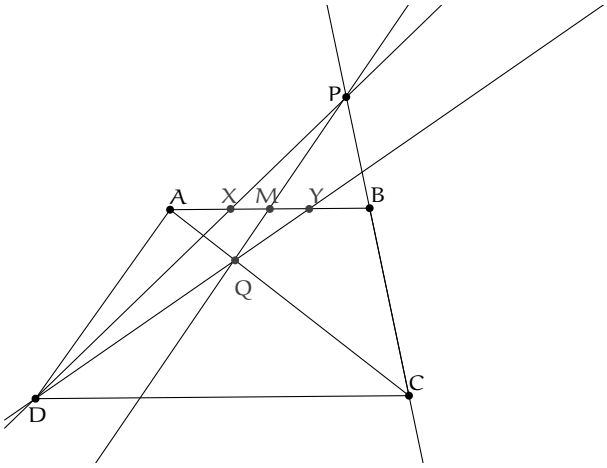
- C'est une conséquence directe de 2. En effet, on a montré $\overrightarrow{GA'} = \frac{1}{2}\overrightarrow{GA}$.
- Soit h l'homothétie de la première question : $h(ABC) = A'B'C'$, donc h envoie H sur l'orthocentre de $A'B'C'$. Or, O est l'orthocentre de $A'B'C'$. En effet, (OA') est perpendiculaire à (BC), donc à $(B'C')$ par le théorème de la droite des milieux, donc c'est la hauteur issue de A' dans $A'B'C'$.
  O, G et H sont donc alignés et, plus précisément, $\overrightarrow{GH} = -2\overrightarrow{GO}$.
- Soit Ω le centre du cercle circonscrit à $A'B'C'$: on sait que $\Omega = h(O)$ donc :

$$\overrightarrow{O\Omega} = \overrightarrow{OG} + \overrightarrow{G\Omega} = \frac{3}{2}\overrightarrow{OG} = \frac{1}{2}\overrightarrow{OH}$$

  Ω est donc le milieu de $[OH]$. Il est donc équidistant des droites AD et OA', donc $\Omega A' = \Omega D$, donc D est sur le cercle circonscrit à $A'B'C'$, et de même pour E et F.

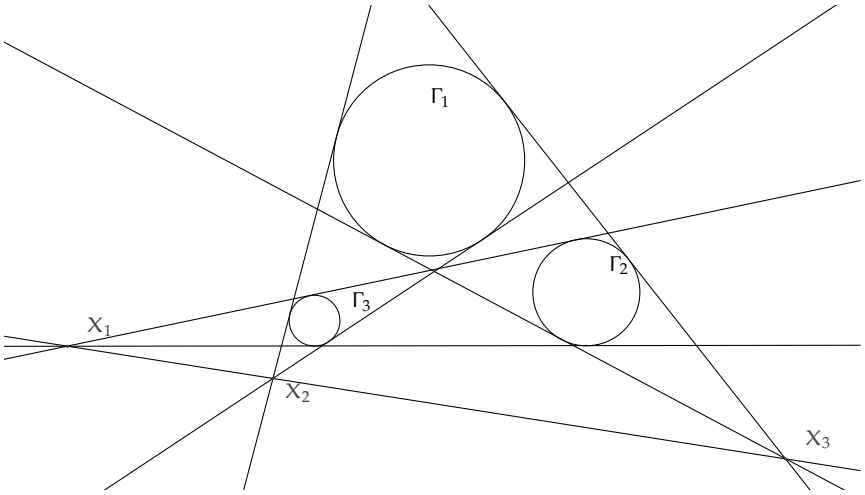
Exercice 6 Soient $ABCD$ un trapèze avec (AB) parallèle à (CD), M le milieu de $[AB]$ et P un point de (BC). On pose $X = (PD) \cap (AB)$, $Q = (PM) \cap (BD)$ et $Y = (PQ) \cap (AB)$. Montrer que M est le milieu de $[XY]$.

Solution de l'exercice 6 Les droites parallèles donnent envie de chercher des homothéties qui les envoient l'une sur l'autre. Deux sont intéressantes : celle de centre Q qui envoie A sur C et B sur D, qu'on note h_Q et celle de centre P qui envoie C sur B et D sur Y, qu'on note h_P.
$h_P \circ h_Q$ est alors une homothétie qui envoie A sur B et Y sur X. Son centre est sur (AB) et sur



(PQ) (car c'est le centre d'une composée d'homothéties de centres P et Q), donc c'est M et, comme M est le milieu de $[AB]$, $h_P \circ h_Q$ est la symétrie centrale de centre M, d'où le résultat.

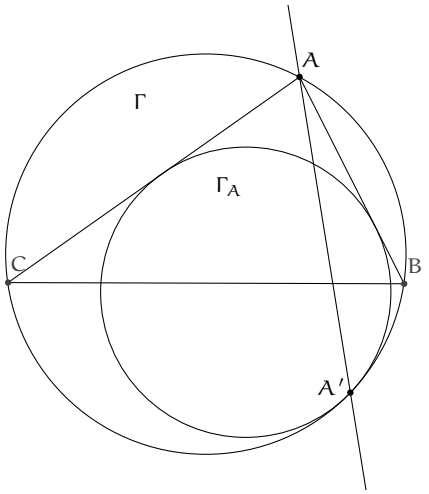
Exercice 7 (Théorème de Monge-d'Alembert)
Soient Γ_1, Γ_2 et Γ_3 trois cercles tels que les disques correspondants soient disjoints. Soient X_1 le point d'intersection des tangentes communes extérieures à Γ_2 et Γ_3. On définit de même X_2 et X_3.
Montrer que X_1, X_2 et X_3 sont alignés.



Solution de l'exercice 7 X_3 est le centre de l'homothétie positive h_1 qui envoie Γ_1 sur Γ_2, et X_1 celui de l'homothétie positive h_2 qui envoie Γ_2 sur Γ_3. $h_2 \circ h_1$ est une homothétie positive qui envoie Γ_1 sur Γ_3, donc son centre est X_2 et $X_2 \in (X_1X_3)$.

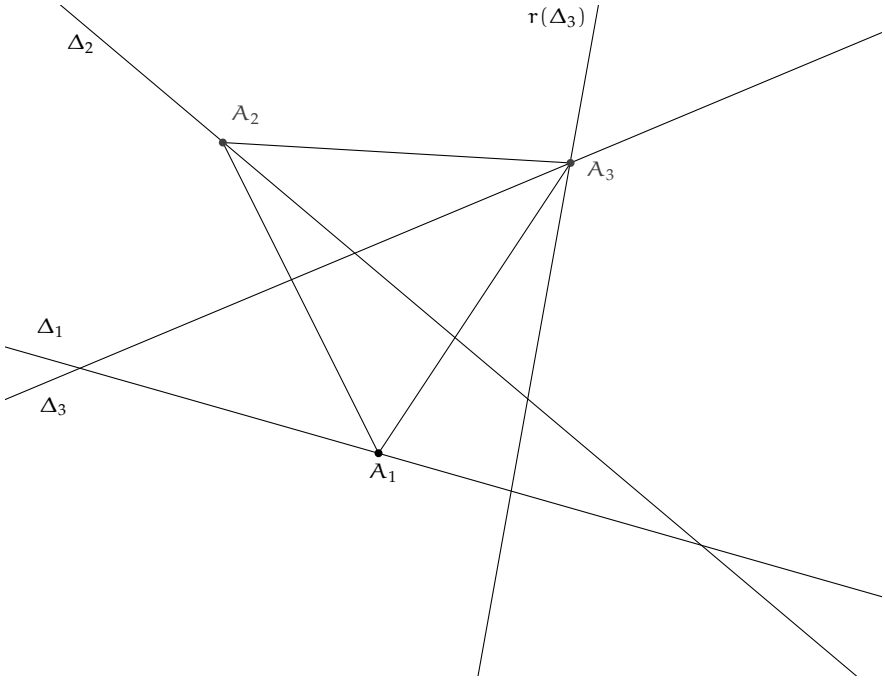
Exercice 8 Soient ABC un triangle et Γ son cercle circonscrit. Soit Γ_A un cercle tangent à (AB) et (AC), et tangent intérieurement à Γ en un point A'. On définit de manière similaire Γ_B, B', Γ_C et C'.

Montrer que les droites (AA'), (BB') et (CC') sont concourantes.



Solution de l'exercice 8 Soient ω le cercle inscrit à (ABC) et X le centre de l'homothétie positive qui envoie Γ sur ω : A' est le centre de l'homothétie positive qui envoie Γ sur Γ_A et A celui de l'homothétie positive qui envoie Γ_A sur ω, donc $X \in (AA')$ et, de même, $X \in (BB')$ et $X \in (CC')$, d'où le résultat.

Exercice 9 Soient (Δ_1), (Δ_2) et (Δ_3) trois droites. Construire un triangle équilatéral ayant un sommet sur chacune des trois droites.

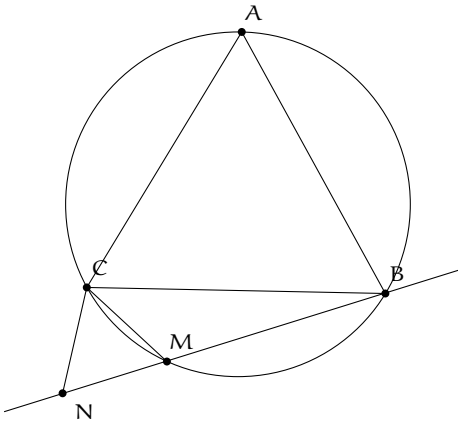


Solution de l'exercice 9 On choisit A_1 arbitrairement sur (Δ_1). Pour tout point A_2, le point A_3 tel que $A_1A_2A_3$ soit équilatéral est l'image de A_2 par la rotation r de centre A_1 et d'angle 60°. A_3 doit donc appartenir à (Δ_3) et à $r(\Delta_2)$, ce qui permet de tracer le triangle.

Exercice 10 Soit ABC un triangle équilatéral et M sur son cercle circonscrit, sur l'arc entre B et C ne contenant pas A.

Montrer que $MB + MC = MA$.

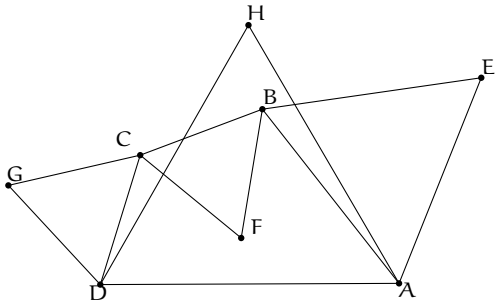
Solution de l'exercice 10 En géométrie, il est plus facile de manipuler des sommes de longueurs quand les points considérés sont alignés. Soit donc N le point de (MB) sur la demi-droite



issue de M ne contenant pas B, tel que MN = MC : par chasse aux angles, $\angle CMN = 60°$, donc CMN est équilatéral. On veut maintenant montrer AM = BN. Or, soit r la rotation de centre C et d'angle 60° : elle envoie A sur B et M sur N, d'où le résultat.

Exercice 11 Soient ABCD un quadrilatère convexe et E, F, G et H tels que ABE, BCF, CDG et DAH soient équilatéraux avec ABE et CDG dirigés vers l'extérieur de ABCD et BCF et DAH dirigés vers l'intérieur.

Montrer que EFGH est un parallélogramme.



Solution de l'exercice 11 On suppose ABCD direct : soient r_1 la rotation de centre A et d'angle 60° et r_2 la rotation de centre C et d'angle −60°. On a :

$$r_2 \circ r_1(E) = r_2(B) = F$$

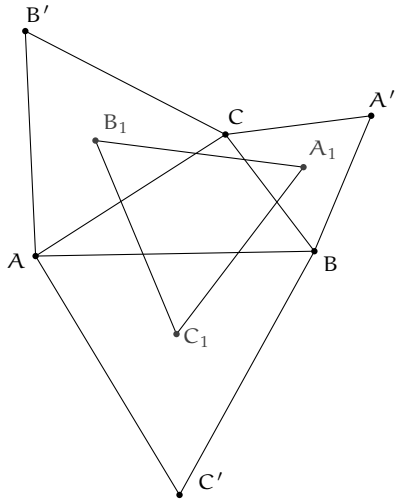
et

$$r_2 \circ r_1(H) = r_2(D) = G$$

donc EH=FG et, de même, EF=GH.

Exercice 12 (Théorème de Napoléon) Soient ABC un triangle et A′, B′ et C′ tels que A′BC, AB′C et ABC′ soient équilatéraux, extérieurs à ABC. Soient A_1, B_1 et C_1 les centres de ces triangles équilatéraux.

Montrer que $A_1B_1C_1$ est équilatéral.



Solution de l'exercice 12 On suppose ABC direct : la figure présentant des triangles équilatéraux, il est naturel de considérer des rotations de 60° ou 120°. On veut les composer pour aboutir à quelque chose de simple, comme une translation. Soient donc r_A, r_B et r_C les rotations de centres A_1, B_1 et C_1 et d'angle 120° : leur composée est une translation car $3*120 = 360$. De plus, on a :

$$r_A \circ r_B \circ r_C(B) = r_A \circ r_B(A) = r_A(C) = B$$

d'où $r_A \circ r_B \circ r_C = \mathrm{Id}$. En particulier, $r_A \circ r_B(C_1) = C_1$. Soit donc $D = r_B(C_1)$: on a $r(D) = C_1$. En faisant une figure avec les angles et les égalités de longueurs, on voit que $A_1DB_1C_1$ est un losange avec un angle en C_1 de 60°, donc $A_1B_1C_1$ est bien équilatéral.

2 Groupe B : géométrie

1 Cours de géométrie

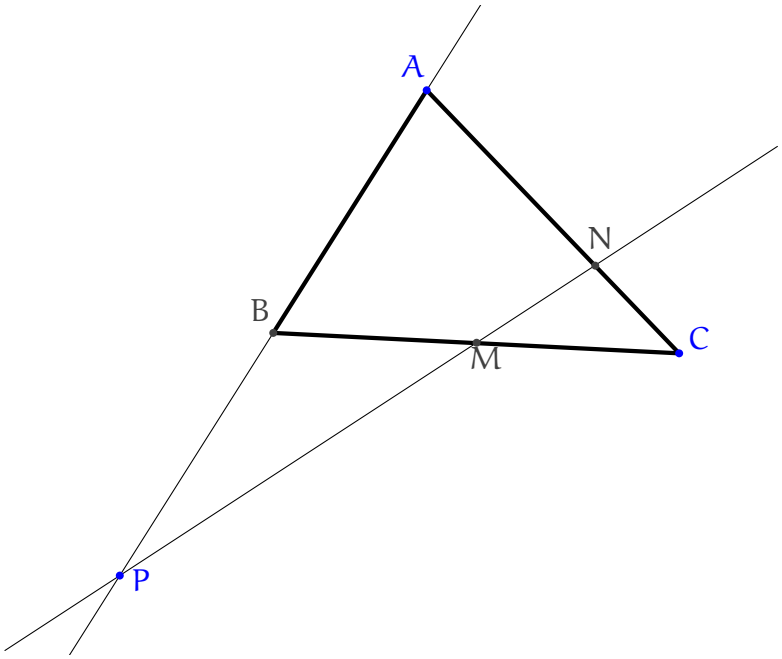
Cette séance a été consacrée essentiellement à un cours d'initiation, illustré par quelques exercices. Nous ne nous attarderons guère sur le cours, qu'on peut trouver dans bien des publications, mais surtout sur les exercices.

Après avoir rappelé le théorème de Thalès, j'ai montré le théorème de Ménélaüs : trois points sur les côtés d'un triangle, $M \in (BC), N \in (CA), P \in (AB)$ sont alignés si et seulement si, en mesure algébrique, $\frac{MB}{MC} \cdot \frac{NC}{NA} \cdot \frac{PA}{PB} = 1$.

Exercice 1

Soit ABC un triangle, M le milieu de BC, N au tiers de AC à partir de C. La droite (MN) coupe (AB) en P. Déterminer la position de P par rapport à A et B.

Solution de l'exercice 1



La relation $\frac{MB}{MC} \cdot \frac{NC}{NA} \cdot \frac{PA}{PB} = 1$ donne $\frac{PA}{PB} = 2$, P est le symétrique de A par rapport à B.

Pour généraliser cette notion de "milieu", "tiers", j'ai introduit les barycentres, qui exigent une certaine pratique du calcul vectoriel, et ai montré le théorème de Céva à l'aide de coordonnées barycentriques : soit trois points sur les côtés d'un triangle, $M \in (BC), N \in (CA), P \in (AB)$; les droites $(AM), (BN), (CP)$ sont concourantes si et seulement si, en mesure algébrique, $\frac{MB}{MC} \cdot \frac{NC}{NA} \cdot \frac{PA}{PB} = -1$.

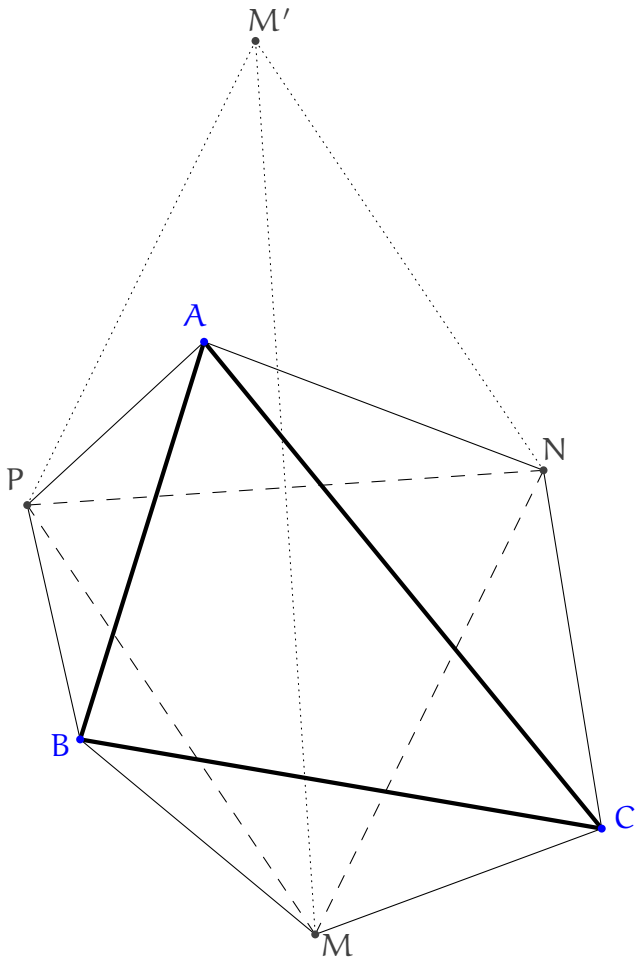
Puis, j'ai rappelé le théorème de Pythagore et sa généralisation, le théorème d'Al Kashi : $c^2 = a^2 + b^2 - 2ab\cos\widehat{C}$. J'ai montré au passage la formule de Héron : l'aire du triangle $S = \sqrt{p(p-a)(p-b)(p-c)}$.

J'ai ensuite abordé les transformations du plan : translations, rotations (composition de deux rotations), homothéties, similitudes, en illustrant à l'aide de deux exercices :

Exercice 2

Sur les côtés d'un triangle ABC, on trace, extérieurement à ABC, des triangles isocèles BMC, CNA, APB ayant tous des angles au sommet de 120°. Montrer que le triangle MNP est équilatéral.

Solution de l'exercice 2

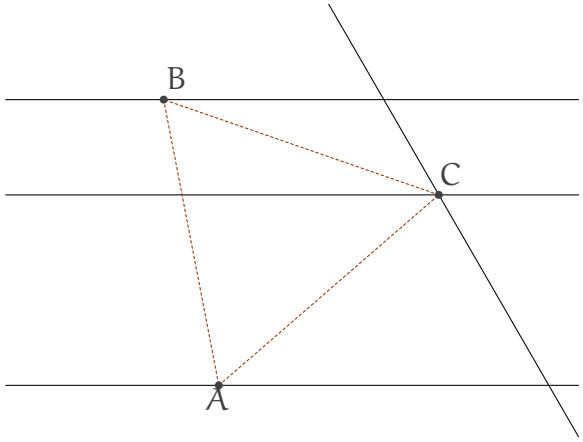


Considérons les rotations de centres M, N, P et d'angles 120°. Comme $120° + 120° + 120° = 360°$, la composée de ces trois rotations est une translation ("rotation d'angle nul et de centre à l'infini"). Mais la première rotation envoie B en C, la deuxième C en A et la troisième A en B, de sorte que la composée de ces trois rotations envoie B en B : c'est donc l'identité. Or, la première rotation envoie M en lui-même, puisqu'il est le centre de la rotation. La seconde envoie ce même M en un point M′, et la troisième, M′ en M puisque la composée des trois est l'identité. Par définition de la rotation, les triangles MNM′ et M′PM sont tous deux isocèles, d'angles en N et P égaux à 120°. La médiatrice de MM′ est axe de symétrie de chacun des deux triangles, donc bissectrice de $\widehat{MNM'}$ et de $\widehat{M'PM}$. On en déduit que les triangles MNP et M′NP ont chacun deux angles de 60°, donc trois car la somme des angles d'un triangle vaut 180° : ces triangles sont tous deux équilatéraux, ce qui achève la démonstration.

Exercice 3

Comment placer, sur trois droites parallèles, des points A, B, C de sorte que ABC soit un triangle équilatéral ?

Solution de l'exercice 3



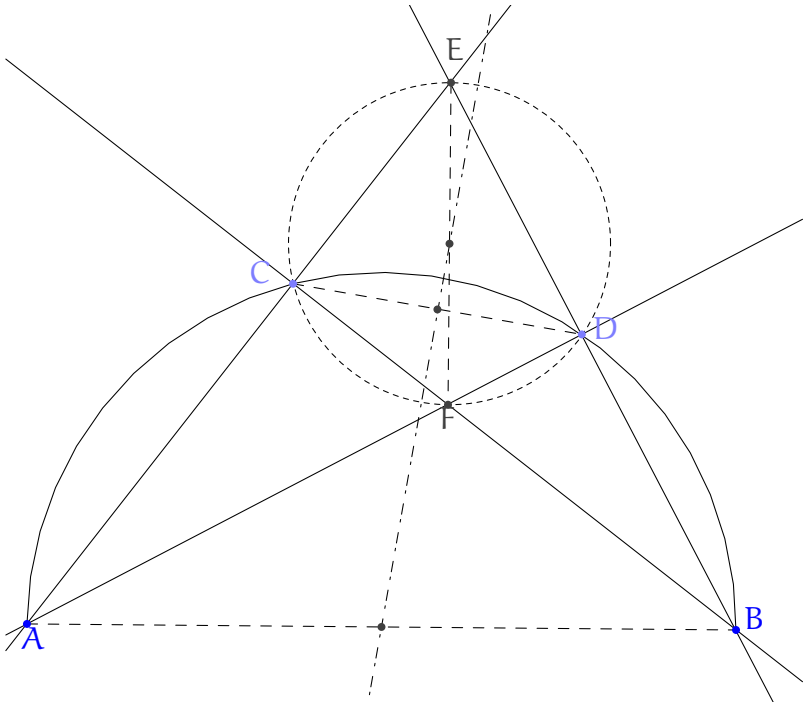
Plaçons A sur l'une des droites. La rotation de centre A et d'angle 60° transforme B en C. Mais il transforme également la droite contenant B en une droite, qui fait avec les parallèles un angle de 60°. Cette transformée coupe donc la troisième droite en un point, qui ne peut être que C : c'est le seul point qui soit simultanément sur la troisième droite, comme doit l'être le point C, et transformé par la rotation de centre A d'un point de la deuxième droite, comme doit l'être à nouveau le point C. Ayant les points A et C, il est facile de compléter le triangle équilatéral : B est transformée de C par une rotation de centre A et de 60° en sens inverse.

Puis, j'ai abordé rapidement le cercle, notamment les angles inscrits et la condition nécessaire et suffisante pour que quatre points soient cocycliques. Je n'ai pas parlé du cas de la tangente, mais j'ai mentionné le cas particulier de l'angle droit, illustré par l'exercice que voici :

Exercice 4

C et D sont deux points situés sur un demi-cercle de diamètre AB. Les droites (AC) et (BD) se coupent en E, les droites (AD) et (BC) se coupent en F. Montrer que les milieux de AB, CD, EF sont alignés.

Solution de l'exercice 4



Puisque AB est un diamètre, les angles inscrits $\widehat{ACB}$ et $\widehat{ADB}$ sont droits, d'où l'on déduit que les angles $\widehat{ECF}$ et $\widehat{EDF}$ sont eux aussi droits : C et D sont donc situés sur le cercle de diamètre EF. Le milieu de EF, centre de ce cercle, est équidistant de C et D, il appartient donc à la médiatrice de CD, tout comme le milieu de AB, centre du demi-cercle auquel appartiennent par hypothèse C et D. La médiatrice passe donc par les trois milieux de AB, CD et EF, d'où le résultat.

Je n'ai pas eu le temps de faire un autre exercice que j'avais prévu, et que nous avons utilisé comme exercice du test.

J'ai terminé le cours en présentant la loi des sinus : soit ABC un triangle, α, β, γ ses angles en A, B, C respectivement, R le rayon de son cercle circonscrit.

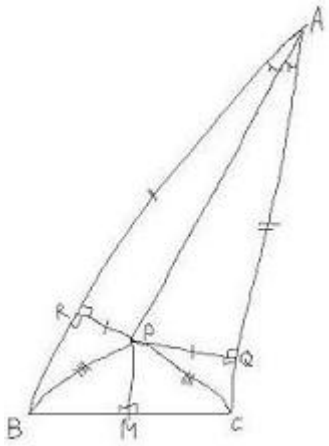
$$\frac{BC}{\sin\alpha} = \frac{CA}{\sin\beta} = \frac{AB}{\sin\gamma} = 2R$$

Mais je n'ai pas pu aborder les points remarquables du triangle, G, O, H, I, droite et cercle d'Euler... avec trois exercices initialement envisagés !

2 TD de géométrie

Théorème 2.1. Tout triangle est isocèle.

Démonstration. Soit ABC un triangle, supposons par l'absurde qu'il soit non isocèle en A. On trace une magnifique figure, sur laquelle P est l'intersection de la bissectrice du sommet A et la médiatrice de BC. Soit Q et R les projetés orthogonaux de P sur AC et AB (c'est-à-dire, Q est l'intersection de AC et de la perpendiculaire à AC issue de P).



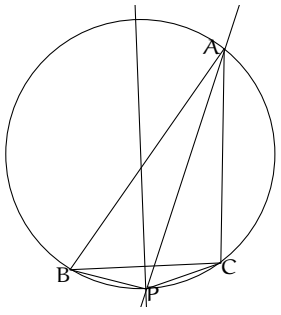
Les triangles APR et APQ ont deux angles communs, donc sont semblables. Comme ils ont AP en commun, ils sont même isométriques, donc $AR = AQ$ et $PR = PQ$. Le point P est sur la médiatrice de BC, donc $PB = PC$, puis par théorème de Pythagore, $RB^2 = PB^2 - PR^2 = PC^2 - PQ^2 = QC^2$. Finalement, $AB = AR + RB = AQ + QC = AC$, dont ABC est isocèle en A, c'est absurde. Donc ABC est isocèle en A. □

Cette théorème est bien entendu totalement faux. Donc la preuve est fausse. Mais ou est l'erreur ? Elle est subtile : elle est dans la dernière ligne, quand on a écrit $AB = AR + RB$ et son symétrique. Sur notre immonde figure à main levée, il semblait que P était à l'intérieur du triangle, et du coup R était sur le segment AB. Cela n'a aucune raison d'être vrai si P est a l'extérieur du triangle : le point B peut être situé entre A et R, et alors la relation correcte est $AB + BR = AR$. De fait, on a même prouvé, par notre raisonnement, que l'un des points P et Q est en dehors du triangle.

Moralité : ne JAMAIS faire de géométrie sur des mauvaises figures. Il est trop facile de dire des choses fausses, et au contraire on pourrait rater des informations qui seraient visibles sur une meilleure figure (ou, idéalement, plusieurs figures), un alignement par exemple.

Exercice 1 Soit ABC non isocèle en A. Alors la bissectrice du sommet A et la médiatrice de BC s'intersectent en un point que nous nommerons P. Où est-il ?

Solution de l'exercice 1



On trace plusieurs magnifiques figures, qui nous permettent de conjecturer que P est sur le cercle circonscrit à ABC, reste à le montrer, mais on ne sait pas trop comment partir. Que faut-il montrer ? Que trois objets, les deux droites et le cercle, s'intersectent. Pour cela, il suffit de montrer que l'intersection de deux de ces objets appartient au troisième. Appelons donc P′ l'intersection du cercle avec la bissectrice (autre que A), et montrons qu'il est sur la médiatrice,

c'est-à-dire que $P'B = P'C$. L'intérêt de regader P' au lieu de P, c'est que l'on dispose ainsi de beaucoup plus d'information sur les angles. Ainsi, par angle inscrit et définition de la bissectrice, $\widehat{P'BC} = \widehat{P'AC} = \widehat{BAP'} = \widehat{BCP'}$. Donc BCP' est isocèle, et on a fini.

Exercice 2 Soit ABC un triangle. En utilisant le théorème de Céva, montrer que les médianes sont concourantes, que les hauteurs sont concourantes, puis que les bissectrices intérieures sont concourantes.

Solution de l'exercice 2 Notons a, b et c les longueurs des segments BC, CA, AB, et $\widehat{A}$, $\widehat{B}$ et $\widehat{C}$ les angles correspondant aux trois sommets.

- Soit M le milieu de BC. Alors $\frac{\overline{MB}}{\overline{MC}} = -1$, et de même pour les autres côtés, et le théorème de Céva conclut.
- Pour la hauteur, il faut commencer par traiter à part le cas du triangle rectangle. Ensuite, soit H le pied de la hauteur issue de A. Alors BH vaut $c \cdot \sin(\widehat{B})$ (ou $AH \cdot \tan(\widehat{B})$). Ainsi,

$$\frac{HB}{HC} = \frac{c \cdot \sin(\widehat{B})}{b \cdot \sin(\widehat{C})} = \frac{\tan(\widehat{B})}{\tan(\widehat{C})}.$$

  Examinons maintenant le signe de $\frac{\overline{HB}}{\overline{HC}}$: c'est $+$ si H est sur $[BC]$ et $-$ sinon, et on vérifie que le nombre de pieds de hauteur non situés sur leur segment de triangle vaut 0 (triangle aigu) ou 2 (triangle obtus). Dans tous les cas, le produit intervenant dans le théorème de Céva vaut -1.
- Soit I l'intersection de la bissectrice interne du sommet A avec BC. On applique la loi des sinus dans AIB et AIC :

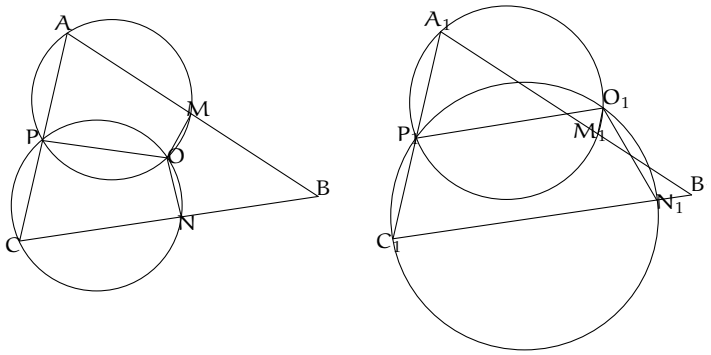
$$IB = \frac{AI \cdot \sin(\widehat{A}/2)}{\sin(\widehat{B})} = \frac{c \cdot \sin(\widehat{A}/2)}{\sin(\widehat{AIB})}.$$

  Or, $\sin(\widehat{AIB}) = \sin(\widehat{AIC})$ (les angles sont supplémentaires). Finalement, $\frac{\overline{IB}}{\overline{IC}} = \frac{\sin(\widehat{B})}{\sin(\widehat{C})} = \frac{c}{b}$. Ces relations sont importantes et à retenir. Elles permettent de conclure avec le théorème de Céva.

J'ai ensuite montré que G, H et O sont alignés, et que $GH = 2GO$, en introduisant l'homothétie de centre G et de rapport $-1/2$, et le triangle dont ABC est le triangle des milieux. C'est fait dans un des autres TD, qui montre de plus des propriétés du cercle d'Euler : je vous conseille vivement de le lire.

Exercice 3 Soit ABC un triangle, soient M, N et P des points respectivement sur les côtés AB, BC et CA du triangle. Montrer que les cercles circonscrits au trois triangles PAM, MBN et NCP sont concourants.

Solution de l'exercice 3 On doit montrer que trois objets sont concourants, et pour cela la méthode est toujours la même : on introduit un point O appartenant à deux des cercles, disons PAM et MBN, et on cherche à montrer qu'il est sur le troisième. On dispose de plein de cercles, ce qui permet d'utiliser le théorème de l'angle inscrit. On l'applique dans APM : $\widehat{MAP} = 180° - \widehat{POM}$, puis dans CNP : $\widehat{PCN} = 180° - \widehat{NOP}$. Finalement, $\widehat{NOM} = 360° - \widehat{POM} - \widehat{NOP} = \widehat{MAP} + \widehat{PCN} = 180° - \widehat{MBN}$ car la somme des angles de ABC fait 180°. La réciproque du théorème de l'angle inscrit dit que $ONBM$ sont cocycliques, ce qui conclut.



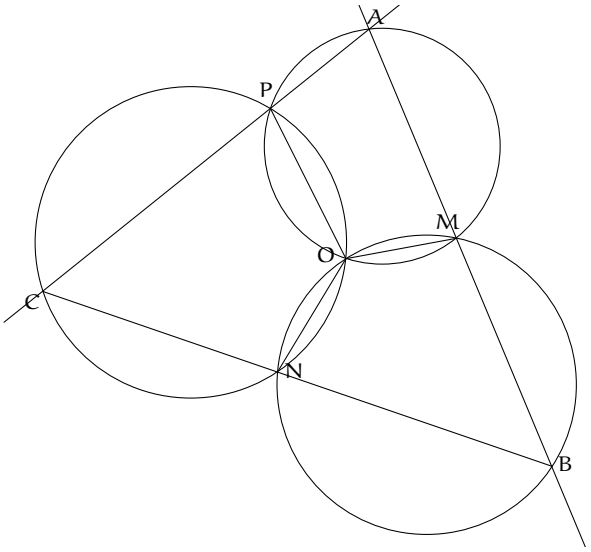
Attention ! Cette preuve ne suffit pas ! Nous avons traité le cas de la figure de gauche : le cas où O est à l'intérieur de ABC. Ce n'est pas le seul cas, regardons par exemple la deuxième figure. Le point O_1 est situé du même côté que A par rapport à la corde P_1M_1. Ainsi, les angles $\widehat{M_1O_1P_1}$ et $\widehat{M_1A_1P_1}$ ne sont plus supplémentaires, mais égaux. Il faudrait refaire le raisonnement à part pour traiter ce cas (plus d'autres cas dégénérés, par exemple si O est confondu avec M_1, alors l'angle $\widehat{M_1O_1P_1}$ n'est plus défini). Je laisse ces cas manquants en exercice.

On remarque que les preuves des cas non dégénérés se ressemblent beaucoup. Ce n'est pas un hasard, et tout devient clair quand on introduit la notion d'angle de droites. Soient D_1 et D_2 deux droites. Comment définit un angle entre elles ? On pourrait donner un nom aux points, par exemple B l'intersection de D_1 et D_2, A un point différent de B sur D_1, C un point différent de B sur D_2, et dire que l'angle entre les droites est l'angle $\widehat{ABC}$, mais cela ne marche pas : le choix de ABC n'est pas canonique, et un autre choix de ces points aurait donné une autre valeur. Par exemple, si on appelle A' le symétrique de A par rapport à B, alors les angles $\widehat{ABC}$ et $\widehat{A'BC}$ ne sont pas égaux, mais supplémentaires. Une solution est de décréter que l'angle entre D_1 et D_2 est l'ensemble $\{\widehat{ABC}, \widehat{A'BC}\}$. Avec cette définition, le théorème de l'angle inscrit dit que, ABCD est inscriptible si et seulement si l'angle de droites entre (AC) et (AD) est égal à l'angle de droites entre (BC) et (BD), et ce quel que soit la position relative de A et B par rapport à la corde CD. Cette version du théorème permettrait de traiter à la fois tous les cas non dégénérés de l'exercice.

La même subtilité est présente dans les deux exercices suivants : pour être complet, il faudrait traiter plusieurs cas, ou bien raisonner en termes d'angles de droites. Je ne le ferai pas dans ce cours.

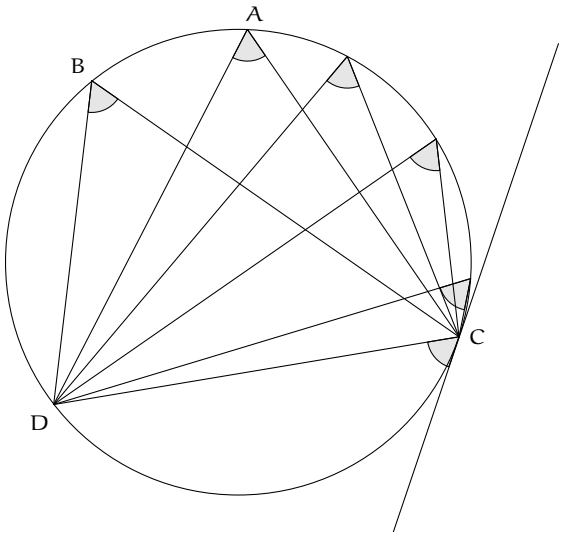
Exercice 4 On considère trois cercles $\mathcal{C}_1$, $\mathcal{C}_2$ et $\mathcal{C}_3$ distincts s'intersectant au point O. Soient M, N et P les intersections autres que 0 respectivement entre $\mathcal{C}_1$ et $\mathcal{C}_2$, $\mathcal{C}_2$ et $\mathcal{C}_3$ et $\mathcal{C}_3$ et $\mathcal{C}_1$. Soit A un point sur le cercle passant sur $\mathcal{C}_1$ la droite AP intersecte $\mathcal{C}_3$ en un autre point C, la droite AM intersecte $\mathcal{C}_3$ en un autre point B. Montrer que B, N et C sont alignés.

Solution de l'exercice 4



L'angle $\widehat{ONC}$ est supplémentaire à $\widehat{CPO}$, donc égal à $\widehat{OPA}$. Cet angle $\widehat{OPA}$ est supplémentaire à $\widehat{AMO}$, donc égal à $\widehat{OMB}$. Enfin, $\widehat{OMB}$ est supplémentaire à $\widehat{BNO}$; On a montré que $\widehat{ONC} + \widehat{BNO} = 180°$, ce qui conclut.

Une remarque avant l'exercice suivant : que se passe-t-il dans le théorème de l'angle inscrit si l'un des points, disons A, se rapproche du point C sur le cercle ? Et bien, l'angle $\widehat{DAC}$ est constant, égal à l'angle $\widehat{DBC}$, mais il se rapproche de plus en plus de l'angle entre la corde CD et la tangente au cercle passant par C : cet angle avec la tangente est lui aussi égal à $\widehat{DBC}$.

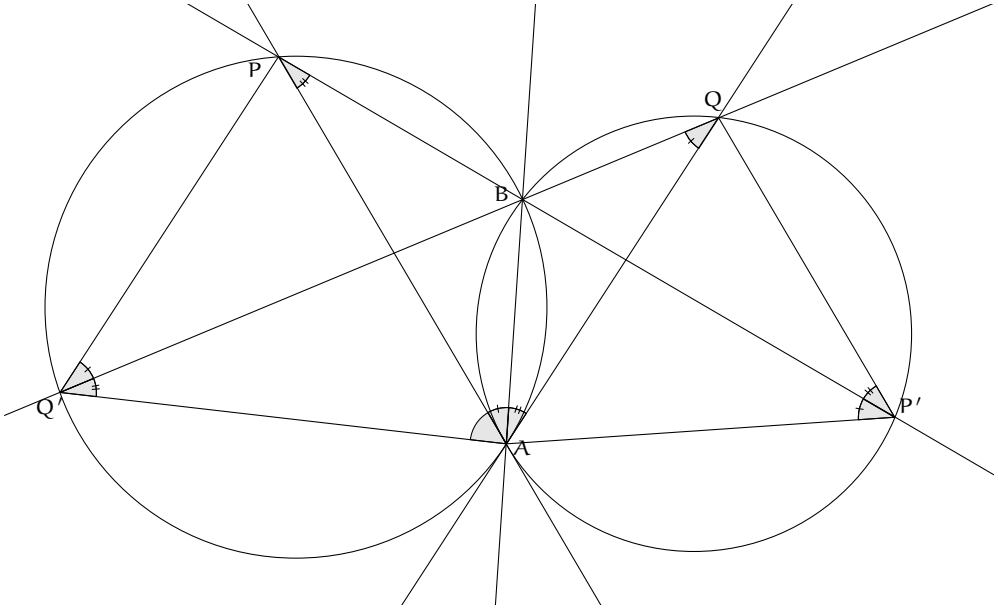


Exercice 5 Soient deux cercles $\mathcal{C}_1$ et $\mathcal{C}_2$ s'intersectant en A et B. Soit P (resp. Q) l'intersection de $\mathcal{C}_1$ (resp. $\mathcal{C}_2$) avec la tangente à $\mathcal{C}_2$ (resp. $\mathcal{C}_1$) passant par A. Soit P' (resp. Q') l'intersection autre que B de PB avec $\mathcal{C}_2$ (resp. de QB avec $\mathcal{C}_1$). Montrer que $PP' = QQ'$.

Solution de l'exercice 5

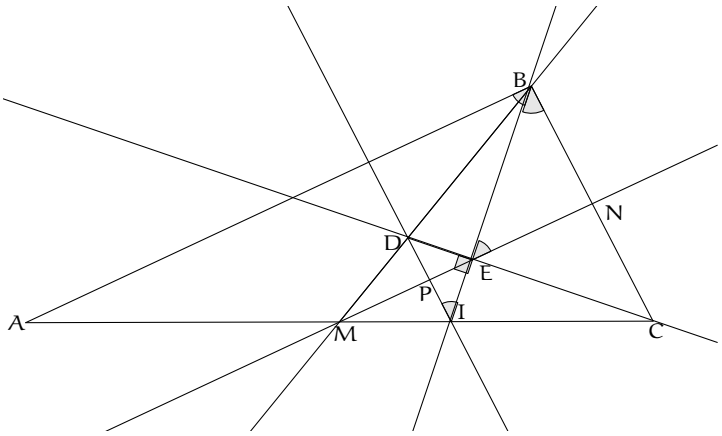
Le théorème de l'angle inscrit donnne les égalités d'angle indiquées sur la figure. Appelons α l'angle $\widehat{BQ'P}$ (simple tiret sur la figure), β l'angle $\widehat{APB}$ (double tiret sur la figure). On

remarque notamment que les triangles PAP' et $Q'AQ$ sont semblables (ils ont deux angles égaux). Le résultat à montrer est donc équivalent à prouver que ces triangles sont isométriques, pour le prouver il faut montrer que $AQ' = AP$, donc que $AQ'P$ est isocèle. Introduisons γ l'angle $\widehat{PAQ'}$. La somme des angles dans le triangle $Q'AQ$ nous dit que $2\alpha + 2\beta + \gamma = 180°$. En examinant la somme des angles du triangle APQ', on trouve donc que $\widehat{Q'PA} = \alpha+\beta$, donc $\widehat{Q'PA} = \widehat{AQ'P}$, et on a terminé.



Exercice 6 Soit ABC un triangle tel que $BA > BC$. Soit M le milieu de AC, la bissectrice intérieure de l'angle $\widehat{B}$ coupe AC en I. La parallèle à BC passant par I coupe AM en E. La parallèle à BA passant par M coupe AI en D. Que vaut l'angle $\widehat{EDI}$?

Solution de l'exercice 6



On fait quelques jolies figures, qui nous permettent de conjecturer que l'angle en question vaut 90°. On regarde ensuite quelles informations on peut obtenir sur notre figure. On introduit N (resp. P) l'intersection de EM avec BC (resp. DI). Le théorème de Thalès appliqué dans ABC dit que $BN = NC$. On le réapplique dans BNM et NMC pour obtenir que

$DP/BN = MP/MN = IP/NC$, et donc $PD = PI$. Grâce aux angles alternes-internes, opposés et à la définition de la bissectrice, on obtient : $\widehat{PIE} = \widehat{IBC} = \widehat{ABI} = \widehat{BEN} = \widehat{PEI}$ et donc PEI est isocèle et $PE = PD = PI$. Ainsi, D est sur le cercle de diamètre EI, donc l'angle cherché vaut $90°$.

Une remarque : l'hypothèse $BA > BC$, donnée pour que I soit « à gauche de M »sur la figure, n'est pas nécessaire, l'exercice marche aussi si $BC > BA$.

3 Cours/TD de géométrie

Voir le cours de géométrie du groupe C, à partir de la page 60.

3 Groupe C

1 Cours d'arithmétique

- Calculs de PGCD -

On note (a, b) le PGCD des entiers a et b. On rappelle que $(a, b) = (a, b + ca)$ avec a, b, c des entiers. Ceci est à la base de l'algorithme d'Euclide pour calculer le pgcd de deux entiers : si $a = bq + r$, $0 \leqslant r < a$ est la division euclidienne de a par b, $(a, b) = (r, b) = (b, r)$, et en calculant ainsi la suite des restes de la division euclidienne du premier argument par le second, on obtient une suite de restes positifs strictement décroissante, qui aboutit donc à 0. La dernière étape de calcul donne ainsi un entier naturel d tel que $(a, b) = (d, 0) = d$, et on a ainsi calculé le pgcd de a et b.

Exercice 1 Soit a, b deux entiers premiers entre eux. Montrer que $\left(\dfrac{a^n - b^n}{a - b}, a - b\right) = (a - b, n)$.

Solution de l'exercice 1

$$\begin{aligned}
(\frac{a^n - b^n}{a - b}, a - b) &= (a - b, \sum_{k=0}^{n-1} a^k b^{n-k}) \\
&= (a - b, \sum_{k=0}^{n-1} (a^k b^{n-k} - b^n) + nb^n) \\
&= (a - b, \sum_{k=0}^{n-1} b^{n-k}(a^k - b^k) + nb^n) \\
&= (a - b, nb^n)
\end{aligned}$$

car $a - b \mid a^k - b^k$. Comme a et b sont premiers entre eux, $a - b$ et b sont premiers entre eux, donc $(a - b, nb^n) = (a - b, n)$, ce qui conclut.

Exercice 2 Calculer le pgcd de $a^n - 1$ et $a^m - 1$.

Solution de l'exercice 2 Soit $n = mq + r$, $0 \leqslant r < m$ la division euclidienne de n par m. On a alors $a^n - 1 = a^r(a^{mq} - 1) + a^r - 1$ donc $(a^n - 1, a^m - 1) = (a^m - 1, a^r - 1)$, car $a^m - 1 \mid (a^m)^q - 1$. De même, si r_1 est le reste de la division euclidienne de m par r, on obtient $(a^m - 1, a^r - 1) = (a^r - 1, a^{r_1} - 1)$, et ainsi de suite. La suite des exposants est la suite obtenue en appliquant l'algorithme d'Euclide à n et m ; on obtient donc $(a^n - 1, a^m - 1) = (a^{(n,m)} - 1, a^0 - 1) = a^{(n,m)} - 1$.

- Définition des congruences -

Exercice 3 Pour quels entiers naturels n a-t-on $13 \mid 14^n - 27$?

Solution de l'exercice 3 Il suffit de remarquer que $14 = 13 + 1$ et que dans le développement de $(13 + 1)^n$, 13 apparaît toujours en facteur sauf pour le dernier terme, qui est 1.
Ainsi $13 \mid 14^n - 27 \iff 13 \mid 1 - 27 = -26$ ce qui est toujours vérifié.

L'exercice précédent est ici simplement pour illustrer la notion de congruence. On dit que deux entiers a et b sont congrus modulo un entier n, et on note $a \equiv b[n]$, si n divise $b-a$. Dans ce cas, si la question est de savoir si une certaine expression faisant intervenir a est divisible par un entier n, on peut remplacer a par b dans l'expression (pour la simplifier en général), sans modifier le résultat.

En effet, l'addition et la multiplication des entiers sont compatibles avec les congruences. Plus précisément, si $a \equiv b[n]$, alors $a + c \equiv b + c[n]$, $ac \equiv bc[n]$. On calcule donc modulo n comme on calcule dans les entiers, en ajoutant la règle $n = 0$. On note $\bar{a}$ la classe d'équivalence de a modulo n, qui est l'ensemble des entiers congrus à a modulo n. Un élément de cet ensemble est appelé un représentant de $\bar{a}$, et on peut sommer et multiplier des classes comme on le fait avec leurs représentants. On note $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ l'ensemble des classes d'équivalences modulo n, muni des opérations $+$ et $\times$, vérifiant les lois de compatibilité usuelles (associativité, distributivité, commutativité). On dit que $\mathbb{Z}/n\mathbb{Z}$, muni de ces deux opérations, est un anneau commutatif.

- Inversibilité modulo n -

Après avoir dit qu'on pouvait multiplier modulo n, une question naturelle est de savoir si on peut diviser des classes d'équivalence. Autrement dit, si $a \in \mathbb{Z}$, existe-t-il $a' \in \mathbb{Z}$ tel que $aa' \equiv 1[n]$ (on dira que a ou $\bar{a}$ est inversible modulo n et que $\bar{a}'$ est l'inverse de $\bar{a}$ dans $\mathbb{Z}/n\mathbb{Z}$). En revenant à la définition, cela revient à demander s'il existe $a', n' \in \mathbb{Z}$ tels que $aa' + nn' = 1$. La réponse est donnée par le théorème de Bézout :

Théorème 3.1 (Bézout)**.** Si $d = (a, b)$, alors il existe des entiers u et v tels que $au + bv = d$. Il est clair par ailleurs que d divise tout entier de la forme $au + bv$, donc la réponse à notre question est que a est inversible modulo n si et seulement si a et n sont premiers entre eux.

Voyons comment trouver l'inverse de $\bar{a}$, c'est-à-dire comment trouver a', quand a et n sont bien premiers entre eux. On appelle combinaison linéaire entière de a et b tout nombre de la forme $au+bv$ avec u et v des entiers, qu'on appelle les coefficients de la combinaison linéaire. Notre but est de trouver la plus petite combinaison linéaire strictement positive de a et n, qui doit être 1. Pour cela, on applique simplement l'algorithme d'Euclide, qui donne une suite de restes (r_i) et de quotients (q_i) tels que $r_0 = a$, $r_1 = n$, $r_{i-1} = q_i r_i + r_{i+1}$, $r_k = 1$ et on remplace formellement r_0 par a et r_1 par n : $r_2 = a - q_1 n$, $r_3 = n - q_2(a - q_1 n) = a(-q_2) + n(1 + q_1 q_2)$, et ainsi de suite jusqu'à $1 = aa' + nn'$.

Exemple 3.2. Pour inverser 37 modulo 53, on écrit $16 = 53-37$, $5 = 37-2\times16 = 3\times37-2\times53$, $1 = 16 - 3 \times 5 = (-10) \times 37 + 7 \times 53$ donc -10 est inverse de 37 modulo 53.

On note $\mathbb{Z}/n\mathbb{Z}^*$ l'ensemble des classes inversibles de $\mathbb{Z}/n\mathbb{Z}$. La fonction indicatrice d'Euler est définie par $\phi(n) := \mathrm{Card}(\mathbb{Z}/n\mathbb{Z}^*)$. On remarque que si n est premier, tout nombre non multiple de n est premier avec n donc toutes les classes sont inversibles sauf celle de 0, et en particulier, $\phi(n) = n - 1$.

Exercice 4 (Théorème de Wilson) Soit $N > 1$ un entier naturel, montrer que $(N-1)! \equiv -1[N]$ si et seulement si N est premier.

Solution de l'exercice 4 Si N est composé, il existe deux entiers naturels $a, b > 1$ tels que $N = ab$ et si $a \neq b$, comme $a, b < N$, on a $(N-1)! \equiv 0[N]$. Si $a = b$, $N = a^2$ et $2a \leqslant N-1$ sauf si $N = 4$, et alors $(N-1)! \equiv 0[N]$. Si $N = 4$, $6 \not\equiv -1[4]$. Si N est premier, on calcule $(N-1)!$ en regroupant

chaque terme avec son inverse. On obtient ainsi un produit de paires d'inverses, sauf pour 1 et -1 qui sont leurs propres inverses. Ce sont les seuls car si $x \equiv x^{-1}[N]$ alors $x^2 - 1 \equiv 0[N]$ donc $(x-1)(x+1) \equiv 0[N]$ donc $x \equiv \pm 1[N]$ car N est premier. Ainsi, les produits de paires d'inverses se simplifient et il reste $(N-1)! \equiv -1[N]$.

Exercice 5 Montrer que pour tout p premier, l'équation $6n^2 + 5n + 1 \equiv 0[p]$ a toujours des solutions.

Solution de l'exercice 5 Si $p = 2$ ou $p = 3$, $n = 1$ donne une solution. Sinon, on peut résoudre comme on le fait dans les réels : on prend la racine du discriminant sans mal car c'est 1, et on obtient $n = \frac{-5\pm 1}{12}$ (12 est inversible modulo p).

- Lemme chinois -

Soit a, b, n trois entiers, d un diviseur de n, si $a \equiv b[n]$ alors $a \equiv b[d]$ car d divise n qui divise $a - b$. On a donc une fonction « naturelle »de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/d\mathbb{Z}$ qui à $\bar{k}$ associe $\bar{k}$. Elle est compatible avec l'addition et la multiplication.

Théorème 3.3. (Lemme chinois) Soit a et b deux entiers premiers entre eux, alors la fonction

$$\begin{cases} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \bar{k} & \longmapsto & (\bar{k}, \bar{k}) \end{cases}$$

est bijective.

De plus, elle est compatible avec l'addition et la multiplication.

Démonstration. On démontre la bijectivité. Comme les ensembles en question sont de même cardinal, il suffit de montrer l'injectivité. Il faut montrer que si n et m sont deux entiers tels que $n \equiv m[a]$ et $n \equiv m[b]$, alors $n \equiv m[ab]$. C'est le cas car a et b divisent $n - m$ et comme a et b sont premiers entre eux, ab divise $n - m$. □

Cela signifie que pour calculer dans $\mathbb{Z}/ab\mathbb{Z}$, on peut se ramener à calculer dans $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$, et réciproquement. On utilise le lemme chinois en particulier pour dire qu'un système de congruences modulo $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$ est équivalent à une congruence modulo $\mathbb{Z}/ab\mathbb{Z}$, via la bijection.

Exercice 6 On considère le plan muni d'un repère orthonormé d'origine O. On dit qu'un point M est invisible s'il existe un point à coordonnées entières sur $]OM[$. Montrer que pour tout entier naturel L il existe un carré de côté L, parallèle aux axes, tel que tous les points à coordonnées entières dans le carré soient invisibles.

Solution de l'exercice 6 Un point $M = (a, b) \in \mathbb{Z}^2$ est invisible si $\gcd(a, b) > 1$ car si $d \neq 1$ divise a et b, $(\frac{a}{d}, \frac{b}{d})$ est sur $]OM[$. Si on se donne $(p_{i,j})_{0 \leqslant i,j \leqslant L}$ des nombres premiers deux à deux distincts, alors d'après le lemme chinois il existe des entiers a et b tels que pour tous $0 \leqslant i, j \leqslant L$, $a \equiv -i[p_{i,j}]$ $b \equiv -j[p_{i,j}]$. Alors $\gcd(a + i, b + j) \geqslant p_{i,j} > 1$ donc tous les points $(a+i, b+j)$ sont invisibles, et le carré de côté L dont le coin inférieur gauche est (a, b) répond au problème.

Le théorème chinois permet de montrer directement la multiplicativité de l'indicatrice d'Euler, car la bijection se restreint en une bijection entre $\mathbb{Z}/ab\mathbb{Z}^*$ et $\mathbb{Z}/a\mathbb{Z}^* \times \mathbb{Z}/b\mathbb{Z}^*$, d'où l'on déduit que pour a et b premiers entre eux, $\phi(ab) = \phi(a)\phi(b)$. Par récurrence, on voit alors

que si $n = \prod_i p_i^{\alpha_i}$ est la décomposition en facteurs premiers de n, alors $\phi(n) = \prod_i \phi(p_i^{\alpha_i}) = \prod_i p_i^{\alpha_i - 1}(p_i - 1)$ car le nombre d'entiers naturels premiers avec p^k inférieurs à p^k est $p^k - p^{k-1}$ donc $\phi(p^k) = p^{k-1}(p-1)$.

- Ordre d'un élément -

Si $a \in \mathbb{Z}/n\mathbb{Z}^*$, en considérant l'ensemble des puissances de a dans $\mathbb{Z}/n\mathbb{Z}$, on voit par principe des tiroirs que deux d'entre elles sont égales, donc il existe des entiers $k > l$ tels que $a^k \equiv a^l [n]$ d'où $a^{k-l} \equiv 1[n]$. En particulier, il existe un plus petit entier naturel non nul $w(a)$ tel que $a^{w(a)} \equiv 1[n]$ qu'on appelle l'ordre de a (modulo n).

Théorème 3.4 (Euler)**.** Si $a \in \mathbb{Z}/n\mathbb{Z}^*$ alors $a^{\phi(n)} \equiv 1[n]$.

Corollaire 3.5 (petit théorème de Fermat)**.** Si $a \in \mathbb{Z}/p\mathbb{Z}^*$ avec p premier, alors $a^{p-1} \equiv 1[n]$.

Démonstration. La multiplication par a effectue une permutation de $\mathbb{Z}/n\mathbb{Z}^*$ (c'est une injection car a est inversible, donc une bijection par égalité des cardinaux). On a donc $\prod_{r \in \mathbb{Z}/n\mathbb{Z}^*} r \equiv \prod_{r \in \mathbb{Z}/n\mathbb{Z}^*} ar \equiv a^{\phi(n)} \prod_{r \in \mathbb{Z}/n\mathbb{Z}^*} r[n]$ donc en simplifiant, on obtient $a^{\phi(n)} \equiv 1[n]$. □

Exercice 7 Trouver tous les entiers naturels n tels que n divise $2^n - 1$.

Solution de l'exercice 7 Le nombre 1 convient. Soit p le plus petit diviseur premier de $n \neq 1$. Comme $2^n \equiv 1[n]$, on a aussi $2^n \equiv 1[p]$, et par le petit théorème de Fermat, $2^{p-1} \equiv 1[p]$, donc l'ordre de 2 modulo p divise le PGCD de n et $p-1$, donc vaut 1 car $p-1$ est plus petit que le plus petit nombre premier divisant n, donc est premier avec n. Ainsi $2 \equiv 1[p]$ donc $p = 1$, absurde. Ainsi, 1 est la seule solution.

2 TD d'arithmétique

- Énoncés des exercices -

Exercice 1

a) Prouver qu'il n'existe pas d'entiers a, b tels que $a^2 - 3b^2 = 8$.

b) Prouver qu'il n'existe pas d'entiers strictement positifs a, b tels que $a^2 + b^2 = 3c^2$.

Exercice 2

a) Prouver que le nombre $100\ldots00500\ldots001$ (il y a 100 zéros devant et 100 zéros derrière le 5) n'est pas le cube d'un entier.

b) Prouver que le nombre $a^3 + b^3 + 4$ n'est jamais le cube d'un entier pour a et b dans $\mathbb{N}$.

c) Prouver que l'équation $6m^3 + 3 = n^6$ n'a pas de solutions en nombres entiers.

Exercice 3 Prouver que parmi 52 nombres entiers quelconques il y en a toujours deux dont la somme ou la différence est divisible par 100.

Exercice 4

a) Montrer que la fraction $\frac{12n+1}{30n+2}$ est irréductible pour tout $n \in \mathbb{N}$.

b) Trouver $\text{pgcd}(2^{100}-1, 2^{120}-1)$.

Exercice 5 Montrer que quel que soit n, $n!$ n'est jamais divisible par 2^n, mais qu'il existe une infinité d'entiers n tels que $n!$ soit divisible par 2^{n-1}.

Exercice 6 Prouver que pour tout entier $n > 0$ le nombre $19 \times 8^n + 17$ est composé (c'est-à-dire n'est pas premier).

Exercice 7 Déterminer tous les entiers strictement positifs premiers avec tous les nombres de la forme $2^n + 3^n + 6^n - 1$, pour n entier naturel.

Exercice 8 Trouver tous les couples (a, b) d'entiers strictement positifs tels que $ab^2 + b + 7$ divise $a^2b + a + b$.

- Solutions des exercices -

Solution de l'exercice 1

a) La partie gauche est congrue à 0 ou 1 mod 3, alors que $8 \equiv 2 \mod 3$. Il n'y a donc pas de solution.

b) On suppose qu'il existe des nombres entiers strictement positifs tels que $a^2 + b^2 = 3c^2$. Choisissons une solution (a, b, c) qui minimise la somme $a+b+c \in \mathbb{N}^*$. D'après l'équation, $a^2 + b^2$ est divisible par 3, ce qui n'est possible que si a et b sont divisibles par 3. Écrivons $a = 3a_1$ et $b = 3b_1$. Alors $3(a_1^2 + b_1^2) = c^2$ et c est aussi divisible par 3. En notant $c = 3c_1$, on obtient finalement $a_1^2 + b_1^2 = 3c_1^2$, ce qui signifie que (a_1, b_1, c_1) est une solution de notre équation. Or $a_1 + b_1 + c_1 < a + b + c$, et la contradiction apparaît.

Solution de l'exercice 2

a) On a
$$1\ldots00500\ldots001 = 1\ldots00499\ldots994 + 7 \equiv 7 \pmod 9$$
tandis qu'un cube ne peut être congru qu'à 0, 1 ou 8 mod 9.

b) Un cube ne peut être congru qu'à 0, 1 ou 8 mod 9, tandis que les restes possibles de la division de $a^3 + b^3 + 4$ par 9 sont $2, 3, 4, 5$ et 6.

c) Un cube est congru à $0, 1$ ou 6 mod 7, tandis que les restes possibles de la division de $6m^3 + 3$ par 7 sont $2, 3$ et 4.

Solution de l'exercice 3 On répartit les restes de division par 100 en les 51 groupes suivants
$$\{0\}, \{1, 99\}, \{2, 98\} \ldots \{49, 51\}, \{50\}$$
D'après le principe des tiroirs, deux de nos 52 nombres ont les restes de division par 100 qui se trouvent dans le même groupe. Alors leur somme ou leur différence est divisible par 100.

Solution de l'exercice 4

a) D'après l'algorithme d'Euclide, on a $\text{pgcd}(30n + 2, 12n + 1) = \text{pgcd}(12n + 1, 6n) = \text{pgcd}(6n, 1) = 1$

b) On a $\text{pgcd}(2^{120} - 1, 2^{100} - 1) = \text{pgcd}(2^{100} - 1, 2^{20} - 1) = 2^{20} - 1$ car $2^{100} - 1 = (2^{20})^5 - 1$ est divisible par $2^{20} - 1$.

Solution de l'exercice 5 Dans le produit $n!$ des entiers inférieurs ou égaux à n, le facteur 2 apparaît $\left[\frac{n}{2}\right]$ fois pour les entiers pairs, $\left[\frac{n}{4}\right]$ fois de plus pour les multiples de 4, ... $\left[\frac{n}{2^k}\right]$ fois de plus pour les multiples de 2^k : en tout, l'exposant de 2 dans la décomposition de $n!$ vaut $\left[\frac{n}{2}\right] + \cdots + \left[\frac{n}{2^k}\right] + \ldots$. Les termes de cette somme sont nuls à partir d'un certain rang q, donc la somme est inférieure ou égale à $\frac{n}{2} + \cdots + \frac{n}{2^{q-1}} = n\left(1 - \frac{1}{2^{q-1}}\right) < n$.

Si $n = 2^q$, alors pour $k \leqslant q$, on a $\left[\frac{n}{2^k}\right] = 2^{q-k}$, et la somme $2^{q-1} + 2^{q-2} + \cdots + 2 + 1 = 2^q - 1 = n - 1$ donc $n!$ est divisible par 2^{n-1}.

Solution de l'exercice 6 Tout d'abord, on note que, dès lors que $n > 0$, $19 \times 8^n + 17 > 13 > 5 > 3$. On conclut en remarquant que, si $n > 0$, le nombre $19 \times 8^n + 17$ est divisible soit par 3, soit par 13, soit par 5 :

– Si $n = 2k$ est pair, alors

$$19 \times 8^n + 17 \equiv 1 \times (-1)^{2k} - 1 \equiv 1 - 1 \equiv 0 \pmod 3$$

– Si $n = 4k + 1$, alors

$$19 \times 8^{4k+1} + 17 \equiv 6 \times ((-5)^2)^{2k} \times (-5) + 4 \equiv 6 \times (-1)^{2k} \times (-5) + 4 \equiv -30 + 4 \equiv 0 \pmod{13}$$

– Si $n = 4k + 3$, alors

$$19 \times 8^{4k+3} + 17 \equiv (-1) \times (3^2)^{2k} \times 3^3 + 2 \equiv (-1) \times (-1)^{2k} \times 2 + 2 \equiv 0 \pmod 5$$

Solution de l'exercice 7 On cherche les nombres premiers qui ne divisent aucun des $2^n + 3^n + 6^n - 1$ pour n entier naturel.

2 n'en fait pas partie, car il divise $2 + 3 + 6 - 1$.

3 n'en fait pas partie non plus, car il divise $2^2 + 3^2 + 6^2 - 1$.

Soit $p \geqslant 5$ premier. 2, 3 et 6 sont premiers avec p, donc $2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod p$.

$6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) = 3 \times 2^{p-1} + 2 \times 3^{p-1} + 6^{p-1} - 6 \equiv 3 + 2 + 1 - 6 = 0 \pmod p$. Donc p divise $6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1)$, et comme p est premier avec 6, p divise $2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

Il n'existe pas de nombre premier qui ne divise aucun des $2^n + 3^n + 6^n - 1$ pour n entier naturel, donc le seul entier premier avec tous les nombres de cette forme est 1.

Solution de l'exercice 8 Si $ab^2 + b + 7$ divise $a^2b + a + b$, alors il divise également $a(ab^2 + b + 7) - b(a^2b + a + b) = 7a - b^2$. Plusieurs possibilités se présentent alors à nous.

– Si $7a < b^2$, alors $0 < b^2 - 7a < b^2 < ab^2 + b + 7$, donc $ab^2 + b + 7$ ne peut pas diviser $b^2 - 7a$.
– Si $7a = b^2$, donc b est divisible par 7 : on écrit $b = 7k$ puis $a = 7k^2$, et on constate que tous les couples $(7k^2, 7k)$ sont solutions.
– Si $7a > b^2$, alors $7a - b^2 > 0$ donc $ab^2 < ab^2 + b + 7 \leqslant 7a - b^2 < 7a$ et $b \leqslant 2$:
  – si $b = 1$, alors $a + 8$ doit diviser $7a - 1$, donc $7a - 1 - 7(a + 8) = -57 = -3 \times 19$ aussi : on a $a + 8 = 19$ ou $a + 8 = 57$, et réciproquement les couples $(11, 1)$ et $(49, 1)$ sont tous les deux solutions du problème ;
  – si $b = 2$, alors $4a + 9$ doit diviser $7a - 4$, donc $4(7a - 4) - 7(4a + 9) = -79$ aussi : puisque 79 est premier, on doit avoir $4a + 9 = 79$, qui n'a pas de solution entière.

Les solutions du problème sont les couples $(11, 1)$, $(49, 1)$ et $(7k^2, 7k)$ pour $k \geqslant 1$.

3 Cours/TD d'arithmétique

- Exercices -

Exercice 1

Trouver tous les entiers congrus simultanément à 1 modulo 2, à 2 modulo 3, à 3 modulo 5 et à 4 modulo 7.

Exercice 2

Montrer que pour tout entier $n \geqslant 1$, dans toute suite arithmétique de raison r (ensemble des $a_k = a + kr$ pour $k \in \mathbb{N}$, a étant un entier donné quelconque) on peut trouver n termes consécutifs $a_{K+1}, ...a_{K+n}$ tous composés (c'est-à-dire non premiers).

Exercice 3

On considère une suite (p_n) de nombres premiers définie par p_0, p_1 et pour tout $n \geqslant 1$, p_{n+1} est le plus grand facteur premier de $p_{n-1} + p_n + 100$. Montrer que cette suite est bornée (c'est-à-dire qu'il existe P tel que pour tout n, $p_n \leqslant P$).

Exercice 4

Montrer que pour tout $n \geqslant 2$, on peut trouver un ensemble $A = \{a_1, a_2, \cdots a_n\}$ de n entiers distincts tous $\geqslant 2$ tel que pour tout entier k tel que $1 \leqslant k \leqslant n$ le produit des $n-1$ entiers de A autres que a_k soit congru à 1 ou -1 modulo a_k.

Exercice 5

Soit p un nombre premier. A quelle condition existe-t-il un entier k tel que $k^2 \equiv -1 \pmod{p}$?

Exercice 6

Trouver tous les triplets d'entiers (x, y, z) tels que $x^2 + y^2 + z^2 - 2xyz = 0$.

Exercice 7

Soient a et b des entiers naturels non nuls et premiers entre eux, tels que $a \geqslant 2$. Montrer que si $a^m + b^m$ divise $a^n + b^n$, alors m divise n.

Exercice 8

Montrer qu'il n'existe aucun entier $n > 1$ tel que n divise $2^n - 1$.

Exercice 9

Trouver tous les couples d'entiers positifs (x, y) tels que : $7^x - 3 \cdot 2^y = 1$.

- Solutions -

Solution de l'exercice 1

C'est une mise en pratique immédiate du théorème chinois : $2, 3, 5, 7$ étant deux à deux premiers entre eux, puisqu'ils sont premiers, n'importe quel système d'équations : $x \equiv a \pmod{2}, x \equiv b \pmod{3}, x \equiv c \pmod{5}, x \equiv d \pmod{7}$ admet une infinité de solutions, de la forme : $x \equiv N \pmod{2 \times 3 \times 5 \times 7}$. On commence par résoudre les deux dernières équations : $x \equiv 4 \pmod{7}$ entraine $x \equiv 4, 11, 18, 25$ ou $32 \pmod{5 \times 7}$. Comme 5 et 7 sont premiers entre eux, $4, 11, 18, 25, 32$ prennent toutes les valeurs possibles modulo 5, donc une fois la valeur voulue 3 : $x \equiv 3 \pmod{5}$ et $x \equiv 4 \pmod{7}$ entraine $x \equiv 18 \pmod{35}$. Alors $x \equiv 18, 53$ ou $88 \pmod{3 \times 35}$. Parmi ces trois valeurs, une et une seule, 53, est congrue à 2 modulo 3. Donc

$x \equiv 53$ ou $203 \pmod{2 \times 105}$). Une et une seule de ces deux valeurs est congrue à 1 modulo 2, en l'occurrence 53. Ainsi, la solution du problème est : $x \equiv 53 \pmod{210}$.

Solution de l'exercice 2

C'est une conséquence du théorème chinois. Pour prouver que des nombres sont non premiers, il suffit de leur trouver des diviseurs. Par exemple, n nombres premiers distincts, donc premiers entre eux deux à deux, $p_1, p_2, \cdots p_n$. On cherchera donc x tel que $x+r$ divisible par p_1, $x+2r$ divisible par $p_2, \cdots x+nr$ divisible par p_n, ce qui peut s'écrire : $x \equiv -r \pmod{p_1}$, $x \equiv -2r \pmod{p_2}, \cdots x \equiv -nr \pmod{p_n}$. Le théorème chinois affirme qu'il existe une infinité de tels x, qui peuvent s'écrire : $x \equiv R \pmod{p_1 p_2 \cdots p_n}$. Mais encore faut-il que ce x soit dans la suite arithmétique donnée, donc que $x = a + kr$, ou encore $x \equiv a \pmod{r}$. Si l'on a choisi nos p_i tous premiers avec r, nous avons une nouvelle application du théorème chinois, qui fournit une infinité de tels x sous la forme : $x \equiv Q \pmod{r \times p_1 p_2 \cdots p_n}$. Et il reste une dernière chose à vérifier : que $x + r$ n'est pas égal à p_1 ni $x + 2r$ à p_2 ni $x + nr$ à p_n. Il suffit pour cela que x soit plus grand que tous les p_i, par exemple qu'il soit plus grand que leur produit : parmi les $x \equiv Q \pmod{rp_1 \cdots p_n}$, si $Q > 0$, tous les $krp_1 \cdots p_n + Q$ pour $k \geqslant 1$ sont largement assez grands pour que le risque soit exclu.

Solution de l'exercice 3

L'idée est de prouver que ces nombres premiers ne croissent que de manière limitée, et qu'à un moment ils se trouveront face à une succession de nombres non premiers qu'ils ne parviendront pas à franchir.

Tout d'abord, ce n'est pas p_n qui croît de manière limitée, mais $b_n = \max(p_n, p_{n-1})$. Par ailleurs, soit l'un des deux nombres premiers p_n ou p_{n-1} est égal à 2, auquel cas p_{n+1} est le plus grand facteur premier de $b_n + 2 + 100$, soit les deux nombres premiers p_n et p_{n+1} sont tous deux impairs, auquel cas $p_{n-1} + p_n + 100$ est pair et distinct de 2, son plus grand facteur premier est au plus la moitié : $\frac{p_{n-1}+p_n+100}{2} \leqslant b_n + 50$ car par hypothèse p_n et p_{n-1} sont tous deux inférieurs ou égaux à b_n. Dans tous les cas, $b_{n+1} \leqslant b_n + 102$.

Or il n'est pas difficile de trouver une plage de 102 nombres consécutifs tous composés : par exemple, $103! + 2$ est divisible par 2, $103! + 3$ est divisible par 3, $\cdots 103! + 103$ est divisible par 103. Mais encore faut-il initialiser la récurrence : rien ne prouve que $b_1 \leqslant 103! + 1$.

On peut néanmoins affirmer qu'il existe un k tel que $b_1 \leqslant k \cdot 103! + 1$. Et l'hypothèse de récurrence que nous utiliserons est que pour tout n, $b_n \leqslant k \cdot 103! + 1$. C'est manifestement vrai pour $n = 1$ (initialisation), et si c'est vrai pour n donné, la relation ci-dessus entraîne que $b_{n+1} \leqslant b_n + 102 \leqslant k \cdot 103! + 103$. Or b_{n+1} est par définition un nombre premier, et aucun des nombres $k \cdot 103! + 2$, $k \cdot 103! + 3, \cdots k \cdot 103! + 103$ n'est premier, donc nécessairement $b_{n+1} \leqslant k \cdot 103! + 1$, ce qui achève la démonstration.

Solution de l'exercice 4

Démontrons-le par récurrence : pour $n = 2$ (initialisation), l'ensemble $A_2 = \{2, 3\}$ convient, puisque $2 \equiv -1 \pmod{3}$ et $3 \equiv 1 \pmod{2}$. Supposons donc qu'un tel ensemble existe avec n éléments, $A_n = \{a_1, a_2 \cdots a_n\}$ et construisons l'ensemble A_{n+1} en ajoutant un $(n+1)$–ième élément a_{n+1} à A_n. Pour que la condition de l'énoncé soit remplie, a_{n+1} doit être congru à 1 ou -1 modulo $a_1 a_2 \cdots a_n$, on choisira donc : soit $a_{n+1} = (a_1 a_2 \cdots a_n) + 1$ soit $a_{n+1} = (a_1 a_2 \cdots a_n) - 1$. Ces deux valeurs conviennent toutes les deux, car si l'on considère un élément a_k pour $1 \leqslant k \leqslant n$, par hypothèse de récurrence le produit des $(n-1)$ éléments de A_n autres que a_k est congru à 1 ou -1 modulo a_k, et a_{n+1} est lui aussi congru à 1 ou -1 modulo a_k, donc le produit des n éléments de A_{n+1} autres que a_k est bien congru à 1 ou -1 modulo a_k.

Solution de l'exercice 5

Trouver une condition nécessaire et suffisante exige des outils mathématiques que vous n'avez pas, mais vous pouvez au moins trouver une condition nécessaire. Si $k^2 \equiv -1 \pmod p$, $k^4 \equiv 1 \pmod p$, donc l'ordre de k - plus petit exposant n tel que $k^n \equiv 1 \pmod p$ - divise 4. Si $-1 \neq 1 \pmod p$, donc si $p \neq 2$ (pour $p = 2$, la condition est vérifiée), cet ordre n'est pas 2 car $k^2 \equiv -1 \pmod p$, ce n'est a fortiori pas 1 car si $k \equiv 1 \pmod p$, on aurait $k^2 \equiv 1 \pmod p$, donc c'est nécessairement 4. Or tout autre n tel que $k^n \equiv 1 \pmod p$ est divisible par l'ordre 4 de k : sinon, on aurait $n = 4k + r$ avec $0 \leqslant r < 4$ et $k^r \equiv 1 \pmod p$ ce qui contredirait la minimalité. Par ailleurs, d'après le théorème de Fermat, comme k n'est pas divisible par p (sinon on aurait $k^2 \equiv 0 \pmod p$ -, $k^{p-1} \equiv 1 \pmod p$, ce qui entraîne que $p - 1$ est divisible par 4. Une condition nécessaire est donc que $p = 2$ ou $p \equiv 1 \pmod 4$.

Donnons un aperçu de la preuve que cette condition est suffisante. On travaille dans l'ensemble des classes de congruence modulo p : a et b sont dans la même classe si $a \equiv b \pmod p$. Cet ensemble de classes, $\mathbb{Z}/p\mathbb{Z}$, est muni d'une addition et d'une multiplication, car si $a \equiv b \pmod p$ et $a' \equiv b' \pmod p$, $a + a' \equiv b + b' \pmod p$ et $aa' \equiv bb' \pmod p$. Les éléments k et $-k$ ont même carré : les "carrés parfaits" (on les appelle : résidus quadratiques) de $\mathbb{Z}/p\mathbb{Z}$ sont donc 0 et au plus la moitié des $p-1$ autres éléments. En réalité, c'est exactement la moitié des $p - 1$ autres éléments, et un entier donné, par exemple -1, a "une chance sur deux" d'être résidu quadratique (pour environ la moitié des nombres premiers, -1 est résidu quadratique). Car - et c'est là qu'il conviendrait d'approfondir - l'équation $x^2 = a$ ne peut pas avoir plus de deux racines distinctes, et plus généralement un polynôme de degré d ne peut pas avoir plus de d racines distinctes, tout comme dans l'ensemble des réels par exemple. Or dans $\mathbb{Z}/p\mathbb{Z}$, l'équation : $x^{p-1} = 1$ a $p - 1$ racines distinctes : tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$. Si p est impair, et x non nul, $x^{\frac{p-1}{2}}$ a pour carré 1, il est donc égal soit à 1 soit à -1. Si x est résidu quadratique, il existe y tel que $y^2 = x$, donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$: tous les résidus quadratiques sont racines de $x^{\frac{p-1}{2}} = 1$. Mais comme il existe $\frac{p-1}{2}$ résidus quadratiques, et que cette équation de degré $\frac{p-1}{2}$ ne peut pas avoir plus de $\frac{p-1}{2}$ racines, toutes ses racines sont résidus quadratiques. Dès lors, si $(-1)^{\frac{p-1}{2}} = 1$, -1 est résidu quadratique. Or si $p \equiv 1 \pmod 4$, $(-1)^{\frac{p-1}{2}} = 1$, d'où le résultat.

Solution de l'exercice 6

Tout d'abord, puisque $x^2 + y^2 + z^2$ est pair, x, y, z ne peuvent pas être tous trois impairs : l'un au moins est pair, ce qui entraîne que $2xyz = x^2 + y^2 + z^2$ est divisible par 4. Mais modulo 4, un carré ne peut être congru qu'à 0 ou 1. Donc pour que $x^2 + y^2 + z^2 \equiv 0 \pmod 4$, il est nécessaire que x^2, y^2 et z^2 soient tous trois $\equiv 0 \pmod 4$, donc x, y, z tous trois pairs.

Montrons par récurrence que pour tout n, x, y, z doivent être tous trois multiples de 2^n. C'est vrai, nous venons de le voir, pour $n = 1$: la récurrence est initialisée. Supposons cela vrai pour $n \geqslant 1$, et posons $x = 2^n x_n$, $y = 2^n y_n$ et $z = 2^n z_n$. L'équation s'écrit : $2^{2n}(x_n^2 + y_n^2 + z_n^2) = 2^{3n+1} x_n y_n z_n$, ou encore $x_n^2 + y_n^2 + z_n^2 = 2^{n+1} x_n y_n z_n$. Comme $n \geqslant 1$, $x_n^2 + y_n^2 + z_n^2$ est divisible par 4, donc d'après le raisonnement ci-dessus, x_n, y_n et z_n sont tous les trois pairs, ce qui signifie que x, y, z sont tous trois divisibles par 2^{n+1}.

Or, un entier non nul ne peut pas être divisible par toutes les puissances de 2. Si k est l'exposant de 2 dans la décomposition en facteurs premiers de x, pour $n > k$, x n'est pas divisible par 2^n. La récurrence ci-dessus implique donc que x, y et z sont nécessairement tous trois nuls. La seule solution de l'équation est $(0, 0, 0)$.

Solution de l'exercice 7

Ecrivons la division euclidienne de n par m : $n = mq + r$ avec $0 \leqslant r < m$. Si q est impair, a^m+b^m divise $a^{qm}+b^{qm}$, donc on utilisera la relation : $a^n+b^n = a^r(a^{qm}+b^{qm})-b^{qm}(a^r-b^r)$ pour en déduire que $a^m + b^m$ doit diviser $a^r - b^r$, ce qui n'est possible que si $r = 0$ car $|a^r - b^r| < a^m + b^m$. Si q est pair, $a^m + b^m$ divise $a^{2m} - b^{2m}$, donc également $a^{qm} - b^{qm}$, et on utilisera la relation : $a^n + b^n = a^r(a^{qm} - b^{qm}) + b^{qm}(a^r + b^r)$ pour en déduire que $a^m + b^m$ doit diviser $a^r + b^r$, ce qui n'est jamais possible car $0 < a^r + b^r < a^m + b^m$. Donc $a^m + b^m$ ne peut diviser $a^n + b^n$ que si q est impair et $r = 0$, c'est-à-dire si n est multiple impair de m.

Solution de l'exercice 8

Soit p le plus petit facteur premier de n, et k l'ordre de 2 par rapport à p, c'est-à-dire le plus petit exposant non nul tel que $2^k \equiv 1 \pmod{p}$. D'après le théorème de Fermat, $k \leqslant p-1 < n$, et l'on a par ailleurs $k \geqslant 2$ car 2 n'est pas congru à 1 modulo p. Or, par hypothèse, $2^n \equiv 1 \pmod{p}$, ce qui entraîne : k divise n. k est donc un facteur de n strictement plus petit que p, ce qui contredit le fait que p est le plus petit facteur premier de n. On en conclut (raisonnement par l'absurde) qu'il n'existe aucun $n > 1$ qui divise $2^n - 1$.

Solution de l'exercice 9

Il s'agit d'une équation diophantienne, c'est-à-dire d'une équation à résoudre en nombres entiers. Certaines de ces équations diophantiennes sont parmi les problèmes les plus difficiles des mathématiques.

Ecrivons l'équation : $7^x - 1 = 3 \cdot 2^y$. On ne peut pas avoir $x = 0$ car le membre de droite ne peut pas être nul. Or pour $x \geqslant 1$, le membre de gauche est divisible par $7 - 1 = 6$. Plus précisément, après simplification par $7-1$, on trouve : $7^{x-1}+7^{x-2}+\cdots+7+1 = 2^{y-1}$. On voit là une première solution évidente : $x = 1, y = 1$. Pour $x > 1$, le membre de gauche contient x termes tous impairs, et le membre de droite est une puissance de 2 autre que 1. Donc x doit être pair, pour que la somme de gauche soit paire. On peut donc grouper les termes deux par deux et factoriser $(7 + 1)$ à gauche : $(7 + 1)(7^{x-2} + 7^{x-4} + \cdots + 49 + 1) = 8 \cdot 2^{y-4}$. D'où une deuxième solution évidente : $x = 2, y = 4$. Pour $x > 2$, après simplification par 8, le membre de gauche contient une somme de $\frac{x}{2}$ termes, tous impairs, distincte de 1 et égale à une puissance de 2, donc paire, ce qui entraîne que $\frac{x}{2}$ doit être pair, et on peut factoriser à gauche $7^2+1 = 50$: $(7^2 + 1)(7^{x-4} + 7^{x-8} + \cdots + 1) = 2^{y-4}$. Mais 50 ne peut pas diviser une puissance de 2, donc il n'existe pas de racine pour $x > 2$. Les seuls couples solution sont donc : $(1, 1)$ et $(2, 4)$.

4 Inégalités

- Réordonnement -

Cette inégalité, très utile, est relativement intuitive : c'est en multipliant les plus grands entre eux puis les plus petits entre eux avant de sommer les produits que l'on obtient le plus grand résultat.

Théorème 3.6. Soit $a_1 \leqslant \cdots \leqslant a_n$ et $b_1 \leqslant \cdots \leqslant b_n$ des suites de réels, et σ une permutation de $\{1, \cdots, n\}$. Alors la somme

$$S(\sigma) = \sum_{i=1}^{n} a_i b_{\sigma(i)}$$

est maximale lorsque σ est l'identité, et minimale lorsque pour tout i, $\sigma(i) = n+1-i$. C'est-à-dire que si on veut la plus grande somme possible, il faut ranger les deux suites dans le même ordre, et dans l'ordre contraire si on veut l'inverse.

Démonstration. Il existe un nombre fini de permutations, donc il y en a bien une pour laquelle S sera maximale. Si pour un certain couple (i,j) on a $i < j$ et $\sigma(i) > \sigma(j)$, alors soit σ' la permutation qui est identique à σ sur $\{1,\cdots,n\}$ et qui envoie i sur $\sigma(j)$ et inversement. Il est clair que

$$(a_i - a_j)(b_{\sigma(i)} - b_{\sigma(j)}) \leqslant 0$$

donc que

$$a_i b_{\sigma(i)} + a_j b_{\sigma(j)} \leqslant a_i b_{\sigma'(i)} + a_j b_{\sigma'(j)}$$

Alors $S(\sigma) \leqslant S(\sigma')$. On en conclut que $S(\sigma)$ sera maximale pour σ l'identité. Le raisonnement pour trouver le minimum de S est bien sûr similaire. □

Ceci permet de démontrer une inégalité bien utile :

Théorème 3.7. Inégalité de Tchebycheff
Avec les notations précédentes,

$$a_1 b_1 + \cdots + a_n b_n \geqslant \frac{(a_1 + \cdots + a_n)(b_1 + \cdots + b_n)}{n}$$

En effet, on a pour tout i :

$$a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \geqslant a_{1+i} b_1 + a_{2+i} b_2 + \cdots + a_i b_n$$

par l'inégalité du réordonnement. Il suffit alors de sommer les n inégalités obtenues pour avoir le résultat.
Quelques exemples d'application sont les bienvenus.

Exemple 3.8. Soit $x_1 \leqslant \cdots \leqslant x_n$ et $y_1 \leqslant \cdots \leqslant y_n$ des réels, et $z_1,\cdots,z_n$ une permutation quelconque des y_i, montrer que

$$\sum_{i=1}^{n} (x_i - y_i)^2 \leqslant \sum_{i=1}^{n} (x_i - z_i)^2$$

Exemple 3.9. Montrer que pour tous réels positifs a, b, c,

$$a^3 + b^3 + c^3 \geqslant 3abc$$

On peut d'ailleurs généraliser...

- Cauchy-Schwarz -

Théorème 3.10. Soit $a_1,\cdots,a_n$ et $b_1,\cdots,b_n$ des réels, on a

$$(a_1 b_1 + \cdots + a_n b_n)^2 \leqslant (a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) \tag{V.1}$$

avec égalité ssi les suites sont "proportionnelles" (a_i/b_i est constant).

Démonstration. On évalue le discriminant du polynôme du second degré

$$p(x) = (a_1x + b_1)^2 + \cdots + (a_nx + b_n)^2$$

qui est positif sur $\mathbb{R}$ donc a au plus une racine. □

Cette inégalité est très souvent d'un bon secours, bien plus qu'on ne l'imagine :

Axiome 1. Tout problème d'inégalités d'Olympiades admettant au moins trois solutions différentes possède une solution où Cauchy-Schwarz joue un rôle important.

Exemple 3.11. Montrer l'inégalité entre la moyenne arithmétique et la moyenne quadratique : pour $n \in \mathbb{N}^*$, si $a_1, \cdots, a_n \in \mathbb{R}^+$,

$$\frac{a_1 + \cdots + a_n}{n} \leqslant \sqrt{\frac{a_1^2 + \cdots + a_n^2}{n}}$$

Exemple 3.12. Montrer l'inégalité entre la moyenne arithmétique et la moyenne harmonique : pour $n \in \mathbb{N}^*$, si $a_1, \cdots, a_n \in \mathbb{R}^+$,

$$\frac{n}{\frac{1}{a_1} + \cdots \frac{1}{a_n}} \leqslant \frac{a_1 + \cdots + a_n}{n}$$

Exemple 3.13. Soit $a_1, \cdots, a_n$ des réels positifs de somme 1,. Trouver le minimum de $a_1^2 + \cdots + a_n^2$.

Remarque 3.14. Il ne faut ainsi pas hésiter à chercher des cas particuliers, par exemple lorsque tous les a_i sont égaux.

- Exercices -

Exercice 1 Soit $a_1, \cdots, a_n$ des entiers strictement positifs tous différents. Montrer que

$$\sum_{i=1}^{n} \frac{a_i}{i^2} \geqslant \sum_{i=1}^{n} \frac{1}{i}$$

(IMO 1978)

Exercice 2 Soit $a, b, c > 0$, montrer que

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} \geqslant \frac{3}{2}$$

(Inégalité de Nesbitt)

Exercice 3 Soit $a_1, \cdots, a_n$ des réels strictement positifs, et $a_{n+1} = a_1$. Montrer que

$$\sum_{i=1}^{n} \frac{a_i^2}{a_{i+1}} \geqslant \sum_{i=1}^{n} a_i.$$

(Olympiades chinoises 1984)

Exercice 4 Soient $a, b, c, d, e \in \mathbb{R}^+$ tels que $a+b+c+d+e = 8$ et $a^2+b^2+c^2+d^2+e^2 = 16$. Quelle est la valeur maximale de e ? (Olympiades américaines, 1992)

Exercice 5 Soit $a_1, \cdots, a_n$ et $b_1, \cdots, b_n$ des suites de réels. Montrer :

$$\sum_{i=1}^{n} a_i \sum_{i=1}^{n} b_i \sum_{i=1}^{n} \frac{1}{a_i b_i} \geqslant n^3$$

(D'après IMO 1969)

Exercice 6 Soit a, b, c les longueurs d'un triangle, montrer que :

$$a^2b(a-b) + b^2c(b-c) + c^2a(c-a) \geqslant 0$$

(IMO 1983)

Exercice 7 Soit $n \geqslant 3$ et $a_1, \cdots, a_n$ des réels strictement positifs tels que :

$$(a_1^2 + \cdots + a_n^2)^2 > (n-1)(a_1^4 + \cdots + a_n^4)$$

Montrer que pour tout triplet (a_i, a_j, a_k) tel que i, j, k soient distincts correspond aux longueurs des côtés d'un triangle non dégénéré. (ITYM 2011)

Exercice 8 Soit $x, y, z > 1$ tels que $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$. Montrer :

$$\sqrt{x+y+z} \geqslant \sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1}$$

(Shortlist IMO 2000)

- Solutions -

Solution de l'exercice 1
Notons $b_1, \cdots, b_n$ le réordonnement de la suite (a_i) dans l'ordre croissant. La suite $\left(\frac{1}{i^2}\right)$ est rangée dans l'ordre décroissant, donc d'après l'inégalité du réordonnement :

$$\sum_{i=1}^{n} \frac{a_i}{i^2} \geqslant \sum_{i=1}^{n} \frac{b_i}{i^2}$$

Le fait que la suite (b_i) soit strictement croissante (les a_i sont distincts) et à valeurs entières permet d'affirmer que $b_i \geqslant i$ pour tout i, d'où le résultat.

Solution de l'exercice 2
Sans restriction, supposons $a \geqslant b \geqslant c$. En appliquant deux fois l'inégalité du réordonnement :

$$\frac{c}{a+b} + \frac{b}{a+c} + \frac{a}{c+b} \geqslant \frac{b}{a+b} + \frac{a}{a+c} + \frac{c}{c+b}$$

$$\frac{c}{a+b} + \frac{b}{a+c} + \frac{a}{c+b} \geqslant \frac{a}{a+b} + \frac{c}{a+c} + \frac{b}{c+b}$$

Il suffit alors d'additionner les deux inégalités pour obtenir la formule cherchée.

Solution de l'exercice 3
On peut procéder par réordonnement, en remarquant que les suites (a_i^2) et $(1/a_i)$ sont triées en ordre contraire, ce qui permet de majorer le terme de droite par celui de gauche.
On peut également utiliser Cauchy-Schwarz :

$$\left(\sum_{i=1}^{n} a_i\right)^2 = \left(\sum_{i=1}^{n} \sqrt{a_{i+1}}\frac{a_i}{\sqrt{a_{i+1}}}\right)^2 \leqslant \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} \frac{a_i^2}{a_{i+1}}\right)$$

Solution de l'exercice 4
On applique Cauchy-Schwarz aux suites (a, b, c, d) et $(1, 1, 1, 1)$:

$$(8-e)^2 \leqslant 4 \times (16-e^2)$$

d'où l'on tire $5e^2 \leqslant 16e$ et finalement $0 \leqslant e \leqslant \frac{16}{5}$. Et, cette valeur de e convient (on a alors $a = b = c = d = \frac{6}{5}$, qui est bien sûr le cas d'égalité de Cauchy-Schwarz).

Solution de l'exercice 5
Par souci de simplicité, les bornes des sommes sautent joyeusement (ce sont toujours les mêmes). Avec trois sommes au lieu de deux, appliquer mécaniquement Cauchy-Schwarz une fois ne suffit pas. Mais ter repetita placent, et on va donc l'utiliser trois fois :

$$\sum a_i \sum b_i \geqslant \left(\sum \sqrt{a_i b_i}\right)^2$$

qui est la manière classique. Et, avec un cas particulier bien connu maintenant :

$$\sum \frac{1}{a_i b_i} \geqslant \frac{1}{n}\left(\sum \frac{1}{\sqrt{a_i b_i}}\right)^2.$$

La troisième fois reprend l'exemple : on pose $c_i = \sqrt{a_i b_i}$ et on obtient

$$\sum c_i \sum \frac{1}{c_i} \geqslant n^2,$$

ce qui permet de conclure.

Solution de l'exercice 6
Bon d'accord, il y a une solution très rapide : on réécrit l'inégalité sous la forme :
$a(b-c)^2(b+c-a)+b(a-b)(a-c)(a+b-c) \geqslant 0$ et on peut supposer $a \geqslant b \geqslant c$, le résultat en découle.
Mais on peut aussi utiliser Cauchy-Schwarz...Si l'on se représente le triangle a, b, c avec son cercle inscrit et ses bissectrices, on peut écrire $a = y + z, b = x + z, c = x + y$ où x, y, z sont des réels positifs (on a $x = \frac{b+c-a}{2}$, etc.). Ceci est souvent utile en géométrie, et transforme l'inégalité en

$$x^3z + z^3y + y^3x \geqslant x^2yz + y^2xz + z^2xy$$

En divisant par xyz et multipliant par $x + y + z$, on obtient :

$$(x+y+z)^2 \leqslant (x+y+z)\left(\frac{x^2}{y} + \frac{y^2}{z} + \frac{z^2}{x}\right)$$

et Cauchy-Schwarz s'applique aux suites $\sqrt{y}, \sqrt{z}, \sqrt{x}$ et $\frac{x}{\sqrt{y}}, \frac{y}{\sqrt{z}}, \frac{z}{\sqrt{x}}$.

Solution de l'exercice 7
Le cas $n = 3$ se traite à part. Sans restriction, $a_1 \geqslant a_2 \geqslant a_3$. L'inégalité se réécrit :

$$(a_1 + a_2 + a_3)(a_1 + a_2 - a_3)(a_2 + a_3 - a_1)(a_3 + a_1 - a_2) > 0$$

dont trois facteurs sont évidemment positifs, d'où $a_1 < a_2 + a_3$, ce qui correspond bien à l'inégalité triangulaire.
Pour $n \geqslant 4$, montrons sans restriction le résultat pour (a_1, a_2, a_3). Par inégalité de Cauchy-Schwarz,

$$(n-1)\left(\frac{a_1^4 + a_2^4 + a_3^4}{2} + \frac{a_1^4 + a_2^4 + a_3^4}{2} + \sum_{k=4}^{n} a_k^4\right) \geqslant \left(\sqrt{2(a_1^4 + a_2^4 + a_3^4)} + \sum_{k=4}^{n} a_k^2\right)^2$$

donc, d'après l'énoncé,

$$(a_1^2 + \cdots + a_n^2)^2 > \left(\sqrt{2(a_1^4 + a_2^4 + a_3^4)} + \sum_{k=4}^{n} a_k^2\right)^2$$

et on en déduit $a_1^2 + a_2^2 + a_3^2 > \sqrt{2(a_1^4 + a_2^4 + a_3^4)}$, ce qui rejoint le cas $n = 3$.

Solution de l'exercice 8
D'après Cauchy-Schwarz,

$$(x + y + z)\left(\frac{x-1}{x} + \frac{y-1}{y} + \frac{z-1}{z}\right) \geqslant (\sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1})^2$$

Or $\frac{x-1}{x} + \frac{y-1}{y} + \frac{z-1}{z} = 3 - \frac{1}{x} - \frac{1}{y} - \frac{1}{z} = 1$ d'après l'énoncé, ce qui permet de conclure.

4 Groupe D

1 Cours de combinatoire : graphes finis et infinis

Dans ce cours, nous verrons principalement deux grands résultats sur les graphes : le théorème des mariages de Hall et le théorème de Ramsey. Le premier résultat nous informe que, dans un graphe biparti contenant *beaucoup* d'arêtes, il est possible d'apparier les sommets du graphe. Le second, quant à lui, concerne les grands graphes complets bicolores, dont on peut extraire de *pas si grands* graphes complets monochromatiques.

Dans chaque cas, on étudiera l'extension de ces résultats à des graphes *infinis* : quels théorèmes s'appliquent naturellement aux graphes infinis ? Et sous quelle forme ? En effet, comme on peut s'y attendre, deux énoncés équivalents sur les graphes finis ne le sont plus nécessairement sur les graphes infinis.

- Théorème des mariages de Hall -

Théorème 4.1 (Théorème des mariages de Hall)**.** Soit $\mathcal{G} = (A \cup B, E)$ un graphe biparti fini, dont les deux composantes indépendantes sont A et B, et dont les arêtes forment l'ensemble E. À tout sous-ensemble X de A, on associe le sous-ensemble $E(X) = \{b \in B : \exists a \in X, (a, b) \in E\}$ des sommets de B reliés à au moins un sommet de X. Les deux propositions suivantes sont équivalentes :

1. il existe injection $f : A \to B$ telle que chaque paire $(a, f(a))$ soit une arête appartenant effectivement à E — on appelle une telle fonction un *couplage saturant* de A ;
2. pour toute partie $X \subseteq A$, $|E(X)| \geqslant |X|$.

Démonstration. Avant l'effort, le réconfort : montrons d'abord que la proposition 1 implique la proposition 2. Pour ce faire, supposons que la proposition 1 est bien vérifiée. On considère alors une partie $X \subseteq A$, et $f : A \to B$ un couplage saturant. Alors $f(X) \subseteq E(X)$, de sorte que $|E(X)| \geqslant |f(X)| = |X|$, donc que la proposition 2 est vérifiée aussi.

Passons maintenant à la partie difficile : comme souvent en théorie des graphes, on va procéder par récurrence (même s'il existe d'autres manières de procéder, la littérature étant abondante sur ce sujet) et montrer que la proposition 2 implique la proposition 1. Tout d'abord, notons que le résultat est évident si $|A| = 1$. On suppose donc que $|A| \geqslant 2$, et on distingue deux cas :

- Si tout sous-ensemble *propre* X de A (c'est-à-dire tel que $\emptyset \subsetneq X \subsetneq A$) est tel que $|E(X)| \geqslant |X|+1$, alors on apparie au hasard un sommet $a \in A$ et un sommet $b \in B$ tel que $(a, b) \in E$ et on décide que $f(a) = b$. Le graphe $\mathcal{G}'$ induit par les sommets $A \cup B \setminus \{a, b\}$ est un sous-graphe strict de $\mathcal{G}$, et satisfait la proposition 2, donc l'hypothèse de récurrence indique qu'on peut apparier ses sommets sans encombre. Ce faisant, on a apparié l'ensemble des sommets de $\mathcal{G}$.
- Si A admet un sous-ensemble *propre* X tel que $|E(X)| = |X|$, considérons les graphes $\mathcal{G}'$ et $\mathcal{G}''$, respectivement induits par les sommets $X \cup E(X)$ et $(A \cup B) \setminus (X \cup E(X))$: ce sont deux sous-graphes stricts de $\mathcal{G}$, et il est clair que $\mathcal{G}'$ satisfait la proposition 2. En outre, si X' est une partie de $A \setminus X$, soit $Y = E(X') \setminus E(X)$. Alors $E(X \cup X') = E(X) \cup Y$, donc $|Y| = |E(X \cup X')| - |E(X)| \geqslant |X \cup X'| - |X| = |X'|$: cela signifie que $\mathcal{G}''$ satisfait également la proposition 2. On peut donc apparier les éléments de $X \cup E(X)$, ainsi que les ceux de $(A \cup B) \setminus (X \cup E(X))$, montrant ainsi que la proposition 1 est vérifiée.

Les propositions 1 et 2 s'impliquant l'une l'autre, elles sont bien équivalentes. □

On peut également reformuler le théorème des mariages de Hall de manière plus imagée comme suit : supposons que l'on veut marier n filles à n garçons, de manière à ce que chaque individu aime bien son époux(se). Cela nous est possible si et seulement si, dès qu'on prend un groupe de k filles, l'ensemble des garçons qu'aime bien au moins une des filles de groupe est de cardinal k ou plus.

Exercice 1 Sur une planète extrasolaire vit une espèce alien dont la population est composée de 3 sexes : les hommes, les femmes et les matheux. Une famille épanouie consiste en l'union de 3 personnes, une de chaque sexe, qui s'aiment toutes mutuellement. En outre, l'amitié est réciproque : si x aime y, alors y aime x.

Cette espèce veut envoyer n individus de chaque sexe coloniser l'espace, et souhaiterait former autant de familles épanouies que possible avec ces $3n$ personnes. La seule information dont on dispose est que chaque individu aime au moins k personnes de chacun des deux autres sexes :

1. Montrer que, si $n = 2k$, il se peut que l'on ne puisse former aucune famille épanouie.
2. Montrer que, si $4k \geqslant 3n$, il est possible de former n familles épanouies disjointes.

Une fois le théorème des mariages de Hall prouvé pour tous les graphes bipartis finis, une question naturelle se pose : qu'arrive-t-il si on considère un graphe biparti infini dénombrable ? La difficulté est que l'on peut écrire le théorème de plusieurs manières différentes, qui seront équivalentes si l'on regarde un graphe fini, mais ne le seront pas si l'on regarde un graphe infini. Si on s'y prend de manière naïve, en effet, on fait chou blanc :

Exercice 2 (Théorème *infini* des mariages de Hall — extension naïve) Soit $\mathcal{G} = (A \cup B, E)$ un graphe biparti infini dénombrable, dont les deux composantes A et B sont infinies. À tout sous-ensemble X de A, on associe le sous-ensemble $E(X) = \{b \in B : \exists a \in X, (a, b) \in E\}$ des sommets de B reliés à au moins un sommet de X. Montrer que les deux propositions suivantes ne sont *pas* équivalentes :

1. il existe un couplage saturant $f : A \to B$;
2. pour toute partie finie $X \subseteq A$, $E(X)$ est infini, ou bien de cardinal $|E(X)| \geqslant |X|$.

Cela dit, il est toujours possible d'étendre le théorème de manière moins naïve, et alors nos efforts seront couronnés de succès. En particulier, si on oblige le graphe $\mathcal{G}$ à n'avoir que des sommets de degré fini, alors tout se passe bien :

Exercice 3 (Théorème *infini* des mariages de Hall — extension moins naïve) Soit $\mathcal{G} = (A \cup B, E)$ un graphe biparti infini dénombrable, dont les deux composantes A et B sont infinies, et dont tout sommet est de degré fini. À tout sous-ensemble X de A, on associe le sous-ensemble $E(X) = \{b \in B : \exists a \in X, (a, b) \in E\}$ des sommets de B reliés à au moins un sommet de X. Montrer que les deux propositions suivantes sont équivalentes :

1. il existe un couplage saturant $f : A \to B$;
2. pour toute partie finie $X \subseteq A$, $E(X)$ est de cardinal $|E(X)| \geqslant |X|$.

Exercice 4 Soit $\mathcal{G} = (A \cup B, E)$ un graphe biparti dont les deux composantes indépendantes, A et B, sont infinies dénombrables. On suppose que tout sommet est de degré fini non nul et que, pour toute arête $(a, b) \in E$ avec $a \in A$ et $b \in B$, $\deg(a) = \deg(b)$. Montrer qu'il existe un couplage saturant bijectif $f : A \to B$.

- Théorèmes de coloriage -

Théorème 4.2 (Théorème de Ramsey bicolore)**.** Soit g, r et b trois entiers naturels non nuls tels que $g \geqslant \binom{r+b-2}{r-1}$. Alors tout graphe complet K_g dont les arêtes sont coloriées en rouge et bleu contient soit un sous-graphe K_r dont les arêtes sont coloriées en rouge, soit un sous-graphe K_b dont les arêtes sont coloriées en bleu.

Démonstration. On procède par récurrence sur r et b. Tout d'abord, si $r = 1$ ou $b = 1$, le résultat est évident (vu que le graphe K_1 ne comporte aucune arête).

Ensuite, si $r \geqslant 2$ et $b \geqslant 2$, considérons un sommet v du graphe K_g. v est appartient à $g - 1 \geqslant \binom{r+b-2}{r-1} - 1 = \binom{r+b-3}{r-2} + \binom{r+b-3}{r-1} - 1$ arêtes, donc soit v appartient à au moins $\binom{r+b-3}{r-2}$ arêtes rouges, soit v appartient à au moins $\binom{r+b-3}{r-1}$ arêtes bleues.

- Si v est relié à $R \geqslant \binom{r+b-3}{r-2}$ sommets par des arêtes rouges, on considère le sous-graphe K_R formé par ces R sommets. Par hypothèse de récurrence, K_R contient soit un sous-graphe K_b dont les arêtes sont bleues (et a fortiori K_g contient K_b), soit un sous-graphe K_{r-1} dont les arêtes sont rouges ; dans ce second cas, en adjoignant le sommet v au graphe K_{r-1}, on obtient bien un sous-graphe K_r du graphe K_n, et dont les arêtes sont rouges.
- Si v est relié à $B \geqslant \binom{r+b-3}{r-1}$ sommets par des arêtes bleues, alors, pour exactement les mêmes raisons, K_g contient soit un sous-graphe K_r dont les arêtes sont rouges, soit un sous-graphe K_b dont les arêtes sont bleues.

Dans tous les cas, on en déduit que K_g contient effectivement soit un sous-graphe K_b dont les arêtes sont bleues, soit un sous-graphe K_r dont les arêtes sont rouges. Ceci clôt notre récurrence, et donc la preuve du théorème. □

Intuitivement, le théorème de Ramsey dit que, pour obtenir soit un graphe complet K_r avec des arêtes rouges, soit un graphe complet K_b avec des arêtes bleues, il suffit de colorier en rouge et bleu les arêtes d'un très gros graphe complet. En particulier, on peut s'intéresser à l'entier minimal $R_2(r, b)$ tel que tout graphe complet bicolore K_g avec $g \geqslant R_2(r, b)$ contient un de nos graphes K_r ou K_b. Le nombre $R_2(r, b)$ est appelé *nombre de Ramsey bicolore*.

En outre, on peut étendre le théorème de Ramsey au cas où on colorie les arêtes du graphe K_g avec n couleurs au lieu de 2 : il existe un entier minimal $R_n(s_1, \dots, s_n)$, appelé *nombre de Ramsey à n couleurs*, tel que tout graphe complet n-colore K_g avec $g \geqslant R_n(s_1, \dots, s_n)$ contient un graphes K_{s_i} monochrome :

Exercice 5 (Théorème de Ramsey à n couleurs)**.** On considère $n \geqslant 2$ couleurs $C_1, \dots, C_n$ et n entiers naturels $s_1 \geqslant \cdots \geqslant s_n \geqslant 2$. Soit

$$g \geqslant \frac{n}{n-1} \frac{(s_1 + \cdots + s_n - 2n)!}{(s_1 - 2)! \dots (s_n - 2)!} \prod_{j=1}^{n-1} (s_j - 1)$$

un entier naturel, et K_g un graphe complet à g sommets dont on a colorié les arêtes avec les n couleurs ci-dessus. Montrer qu'il existe un entier i tel que K_g contient un sous-graphe complet K_{s_i} à s_i sommets dont toutes les arêtes sont de couleur C_i.

Cette généralisation à n couleurs permet de résoudre de multiples problèmes, par exemple en théorie des nombres :

Exercice 6 (Théorème de Schur)**.** Soit $(P_1, \dots, P_n)$ une partition de l'ensemble $\mathbb{N}^*$ des entiers naturels non nuls. Montrer qu'il existe un ensemble P_i et deux éléments $x, y \in P_i$ tels que $x + y \in P_i$.

On peut alors s'interroger sur la généralisation éventuelle de ce théorème à des graphes infinis : si on colorie en bleu et rouge les arêtes d'un graphe infini, obtient-on une composante bleue ou rouge infinie ? La réponse est oui !

Exercice 7 (Théorème *infini* de Ramsey)**.** Soit K_∞ un graphe complet infini dont on colorie les arêtes avec k couleurs. Alors K_∞ contient un sous-graphe complet infini dont les arêtes sont toutes de la même couleut.

De manière générale, les résultats sur le coloriage des graphes se montrent bien en utilisant des notions de *compacité* : si on dispose d'un coloriage *local* des sommets ou des arêtes d'un graphe, on peut l'étendre peu à peu en un coloriage de plus en plus grand, jusqu'à colorier toute partie finie du graphe, et finalement le graphe lui-même.

Exercice 8 On admet que tout graphe planaire fini admet un coloriage de ses sommets en bleu, rouge, vert tel que nul cycle de longueur impaire ne soit monochrome. Montrer que ce résultat s'étend aux graphes planaires infinis dénombrables.

- Solutions des exercices -

Solution de l'exercice 1 On traite les questions l'une après l'autre.

1. On identifie l'ensemble des $3n = 6k$ individus au produit cartésien $\{F, H, M\} \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z})$ — les triplets (F, i, j) représentent les femmes, les paires (H, i, j) les hommes, les paires (M, i, j) les matheux. Supposons alors que chaque femme (F, i, x) aime uniquement les hommes (H, i, y) et les matheux (M, i, y) et que chaque homme (H, i, x) aime uniquement les femmes (F, i, y) et les matheux $(M, i + 1, y)$ — où (i, x, y) décrit l'ensemble $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z})^2$. On a ici une configuration où chacun aime k personnes des deux autres sexes, mais où nulle famille épanouie ne peut exister.
2. On va appliquer deux fois successivement le théorème des mariages de Hall. On introduit d'abord le graphe $\mathcal{G} = (F \cup H, E)$ dont les arêtes sont les paires (f, h) telles que f aime h. Soit $X \subseteq F$ un ensemble non vide de femmes, et $E(X)$ l'ensemble des hommes aimés par au moins une femme $f \in X$. Si $|X| \leqslant k$, alors nécessairement $|E(X)| \geqslant k \geqslant |X|$; si $|X| > k$, alors soit h un homme quelconque. h aime au moins k femmes, et $k + |X| > 2k \geqslant n$, de sorte que h aime au moins une femme appartenant à X, c'est-à-dire que $h \in E(X)$: dans ce deuxième cas, $|E(X)| = |H| = n \geqslant |X|$. $\mathcal{G}$ vérifie donc la propriété 2 du théorème des mariages de Hall : on peut scinder les hommes et les femmes en n couples $c_1, c_2, \ldots, c_n$ dont les deux membres s'aiment.

   Maintenant, soit C l'ensemble $\{c_1, c_2, \ldots, c_n\}$ des couples ainsi formés, et $\mathcal{G}' = (M \cup C, E')$ le graphe dont les arêtes sont les paires (m, c) telles que m aime les deux membres du couple c : on dit que m et que le couple c *s'aiment*. Soit m un matheux quelconque ; il existe au plus $n - k$ couples dont il n'aime pas la femme, et $n - k$ couples dont il n'aime pas l'homme, donc m aime au moins $2k - n$ couples. Réciproquement, soit $c = (f, h)$ un couple quelconque ; il existe au plus $n - k$ matheux que f n'aime pas, et $n - k$ mahteux que m n'aime pas, donc c aime au moins $2k - n$ matheux.

   Soit $Y \subseteq M$ un ensemble non vide de matheux, et $E'(Y)$ l'ensemble des couples aimés par au moins un matheux $m \in Y$. Si $|Y| \leqslant 2k - n$, alors nécessairement $|E'(Y)| \geqslant 2k - n \geqslant |Y|$; si $|Y| > 2k - n$, alors soit c un couple quelconque. c aime au moins $2n - k$ matheux, et $2n - k + |Y| > 4n - 2k \geqslant n$, de sorte que c aime au moins un matheux appartenant à Y, c'est-à-dire que $c \in E'(Y)$: dans ce deuxième cas, $|E(Y)| = |M| = n \geqslant |Y|$. $\mathcal{G}'$ vérifie

donc la propriété 2 du théorème des mariages de Hall : on peut scinder les matheux et les couples en n paires qui s'aiment mutuellement. Cela revient à scinder $F \cup H \cup M$ en n familles épanouies, ce qui était l'objectif de notre démonstration.

Solution de l'exercice 2 Il nous suffit de trouver un exemple de graphe satisfaisant la propriété 2 mais pas la propriété 1 : le voici. On considère le graphe $\mathcal{G} = (A \cup B, E)$ où $A = \{0\} \times \mathbb{N}$, $B = \{1\} \times \mathbb{N}$, et où $((0,i),(1,j)) \in E$ si et seulement si $i = 0$ ou $i = j+1$. Tout d'abord, si $X \subseteq A$ est une partie telle que $(0,0) \in X$, alors $E(X) = B$ est bien infini ; si $(0,0) \notin X$, alors $E(X) = \{(1,j) : (0,j+1) \in X\}$ est de même cardinal que X. Cela montre que $\mathcal{G}$ satisfait la propriété 2.

Cependant, si $f : A \to B$ est un couplage saturant, alors f envoie la paire $(0,0)$ sur une paire $(1,i)$, avec $i \in \mathbb{N}$. Mais alors f envoie également la paire $(0,i+1)$ sur la paire $(1,i)$, et ne peut être injective, ce qui contredit son caractère de couplage saturant. Ainsi, la propriété 1 n'est pas satisfaite.

Solution de l'exercice 3 Tout d'abord, la propriété 1 implique, comme dans le cas du théorème des mariages *fini*, la propriété 2. On se penche donc sur le sens réciproque : soit $\mathcal{G} = (A \cup B, E)$ un graphe vérifiant la propriété 2.

On numérote alors les sommets de $A = \{a_0, a_1, \ldots\}$, puis les ensembles de sommets $A_n = \{a_0, a_1, \ldots, a_n\}$ ainsi que $E(A_n) = \{b \in B : \exists a \in A_n, (a,b) \in E\}$. On considère alors, pour chaque entier naturel n, le sous graphe $\mathcal{G}_n$ induit par les sommets $A_n \cup E(A_n)$. $\mathcal{G}_n$ est fini et satisfait la propriété 2, donc il existe un couplage saturant $f_n : A_n \to E(A_n)$.

On procède maintenant en utilisant des arguments de compacité : en utilisant le principe des tiroirs, il existe un élément b_0 voisin de a_0 tel que l'ensemble $F_0 = \{n \in \mathbb{N} : f_n(a_0) = b_0\}$ est infini. Puis il existe un élément b_1 voisin de a_1 tel que l'ensemble $F_1 = \{n \in F_0 : n \geqslant 1, f_n(a_1) = b_1\}$ est infini (et alors $b_1 \neq b_0$). On continue par récurrence, en choissant un élément b_{k+1} voisin de a_{k+1} tel que l'ensemble $F_{k+1} = \{n \in F_k : n \geqslant k+1, f_n(a_{k+1}) = b_{k+1}\}$ est infini. Ce faisant, il s'avère que la fonction $f_\infty : A \to B$ telle que $f_\infty(a_k) = b_k$ pour tout entier naturel k est bien un couplage saturant.

Solution de l'exercice 4 On montre tout d'abord que le graphe $\mathcal{G}$ satisfait le critère 2 de l'extension moins naïve du théorème des mariages de Hall : si $X \subseteq A$ est un ensemble fini, alors

$$\begin{aligned} |E(X)| &= \sum_{b \in E(X)} \frac{\deg(b)}{\deg(b)} = \sum_{a \in A, b \in E(X) : (a,b) \in E} \frac{1}{\deg(b)} \\ &\geqslant \sum_{a \in X, b \in E(X) : (a,b) \in E} \frac{1}{\deg(b)} = \sum_{a \in X} \sum_{b \in B : (a,b) \in E} \frac{1}{\deg(a)} = \sum_{a \in X} \frac{\deg(a)}{\deg(a)} = |X| \end{aligned}$$

En particulier, on en déduit l'existence d'un couplage saturant $f : A \to B$; en outre, A et B jouant des rôles symétriques, il existe également un couplage saturant $g : B \to A$.

On numérote alors les éléments de $B = \{b_0, b_1, \ldots\}$, puis on construit une suite de couplages saturants $f_n : A \to B$ tels que $\{b_0, b_1, \ldots, b_{n-1}\} \subseteq f_n(A)$. On part de $f_0 = f$, puis on procède comme suit : si $b_n \in f_n(A)$, alors $f_{n+1} = f_n$; si $b_n \notin f_n(A)$, les choses se corsent. On construit alors par récurrence la suite (u_k) telle que $u_0 = b_n$, $u_{2k+1} = g(u_{2k})$ et $u_{2k+2} = f_n(u_{2k+1})$. Notons que, puisque $f \circ g$ est injective et que $u_0 \notin f(A)$, on sait que u_0 n'est égal à aucun autre terme u_k, donc les termes u_{2k+2} sont deux à deux distincts, et les termes u_{2k+1} se retrouvent deux à deux distincts eux aussi. On définit alors $f_{n+1} : A \to B$ de sorte que $f_{n+1}(u_{2k+1}) = u_{2k}$ pour tout entier k, et $f_{n+1}(v) = f_n(v)$ si $v \notin \{u_k : k \in \mathbb{N}\}$.

Enfin, numérotons les éléments de $A = \{a_0, a_1, \ldots\}$ puis procédons par compacité : il existe un élément β_0 voisin de a_0 tel que l'ensemble $F_0 = \{n \in \mathbb{N} : f_n(a_0) = \beta_0\}$ est infini. Puis il existe un élément α_0 voisin de b_0 tel que l'ensemble $F'_0 = \{n \in \mathbb{N} : f_n(\alpha_0) = b_0\}$ est infini (on peut éventuellement avoir $a_0 = \alpha_0$). On continue par récurrence, dès lors que l'on dispose des ensembles F'_k et des points α_i, β_i tels que $i \leqslant k$: on choisit un élément β_{k+1} voisin de a_{k+1} tel que l'ensemble $F_{k+1} = \{n \in \mathbb{N} : n \geqslant k+1, f_n(a_{k+1}) = \beta_{k+1}\}$ est infini, puis un élément α_{k+1} voisin de b_{k+1} tel que l'ensemble $F'_{k+1} = \{n \in \mathbb{N} : n \geqslant k+1, f_n(\alpha_{k+1}) = b_{k+1}\}$ est infini. Notons que, ce faisant, les α_i et les β_i sont deux à deux distincts. En outre, il s'avère que la fonction $f_\infty : A \to B$ telle que $f_\infty(a_k) = \beta_k$ pour tout entier naturel k est bien un couplage saturant et bijectif.

Solution de l'exercice 5 L'idée est de procéder de la même manière que dans la preuve du théorème de Ramsey bicolore. On obtiendra alors une borne supérieure sur le nombre de Ramsey à n couleurs, borne que l'on pourra elle-même majorer pour aboutir à la relation demandée.

Tout d'abord, notons que le théorème de Ramsey à n couleurs n'a que peu d'intérêt quand $n = 1$ (on a $R_1(s_1) = s_1$) ou quand $s_n = 1$ (tout graphe à au moins 1 sommet convient). En outre, par symétrie, il est bénin de considérer uniquement les cas où $s_1 \geqslant s_2 \geqslant \cdots \geqslant s_n$. on va montrer par récurrence que la fonction R_n est bien définie, et en obtenir un majorant.

Supposons donc que l'on dispose d'un entier k tel que $R_n(s_1, \ldots, s_n)$ est bien défini dès lors que $\sum_{i=1}^n s_i \leqslant k : k = n$ est un tel entier. Montrons que $R_n(s_1, \ldots, s_n)$ est aussi défini quand $\sum_{i=1}^n s_i = k+1$. Pour cela, de deux choses l'une.

- Si $s_n = 1$, on a déjà dit que $R_n(s_1, \ldots, s_n) = 1$, qui est donc bien défini.
- Si $s_n \geqslant 2$, on va montrer que $R_n(s_1, \ldots, s_n) \leqslant g$, où $g = 2 - n + \sum_{i=1}^n R_n[s_1, \ldots, s_n]_i$, où $[s_1, \ldots, s_n]_i$ désigne le n-uplet $(s_1, \ldots, s_{i-1}, s_i - 1, s_{i+1}, \ldots, s_n)$. En effet, si K_g est un graphe complet à g sommets, on colorie ses arêtes avec de n couleurs $C_1, \ldots, C_n$, puis on choisit un sommet quelconque v de K_g. Par principe des tiroirs, il existe une couleur C_i telle que v est relié à au moins $g-1$ sommets, donc à $R_n[s_1, \ldots, s_n]_i$ sommets par des arêtes de couleur C_i : soit K' le sous-graphe induit par cet ensemble de sommets. Si K' contient un sous-graphe complet K_{s_j} de couleur C_j (avec $i \neq j$) , alors K_g contient également ce sous-graphe complet ; si K' contient un sous-graphe complet K_{s_i-1} de couleur C_i, alors en adjoignant le sommet v à ce sous-graphe, on forme un sous-graphe complet K_{s_i} de K_g, qui entièrement colorié avec C_i. Par hypothèse de récurrence, on est forcément dans un des deux cas ci-dessus : cela signifie que $R_n(s_1, \ldots, s_n)$ est bien défini, et au plus égal à g.

On déduit de tout ceci que $R_n(s_1, \ldots, s_n)$ est majoré par la fonction $S_n(s_1, \ldots, s_n)$, symétrique en ses variables, telle que

- $S_n(s_1, \ldots, s_{n-1}, 1) = 1$ et
- $S_n(s_1, \ldots, s_n) = 2 - n + \sum_{i=1}^n S_n[s_1, \ldots, s_n]_i$ si $s_1 \geqslant \cdots \geqslant s_n \geqslant 2$.

En introduisant la fonction $T_n = (n-1)S_n - (n-2)$, on obtient $T_n(s_1, \ldots, s_{n-1}, 1) = 1$ et $T_n(s_1, \ldots, s_n) = \sum_{i=1}^n T_n[s_1, \ldots, s_n]_i$ si $s_1 \geqslant \cdots \geqslant s_n \geqslant 2$.

En outre, étudions ici un objet combinatoire : les *chemins progressants* dans $\mathbb{Z}^n$: il s'agit de chemins finis où l'on passe d'un point au suivant en ajoutant 1 à une coordonnée. Le nombre de chemins progressant d'origine $(a_1, \ldots, a_n)$ et d'extrémité $(b_1, \ldots, b_n)$ est égal au coefficient multinomial $\frac{(b_1+\cdots+b_n-a_1-\cdots-a_n)!}{(b_1-a_1)!\ldots(b_n-a_n)!}$: on a simplement décidé des $b_i - a_i$ instants où l'on décidait d'augmenter la i-ème coordonnée.

La relation de récurrence sur T_n nous indique alors que $T_n(s_1, \ldots, s_n)$ est égal aux nombres

de chemins progressants de $\mathbb{Z}^n$ dont :
- l'origine a une coordonnée égale à 1 ;
- nul autre point n'a de coordonnée égale à 1 ;
- l'extrémité est le point $(s_1, \dots, s_n)$.

L'origine d'un tel chemin a donc une unique coordonnée égale à 1 : on en déduit donc que $T_n(s_1, \dots, s_n)$ est égal à la somme des $\frac{(s_1+\cdots+s_n-a_1-\cdots-a_n)!}{(s_1-a_1)!\dots(s_n-a_n)!}$, où :
- on a choisi un $i \leqslant n$ tel que $a_i = 2$;
- chaque coefficient a_j (avec $i \neq j$) est compris entre 2 et s_j.

En particulier, chacun des coefficients multinomiaux vaut au plus $\frac{(s_1+\cdots+s_n-2n)!}{(s_1-2)!\dots(s_n-2)!}$; pour chaque $i \leqslant n$, on additionne $\prod_{j\neq i}(s_j-1) \leqslant \prod_{j=1}^{n-1}(s_j-1)$ tels coefficients, soit au plus $n\prod_{j=1}^{n-1}(s_j-1)$ coefficients multinomiaux au total.

Il s'ensuit que $T_n(s_1, \dots, s_n) \leqslant n\frac{(s_1+\cdots+s_n-2n)!}{(s_1-2)!\dots(s_n-2)!}\prod_{j=1}^{n-1}(s_j-1)$. Or, $R_n(s_1, \dots, s_n)$ est un entier tel que

$$R_n(s_1, \dots, s_n) \leqslant S_n(s_1, \dots, s_n) = \frac{T_n(s_1, \dots, s_n)+n-2}{n-1} < 1 + \frac{1}{n-1}T_n(s_1, \dots, s_n).$$

Cela montre que, si g est un entier tel que

$$g \geqslant \frac{1}{n-1}T_n(s_1, \dots, s_n) = \frac{n}{n-1}\frac{(s_1+\cdots+s_n-2n)!}{(s_1-2)!\dots(s_n-2)!}\prod_{j=1}^{n-1}(s_j-1),$$

alors $g \geqslant R_n(s_1, \dots, s_n)$, ce qui conclut l'exercice.

Solution de l'exercice 6 On considère le nombre de Ramsey à n couleurs $R_n(3, 3, \dots, 3)$, que l'on notera R dans la suite. Soit alors le graphe complet K_R dont les sommets sont les entiers $\{0, 1, \dots, R-1\}$. on en colorie les arêtes avec n couleurs $C_1, C_2, \dots, C_n$: on colorie l'arête (i, j) avec la couleur C_k telle que $|i-j| \in P_k$. Alors, par définition du nombre de Ramsey à n couleurs, K_R admet un triangle monochromatique : on suppose, sans perte de généralité, que ses arêtes sont de couleur C_1, et on note $i < j < k$ ses trois sommets. En particulier, si on pose $x = k-j$, $y = j-i$ et $z = k-i$, alors x, y et z appartiennent à P_1, et $x + y = z$.

Solution de l'exercice 7 On va procéder, comme d'habitude, par récurrence : on crée une suite d'ensembles infinis $F_0 \supseteq F_1 \supseteq \dots$ de sommets de K_∞, une suite de couleurs $C_0, C_1, \dots$ et une suite de sommets distincts a_0, puis $a_1 \in F_0$,$a_2 \in F_1, \dots$ tels que, pour un entier i donné, arêtes de la forme (a_i, v) avec $v \in F_i$ sont toutes de coloriées avec la couleur C_i.

Tout d'abord, on commence en prenant un sommet $a_0 \in K_\infty$: a_0 appartient à une infinité d'arêtes, coloriées en seulement k couleurs, donc on peut choisir une couleur C_0 et un ensemble F_0 de sommets tels que (a_0, v) soit toujours de la couleur C_0 quelque soit $v \in F_0$.

Ensuite, on suppose qu'on dispose déjà des sommets $a_0, \dots, a_i$, des couleurs $C_0, \dots, C_i$ et des ensembles $F_0 \supseteq \cdots \supseteq F_i$. Alors on choisit un sommet $a_{i+1} \in F_i$ quelconque, différent de tous les a_i vus jusque là. Puisque F_i est infini, il existe une couleur C_{i+1} et un ensemble $F_{i+1} \subseteq F_i$ infini tel que l'arete (a_i, v) soit de couleur C_{i+1} pour tout sommet $v \in F_{i+1}$. Ce processus nous permet bien d'obtenir des suites (F_n), (C_n) et (a_n) infinies.

Maintenant, vu que la suite (C_n) prend un nombre fini de valeurs, il existe une couleur C_∞ telle que l'ensemble $X = \{n \in \mathbb{N} : C_n = C_\infty\}$ soit infini. Le sous-graphe induit par l'ensemble de sommets $a_X = \{a_n : n \in X\}$ est un graphe complet infini dont toutes les arêtes sont de couleur C_∞, ce qui prouve le théorème 7.

Solution de l'exercice 8 Soit $G = (V, E)$ un graphe planaire tel que V est infini dénombrable. On numérote l'ensemble de ses sommets $V = \{v_0, v_1, \ldots\}$. En outre, pour tout entier naturel n, on considère l'ensemble de sommets $V_n = \{v_0, v_1, \ldots, v_n\}$, ainsi que le sous-graphe fini G_n induit par V_n. Alors il existe un coloriage $C_n : V_n \to \{\text{bleu, rouge, vert}\}$ de G_n sans cycle monochrome de longueur impaire.

En particulier, il existe un ensemble infini $F_0 \subseteq \mathbb{N}$ et une couleur c_0 tels que $C_k(v_0) = c_0$ pour tout entier $k \in F_0$. Puis, si on dispose d'un ensemble infini $F_n \subseteq \mathbb{N}$ et de couleurs $c_0, c_1, \ldots, c_n$ tels que $C_k(v_i) = c_i$ pour tous les entiers $k \in F_n$ et $i \leqslant n$, alors il existe un ensemble infini $F_{n+1} \subseteq F_n$ et une couleur c_{n+1} tels que $C_k(v_{n+1}) = c_{n+1}$ pour tout entier $k \in F_{n+1}$ tel que $k \geqslant n+1$. On considère alors le coloriage $C_\infty : V \to \{\text{bleu, rouge, vert}\}$ tel que $C_\infty(v_n) = c_n$ pour tout entier $n \in \mathbb{N}$. Il apparaît alors que C_∞ n'admet pas de cycle monochrome de longueur impaire.

En effet, supposons qu'un tel cycle $\mathcal{C}$ existe : $\mathcal{C}$ étant fini, il existe un entier n tel que $\mathcal{C}$ ne contient que des sommets de V_n. En outre, on considère un entier $\ell \in F_n$ et le coloriage associe C_ℓ. Puisque $C_\ell(v_k) = c_k = C_\infty(v_k)$ pour tout entier $k \leqslant n$, il s'ensuit que $\mathcal{C}$ est un cycle monochrome de longueur impaire pour le coloriage C_ℓ : l'existence d'un tel cycle est incompatible avec la définition de C_ℓ. On en conclut donc que notre supposition était fausse, ce qui conclut l'exercice.

2 TD de combinatoire

- Exercices -

Exercice 1 Une araignée possède 8 chaussettes identiques et 8 chaussures identiques. Dans combien d'ordres différents peut-elle se chausser, sachant qu'évidemment, sur chaque patte, elle doit mettre la chaussure après la chaussette ?

Exercice 2 On considère n entiers positifs $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n \leqslant 2n$ tels que le plus petit commun multiple de n'importe quelle paire prise parmi eux est strictement supérieur à $2n$. Montrer que $a_1 > \lfloor \frac{2n}{3} \rfloor$.

Exercice 3 (Théorème de Erdös-Szekeres) D'une suite $mn+1$ nombres réels, montrer qu'on peut extraire
- une sous-suite croissante de $m+1$ réels
- ou une sous-suite décroissante $n+1$ réels.

Exercice 4 On considère plusieurs cercles de longueur totale 10 dans un carré de côté 1. Montrer qu'il existe une droite qui intersecte au moins quatre de ces cercles.

Exercice 5 Soient n points dans le plan. Montrer qu'on peut en choisir au moins $\sqrt{n}$ d'entre eux tels qu'ils ne forment pas de triangle équilatéral.

Exercice 6 Soient 2013 points dans le plan tels que toute droite passant par deux de ces points passe par un troisième. Montrer que trois d'entre eux ne peuvent jamais former de triangle équilatéral.

Exercice 7 Etant donné un graphe, montrer qu'il existe une coloration des sommets en noir et blanc tel que chaque sommet blanc a au moins autant de voisins noirs que de voisins blancs, et que similairement, chaque sommet noir a au moins autant de voisins blancs que de voisins noirs.

Exercice 8 (Identités de Vandermonde et d'anti-Vandermonde) Soient a, b,n des entiers. On choisit la convention $\binom{n}{k} = 0$ pour $k > n$. Montrer que :

1. $$\sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k} = \binom{a+b}{n}$$

2. $$\sum_{k=0}^{n} \binom{k}{a}\binom{n-k}{b} = \binom{n+1}{a+b+1}$$

Exercice 9 Soient m et n deux entiers strictement positifs. Soient $a_1, \cdots a_m$ des entiers distincts pris parmi $\{1, \cdots n\}$ vérifiant la condition suivante : si pour $1 \leqslant i \leqslant j \leqslant m$, on a $a_i + a_j \leqslant n$, alors il existe $k, 1 \leqslant k \leqslant m$ tel que $a_i + a_j = a_k$. Montrer alors que :

$$\frac{a_1 + a_2 + \cdots + a_m}{m} \geqslant \frac{n+1}{2}$$

Exercice 10 Dans un tournoi, chaque participant joue un match contre chaque autre participant. Le gagnant d'un match gagne 1 point, le perdant 0 point, et si le match est nul les deux joueurs gagnent un demi-point. À la fin du tournoi, les participants sont classés selon leur score (en cas d'égalité, l'ordre est aribtraire). On remarque alors que chaque participant a remporté la moitié de ses points contre les dix derniers du classement. Combien de personnes participaient au tournoi ?

Exercice 11 Dans une école, il y a 2013 filles et 2013 garçons. Chaque élève rejoint au plus 100 clubs dans l'école. On suppose par ailleurs que pour chaque paire composée d'un garçon et d'une fille, ils ont au moins un club en commun. Montrer qu'il y a un club avec au moins 11 garçons et 11 filles.

Exercice 12 Soit $n \in \mathbb{N}$ cercles de même rayon tel que chacun intersecte au moins un autre cercle. On suppose par ailleurs que deux de ces cercles ne sont jamais tangents. Montrer que le nombre p des points d'intersection ainsi formés est supérieur à n.

Exercice 13 On considère un tableau $M \times N$ (de M lignes et N colonnes), qui contient plus de colonnes que de lignes ($N > M$). On place des étoiles dans certaines cases du tableau, et on suppose que chaque ligne et chaque colonne contient au moins une étoile. Montrer qu'il existe une case contenant une étoile tel que le nombre d'étoiles sur sa ligne est strictement plus grand que le nombre d'étoiles sur sa colonne.

Exercice 14 Soient m et n des entiers strictement positifs. On se donne un rectangle $a \times b$ et on suppose qu'il peut être pavé en utilisant uniquement des tuiles horizontales $1 \times m$ et des tuiles verticales $n \times 1$. Montrer qu'il peut être pavé en utilisant uniquement un de ces types de tuiles.

- Solutions -

Solution de l'exercice 1 Numérotons les pattes de l'araignée de 1 à 8. Soit a_i l'action consistant à mettre une chaussette sur la i-ième patte, et b_i l'action consistant à mettre une chaussure sur la i-ième patte. Il y a 16! façons d'ordonner les 16 actions (a_i) et (b_i). Considérons l'un de ces ordres. À partir de cet ordre, on s'autorise à échanger, pour tout i, les positions des actions a_i et b_i, ce qui permet d'atteindre 2^8 ordres différents. Parmi ces ordres, seul un correspond à une façon correcte de se chausser : l'ordre pour lequel pour tout i, a_i apparaît avant b_i. L'araignée peut donc se chausser de $16!/2^8 = 81729648000$ façons différentes.

Solution de l'exercice 2 On suppose par l'absurde que $a_1 \leqslant \lfloor \frac{2n}{3} \rfloor$. Alors $3a_1 \leqslant 2n$. Les $n+1$ entiers positifs de l'ensemble $\{2a_1, 3a_1, a_2, \ldots, a_n\}$ appartiennent alors à $\{1, 2, \ldots, 2n\}$, et leurs parties entières appartiennent à l'ensemble $\{1, 3, 5, \ldots, 2n-1\}$ (la partie entière d'un entier m est le plus grand diviseur impair de m). Par le principe des tiroirs, deux de ces $n+1$ entiers ont la même partie impaire, ce qui montre que l'un divise l'autre, qui est égal au PPCM des deux : l'énoncé rend clairement une telle situation impossible.

Solution de l'exercice 3 On note $a_1, a_2, \ldots, a_{mn+1}$ ces nombres. On note c_k la longueur de la plus longue sous-suite croissante commençant par a_k, et d_k la longueur de la plus longue sous-suite décroissante commençant par a_k. Remarquons alors que si $k \neq l$ sont deux indices, $(c_k, d_k) \neq (c_l, d_l)$. En effet, dans la situation contraire, et quitte à suppose $k < l$ on traite deux cas :

- Si $a_k \leqslant a_l$, on peut prolonger la sous-suite croissante commençant par a_l en une sous-suite commençant par a_k de longueur $c_l + 1 > c_k$, ce qui contredit la maximalité de c_k.
- Sinon, on prolonge une sous-suite décroissante pour obtenir la une contradiction sur la maximalité de d_k.

Or, d'après le principe des tiroirs, les $mn+1$ couples (c_k, d_k) ne peuvent pas tous appartenir à $\{1, \ldots m\} \times \{1, \ldots n\}$. D'où le résultat.

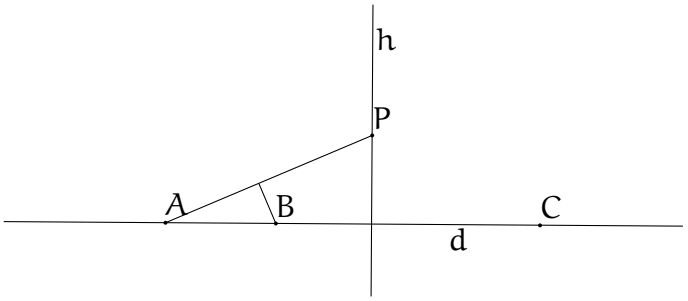
Solution de l'exercice 4 On fixe un côté du carré et on projette tous les cercles sur ce côté. Un cercle de circonférence l se projette sur un segment de longueur l/π. La somme des projections de tous les cercles vaut donc $10/\pi$, qui a le bon goût de valoir plus de trois fois le côté du carré. Il existe donc un point de ce côté qui appartient aux projections d'au moins 4 cercles, et la perpendiculaire au côté passant par ce point convient.

Solution de l'exercice 5 On choisit un repère quelconque et on note (x_i, y_i) les coordonnées du point A_i pour $i \in \{1, \ldots, n\}$. En évitant un nombre fini de repères, on peut en trouver un tel que les x_i sont distincts et tels que les y_i sont distincts. Quitte à les renommer, on peut supposer les x_i ordonnés selon $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$. D'après le théorème de Erdös-Szekeres, on peut trouver une sous-suite monotone de (y_n) de longueur $\lfloor \sqrt{n} \rfloor$. Les points correspondants ne peuvent former de triangle équilatéral.

Solution de l'exercice 6 Ceci est une conséquence du théorème de Sylvester : *Soit S un ensemble fini de points est tel que toute droite passant par deux de ces points passe par un troisième. Alors ces points sont alignés.*

Supposons par l'absurde que ce ne soit pas le cas. Parmi les couples (d, P) formés d'une droite d passant par deux points de S et un point P de S qui n'est pas sur d, il en existe un qui minimise la distance de P à d. Soit h la perpendiculaire à d passant par P. Elle divise d, qui contient par hypothèse trois points S, en deux demi-droites. D'après le principe des tiroirs, il y en a une qui contient deux points de S. Si on note A le plus éloigné et B le plus proche des

h, la distance de B à (AP) est inférieure strictement à la distance de P à d, ce qui fournit la contradiction voulue.



Solution de l'exercice 7 Parmi toutes les configurations possibles, choisissons une de celles qui maximisent le nombre d'arêtes bicolores. Montrons qu'elle convient. Par l'absurde, et sans perte de généralité, il existe un sommet blanc A qui a strictement plus de voisins blancs que de voisins noirs. De ce sommet partent plus d'arêtes monocolores que d'arêtes bicolores. En inversant la couleur de A on se retrouve donc dans une situation avec strictement plus d'arêtes bicolores, ce qui constitue une contradiction.

Solution de l'exercice 8 La principale difficulté en double-comptage est de choisir la grandeur à double-compter.

1. Ici, il paraît assez naturel de double-compter le nombre de manières de choisir n personnes parmi a filles et b garçons. Dans un premier temps, ce nombre vaut $\binom{a+b}{n}$. D'autre part, si on commence par choisir k filles parmi a, il ne reste plus que $n-k$ garçons parmi b. En faisant varier k entre 0 et n, on partitionne toutes les possibilités. D'où :
$$\sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k} = \binom{a+b}{n}$$
2. De la même façon, on double-compte le nombre de manières de choisir $a+b+1$ personnes parmi $n+1$ individus : $\binom{n+1}{a+b+1}$. Maintenant, au lieu de partitionner selon le nombre de filles, on partitionne selon le choix du $a+1$-ième élément en notant ce paramètre $k+1$. Une fois ce choix fait, il reste a personnes à choisir par k puis b parmi $n-k$. Il reste à faire varier $k+1$ entre 1 et $n+1$ pour conclure :
$$\sum_{k=0}^{n} \binom{k}{a}\binom{n-k}{b} = \binom{n+1}{a+b+1}$$

Solution de l'exercice 9 Quitte à les renommer, on peut supposer les a_i ordonnés de façon croissante. Quelques essais amènent à conjecturer que pour $1 \leqslant i \leqslant n$, on a $a_i + a_{m+1-i} \geqslant n+1$. Supposons que ce ne soit pas le cas. Soit alors $j \leqslant n/2$ tel que $a_j + a_{m+1-j} \leqslant n$. Par hypothèse, il existe donc $1 \leqslant k \leqslant m$ tel que $a_j + a_{m+1-j} = a_k$, avec $m+1-j < k \leqslant m$ car les a_i sont croissants et strictement positifs. De la même façon, les j sommes
$$a_1 + a_{m+1-j}, a_2 + a_{m+1-j}, \ldots, a_j + a_{m+1-j}$$
sont inférieures ou égales à n tout en étant distinctes et supérieures strictement à a_{m+1-j}. Chacune de ces sommes vaut donc a_l pour un certain $l > m+1-j$, ce qui ne fait que $j-1$ choix. Contradiction.

Solution de l'exercice 10 Nous procédons par double-comptage sur le nombre de points distribués dans le tournoi. Chaque match correspond à la distribution de 1 point, et donc le score total obtenu par k dans les matchs qu'ils jouent entre eux est de $k(k-1)/2$. Ainsi, le score total des participants est de $n(n-1)/2$.

D'autre part, les 10 derniers participants ont obtenu 45 points en jouant entre eux. Leur score total dans le tournoi est donc de 90 points. Les autres $n-10$ participants ont obtenu $(n-10)(n-11)/2$ points en jouant entre eux, et donc un total de $(n-10)(n-11)$ points. Le score de tous les participants est donc de $90+(n-10)(n-11)$ points. En comparant ces deux valeurs, on obtient l'équation $n^2-41n+400=0$, qui a deux solutions : 16 et 25.

Le tournoi ne pouvait pas contenir 16 participans. En effet, dans ce cas, le score total des 10 derniers participants est 90, et celui des 6 premiers est 30. Les dix derniers ont donc obtenu en moyenne plus de points que les premiers, ce qui est absurde. Le tournoi ne pouvait donc avoir que 25 participants.

Solution de l'exercice 11 Raisonnons par l'absurde en suppose que tout club qui contient au moins 11 garçons contient au plus 10 filles. Procédons par double-comptage sur le nombre S de triplets (g,f,c) où c est un club qui auquel participe le garçon g et la fille f. Pour chaque paire d'un garçon et d'une fille, au moins un club convient. D'où $S \geqslant 2013^2$.

Considérons maintenant X l'ensemble des clubs avec au plus 10 garçons, et Y les clubs avec au moins 11 garçons, donc au plus 10 filles. Alors chacune des 2013 filles appartient à au plus 100 clubs de X, donc au plus 100×10 triplets (g,f,c) avec $c\in X$. De même, chaun des 2013 garçons appartient à au plus 100 clubs de Y, donc au plus 100×10 triplets (g,f,c) avec $c\in Y$. Ainsi, il existe au plus 2013×1000 triplets (g,f,c) tels que $c\in X$, et au plus 2013×1000 triplets (g,f,c) tels que $c\in Y$, donc $S\leqslant 2013\times 1000\times 2<2013^2$, ce qui est absurde.

Solution de l'exercice 12 Notons $A_1,A_2,\dots,A_p$ ces points d'intersection et $C_1,C_2,\dots C_n$. Pour $1\leqslant i\leqslant p$, notons a_i le nombre de cercles auxquels A_i appartient.

Soit $X=\{(i,k)\in\{1,\dots,p\}\times\{1,\dots,n\} | A_i\in C_k\}$. Double-comptons la somme suivante en procédant selon les points d'intersection :

$$\sum_{(i,k)\in X}\frac{1}{a_i}=\sum_{i_0=1}^{p}\left(\sum_{(i_0,k)\in X}\frac{1}{a_{i_0}}\right)=\sum_{i_0=1}^{p}1=p$$

…puis selon les cercles :

$$\sum_{(i,k)\in X}\frac{1}{a_i}=\sum_{k_0=1}^{n}\left(\sum_{(i,k_0)\in X}\frac{1}{a_i}\right)\geqslant\sum_{k_0=1}^{n}1\geqslant n$$

où la pénultième inégalité se justifie ainsi.

Soit C_{k_0} un cercle quelconque, et m l'indice d'un point d'intersection tel que $(m,k_0)\in X$ et a_m soit maximal. Ce point existe car C_{k_0} intersecte au moins un cercle. A_m appartient à a_m-1 autres cercles qui intersectent de nouveau C_{k_0} en a_m-1 points distincts car les cercles sont de même rayon, et non tangents. Ainsi, par minimalité de $1/a_m$,

$$\sum_{(i,k_0)\in X}\frac{1}{a_i}\geqslant a_m\frac{1}{a_m}\geqslant 1$$

Cela conclut.

Notons que cela revient à écrire $1/a_i$ dans un tableau $p \times n$ puis à sommer par lignes ou par colonnes.

Solution de l'exercice 13 On numérote toutes les cases étoilées $E_1, E_2, \ldots, E_p$ et pour chaque case E_i on note c_i le nombre de cases étoilées dans sa colonne et l_i dans sa ligne. Supposons par l'absurde que pour tout i, $c_i \geqslant l_i$. On va alors considérer les deux sommes :

$$\sum_{i=1}^{p} \frac{1}{c_i} \leqslant \sum_{i=1}^{p} \frac{1}{l_i}$$

Calculons la première somme selon les colonnes.

$$\sum_{i=1}^{p} \frac{1}{c_i} = \sum_{k=1}^{N} \left(\sum_{E_i \in k^e \text{colonne}} \frac{1}{c_i} \right) = \sum_{k=1}^{N} 1 = N$$

où l'avant-dernière égalité découle de la définition de c_i et de ce que chaque colonne contient au moins une étoile.

De la même manière, on calcule la somme des $1/l_i$, ce qui permet d'écrire :

$$N = \sum_{i=1}^{p} \frac{1}{c_i} \leqslant \sum_{i=1}^{p} \frac{1}{l_i} = M$$

Cela constitue la contradiction souhaitée.

Solution de l'exercice 14 L'existence d'un pavage avec des tuiles entières montre que a et b sont entiers. Il suffit alors de montrer que m divise b ou que n divise a.

Découpons le rectangle en carré unitaire (côté 1) où on numérote les lignes de 0 à $a-1$ et les colonnes de 0 à $b-1$. On pose $\omega_m = e^{\frac{2i\pi}{m}}$ et $\omega_n = e^{\frac{2i\pi}{n}}$ et dans la case (i,j) du tableau, on note le nombre $\omega_n^i \omega_m^j$.

Considérons une tuile horizontale qui commence par exemple à l'indice (i_0, j_0). La somme des nombres sous cette tuile vaut alors :

$$\omega_n^{i_0}\omega_m^{j_0} + \omega_n^{i_0}\omega_m^{j_0+1} + \ldots \omega_n^{i_0}\omega_m^{j_0+m-1} = \omega_n^{i_0}\omega_m^{j_0} \left(\sum_{k=0}^{m-1} \omega_m^k \right) = \omega_n^{i_0}\omega_m^{j_0} \frac{1-\omega_m^m}{1-\omega_m} = 0$$

De même, le somme des nombres sous une tuile verticale vaut 0.

Or, le rectangle est pavé uniquement à l'aide de ces deux types de tuile. La somme des tous les nombres écrits dans le rectangle, qui est donc nulle, se calcule d'autre part selon :

$$(\omega_n^0 + \omega_n^1 + \omega_n^2 + \cdots + \omega_n^{a-1})(\omega_m^0 + \cdots + \omega_m^{b-1}) = \frac{1-\omega_n^a}{1-\omega_n} \frac{1-\omega_m^b}{1-\omega_b} = 0$$

L'un des deux facteurs est donc nul, ce qui signifie bien que n divise a ou m divise b.

3 Cours/TD de combinatoire

- Définition et premiers exemples -

Les séries génératrices sont un outil algébrique qui permet de reformuler des problèmes de combinatoire afin de les transformer en des problèmes de manipulation d'expressions algébriques. En particulier, en combinatoire, il s'agit souvent de déterminer le nombre d'objets d'un certain type qui sont de taille n, ce qui donne lieu à une suite $(a_n)_n$ dont on cherche à déterminer le n-ième terme. La fonction génératrice associée à la suite a_n est la série ("somme infinie") formelle

$$a_0 + a_1 x + a_2 x^2 + \ldots = \sum_{k \geqslant 0} a_k x^k.$$

En particulier, la série génératrice d'une suite finie est un polynôme.

Exemple 4.3. Soit n un entier strictement positif. La suite (finie) des coefficients binomiaux $\left(\binom{n}{k}\right)_{k \in \{0,\ldots,n\}}$ a pour série génératrice le polynôme

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n.$$

Cela a-t-il vraiment un sens de parler de "somme infinie" ? C'est une vaste question, et on ne va pas trop l'aborder ici. Il y a deux points de vue pour voir une série : d'une part le point de vue algébrique et formel que nous utilisons ici, où x n'est qu'une variable sans aucun sens particulier, de sorte que finalement, une série génératrice, c'est juste une autre manière de noter une suite, de sorte à ce que les opérations que nous allons définir plus bas apparaissent naturellement. C'est dans ce cadre que nous nous plaçons, et il n'y a aucun souci à se faire de ce côté, tant que x reste une variable formelle à laquelle on ne fait pas prendre de valeurs réelles. D'autre part, on peut voir une série du point de vue analytique, et regarder pour quelles valeurs réelles de x la série "converge", c'est-à-dire que la suite de ses sommes partielles

$$\sum_{k=0}^{n} a_n x^n$$

converge, ce qui est équivalent à dire que la suite des "restes"

$$\sum_{k=n}^{\infty} a_n x^n$$

tend vers 0. On voit clairement que $x = 0$ est toujours une telle valeur. S'il existe un intervalle autour de 0 où la série converge, alors elle y coïncide avec une fonction dérivable autant de fois que nous voulons, et les dérivées coïncident avec les dérivées de la série au sens formel que nous allons voir plus bas. Bref, il y a une forte interaction entre les points de vue algébrique et analytique, mais pour ce qu'on fait aujourd'hui, on peut tout à fait rester dans le point de vue algébrique en n'utilisant le point de vue analytique que comme aide pour comprendre certains résultats formels. Dans tous les cas, il faut être très prudent quand on veut évaluer une série en un réel non nul

Un exemple fondamental de série génératrice est la série génératrice de la suite constante égale à 1. D'une part, elle est clairement égale à

$$A(x) = \sum_{n \geqslant 0} x^n$$

On l'appelle la série géométrique (car c'est la somme des termes d'une suite géométrique). On remarque alors que $A(x) - 1 = xA(x)$, donc $(1-x)A(x) = 1$. Cela signifie que la série formelle $A(x)$ a un inverse : la série formelle $1 - x$. On notera cela d'une manière un peu plus suggestive :

$$\sum_{n \geqslant 0} x^n = \frac{1}{1-x}. \tag{V.2}$$

où $\frac{1}{1-x}$ est ce qu'on appelle une fraction rationnelle, c'est-à-dire un quotient de deux polynômes. Comment comprendre d'où vient cette formule ? Revenons une seconde au point de vue analytique, et prenons un x réel différent de 1. La formule de la somme des termes d'une suite géométrique nous dit que pour tout $N \geqslant 0$,

$$1 + x + x^2 + \ldots + x^N = \frac{1 - x^{N+1}}{1-x}$$

Lorsque $|x| \geqslant 1$, cette somme diverge quand N tend vers l'infini, donc nous ne pouvons pas en faire grand chose. Mais que se passe-t-il si $x \in]-1, 1[$? Alors x^{N+1} tend vers 0, donc le côté droit de la formule ci-dessus tend vers $\frac{1}{1-x}$. Nous venons de voir que la série $\sum_{n \geqslant 0} x^n$ converge sur l'intervalle $]-1, 1[$ et que sur cet intervalle la fonction $x \mapsto \sum_{n \geqslant 0} x^n$ coïncide avec la fonction $x \mapsto \frac{1}{1-x}$.

On cherchera souvent à trouver ce genre de "formes closes" pour les séries génératrices, c'est-à-dire les écrire comme un quotient $\frac{P}{Q}$ de deux polynômes avec $Q(0) \neq 0$. C'est loin d'être toujours possible, mais ça l'est dans l'immense majorité des cas pouvant intervenir dans un contexte olympique. En particulier, si une suite vérifie une récurrence linéaire, sa série génératrice vérifie une équation du premier degré, et on obtient donc toujours une forme close.

Exemple 4.4. La suite de Fibonacci est définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$. Déterminons sa série génératrice, notée $F(x)$. Pour cela, on multiplie sa relation de récurrence par x^{n+2} et somme pour $n \geqslant 0$. On obtient :

$$F(x) - x = (x + x^2)F(x),$$

d'où

$$F(x) = \frac{x}{1 - x - x^2}.$$

- Opérations sur les séries génératrices -

La somme de deux séries génératrices se définit de manière assez évidente en sommant les suites correspondantes.

Pour le produit, c'est un peu plus compliqué. Il se fait par analogie avec le produit des polynômes :

$$\left(\sum_{m\geqslant 0} a_m x^m\right)\left(\sum_{n\geqslant 0} b_n x^n\right) = \sum_{m,n\geqslant 0} a_m b_n x^{m+n} = \sum_{n\geqslant 0}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$$

Le produit est donc également une série génératrice, correspondant à la suite $\left(\sum_{k=0}^{n} a_k b_{n-k}\right)_n$. D'une certaine manière, on peut donc dire qu'une série génératrice, c'est une manière de noter une suite de telle sorte que ce produit apparaisse naturellement grâce à la relation $x^k x^{n-k} = x^n$.

Remarque 4.5. Soit $(a_n)_n$ une suite. Alors d'après la définition du produit, la suite génératrice de la suite (S_n) définie par $S_n = \sum_{k=0}^{n} a_k$ s'obtient simplement en multipliant celle de S_n par $\sum_{k\geqslant 0} x^k = \frac{1}{1-x}$. En particulier, une forme close pour $(a_n)_n$ donne directement une forme close pour $(S_n)_n$.

Pour ce qui est du quotient, l'analogie avec les polynômes ne fonctionne plus puisque l'inverse d'un polynôme de degré supérieur ou égal à 1 n'est plus un polynôme. En revanche, nous avons vu qu'en tant que série formelle, $1-x$ a un inverse, qui est une série formelle. Plus généralement, nous avons le lemme suivant :

Lemme 4.6. La série formelle $\sum_{i\geqslant 0} a_i x^i$ a un inverse si et seulement si $a_0 \neq 0$.

Démonstration. On veut trouver une série formelle $\sum_{j\geqslant 0} b_j x^j$ telle que

$$\left(\sum_{i\geqslant 0} a_i x^i\right)\left(\sum_{j\geqslant 0} b_j x^j\right) = \sum_{k\geqslant 0}\left(\sum_{i=0}^{k} a_i b_{k-1}\right) x^k = 1.$$

On identifie tout simplement les coefficients, ce qui donne une infinité d'équations avec les a_i et les b_i. La première est $a_0 b_0 = 1$. Cela nous dit que $a_0 \neq 0$ est effectivement une condition nécessaire. Dans ce cas, on choisit simplement $b_0 = \frac{1}{a_0}$. La deuxième équation est

$$a_0 b_1 + a_1 b_0 = 0.$$

Cela nous donne, en réutilisant encore le fait que $a_0 \neq 0$, que $b_1 = -\frac{a_1 b_0}{a_0}$. On voit qu'on peut faire une récurrence : si on suppose $b_0, \ldots, b_{n-1}$ construits pour un certain n, l'équation $a_0 b_n + \ldots + a_n b_n = 0$ avec la condition $a_0 \neq 0$ nous donne b_n. □

En particulier, les fractions rationnelles de la forme $\frac{P}{Q}$ avec P et Q des polynômes et $Q(0) \neq 0$ peuvent s'écrire comme des séries formelles.

La dérivée au sens formel d'une série génératrice se définit sans trop de problèmes par analogie avec les polynômes :

$$\left(\sum_{n\geqslant 0} a_n x^n\right)' = \sum_{n\geqslant 1} n a_n x^{n-1}.$$

Exemple 4.7. Soit de nouveau $A(x)$ la série géométrique ci-dessus. Par définition, sa dérivée est $\sum_{n\geqslant 1} n x^{n-1}$, et en dérivant $\frac{1}{1-x}$, on obtient $\sum_{n\geqslant 1} n x^{n-1} = \frac{1}{(1-x)^2}$.

Si on continue ainsi, on peut obtenir des formules pour $(1-x)^{-k}$ pour tout entier naturel k. En généralisant la notion de coefficient binomial, nous allons en fait pouvoir étendre la formule du binôme aux exposants quelconques.

Définition 4.8. Soient r un réel et k un entier naturel. Alors on définit le coefficient binomial généralisé $\binom{r}{k}$ par

$$\binom{r}{k} = \frac{r(r-1)\dots(r-k+1)}{k!}.$$

Proposition 4.9. (Formule du binôme généralisée) Pour tout entier n, on a

$$(1+x)^n = \sum_{k\geqslant 0} \binom{n}{k} x^k.$$

En particulier, sachant que par définition pour tout k

$$\binom{-1}{k} = \frac{(-1)(-2)\dots(-k)}{k!} = (-1)^k \text{ et } \binom{-2}{k} = \frac{(-2)(-3)\dots(-2-k+1)}{k!} = (-1)^k(k+1).$$

on retrouve les expressions de $(1-x)^{-1}$ et de $(1-x)^{-2}$ plus haut. Puisque les coefficients de la forme $\binom{-n}{k}$ avec n un entier naturel jouent un rôle particulièrement important quand on travaille avec les séries formelles, il peut être utile d'avoir la formule suivante, qui les relie aux coefficients binomiaux usuels.

Proposition 4.10. Soient n et k des entiers naturels. Alors

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}.$$

Une situation où on peut voir qu'il faut prendre des précautions en manipulant les séries formelles apparaît lorsqu'il s'agit de les composer. Si f et g sont des séries génératrices, il faut faire très attention au fait que $f(g(x))$ *n'est pas toujours défini.* En effet, le terme constant de $f(g(x))$ devrait être $f(g(0))$, ce qui n'a pas vraiment de sens puisque nous avons remarqué qu'une série formelle ne pouvait a priori être évaluée qu'en $x = 0$. Bien entendu, analytiquement, on pourrait définir $f(g(x))$ quand même à condition que f converge en $g(0)$, mais pour les séries formelles, nous allons dire que $f(g(x))$ n'est pas défini si $g(0) \neq 0$, c'est-à-dire si g a un terme constant non nul. En revanche, si $g(0) = 0$, $f(g(x))$ est bien définie : en effet, il suffit de montrer que pour tout n, on peut déterminer son coefficient de degré n après un nombre fini d'opérations (de même qu'on dit qu'on a bien défini une suite si on arrive à déterminer son n-ième terme après un nombre fini d'opérations). Pour cela, on écrit $f = \sum_{k\geqslant 0} a_k x^k$, et $g(x) = xh(x)$ avec $h(x)$ une autre série formelle, ce qui donne

$$f(g(x)) = a_0 + a_1 x h(x) + a_2 x^2 h(x)^2 + \dots + a_n x^n h(x)^n + a_{n+1} x^{n+1} h(x)^{n+1} + \dots$$

et toutes les contributions au coefficient de degré n interviennent donc dans les $n+1$ premiers termes ci-dessus, ce qui permet de les déterminer.

- Décomposition en éléments simples -

Supposons que l'on dispose d'une forme close de la série génératrice $f(x) = \frac{P(x)}{Q(x)}$ d'une suite (a_n). Pour en déduire une formule pour a_n pour tout n, on va faire une *décomposition en éléments simples*. Autrement dit, on va écrire la série génératrice comme une somme d'un polynôme (appelé la partie entière) et de termes de la forme $b(1-ax)^{-k}$, appelés éléments simples, car pour ce type de termes, les coefficients sont facilement déterminables grâce à la formule du binôme ci-dessus. Pour cela, on commence par faire la division euclidienne de P par Q afin de mettre en évidence la partie entière : on écrit $P = EQ + R$ avec E et R des polynômes et $\deg R < \deg Q$, d'où $f = E + \frac{R}{Q}$. Ensuite , on factorise le dénominateur Q (bien entendu, cela peut être difficile en pratique dans le cas général, mais dans les cas particuliers que nous croiserons ce sera tout à fait faisable). À une constante multiplicative près, Q s'écrira sous la forme $\prod_i (1-a_i x)^{m_i}$. Les éléments simples qui peuvent intervenir seront alors les $(1-a_i x)^{-j}$ avec $1 \leqslant j \leqslant m_i$. On cherche donc à déterminer des constantes $b_{i,j}$ telles que

$$f(x) = E(x) + \sum_i \sum_{1 \leqslant j \leqslant m_i} \frac{b_{i,j}}{(1-a_i x)^j}.$$

Il y a plusieurs méthodes pour faire cela. Dans certains cas particuliers, cela se fait de tête, ou en trifouillant un peu l'expression à la main. On peut aussi tout remettre au même dénominateur, identifier les coefficients et résoudre le système linéaire que cela fait apparaître, ou alors d'évaluer pour diverses valeurs de x et résoudre un système linéaire également. Pour déterminer b_{i,m_i}, on peut multiplier le tout par $(1-a_i x_i)^{m_i}$ et évaluer en $x = \frac{1}{a_i}$. Multiplier le tout par x et faire tendre x vers l'infini peut donner une équation linéaire avec les $b_{i,1}$. Le but n'étant pas de faire un cours complet de décomposition en éléments simples, nous allons nous contenter de montrer comment cela fonctionne en pratique à l'aide des exemples et exercices qui vont suivre.

Exemple 4.11. Décomposons en éléments simples la série génératrice de la suite (F_n) des nombres de Fibonacci. D'après l'exemple ci-dessus, la fonction génératrice est $\frac{x}{1-x-x^2}$. On a bien que le degré du numérateur est strictement inférieur au degré du dénominateur. Le polynôme du second degré $1-x-x^2$ s'écrit $(1-\alpha x)(1-\beta x)$ avec $\alpha = \frac{1+\sqrt{5}}{2}$ et $\beta = \frac{1-\sqrt{5}}{2}$. On cherche donc à écrire

$$\frac{x}{(1-\alpha x)(1-\beta x)} = \frac{A}{1-\alpha x} + \frac{B}{1-\beta x}$$

pour des constantes réelles A et B. Pour déterminer A, il suffit de tout multiplier par $(1-\alpha x)$, puis d'évaluer en $x = \frac{1}{\alpha}$. Cela donne

$$A = \frac{1}{\alpha - \beta} = \frac{1}{\sqrt{5}}.$$

De même, en multipliant par $(1-\beta x)$ et en évaluant en $\frac{1}{\beta}$, on trouve $B = -\frac{1}{\sqrt{5}}$. Ainsi,

$$\sum_{n \geqslant 0} F_n x^n = \frac{1}{\sqrt{5}} \left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x} \right) = \frac{1}{\sqrt{5}} \sum_{n \geqslant 0} (\alpha^n - \beta^n) x^n,$$

et par identification des coefficients, on retrouve la formule bien connue

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

- Comment associer une série génératrice à un problème de comptage -

La manière dont on utilise les séries génératrices pour les problèmes de comptage repose sur un principe que vous connaissez déjà. Regardons la formule bien connue $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$. Dans chaque parenthèse, on a choisi x, ou pas : le + correspond donc au connecteur logique « ou », et le produit au connecteur logique « et » : j'ai choisi x dans la première parenthèse et je n'ai pas choisi x dans la deuxième parenthèse et.... Le coefficient du terme de degré k correspond au nombre de manières que l'on a de faire cela en ayant choisi k fois x à la fin.

Exemple 4.12. Combien de manières a-t-on de repartir 80 glaces parmi les 62 stagiaires du stage Animath ? Chaque stagiaire a 0 ou 1, ou 2... glaces, donc la série génératrice qui compte le nombre de manières de donner des glaces à un stagiaire est $\sum_{k\geqslant 0} x^k$: le coefficient devant chaque x^k est égal à 1 puisqu'il y a une seule manière de faire en sorte que le stagiaire ait k glaces. Ensuite, il y a 62 stagiaires, donc la série génératrice qui compte le nombre de manières de donner des glaces au stagiaire 1 et au stagiaire 2, etc. est $(1+x+x^2+\ldots)^{62}$. Choisir un nombre de glaces à donner à chaque stagiaire pour que le total des glaces distribuées soit 80 revient à choisir un terme dans chaque parenthèse de sorte à ce que la somme des degrés des termes choisis vaille 80, qui est aussi le nombre de termes de degré 80 (avec un coefficient 1 devant) que l'on obtient en développant ce produit, qui est aussi le coefficient final que l'on obtient devant le terme de degré 80 une fois que l'on aura regroupé tous les termes. Autrement dit, nous voulons déterminer le coefficient de degré 80 de notre série génératrice. Or d'après les formules que nous avons vues

$$(1+x+x^2+\ldots)^{62} = \frac{1}{(1-x)^{62}} = \sum_{n\geqslant 0} \binom{-62}{n} (-1)^n x^n.$$

Le nombre cherché est donc

$$\binom{-62}{80} = \binom{62+80+1}{80} = \binom{143}{80},$$

ce qui correspond bien au résultat que l'on trouve en résolvant l'exercice directement sans séries génératrices.

Remarque 4.13. A priori, il suffirait de développer $(1+x+\ldots+x^{62})^{62}$. Cependant, avec les séries génératrices, on a tout intérêt à garder tous les termes, vu que cela simplifie notablement les calculs (voire les rend faisables).

Essayons de comprendre de manière un peu plus théorique ce qui se passe pour le produit. Soient A et B deux ensembles disjoints. Supposons que le nombre de manières de choisir k objets dans A (respectivement B) vaut a_k (respectivement b_k). La série génératrice associée au choix d'objets dans A (respectivement B) est donc $f(x) = \sum_{k\geqslant 0} a_k x^k$ (respectivement $g(x) = \sum_{k\geqslant 0} b_k x^k$). Alors la série génératrice associée au choix d'objets dans $A \cup B$ est le produit $f(x)g(x)$. En effet, choisir n objets dans $A \cup B$ revient à en choisir j dans A puis $n-j$ dans B, pour $j = 0, 1 \ldots, n$. Le nombre de manières de choisir n objets dans $A \cup B$ est donc

$$a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0,$$

qui, par la définition du produit, est bien le coefficient du terme de degré n dans $f(x)g(x)$.

Exemple 4.14. La série génératrice associée à l'ensemble des entiers naturels est $\sum_{k\geqslant 0} x^k$: choisir un entier naturel, c'est choisir 0, ou 1, ou 2, etc. La série génératrice des entiers pairs est $\sum_{i\geqslant 0} x^{2i}$, celle des entiers impairs est $\sum_{j\geqslant 0} x^{2j+1}$. Le nombre de manières d'écrire un entier n comme la somme d'un entier pair et d'un entier impair sera la coefficient de degré n du produit de ces deux séries. En effet, on veut $n = 2a + b$, d'où $x^n = x^{2a}x^b$. Le nombre de manières d'écrire n sous la forme $2a + b$ correspond donc au nombre de manières d'obtenir un terme x^n en développant

$$\left(\sum_{a\geqslant 0} x^{2a}\right)\left(\sum_{b\geqslant 0} x^b\right),$$

qui est aussi le coefficient du terme de degré n dans ce développement, car tous les termes entre parenthèses ont des coefficients 1.

Exercice 1 Les élèves ayant mangé un peu trop de glaces, Igor va au marché pour acheter des fruits pour les 62 stagiaires du stage Animath. Combien de paniers de 62 fruits différents peut-il assembler sachant que
- les pommes se vendent par lots de 2 ;
- les bananes se vendent par lots de 5 ;
- il ne reste plus que 4 oranges ;
- il ne reste plus qu'une poire.

- Partitions -

Une partition d'un entier strictement positif n est une représentation de n comme somme d'autres entiers strictement positifs, regardée à permutation des termes près. Par exemple 4 peut être partitionné en $1+1+1+1$, $1+1+2$, $2+2$, $1+3$, 4. Les séries génératrices constituent un outil très puissant pour traiter des problèmes sur les partitions.

Exercice 2 Pour tout n, trouver le nombre a_n de manières de payer n euros avec des pièces de 1 et de 2 euros (sans tenir compte de l'ordre).

Exercice 3 Soit a_n le nombre de manières de partitionner n en des entiers deux à deux distincts, et b_n le nombre de manières de partitionner n en des entiers impairs. Montrer que $a_n = b_n$.

Exercice 4 Soit $b \geqslant 2$ un entier. Redémontrer, en utilisant une série génératrice, le fait que tout entier naturel admet une décomposition unique en base b.

Le problème suivant n'est pas un problème de partitions à proprement parler, mais se résout avec le même genre de principes.

Exercice 5 Combien de triplets (a, b, c) d'entiers y a-t-il satisfaisant à l'équation $a + b + c = 6$ ainsi qu'aux conditions $-1 \leqslant a \leqslant 2$ et $1 \leqslant b, c \leqslant 4$?

Exercice 6 (Shortlist 1998) Soit $a_1, a_2, \ldots$ une suite croissante d'entiers naturels telle que tout entier naturel peut être représenté de manière unique sous la forme $a_i + 2a_j + 4a_k$, où i, j, k ne sont pas nécessairement distincts. Déterminer a_{1998}.

Exercice 7 Soit n un entier strictement positif. Combien y a-t-il de polynômes P à coefficients dans $\{0, 1, 2, 3\}$ tels que $P(2) = n$?

- Autres exemples -

Exercice 8 Peut-on partitionner l'ensemble $\mathbb{N}^*$ en un nombre fini (supérieur strictement à un) de progressions arithmétiques de raisons deux à deux distinctes ?

Exercice 9 Un sous-ensemble de $\{1,\dots,n\}$ est égoïste s'il contient son propre cardinal, et si tous ses autres éléments sont plus grands que ce dernier, autrement dit, si son cardinal est égal à son plus petit élément. Calculer le nombre $b(n)$ de sous-ensembles égoïstes de $\{1,\dots,n\}$.

- Solutions des exercices -

Solution de l'exercice 1 Nous allons résoudre le problème plus généralement pour n stagiaires. Il s'agit de déterminer le nombre de manières d'écrire n sous la forme $n = 2a + 3b + c + d$ avec a, b, c, d des entiers naturels et $c \leqslant 4$, $d \leqslant 1$, donc d'écrire x^n sous la forme $x^{2a}x^{2b}x^cx^d$, qui est aussi le coefficient de x^n dans le développement de :

$$\underbrace{\left(\sum_{k\geqslant 0} x^{2k}\right)}_{\text{pommes}}\underbrace{\left(\sum_{k\geqslant 0} x^{5k}\right)}_{\text{bananes}}\underbrace{(1+x+x^2+x^3+x^4)}_{\text{oranges}}\underbrace{(1+x)}_{\text{poires}}.$$

Cette série génératrice vaut

$$\frac{1}{1-x^2}\frac{1}{1-x^5}\frac{1-x^5}{1-x}(1+x) = \frac{1}{(1-x)^2} = 2x + 3x^2 + 4x^3 + \dots$$

et le coefficient de degré n est donc $n+1$. En particulier, la solution du problème est 63.

Solution de l'exercice 2 Chaque manière de payer n euros avec r pièces de 1 et s pièces de 2 peut être encodée sous la forme $x^rx^{2s} = x^n$ Les entiers r et s peuvent être des entiers naturels quelconques. La série génératrice de la suite (a_n) s'écrit donc

$$\sum_{n\geqslant 0} a_n x^n = \left(\sum_{r\geqslant 0} x^r\right)\left(\sum_{s\geqslant 0} x^{2s}\right) = \frac{1}{1-x}\frac{1}{1-x^2} = \frac{1}{(1-x)^2(1+x)}.$$

Essayons d'écrire cette fraction rationnelle sous la forme $\frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{1+x}$ avec une décomposition en éléments simples. Une multiplication par $(1-x)^2$ suivie d'une évaluation en $x = 1$ donne $B = \frac{1}{2}$. Une multiplication par $1 + x$ suivie d'une évaluation en $x = -1$ donne $C = \frac{1}{4}$. Pour finir, si on multiplie par x et qu'on fait tendre x vers l'infini, on obtient $-A + C = 0$, d'où

$A = \frac{1}{4}$. Nous avons donc

$$\begin{aligned}\sum_{n\geqslant 0} a_n x^n &= \frac{1}{2}\left(\frac{1}{(1-x)^2} + \frac{1}{1-x^2}\right)\\ &= \frac{1}{2}\left(\sum_{i\geqslant 0}(i+1)x^i + \sum_{j\geqslant 0} x^{2j}\right)\\ &= \frac{1}{2}\left(\sum_{k\geqslant 0}(2k+2)(x^{2k}+x^{2k+1})\right)\\ &= \sum_{k\geqslant 0}(k+1)(x^{2k}+x^{2k+1})\\ &= \sum_{n\geqslant 0}\left(\left[\frac{n}{2}\right]+1\right)x^n,\end{aligned}$$

où les crochets représentent la partie entière. On a donc $a_n = \left[\frac{n}{2}\right] + 1$.

Remarque : Bien entendu, cet exercice se fait aussi en calculant les premiers termes à la main, en conjecturant la formule et en la prouvant par récurrence. Cependant, la méthode des séries génératrices a l'avantage de se généraliser à tous les problèmes de ce type, même quand la formule est beaucoup moins devinable.

Solution de l'exercice 3 La série génératrice des a_n est $\prod_{i\geqslant 1}(1+x^i) = \prod_{i\geqslant 1}\frac{1-x^{2i}}{1-x^i}$, celle des b_n est $\prod_{i\geqslant 1}\frac{1}{1-x^{2i+1}}$, on voit donc qu'elles sont égales.

Solution de l'exercice 4 On veut écrire chaque nombre comme somme d'un élément dans chacun des ensembles $A_i = \{0, b^i, 2\cdot b^i, \ldots, (b-1)b^i\}$. La série génératrice donnant les nombres s'écrivant sous cette forme est

$$\prod_{i\geqslant 0}\left(1 + x^{b^i} + \ldots + x^{(b-1)b^i}\right) = \prod_{i\geqslant 0}\frac{1-x^{b^{i+1}}}{1-x^{b^i}} = \frac{1}{1-x} = \sum_{k\geqslant 0} x^k,$$

d'où le résultat.

Solution de l'exercice 5 On commence par généraliser le problème en cherchant la série génératrice de la suite des nombres de solutions de l'équation $a+b+c = n$ avec les mêmes conditions sur a, b, c (bien entendu, ce sera en fait un polynôme). Puisque $-1 \leqslant a \leqslant 2$, la contribution de la variable a est un facteur $x^{-1} + x^0 + x^1 + x^2$. Quant à b et c, ils donnent chacun un facteur $x^1 + x^2 + x^3 + x^4$. La série génératrice cherchée est donc

$$f(x) = (x^{-1} + x^0 + x^1 + x^2)(x^1 + x^2 + x^3 + x^4)^2 = x(1 + x + x^2 + x^3)^3.$$

Ce qui nous intéresse, c'est le coefficient devant x^6 de ce polynôme. Développer directement l'expression ci-dessus est un peu long, et revient en fait quasiment au problème combinatoire initial. On a toujours intérêt à réécrire les choses sous une forme qui fait intervenir des termes du degré le plus grand possible. Ainsi, ici, on peut écrire

$$f(x) = x\left(\frac{1-x^4}{1-x}\right)^3 = x(1-3x^4+3x^8-x^{12})(1-x)^{-3}.$$

Les termes de degré 6 proviennent en choisissant soit 1 soit $-3x^4$ dans la première parenthèse, et donc respectivement le terme de degré 5 ou celui de degré 1 dans la deuxième parenthèse. D'après la formule du binôme, le coefficient qu'on cherche est donc

$$1 \times \left(-\binom{-3}{5}\right) + (-3) \times \left(-\binom{-3}{1}\right) = \binom{7}{5} - 3\binom{3}{1} = 21 - 9 = 12.$$

Solution de l'exercice 6 Cet exercice est un très bon exemple de la manière dont une solution avec les séries génératrices peut nous inspirer une solution n'utilisant pas les séries génératrices. Posons $f(x) = \sum_{n \geqslant 0} x^{a_n}$. Par hypothèse, nous avons

$$f(x)f(x^2)f(x^4) = \sum_{n \geqslant 0} x^n = \frac{1}{1-x}.$$

En effet, chaque terme à gauche est sous la forme $x^{a_i+2a_j+4a_k}$, et par unicité de la représentation, il y a un et un seul terme de chaque degré. Remplaçons x par x^2 : on obtient

$$f(x^2)f(x^4)f(x^8) = \frac{1}{1-x^2},$$

et combinant les deux équations, on a

$$f(x) = \frac{1-x^2}{1-x} f(x^8) = (1+x)f(x^8).$$

En itérant ceci, on a

$$f(x) = \prod_{k \geqslant 0} (1 + x^{8^k}).$$

Les seuls termes de $f(x)$ ayant un coefficient non nul sont ceux dont l'écriture en base 8 ne comporte que les chiffres 0 ou 1. Le n-ième tel nombre se trouve en écrivant n en base 2 et en lisant le résultat en base 8. Ainsi, puisque $1998 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^3 + 2^2 + 2$, on a

$$a_{1998} = 8^{10} + 8^9 + 8^8 + 8^7 + 8^6 + 8^3 + 8^2 + 8 = 1227096648.$$

Maintenant que nous avons le résultat grâce à la théorie des fonctions génératrices, essayons de trouver une solution qui ne les fait pas intervenir. Vu que la suite a_n est clairement unique, il suffit de montrer que la suite (b_n) dont le n-ième terme est l'écriture de n en base 2 lue en base 8, autrement dit, le $n+1$-ième nombre s'écrivant en base 8 avec seulement des 0 et des 1, satisfait la condition de l'énoncé.

Soit un entier naturel m. Considérons les entier c tel que $0 \leqslant c \leqslant 8^m - 1$, c'est-à-dire que l'écriture en base 2 de c comporte au plus $3m$ chiffres, et montrons que c s'écrit sous la forme $b_i + 2b_j + 4b_k$ avec $0 \leqslant b_i, b_j, b_k \leqslant 8^m - 1$, autrement dit $0 \leqslant i, j, k \leqslant 2^m - 1$. En base 2, nous avons $c = \sum_{i=0}^{3m-1} c_i 2^i$ avec pour tout i, $c_i \in \{0, 1\}$. Alors

$$c = \sum_{p=0}^{m-1} \left(c_{3p}2^{3p} + c_{3p+1}2^{3p+1} + c_{3p+2}2^{3p+2}\right) = \sum_{p=0}^{m-1} c_{3p}8^p + 2\sum_{p=0}^{m-1} c_{3p+1}8^p + 4\sum_{p=0}^{m-1} c_{3p+2}8^p,$$

d'où le résultat, en posant $i = \sum_{p=0}^{m-1} c_{3p} 2^p$, $j = \sum_{p=0}^{m-1} c_{3p+1} 2^p$ et $k = \sum_{p=0}^{m-1} c_{3p+2} 2^p$. Ainsi, les 8^m entiers entre 0 et $8^m - 1$ admettent une écriture sous la forme $a_i + 2a_j + 4a_k$ avec $0 \leqslant i, j, k \leqslant 2^m - 1$. D'autre part, tous les nombres de la forme $a_i + 2a_j + 4a_k$ avec $0 \leqslant i, j, k \leqslant 2^m - 1$ sont entre 0 et $8^m - 1$, et il y en a au plus $2^m \times 2^m \times 2^m = 8^m$, donc l'écriture est en fait unique. Ainsi, les suites (a_n) et (b_n) coïncident, ce qui conclut.

Solution de l'exercice 7 Appelons a_n le nombre cherché, et $f(t)$ la série génératrice de la suite (a_n). Pour $i \geqslant 0$ on appelle $A_i = \{2^i, 2^{i+1}, 3 \cdot 2^i\}$, a_n est le nombre de manières différentes d'obtenir n en choisissant au plus un nombre dans chacun des A_i et en sommant tous les nombres choisis. La série génératrice correspondante est

$$f(t) = \prod_{i \geqslant 0} (1 + t^{2^i} + t^{2^{i+1}} + t^{3 \cdot 2^i}) = \prod_{i \geqslant 0} \frac{1 - t^{2^{i+2}}}{1 - t^{2^i}} = \frac{1}{1-t} \frac{1}{1-t^2}.$$

On trouve la même série génératrice que dans l'exercice 2, donc $a_n = \left[\frac{n}{2}\right] + 1$. Pour une solution sans séries génératrices, nous renvoyons vers le polycopié de Grésillon 2011 (Exercice 9 de combinatoire pour les avancés).

Solution de l'exercice 8 Supposons que $\mathbb{N}$ est partitionné en $S_1, \ldots, S_k$, avec $S_i = \{a_i + nr_i,\ n \in \mathbb{N}\}$, et $r_1 < \ldots < r_k$. Alors par hypothèse nous avons

$$\sum_{n \geqslant 1} x^n = \sum_{n \geqslant 0} x^{a_1 + nr_1} + \ldots + \sum_{n \geqslant 0} x^{a_k + nr_k},$$

ce qui donne

$$\frac{x}{1-x} = \frac{x^{a_1}}{1 - x^{r_1}} + \ldots + \frac{x^{a_k}}{1 - x^{r_k}}.$$

Cette relation est valable pour tout x complexe tel que $|x| < 1$. Si on fait tendre x vers $e^{\frac{2i\pi}{r_k}}$, le côté gauche a une limite finie, tandis que le côté droit diverge à cause de son dernier terme. Nous avons donc une contradiction.

Solution de l'exercice 9 Le calcul des premiers termes suggère que $b(n) = F_n$ où F_n est le n-ième terme de la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$. Nous allons présenter deux méthodes pour y arriver :

1. Avec une bijection : il s'agit d'établir la relation de récurrence $b_{n+2} = b_{n+1} + b_n$. Soit $B(n)$ l'ensemble des sous-ensembles égoïstes de $\{1 \ldots, n\}$. Parmi les éléments de $B(n+2)$, ceux qui ne contiennent pas $n+2$ sont clairement en bijection avec $B(n+1)$. Il nous reste à établir une bijection entre les éléments de $B(n+2)$ contenant $n+2$ et $B(n)$. Étant donné sous-ensemble égoïste de $\{1, \ldots, n\}$, augmentons de 1 tous ses éléments, puis, pour le rendre égoïste de nouveau, ajoutons-lui $n+2$ (qui ne lui appartient pas à l'origine, vu que tous ses éléments, après augmentation, ne dépassent pas $n+1$). Nous obtenons bien un élément de $B(n+2)$ contenant $n+2$. Réciproquement, si on part d'un élément de $B(n+2)$ contenant $n+2$, il ne contient pas 1, car le seul élément de $B(n+2)$ contenant 1 est $\{1\}$. Nous pouvons donc lui enlever $n+2$ et soustraire 1 à tous ses éléments, obtenant ainsi un élément de $B(n)$. Les deux opérations que nous avons décrites sont clairement inverses l'une de l'autre, donc nous avons $b_{n+2} = b_{n+1} + b_n$, et le calcul des premiers termes conclut.

2. Avec les séries génératrices : Comment "représenter" un sous-ensemble fini de $\mathbb{N}$ comme un terme d'une série génératrice ? Si on l'écrit $\{k, k+a_1, k+a_1+a_2, \ldots, k+a_1+\ldots+a_{l-1}\}$, il suffit de le coder à l'aide de son plus petit élément k, et des différences $a_1, \ldots, a_l$ successives entre le premier élément et le deuxième, puis entre le deuxième et le troisième, etc. Ainsi, l'ensemble en question sera "représenté" par le terme $x^k x^{a_1} \ldots x^{a_l}$, de degré égal à son plus grand élément. Un ensemble égoïste de plus petit terme k ayant pour cardinal k, les termes qui nous intéressent vérifient $l = k$, et seront obtenus par développement de la série $x^k(x + x^2 + \ldots)^{k-1}$. Pour tout entier $m \geqslant k-1$, le coefficient du terme de degré $k+m$ dans le développement de cette dernière est en effet clairement égal au nombre d'ensembles égoïstes de cardinal k et de plus grand élément $k+m$. Les termes de degré inférieur à n comptent les ensembles égoïstes de cardinal k ne contenant que des entiers inférieurs à n, donc avec les sous-ensemble égoïstes de cardinal k de $\{1, \ldots, n\}$. En sommant sur k afin d'inclure les ensembles égoïstes de toutes les tailles, on obtient la série

$$\begin{aligned}\sum_{k\geqslant 1} x^k(x + x^2 + x^3 + \ldots)^{k-1} &= \sum_{k\geqslant 1} \frac{x^{2k-1}}{(1-x)^{k-1}} \\ &= x \sum_{k\geqslant 1} \left(\frac{x^2}{1-x}\right)^{k-1} \\ &= x \frac{1}{1-\frac{x^2}{1-x}} \\ &= \frac{x(1-x)}{1-x-x^2}.\end{aligned}$$

Il nous suffit maintenant d'extraire la somme des n premiers coefficients de cette série, en prenant le terme de degré n de

$$\frac{1}{1-x} \times \frac{x(1-x)}{1-x-x^2} = \frac{x}{1-x-x^2}.$$

Et dans cette dernière série on reconnaît bien la série génératrice de F_n.

4 Polynômes

Exercice 1 Soit $P, Q \in \mathbb{R}[X]$ deux polynômes réels non constants ayant les mêmes racines, et tels que $P-1$ et $Q-1$ aussi. Montrer que $P = Q$.

Solution de l'exercice 1 Soit p_0 et p_1 le nombre de racines distinctes respectivement de P et $P-1$. Soit n le degré de P, qu'on peut supposer par symétrie supérieur ou égal à celui de Q. Comme P et $P-1$ sont premiers entre eux, ils n'ont aucune racine commune. On remarque que $P-Q = (P-1)-(Q-1)$, donc ce polynôme admet comme racines à la fois les racines de P et celles de $P-1$, donc p_0+p_1 racines. Il suffit de montrer que ce nombre est strictement supérieur à n pour conclure que $P-Q$ est le polynôme nul, soit $P = Q$.

Pour cela, on étudie les racines multiples en considérant le polynôme dérivé $P' = (P-1)'$. Soit $D_0 = \gcd(P, P')$ et $D_1 = \gcd(P-1, P')$. On sait que $\deg(D_i) = n - p_i$. Par ailleurs, D_0 et

D_1 sont premiers entre eux car P et $P-1$ le sont, et divisent P' donc D_0D_1 divise P' d'où en considérant les degrés : $n-p_1+n-p_2 \geqslant n-1$ soit $p_0+p_1>n$, □.

Exercice 2 Soit $a_i \in \mathbb{Z}, i=1,\dots,n$ des entiers deux à deux distincts, et soit $P := \prod_{i=1}^{n}(X-a_i)-1$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Solution de l'exercice 2 Supposons par l'absurde qu'il existe $Q, R \in \mathbb{Z}[X]$ non constants tels que $P=QR$. Alors $P(a_i)=Q(a_i)R(a_i)=-1$ donc $Q(a_i)=\pm 1$ et $R(a_i)=-Q(a_i)$ soit $(Q+R)(a_i)=0$. Comme Q et R sont de degrés strictement inférieurs à n, on obtient $Q+R=0$ donc $P=-Q^2$, donc P est négatif sur les réels. Ceci est absurde car P tend vers $+\infty$ en $+\infty$.

Exercice 3 Soit $p=3q+1$ un nombre premier ($q \in \mathbb{Z}$). Montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Solution de l'exercice 3 D'après le petit théorème de Fermat, le polynôme $X^{3q}-1$ est scindé à racines simples dans $\mathbb{Z}/p\mathbb{Z}$ (ses racines sont les inversibles de $\mathbb{Z}/p\mathbb{Z}$), donc le polynôme X^2+X+1 aussi car il divise X^3-1 qui divise $X^{3q}-1$. Soit j une racine de X^2+X+1. Alors -3 est le carré de $2j+1$ car $(2j+1)^2=4j^2+4j+1=4(j^2+j+1)-3=-3$. Pour penser à cette formule, il suffit de « résoudre »l'équation $j^2+j+1=0$, qui donne $j=\frac{-1\pm\sqrt{-3}}{2}$.

Exercice 4 Calculer $\sum_{i=1}^{n}\prod_{j\neq i}\frac{X-a_j}{a_i-a_j}$ pour $a_1,\dots,a_n \in \mathbb{R}$ deux à deux distincts.

Solution de l'exercice 4 Ce polynôme est de degré au plus $n-1$ et vaut 1 en a_i donc est identiquement égal à 1.

Exercice 5 Soit $A \in \mathbb{R}[X]$ un polynôme réel. Montrer qu'il existe $P, Q \in \mathbb{R}[X]$ tels que $A=P^2+Q^2$ si et seulement si pour tout réel x, $A(x) \geqslant 0$.

Solution de l'exercice 5 Le sens direct est immédiat. Supposons que pour tout $x \in \mathbb{R}$, on a $A(x) \geqslant 0$. Le polynôme réel A se décompose en produit de facteurs irréductibles de degré 1 et de degré 2. Toute racine réelle a une multiplicité paire, ce sans quoi le polynôme changerait de signe en la racine. Ainsi, le produit des facteurs de degré 1 de A est un carré donc une somme de deux carrés (le second étant 0). Un polynôme irréductible P de degré 2 se met sous forme canonique $(X+a)^2+b$ avec $b \geqslant 0$ car le polynôme est irréductible dans $\mathbb{R}$, d'où $P=(X+a)^2+c^2$ où $b=c^2$, donc P est une somme de deux carrés.

Ainsi, A est le produit de sommes de deux carrés, donc est une somme de deux carrés, par l'identité de Lagrange

$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2.$$

Exercice 6 Montrer $X^2-X+1 \mid (X-1)^{n+2}+X^{2n+1}$ pour tout $n \in \mathbb{N}$.

Solution de l'exercice 6 On raisonne modulo X^2-X+1. On a alors $X^2 \equiv X-1$ donc $(X-1)^{n+2}+X^{2n+1} \equiv X^{2n+4}+X^{2n+1} \equiv X^{2n+1}(X^3+1) \equiv 0$ car X^2-X+1 divise X^3+1.

Exercice 7 Montrer que l'ensemble des réels x vérifiant $\sum_{k=1}^{70}\frac{k}{x-k} \geqslant \frac{5}{4}$ est réunion d'intervalles dont la somme des longueurs vaut 1988.

Solution de l'exercice 7 Soit $Q(x)$ le polynôme $\prod_{k=1}^{70}(x-k)$. L'inégalité est équivalente, après multiplication par $Q(x)^2$ et passage du second membre dans le premier, à $P(x) \geqslant 0$ où $P(X)=Q(X)R(X)$ avec $R(X)=4\sum_{k=1}^{70}k\prod_{1\leqslant i\neq k\leqslant 70}(X-i)-5Q(X)$.

On remarque $R(1) < 0$, $R(2) > 0$, $R(3) < 0$, ..., $R(70) > 0$ et $R(+\infty) = -\infty$ donc R a pour racines les r_i tels que $1 < r_1 < 2 < r_2 < \cdots < 70 < r_{70}$, et P a pour racines les r_i et les entiers compris entre 1 et 70 inclus. Or P est négatif en $\pm\infty$ donc P est positif sur la réunion des intervalles $[k, r_k]$ pour $1 \leqslant k \leqslant 70$, dont la longueur totale vaut $\sum_{i=1}^{70}(r_i - i)$. Par les relations coefficients racines, on déduit du coefficient de X^{69} dans R que $\sum_{i=1}^{70} r_i = \frac{9}{5}\sum_{i=1}^{70} i$ donc la longueur totale des intervalles vaut $\frac{4}{5}\sum_{i=1}^{70} i = 1988$.

Exercice 8 Si P est un polynôme à coefficients entiers, on note $w(P)$ le nombre de ses coefficients impairs. Soit $Q_i = (1+x)^i$. Montrer que pour tout suite d'entiers $0 \leqslant i_1 < i_2 < \cdots < i_n$, $w(Q_{i_1} + \cdots + Q_{i_n}) \geqslant w(Q_{i_1})$.

Solution de l'exercice 8 On remarque $w(P \pm Q) \leqslant w(P) + w(Q)$ (inégalité triangulaire), et en ce qui concerne la multiplication, si $\deg(P) < k$ alors $w((1+X^k)P) = w(P)+w(PX^k) = 2w(P)$ $(*)$. En calculant $w(Q_i)$ pour des i petits, on remarque l'égalité polynômiale dans $\mathbb{Z}/2\mathbb{Z}$ suivante, qui se démontre facilement : $(1+X)^{2^k} \equiv 1 + X^{2^k}[2]$, qui nous permet de simplifier le calcul de w, car si $i = 2^k + i'$ avec $i' < 2^k$, $w(Q_i) = w((1+X^{2^k})(1+X)^{i'}) = 2w(Q_{i'})$. Cela va nous permettre de procéder par récurrence sur i_n.

On suppose le résultat acquis pour $i_n < N$ et on considère le cas $i_n = N$. Soit k tel que $2^k \leqslant N < 2^{k+1}$. Si $i_1 \geqslant 2^k$, posons $i_l = 2^k + i'_l$, alors d'après le calcul précédent, $w(Q_{i_1}+\cdots+Q_{i_n}) = 2w(Q_{i'_1}+\cdots+Q_{i'_n})$, $w(Q_{i_1}) = 2w(Q_{i'_1})$. Or, par hypothèse de récurrence, $w(Q_{i'_1}+\cdots+Q_{i'_n}) \geqslant w(Q_{i'_1})$. En multipliant par 2, on obtient donc $w(Q_{i_1} + \cdots + Q_{i_n}) \geqslant w(Q_{i_1})$.

Si $i_1 < 2^k$, soit r tel que $i_r < 2^k \leqslant i_{r+1}$. Alors, en appliquant successivement la remarque $(*)$, l'inégalité triangulaire, et l'hypothèse de récurrence, on obtient l'inégalité

$$w(Q_{i_1} + \cdots + Q_{i_n}) = w\Big(\sum_{1\leqslant l\leqslant r} Q_{i_l} + \sum_{r<l\leqslant n} Q_{i'_l}\Big) + w\Big(\sum_{r<l\leqslant n} Q_{i'_l}\Big) \geqslant w\Big(\sum_{1\leqslant l\leqslant r} Q_{i_l}\Big) \geqslant w(Q_{i_1}),$$

ce qui conclut.

Exercice 9 Trouver les couples (n, m) tels que $n > 2$, $m > 2$, et il existe une infinité d'entiers naturels k tels que $k^n + k^2 - 1$ divise $k^m + k - 1$.

Solution de l'exercice 9 Si (n, m) est un tel couple, soit $P_n(X) = X^n+X^2-1$ et $P_m(X) = X^m+X-1$. Alors le reste R dans la division euclidienne de P_m par P_n est de degré strictement inférieur à n. Ainsi, pour une infinité d'entiers k, $P_n(k)$ divise $R(k)$ et $|P_n(k)| > |R(k)|$, ce qui montre que $R(k) = 0$. R a donc une infinité de racines, ce qui montre que $R = 0$ et que P_n divise P_m. En travaillant modulo $X^n + X^2 - 1$, on a $\frac{X^n}{1+X} \equiv 1 - X$ ($1 + X$ est inversible car -1 n'est pas racine de $X^n + X^2 - 1$) et $X^m + X - 1 \equiv 0$ donc $X^m \equiv 1 - X$, d'où $X^{m+1} + X^m - X^n \equiv 0$ d'où $P_k(X) = X^{k+1} + X^k - 1$ est divisible par P_n, en posant $k = m - n$. Puisque $P_k \neq 0$, on sait que $k + 1 \geqslant n$.

Si $k + 1 = n$ alors P_n divise $P_k - P_n = X^{n-1} - X^2$, donc $n = 3$ et $m = 5$, ce qui convient. Au contraire, si $k \geqslant n$, notons que $P_n(0) = -1$ et que $P_n(1) = 1$: P_n a donc une racine $x \in]0; 1[$. Or, $x^{k+1} < x^n$ et $x^k < x^2$, car $n > 2$. Donc $P_k(x) < P_n(x) = 0$, ce qui absurde car x est une racine de n que P_k ne partage pas.

Ainsi, seul le couple $(3, 5)$ convient.

VI. Quatrième période

Contenu de cette partie

1 Groupe A : arithmétique

1 Cours/TD d'arithmétique

Ceci constitue le premier cours d'arithmétique donné aux groupe A. Ont été étudiées les notions de divisibilité, de nombres premiers, de décomposition en facteurs premiers, de division euclidienne, de pgcd de ppcm ainsi que le théorème de Bézout et le lemme de Gauss. Nous renvoyons le lecteur au polycopié d'Animath à ce sujet : http://www.animath.fr/IMG/pdf/cours-arith1.pdf.

Exercice 1 Soient x et y deux entiers. Montrer que $2x + 3y$ est divisible par 7 si et seulement si $5x + 4y$ l'est.

Solution de l'exercice 1 On utilise le fait que 7 divise $7(x + y)$ et que si un nombre divise deux entiers, il divise leur différence.
Ainsi, si 7 divise $2x + 3y$, alors 7 divise $7x + 7y - (2x + 3y) = 5x + 4y$.
Réciproquement, si 7 divise $5x + 4y$, alors 7 divise $7x + 7y - (5x + 4y) = 2x + 3y$.

Exercice 2 Pour quels entiers n strictement positifs le nombre $n^2 + 1$ divise-t-il $n + 1$?

Solution de l'exercice 2 Les entiers considérés sont strictement positifs. Ainsi, si $n^2 + 1$ divise $n + 1$, alors $n^2 + 1 \leqslant n + 1$, d'où $n^2 \leqslant n$. Et puisque $n > 0$, $n \leqslant 1$. Enfin, n étant entier le seul candidat restant est $n = 1$, et on vérifie qu'il convient : 2 divise 2. C'est bon !

Les exercices suivants on pour but de montrer l'importance de la factorisation dans les exerices faisant appel à la divisibilité.
Exercice 3 Trouver toutes les valeurs de $n \in \mathbb{N}$ telles que $3^{2n} - 2^n$ est premier.

Solution de l'exercice 3 L'expression dont on cherche à discuter de la primalité peut se réécrire $3^{2n} - 2^n = (3^2)^n - 2^n = 9^n - 2^n = (9 - 2)(9^{n-1} + 9^{n-2} \cdot 2 + 9^{n-3} \cdot 2^2 + \cdots + 2^{n-1})$.

Pour $n \geqslant 2$, le facteur de droite est supérieur ou égal 9^1, donc différent de 1. Le facteur de gauche étant lui-même différent de 1, on en déduit donc que $3^{2n} - 2^n$ est composé.

Il suffit de traiter les cas restants à la main : pour $n = 1$, $9 - 2 = 7$ est premier, pour $n = 0$, $0 - 0 = 0$ n'est pas premier.

L'ensemble cherché est donc $\{1\}$.

Remarque 1.1. Factoriser une expression n en $n = ab$ est une méthode très classique pour montrer qu'un nombre n'est pas premier. Mais attention, la factorisation ne représente que la moitié du travail. Il reste à vérifier que les deux facteurs sont des diviseurs stricts. Cela peut se faire en vérfiant que $a > 1$ et $b > 1$ comme tout-à-l'heure, ou en vérifiant que $1 < a < n$, ou encore en vérifiant que $a < n$ et $b < n$.

Exercice 4 Montrer qu'il existe une infinité de $a \in \mathbb{N}$ tels que $n^4 + a$ n'est premier pour aucun entier $n > 0$.

Solution de l'exercice 4 Ici aussi, il s'agit de chercher une factorisation de $n^4 + a$. Les élèves ont immédiatement reconnu l'identité de Sophie Germain, étudiée pendant le cours d'algèbre quelques jours plus tôt. Cela amène à poser $a = 4k^4$ afin d'écrire :

$$n^4 + 4k^4 = (n^2 + 2k^2)^2 - 4n^2 \cdot k^2 = (n^2 + 2k^2)^2 - (2nk)^2 = (n^2 + 2k^2 + 2nk)(n^2 + 2k^2 - 2nk)$$

Pour $k \geqslant 1$, les deux facteurs sont supérieurs strictement à 1. Ainsi les valeurs $\{4 \cdot 1^4, 4 \cdot 2^4, \ldots, 4 \cdot k^4, \ldots, \ldots\}$ constituent une inifinité de valeurs convenables pour a.

Exercice 5 Étant donné $n \in \mathbb{N}$, montrer qu'il existe $r \in \mathbb{N}$ tel qu'aucun des nombres $r+1, r+2, r+3, \ldots r+n$ ne soient premiers.

Solution de l'exercice 5 Choisissons $r = (n+1)! + 1$. Alors, on vérifie facilement que $r+1$ différent de 2 mais est divisible par 2, que $r+2$ est différent de 3 mais est divisible par 3, ...que $r+k$ est différent de $k+1$ mais est divisible par $k+1$,...que $r+n$ est différent de $n+1$ mais est divisible par $n+1$. Ainsi, un tel r convient.

Exercice 6 Combien 24 a-t-il de diviseurs ? et 140 ? et 2012^{2013} ?

Solution de l'exercice 6 Posons-nous directement la question plus générale du nombre de diviseurs de l'entier $n = \prod_{i=1}^{k} p_i^{\alpha_i}$rith

Pour qu'un entier d divise n, il est nécessaire est suffisant que pour tout i, l'exposant de p_i dans sa décomposition en facteurs premiers soit inférieur ou égal à l'exposant correspondant dans la décomposition de n. (Pour plus d'informations à ce sujet, consulter le paragraphe *valuation* p*-adiques* du polycopié d'arithmétique)

Ainsi, si on écrit $d = \prod_{i=1}^{k} p_i^{\delta_i}$, on doit avoir $\delta_i \in \{0, 1, \ldots, \alpha_i\}$ ce qui fait $\alpha_i + 1$ possibilités pour l'exposant de p_i dans d.

Finalement, le nombre de diviseurs de n vaut : $\prod_{i=1}^{k} (\alpha_i + 1)$

En conclusion, $24 = 2^3 \times 3$ admet $4 \times 2 = 8$ diviseurs, $140 = 2^2 \times 5 \times 7$ admet $3 \times 2 \times 2 = 12$ diviseurs et $2012^{2013} = 2^{4026} \times 503^{2013}$ admet $4027 \times 2014 = 8110378$ divieurs.

Exercice 7 Montrer que, pour tout entier n, la fraction $\frac{39n+4}{26n+3}$ est irréductible.

Solution de l'exercice 7 Les exercices de ce types amènent à faire la division euclidienne du numérateur par le dénominateur et à réitérer conformément à l'algorithme d'Euclide. Cela s'écrit :

$$\begin{aligned} 39n+4 &= (26n+3) + (13n+1) \\ 26n+3 &= 2(13n+1) + 1 \end{aligned}$$

Le pgcd de $39n+4$ et $26n+3$ vaut donc 1, ce qui montre que la fraction est irréductible.

Exercice 8 Montrer que pour tout n entier, la fraction $\frac{2n^2+9n-17}{n+6}$ est irréductible.

Solution de l'exercice 8 On procède de la même façon : $2n^2 + 9n - 17 = (2n-3)(n+6) + 1$. Si d divise $2n^2 + 9n - 17$ et $2n - 3$, alors d divise 1. Le pgcd vaut donc 1 et la fraction est donc irréductible.

On conclut le cours en mentionnant le résultat trivial mais non moins utile qu'entre deux carrés parfaits consécutifs, il ne peut en exister un troisième.

Exercice 9 Trouver tous les a entiers positifs tels que $a^2 + 2a$ soit un carré parfait.

Solution de l'exercice 9 On distingue deux cas. Si $a > 0$, on remarque que $a^2 < a^2 + 2a < a^2 + 2a + 1 = (a+1)^2$. Donc $a^2 + 2a$ ne peut être un carré parfait. Si $a = 0$, on trouve $a^2 + 2a = 0$ qui est un carré parfait. C'est donc le seul.

2 Cours d'arithmétique

Cette séance parlait des congruences. L'essentiel de ce qui a été vu pendant la séance est traité sur le cours du site d'Animath, dans le chapitre 3. Je ne vais donc pas refaire le cours entier, mais juste donner un résumé, en renvoyant vers le cours pour plus de précisions. L'adresse de ce cours est à l'adresse http ://www.animath.fr/spip.php ?article255.

J'ai commencé par définir les congruences (définition 3.1.1), en comparant congruences modulo un entier 12 avec les heures écrites sur une horloge à 12 chiffres, puis par analogie en comparant les congruences modulo un entier n quelconque avec les heures écrites autour d'une hypothétique horloge à n chiffres.

J'ai ensuite insité sur la dernière propriété du cours : on peut « additionner » et « multiplier » les modulo. Intuitivement, la propriété sur l'addition peut se visualiser en remarquant que avancer de 15 heures à partir d'une position donnée sur l'horloge à 12 heures, c'est la même chose que d'avancer de 3 heures. Pour visualiser la propriété sur la multiplication, une idée est de regarder modulo 10 : un nombre est congru à son dernier chiffre modulo 10, et on sait bien que pour trouver le dernier chiffre d'un produit de deux nombres, il suffit d'examiner le produit des deux derniers chiffres.

Je suis ensuite passé à la partie 3.2, sur les critères de divisibilité. Si en entier s'écrit $\overline{abcde}$ en base 10, alors il vaut $a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + d \cdot 10 + e$. Si on connaît les valeurs prises par la suite $(10)^n$ modulo k, alors on aura une méthode rapide pour trouver la valeur de $\overline{abcde}$ modulo k.

Par exemple, avec $k = 7$, on vérifie que $10 \equiv 3\,[7]$, $10^2 \equiv 2\,[7]$, $10^3 \equiv -1\,[7]$, et $10^4 \equiv -3\,[7]$. Ainsi, on aura

$$\begin{aligned}\overline{abcde} &\equiv a \cdot (-3) + b \cdot (-1) + c \cdot 2 + d \cdot 3 + e\,[7] \\ &\equiv -3a - b + 2c + 3d + e\,[7]\,.\end{aligned}$$

Un exemple concret : $\overline{17255} \equiv -3 - 7 + 4 + 15 + 5\,[7]$, et donc il est divisible par 7. On peut fabriquer autant de tels critères que l'on veut.

On voit sur cet exemple la grande force de la notion de congruence : elle permet de remplacer des calculs sur des grands nombres par des calculs sur des nombres bien plus petits, donc plus faciles. Un exemple spectaculaire est donné par l'exercice suivant. Il utilise une astuce classique, due au fait que 10 est congru à 1 modulo 9 : un nombre est toujours congru à la somme de ses chiffres modulo 9.

Exercice 1 Calculer la somme des chiffres de la somme des chiffres de la somme des chiffres de $A := 4444^{4444}$.

Solution de l'exercice 1 Notons $S(n)$ la somme des chiffres d'un entier n. Alors notre astuce dit que pour tout n, $S(n) \equiv n\,[9]$. Ainsi, $S(S(S(A))) \equiv A\,[9]$. Calculons donc A modulo 9. On a $4444 \equiv 4 + 4 + 4 + 4 \equiv -2\,[9]$, il faut donc calculer $(-2)^{4444}$ modulo 9. On remarque que $(-2)^3 \equiv 1\,[9]$. On en déduit que $(-2)^{3k+i} \equiv ((-2)^3)^k \cdot (-2)^i \equiv (-2)^i\,[9]$. En particulier, comme $4444 \equiv 4 + 4 + 4 + 4 \equiv 1\,[3]$, donc $(-2)^{4444} \equiv (-2) \equiv 7\,[9]$.

Ainsi, on connaît $S(S(S(A)))$ modulo 9. Pour trouver sa vraie valeur, l'idée à avoir est que $S(n)$ est en général beaucoup plus petit que n. Ainsi, $S(S(S(A)))$ est beaucoup beaucoup beaucoup plus petit que A, et avec un peu de chance il sera suffisamment petit pour pouvoir le déterminer. On écrit donc que $A \leqslant (10^4)^{5000} = 10^{20000}$, donc A a au plus 20000 chiffres, donc

$S(A) \leqslant 20000 \cdot 9 \leqslant 200000$. Donc $S(S(A)) \leqslant 1 + 9 \cdot 5 = 46$, puis $S(S(S(A))) \leqslant 3 + 9 = 12$. Or il vaut 7 modulo 9, c'est donc nécessairement 7.

La seconde partie de la séance fut consacrée a l'étude des équations linéaires modulo n. Nous avons examiné les équations $5x \equiv 10\,[16]$ et $5x \equiv 10\,[15]$. Dans chaque cas, on est tenté de « diviser par 5 ». CELA N'A AUCUN SENS, ET IL NE FAUT SURTOUT PAS LE FAIRE. Les seules opérations que nous avons le droit de faire modulo n sont l'addition et la multiplication, n'allez pas inventer d'autres règles comme une éventuelle division par 5, dans la majorité des cas, ce sera faux.

Résolvons explicitement ces systèmes. Pour le premier, l'équation se réécrit $5x = 16k + 10$. En particulier 5 doit divise 16k, or il est premier avec 16, il divise donc k par lemme de Gauss : on écrit $k = 5k'$ puis on divise par 5, et il reste $x = 16k' + 2$. Réciproquement, on vérifie que les $x \equiv 2\,[16]$ conviennent : dans ce cas, la « division par 5 » aurait donc donné le bon résultat.

Pour le deuxième, il se réecrit $5x = 15k+10$: on divise par 5 et $x = 3k+2$. Réciproquement, les $x \equiv 2\,[3]$ sont solution. Dans ce cas, la « division par 5 » n'aurait pas marché.

Les résultats 3.1.2 et 3.1.3 du cours précisent tout cela. En fait, la « division par 5 » que l'on a envie de faire peut se voir comme une multiplication par $1/5$, et le théorème 3.1.2 dit précisément que, dans certains cas, on a une notion d'inverse modulo n. Ainsi, 5 possède un inverse modulo 16 (par exemple -3), on peut donc multiplier l'équation $5x \equiv 10\,[16]$ par -3, on obtient $x \equiv 5\cdot(-3)\cdot x \equiv 10\cdot(-3) \equiv 2\,[16]$. C'est là l'essence de la proposition 3.1.3. Par contre, 5 n'a pas d'inverse modulo 15 (si vous voulez le prouver, partez du fait que $5 \cdot 3 \equiv 0\,[15]$). Quand on examine la preuve de ces résultats, on remarque que c'est juste une utilisation du théorème de Bézout. En particulier, si on connaît un couple de Bézout pour les entiers c et N (c'est-à-dire x et y tels que $xc + yN = 1$), alors on connaît un inverse de c modulo N : x. La partie 2.3 du cours est donc fondamentale : elle explique comment, à partir de la division euclidienne, on peut construire des couples de Bézout. Ainsi, on dispose d'un algorithme très pratique pour déterminer les inverses modulo N.

Je suis ensuite passé aux systèmes de plusieurs équations, en donnant l'exemple du système $\begin{cases} x \equiv 5\,[7] \\ x \equiv 8\,[11] \end{cases}$. On peut résoudre ce système explicitement, ainsi la première équation nous permet d'écrire x sous la forme $7k + 5$, et ensuite on doit avoir $7k + 5 \equiv 8\,[11]$, autrement dit $7k \equiv 3\,[11]$ puis $k \equiv 2\,[11]$ en multipliant par l'inverse 8 de 7 modulo 11. Ainsi, k est de la forme $11k' + 2$, puis x est de la forme $7(11k' + 2) + 5$, c'est-à-dire $77k' + 19$. Réciproquement, ces nombres sont bien solutions.

En fait un théorème, appelé théorème chinois, 3.4.1 dans le cours, dit que ce genre de méthode est très générale : si m et n sont deux nombres premiers entres eux, si $um+vn = 1$ est une relation de Bézout entre ces deux entiers, alors les solutions du système $\begin{cases} x \equiv a\,[m] \\ x \equiv b\,[n] \end{cases}$ sont exactement les nombres congrus à $s := umb + vna$ modulo mn. En effet, ce nombre est clairement solution (remarquez que $um \equiv 1\,[n]$, c'est le sens de la relation de Bézout), et si x est une autre solution, alors m et n divise $x - s$, donc leur produit divise $x - s$ (car m et n sont premiers entre eux), donc $x \equiv s\,[mn]$. Remarquez à nouveau la grande utilité de l'algorithme d'Euclide : il permet de trouver le coefficients de Bézout, donc de résoudre directement de tels systèmes d'équations.

3 TD d'arithmétique

- Énoncé des exercices -

Exercice 1 Soient $a, b \geqslant 1$ des entiers.

(i) A-t-on a divise b^2 si et seulement si a divise b ?

(ii) A-t-on a^2 divise b^2 si et seulement si a divise b ?

Exercice 2 Trouver tous les entiers n tels que $2^n + 3$ est un carré parfait. Même question avec $2^n + 1$.

Exercice 3 Montrer que si n admet un diviseur impair $m > 1$, alors $2^n + 1$ n'est pas premier.

Exercice 4 Montrer que pour tout p premier et tout entier $0 < k < p$, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ est divisible par p.

Exercice 5 Montrer que la fraction $\frac{12n+1}{30n+2}$ est toujours irréductible.

Exercice 6 Montrer qu'un nombre est divisible par 3 si et seulement si la somme de ses chiffres dans la décomposition en base 10 de ce nombre est un multiple de 3. Montrer ensuite le même résultat pour 9.

Exercice 7 Montrer que si (x, y, z) est une solution de l'équation suivante alors x ou y est un multiple de 2.

$$x^2 + y^2 = z^2$$

Exercice 8 Écrire sous forme d'une fraction le nombre

$$x = 0,5123412341234123412341234123412341234\ldots$$

Exercice 9 Montrer que l'équation

$$x^3 + 3y^3 + 9z^3 = 9xyz$$

n'a pas d'autre solution rationnelle que $x = y = z = 0$. On commencera par chercher les solutions entières.

Exercice 10 Montrer que le produit de cinq nombres consécutifs ne peut pas être un carré.

- Solution des exercices -

Solution de l'exercice 1

(i) Si a divise b, alors comme b divise b^2, on a a divise b^2. En revanche, si a divise b^2, il ne divise pas forcément b. Par exemple 9 divise 3^2 mais 9 ne divise pas 3.

(ii) Si a divise b, on peut écrire $b = ka$ avec $k \geqslant 1$ entier. On élève cette égalité au carré, on obtient $b^2 = k^2a^2$ donc a^2 divise b^2.

Supposons réciproquement que a^2 divise b^2. On va montrer que a divise b. On note pour un nombre n $v_p(n)$ la plus grande puissance de p divisant n (valuation p-adique). Pour tout nombre p premier divisant a, et puisque a^2 divise b^2, on a $v_p(a^2) \leqslant v_p(b^2)$. Or, $v_p(a^2) = 2v_p(a)$ et $v_p(b^2) = 2v_p(b)$. Donc $v_p(a) \leqslant v_p(b)$. Cela montre bien que a divise b.

Solution de l'exercice 2

- Un carré n'est jamais congru à 3 mod 4, donc si $n \geqslant 2$, $2^n + 3$ ne peut jamais être un carré. Pour $n = 1$, on a $2^1 + 3 = 5$ n'est pas le carré d'un entier. Pour $n = 0$, $2^0 + 3 = 4$ est le carré de 2.
- On cherche deux entiers n et x tels que $2^n + 1 = x^2$. On réécrit cette équation $2^n = x^2 - 1 = (x+1)(x-1)$. $x+1$ et $x-1$ sont tous les deux des puissance de 2. Les seules puissances de 2 à distance 2 l'une de l'autre sont 2 et 4. Donc $2^n = 2 \times 4 = 8 = 2^3$. $n = 3$ est la seule solution.

Solution de l'exercice 3 On écrit $n = km$ avec $k \geqslant 1$ et $m > 1$ impair. Comme $a^m + b^m$ se factorise par $a + b$ quand m est impair, l'entier $(2^k)^m + 1$ est divisible par $2^k + 1$, donc n'est pas premier.

Solution de l'exercice 4 Écrivons l'égalité sans dénominateur : $\binom{p}{k} \times k!(p-k)! = p!$. Comme $0 < k < p$, on a $k < p$ et $p - k < p$. Ainsi p divise $\binom{p}{k} \times k!(p-k)!$ mais ne divise pas $k!(p-k)!$. D'après le lemme de Gauss, p divise donc $\binom{p}{k}$.

Solution de l'exercice 5 D'après l'algorithme d'Euclide, $\text{pgcd}(30n + 2, 12n + 1) = \text{pgcd}(12n + 1, 6n) = \text{pgcd}(6n, 1) = 1$.

Solution de l'exercice 6 Soit n un entier naturel et $a_0, \ldots, a_k$ les chiffres de la décomposition de n en base 10, c'est-à-dire $n = a_0 10^0 + a_1 10^1 + \cdots + a_k 10^k$. On $10 \equiv 1$ mod 3 donc par récurrence pour $j \geqslant 1$ on a $10^j \equiv 1$ mod 3. Donc $n \equiv a_0 + \cdots + a_k$ mod 3. Les restes de la division par 3 de n et de la somme des chiffres de la décomposition de n en base 10 sont les mêmes. La preuve précédente est exactement la même pour 9.

Solution de l'exercice 7 On regarde l'équation modulo 4. Si x et y sont tous les deux impairs, alors $x^2 \equiv y^2 \equiv 1$ donc $z^2 = x^2 + y^2 \equiv 2$. Or, un carré ne peut pas être congru à 2 modulo 4.

Solution de l'exercice 8 On a

$$10x = 5,123412341234123412341234\ldots$$

et

$$100000x = 51234,123412341234123412341234123412341234\ldots$$

donc $99990x = 51229$ et finalement $x = \frac{51229}{99990}$. On peut généraliser cette méthode à tout nombre qui admet un développement décimal périodique.

Solution de l'exercice 9 Si on a une solution rationnelle non nulle alors en multipliant par le cube du ppcm des dénominateurs de x, y et z, on obtient une solution entière non nulle. On cherche donc les solutions entières. On suppose par l'absurde qu'on a un triplet d'entiers (x_0, y_0, z_0), dont au moins un terme est non nul, qui vérifie l'équation. On regarde l'équation

modulo 3, on obtient $x_0 \equiv 0 \pmod 3$: x_0 est donc un multiple de 3. On peut écrire $x_0 = 3x_1$ avec x_1 entier. L'équation devient

$$27x_1^3 + 3y_0^3 + 9z_0^3 - 27x_1y_0z_0 = 0,$$

soit

$$9x_1^3 + y_0^3 + 3z_0^3 - 9x_1y_0z_0 = 0.$$

Ainsi, (y_0, z_0, x_1) est une autre solution de l'équation de départ. De même, on peut montrer que $y_0 = 3y_1$ et $z_0 = 3z_1$ avec y_1 et z_1 entiers, donc (x_1, y_1, z_1) est une nouvelle solution.

On obtient que x_0, y_0, z_0 sont divisibles par toute puissance de 3, ce qui est impossible pour des entiers non nuls.

Solution de l'exercice 10 On suppose que a, b, c, d, e sont des entiers consécutifs tels que le produit $abcde$ soit un carré. Si un des cinq nombres contient un facteur premier p supérieur ou égal à 5, alors les quatre autres ne le contiennent pas (car ils sont consécutifs). Comme le produit est un carré, ce facteur premier p apparaît avec une puissance paire. Selon les puissances de 2 et de 3 dans chaque nombre, chacun des nombres a, b, c, d ou e est

1. un carré ;
2. deux fois un carré ;
3. trois fois un carré ;
4. six fois un carré.

On applique le principe des tiroirs, deux des cinq nombres sont dans la même catégorie. Si ces deux nombres sont dans les catégories 2, 3 ou 4, alors leur différence est au moins six, ce qui est impossible car a, b, c, d, e sont consécutifs. Si les deux nombres sont dans la catégorie 1, ils sont tous les deux des carrés. Alors e ne peut pas dépasser 5 car les seuls carrés à distance inférieure à 5 sont 1 et 4. Or $1 \times 2 \times 3 \times 4 \times 5 = 120$, qui n'est pas un carré.

Il est donc impossible que les produit de cinq entiers strictement positifs consécutifs soit un carré.

2 Groupe B : arithmétique

1 Cours/TD d'arithmétique

Exercice 1 Soient x et y des entiers. Montrer que $2x + 3y$ est divisible par 7 si, et seulement si $5x + 4y$ l'est.

Solution de l'exercice 1 Il suffit de remarquer que :

$$(2x + 3y) + (5x + 4y) = 7x + 7y,$$

Cette quantité étant toujours divisible par 7.

Exercice 2 Résoudre dans $\mathbb{Z}$ les équations suivantes :

(i) $x - 1 \mid x + 3$.

(ii) $x + 2 \mid x^2 + 2$

Solution de l'exercice 2

(i) Pour $x \in \mathbb{Z}$,

$$\begin{aligned} x - 1 \mid x + 3 &\iff x - 1 \mid (x + 3) - (x - 1) \\ &\iff x - 1 \mid 4 \end{aligned}$$

Or l'ensemble des diviseurs de 4 est $\{-4, -2, -1, 1, 2, 4\}$. L'ensemble des solutions est donc $\{-3, -1, 0, 2, 3, 5\}$

(ii) Pour $x \in \mathbb{Z}$,

$$\begin{aligned} x + 2 \mid x^2 + 2 &\iff x + 2 \mid x^2 + 2 - (x + 2)^2 \\ &\iff x + 2 \mid -2 - 4x \\ &\iff x + 2 \mid 4(x + 2) - 6 \\ &\iff x + 2 \mid 6. \end{aligned}$$

Or l'ensemble des diviseurs de 6 est $\{-6, -3, -2, -1, 1, 2, 3, 6\}$. L'ensemble des solutions est donc $\{-8, -5, -4, -3, -1, 0, 1, 4\}$

Exercice 3 Montrer que si un nombre premier p divise le produit $a_1 \times \cdots \times a_n$, alors il divise au moins l'un des a_i.

Solution de l'exercice 3 Supposons par l'absurde que p ne divise aucun des a_i pour $i \leqslant n - 1$. Alors p est clairement premier avec chacun des a_i. Ainsi, en écrivant :

$$p \mid a_1 \cdot (a_2 \cdot \cdots \cdot a_n),$$

le théorème de Gauss nous donne que $p \mid a_2 \cdot \cdots \cdot a_n$. En itérant, on aboutit à $p \mid a_n$, ce qui conclut.

Exercice 4 Montrer que si deux entiers premiers entre eux a et b divisent n, alors le produit ab divise également n.

Solution de l'exercice 4 Comme a divise n, on peut écrire $n = ak$ pour un certain entier k. Mais alors b divise ak et comme il est premier avec a, il divise k. Ainsi $k = bk'$ pour un entier k' et puis $n = abk'$, ce qui prouve bien que ab divise n.

Exercice 5 Soit $b \geqslant 2$ un entier. Montrer que tout entier $a \geqslant 0$ s'écrit de façon unique sous la forme :

$$a = a_0 + a_1 b + a_2 b^2 + \cdots + a_k b^k,$$

où k est un entier, les a_i sont des entiers compris entre 0 et $b-1$ et où $a_k \neq 0$.

Solution de l'exercice 5 On obtient l'écriture demandée par divisions euclidiennes successives par b. On écrit d'abord :

$$a = bq_0 + a_0,$$

avec $0 \leqslant a_0 < b$. Si $q_0 = 0$, cette écriture convient. Sinon, on effectue la divison euclidienne de q_0 par b : $q_0 = bq_1 + a_1$ avec $0 \leqslant a_1 < b$. Cela donne :

$$a = a_0 + a_1 b + a_2 b^2.$$

Si $q_1 = 0$, c'est terminé. Sinon, on continue. La suite des q_i est positive et strictement décroissante. Elle finit donc par s'annuler et la procédure s'arrête bien. On a alors la décomposition souhaitée.

Pour prouver l'unicité, considérons des entiers a_i et a'_i compris entre 0 et $b-1$ tels que :

$$a_0 + a_1 b + \cdots + a_k b^k = a'_0 + a'_1 b + \cdots + a'_k b^k.$$

Alors $a_0 - a'_0$ est un multiple de b et on a $-b < a_0 - a'_0 < b$. Nécessairement $a_0 = a'_0$. On peut alors simplifier par a_0, et utiliser le même argument pour a_1, et ainsi de suite.

Exercice 6 Trouver toutes les solutions $(x, y) \in \mathbb{N}^2$ de l'équation :

$$x \wedge y + x \vee y = x + y.$$

Solution de l'exercice 6 Soit $(x, y) \in \mathbb{N}^2$ un couple solution. Notons $d = x \wedge y$. Il existe $x', y' \in \mathbb{N}$ tels que :

$$\begin{cases} x = dx' \\ y = dy' \\ x' \wedge y' = 1. \end{cases}$$

L'équation devient :

$$\begin{aligned} 1 + x'y' = x' + y' &\iff (x'-1)(y'-1) = 0 \\ &\iff x' = 1 \text{ ou } y' = 1. \end{aligned}$$

Ainsi (x, y) est de la forme (d, dk) ou (dk, d) avec $d, k \in \mathbb{N}$.

Réciproquement, ces couples sont bien solution.

Exercice 7 Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. On note q le quotient de la division euclidienne de $a-1$ par b. Soit $n \in \mathbb{N}$. Déterminer, en fonction de q, le quotient de la division euclidienne de $(ab^n - 1)$ par b^{n+1}.

Solution de l'exercice 7 Par définition de q, on a $a-1 = bq+r$ avec $0 \leqslant r < b$. On peut alors écrire :

$$\begin{aligned} ab^n - 1 &= (bq+r+1)b^n - 1 \\ &= qb^{n+1} + b^n(r+1) - 1. \end{aligned}$$

Or, $0 \leqslant b^n(r+1) - 1 < b^{n+1}$ donc la relation ci-dessus est bien la division eucildienne de $ab^n - 1$ par b^{n+1}. Le quotient recherché est donc q.

Exercice 8 Montrer que si $n \geqslant 2$ n'est pas premier, $2^n - 1$ ne l'est pas non plus.

Solution de l'exercice 8 L'idée de l'exercice est d'utiliser la relation

$$x^k - y^k = (x-y)(x^{k-1} + x^{k-2}y + \cdots + y^{k-1}).$$

n n'étant pas premier, on peut écrire $n = ab$ avec $a, b \geqslant 2$. Et alors :

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)(2^{a-1} + \dots),$$

ce qui prouve que $2^n - 1$ n'est pas premier.

Exercice 9 Soient a et b deux entiers natuels non nuls. Montrer que

$$(2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1.$$

Solution de l'exercice 9 Etablissons d'abord le lien entre le reste de la division euclidienne de a par b et celui de la division de $2^a - 1$ par $2^b - 1$. Notons $a = bq + r$ avec $0 \leqslant r < b$. On peut alors écrire :

$$2^a - 1 = 2^{bq+r} - 1 = 2^{bq+r} - 2^r + 2^r - 1 = (2^b - 1)(2^{b(q-1)} + 2^{b(q-1)-1} + \cdots + 1)2^r + 2^r - 1,$$

et on a alors $0 \leqslant 2^r - 1 < 2^b - 1$.

On effectue la divison euclidienne de a par b, et on note les $a_0 = a$, $a_1 = b$, ... les entiers obtenus, qui vérifient $a_{k+1} \wedge a_k = a_k \wedge a_{k-1}$. On peut à présent écrire l'algorithme d'Euclide partant de $2^a - 1$ et de $2^b - 1$ avec ces coefficients :

$$(2^a-1)\wedge(2^b-1) = (2^{a_0}-1)\wedge(2^{a_1}-1) = (2^{a_1}-1)\wedge(2^{a_2}-1) = \cdots = (2^{a_m}-1)\wedge 2^0 - 1 = 2^{a_m} - 1,$$

ce dernier a_m non nul étant bien égal à $a \wedge b$.

2 Cours d'arithmétique

Vu en cours :
- Existence et unicité de la décomposition en facteurs premiers
- Valuation p-adique, lien avec la divisibilité, le PGCD, le PPCM...
- Existence d'une infinité de nombres premiers
- Congruences
- Théorème chinois

Pour plus de détails, vous pouvez consulter le poly d'arithmétique disponible à l'adresse ci-dessous :
http://www.animath.fr/spip.php?article255

Exercice 1 Calculer le nombre de diviseurs d'un entier en fonction de sa décomposition en facteurs premiers.

Solution de l'exercice 1 Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$: choisir un diviseur de n revient à choisir des entiers naturels $\beta_1, \dots, \beta_k$ avec $\beta_i \leqslant \alpha_i$ pour tout i. Il y a α_1+1 choix pour β_1 etc, donc le nombre de diviseurs de n vaut $(\alpha_1+1)\dots(\alpha_k+1)$.

Exercice 2 Soient a et b dans $\mathbb{N}^*$ tels que $a^n | b^{n+1}$ pour tout n de $\mathbb{N}$.
Montrer que $a|b$.

Solution de l'exercice 2 On utilise les valuations p-adiques : la condition signifie que pour tous p et n, $v_p(a) \leqslant \left(1+\frac{1}{n}\right) v_p(b)$ d'où, en passant à la limite, $v_p(a) \leqslant v_p(b)$ et ce pour tout p premier, donc $a|b$.

Exercice 3 Soient $k \geqslant 2$, n dans $\mathbb{N}^*$ et a_1, a_2, …, a_k deux à deux distincts dans $[\![1, n]\!]$ tels que n divise $a_1(a_2-1)$, $a_2(a_3-1)$,…, $a_{k-1}(a_k-1)$.
Montrer que n ne divise pas $a_k(a_1-1)$.

Solution de l'exercice 3 On fixe n et on raisonne par récurrence sur k : pour $k=2$, si n divise $a(b-1)$ et $b(a-1)$, alors n divise $a-b$ donc $a=b$, ce qui est impossible.
Si le résultat est vrai pour $n-1$, on sait que n ne divise pas $a_{k-1}(a_1-1)$. Il existe donc p tel que $v_p(a_{k-1}) + v_p(a_1-1) < v_p(n)$. Or, on sait que $v_p(a_{k-1}) + v_p(a_k-1) \geqslant v_p(n)$.
On a donc :

$$v_p(a_{k-1}) + v_p(a_k-1) \geqslant v_p(n) > v_p(a_{k-1}) + v_p(a_1-1) \geqslant v_p(a_{k-1})$$

donc $v_p(a_k-1) > 0$ donc, comme a_k et a_k-1 sont premiers entre eux, $v_p(a_k) = 0$ donc :

$$v_p(a_k) + v_p(a_1-1) = v_p(a_1-1) \leqslant v_p(a_1-1) + v_p(a_{k-1}) < v_p(n)$$

donc n ne divise pas $a_k(a_1-1)$.

Exercice 4 Trouver tous les triplets d'entiers (x, y, z) tels que :

$$x^2 + y^2 + 1 = 2^z$$

Solution de l'exercice 4 On regarde modulo 4 : on vérifie qu'on a $x^2 \equiv 0 \pmod 4$ si x est pair et $x^2 \equiv 1 \pmod 4$ si x est impair, donc x^2+y^2 est congru à 0, 1 ou 2 modulo 4, donc le membre de gauche n'est jamais divisible par 4, ce qui impose $z \leqslant 1$, donc x^2+y^2 vaut 0 ou 1.

Exercice 5 Soient $A = 2012^{2012}$, B la somme des chiffres de A, C la somme des chiffres de B et D la somme des chiffres de C.
Combien vaut D ?

Solution de l'exercice 5 On a $2012 \equiv 5 \pmod 9$ d'où $2012^{2012} \equiv 5^{2012} \pmod 9$. On étudie donc les puissances de 5 modulo 9 : $5^2 \equiv 7$ donc $5^3 \equiv -1$ et $5^6 \equiv 1$. Or, on peut écrire $2012 = 2 + 6 \times 335$, d'où :

$$2012^{2012} \equiv 5^{2012} \equiv 5^2 \times (5^6)^{335} \equiv 5^2 \equiv 7 \pmod 9$$

donc $D \equiv C \equiv B \equiv A \equiv 7 \pmod 9$.
D'autre part, $A < (10^4)^{2012} = 10^{8048}$ donc A a au plus 8048 chiffres, donc $B \leqslant 9 \times 8048 = 72432$, donc B a au plus 5 chiffres, donc $C \leqslant 45$, et $D \leqslant 13$. La seule possibilité est donc $D = 7$.

Exercice 6 Refaire l'exercice 3 en utilisant des congruences.

Solution de l'exercice 6 L'hypothèse s'écrit $a_i a_{i+1} \equiv a_i \pmod n$ pour tout i donc :

$$a_1 \equiv a_1 a_2 \equiv a_1 a_2 a_3 \equiv \cdots \equiv a_1 \dots a_k \pmod n$$

Or, si n divisait $a_k(a_1 - 1)$, on aurait $a_k a_1 \equiv a_k \pmod n$ et on pourrait écrire :

$$a_2 \equiv a_2 a_3 \equiv \cdots \equiv a_2 a_3 \dots a_k \equiv a_2 \dots a_k a_1 \pmod n,$$

d'où $a_1 \equiv a_2 \pmod n$ donc $a_1 = a_2$ (car a_1 et a_2 sont dans $[\![1, n]\!]\dots$), ce qui est en contradiction avec l'énoncé.

Exercice 7 Un point du plan de coordonnées entières (p, q) est dit invisible si $\text{PGCD}(p, q) > 1$. Soit $n \in \mathbb{N}$. Montrer qu'il existe un carré de côté n dans lequel tous les points à coordonnées entières sont invisibles.

Solution de l'exercice 7 On cherche a et b tels que pour tous i et j de $[\![0, n-1]\!]$, $a + i$ et $b + j$ ne soient pas premiers entre eux. Soient donc $(p_{i,j})_{i,j \in [\![0,n-1]\!]}$ n^2 nombres premiers deux à deux distincts : on veut que pour tous i et j, $a + i$ et $b + j$ soient tous deux divisibles par $p_{i,j}$, soit $a \equiv -i \pmod{p_{i,j}}$ pour tous i et j et $b \equiv -j \pmod{p_{i,j}}$. L'existence de tels a et b est garantie par le théorème chinois.

Exercice 8 Soit $n > 0$. Montrer qu'il existe n entiers consécutifs dont aucun n'est une puissance parfaite.

Solution de l'exercice 8 On cherche à transformer le problème en problème sur les congruences : pour qu'un nombre m ne soit pas une puissance parfaite, il suffit qu'il existe p premier tel que $v_p(m) = 1$, ce qui est par exemple le cas si $m \equiv p \pmod{p^2}$. Soient donc p_1, p_2, …, p_n n nombres premiers distincts (car il y a n conditions à vérifier). D'après le théorème chinois, il existe m tel que :

$$\begin{cases} m \equiv p_1 \pmod{p_1^2} \\ m \equiv p_2 - 1 \pmod{p_2^2} \\ \quad \dots \\ m \equiv p_n - (n-1) \pmod{p_n^2} \end{cases}$$

On a alors, pour tout i de $[\![0, n-1]\!]$, $m + i \equiv p_i \pmod{p_i^2}$ donc $m + i$ n'est pas une puissance parfaite.

3 TD d'arithmétique

- Énoncé des exercices -

Exercice 1 (Algorithme d'Euclide) Soit a et b deux entiers naturels, tels que $a \geqslant 1$. On définit les suites (u_n) et (v_n) telles que $u_0 = a$, $v_0 = b$ puis, si $v_k \neq 0$, $u_{k+1} = v_k$ et v_{k+1} est le reste dans la division Euclidienne de u_k par v_k. Montrer que les suites (u_n) et (v_n) sont nécessairement finies, et que $\text{PGCD}(a, b)$ est égal au dernier terme u_k de la suite.

Exercice 2 Soit a, b et n trois entiers naturels, tels que $a \neq 0$. On note d le PGCD de a et b. Montrer que n divise a et b si et seulement si n divise d. En déduire, pour tout entier $c > 0$, la relation $\text{PGCD}(ac, bc) = c\text{PGCD}(a, b)$.

Exercice 3 Soit a un entier. Montrer que 2 divise $a^2 - a$ et que 3 divise $a^3 - a$.

Exercice 4 Soit $P(X) = aX^3 + bX^2 + cX + d$ un polynôme à coefficients entiers, et x, y deux entiers distincts. Montrer que $x - y$ divise $P(x) - P(y)$.

Exercice 5 Soit y un entier naturel non nul. Montrer que $y - 1$ divise $y^{(y^2)} - 2y^{y+1} + 1$.

Exercice 6 Trouver les entiers n tels que 5 divise $3n - 2$ et 7 divise $2n + 1$.

Exercice 7 Trouver les entiers n tels que 6 divise $n - 4$ et 10 divise $n - 8$.

Exercice 8 Trouver l'ensemble des entiers a tels que l'équation $2a^2 = 7k + 2$ admet une solution k entière.

Exercice 9 (JBMO 2013) Trouver les entiers naturels non nuls a et b tels que $\frac{a^3b-1}{a+1}$ et $\frac{b^3a+1}{b-1}$ sont entiers.

Exercice 10 Trouver l'ensemble des entiers a tels que 35 divise $a^3 - 1$.

Exercice 11 Trouver les entiers a et b tels que $3a^2 = b^2 + 1$.

Exercice 12 Trouver les entiers a, b et c tels que $a^4 + b^4 = c^4 + 3$.

Exercice 13 Montrer que l'équation $a^2 + b^2 + c^2 = 2007$ n'admet pas de solutions entières.

Exercice 14 Soit a, b et n trois entiers. Montrer que $\text{PGCD}(n^a - 1, n^b - 1) = n^{\text{PGCD}(a,b)} - 1$.

Exercice 15 (Ordre d'un élément) Soit a et n deux entiers naturels non nuls, premiers entre eux. Montrer qu'il existe un entier d tel que, pour tout entier $b \in \mathbb{N}$, n divise $a^b - 1$ si et seulement si d divise b.

Exercice 16 Soit $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des congruences modulo n représentant des entiers premiers avec n, a un élément de $(\mathbb{Z}/n\mathbb{Z})^*$. Montrer que la multiplication par a induit en fait une bijection de $\mathbb{Z}/n\mathbb{Z}$ sur lui-même, ainsi qu'une bijection de $(\mathbb{Z}/n\mathbb{Z})^*$ sur lui-même.

Exercice 17 (Petit théorème de Fermat) Soit a et n deux entiers naturels non nuls, premiers entre eux. On note $\varphi(n)$ le nombre d'entiers k tels que $0 < k < n$ et premiers avec 1. Montrer que n divise $a^{\varphi(n)} - 1$.

- Solutions des exercices -

Solution de l'exercice 1 On montre tout d'abord que les suites (u_n) et (v_n) sont finies. En effet, pour tout entier $n \geqslant 0$ tel que u_{n+1} et v_{n+1} sont définis, $0 \leqslant v_{n+1} < v_n = u_{n+1}$, car v_{n+1} et le reste d'une division par v_n. Ainsi, la suite (v_n) s'arrêtant dès qu'un de ses termes vaut 0, elle est nécessairement finie.

En outre, soit q_n tel que $u_n = q_n v_n + v_{n+1}$. Remarquons que, si d est un diviseur de u_n et de v_n, alors d divise $u_n - q_n v_n = v_{n+1}$; si $\overline{d}$ est un diviseur de v_n et de v_{n+1}, alors $\overline{d}$ divise $q_n v_n + v_{n+1} = u_n$. Ainsi, les diviseurs communs à u_n et v_n sont ceux communs à $v_n = u_{n+1}$ et v_{n+1} : ces deux ensembles de diviseurs ont le même plus grand élément maximal, ce qui signifie que $\text{PGCD}(u_n, v_n) = \text{PGCD}(u_{n+1}, v_{n+1})$.

Les termes $\mathrm{PGCD}(u_n, v_n)$ sont donc égaux deux à deux. En particulier, si u_k est le dernier terme de la suite (u_n), alors $v_k = 0$, donc $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(u_0, v_0) = \mathrm{PGCD}(u_k, v_k) = u_k$.

Solution de l'exercice 2 Rappelons-nous la caractérisation du PGCD en utilisant $a\mathbb{Z}$ et $b\mathbb{Z}$: si a et b sont deux entiers naturels non nuls, $\mathrm{PGCD}(a, b)$ est l'entier $d \geqslant 1$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. En particulier, d est l'élément minimal de l'ensemble $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^*$.

Maintenant, soit $d = \mathrm{PGCD}(a, b)$ et $D = \mathrm{PGCD}(ac, bc)$. Puisque $D \in (ac)\mathbb{Z} + (bc)\mathbb{Z}$, il existe des entiers u, v, U et C que $au + bv = d$ et $acu + bcv = D$. En particulier, $D = (au + bv)c$ est divisible par c, et $\frac{D}{c} = au + bv$ est un élément de $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^*$. De même, $(ac)u + (bc)v = cd$ est un élément de $(ac\mathbb{Z} + bc\mathbb{Z}) \cap \mathbb{N}^*$. Par minimalité de d et de D, on en déduit que $cd \geqslant D$ et que $\frac{D}{c} \geqslant d$, c'est-à-dire que $cd = D$.

Solution de l'exercice 3 On pourrait invoquer directement le petit théorème de Fermat, mais on va simplement considérer les deux cas séparément :

- Si $p = 2$, alors $a^2 - a = a(a-1)$: si a est pair, alors $a(a-1)$ aussi ; si a est impair, alors $a - 1$ est pair, donc $a(a-1)$ aussi.
- Si $p = 3$, alors $a^3 - a = a(a-1)(a+1)$: que 3 divise a, $a-1$ ou $a+1$, il divisera toujours $a^3 - a$.

Notons que l'on aurait également pu utiliser des congruences modulo 2 ou 3.

Solution de l'exercice 4 Regardons $P(x)$ et $P(y)$ modulo $x-y$: puisque $x \equiv y \pmod{x-y}$, alors

$$P(x) \equiv ax^3 + bx^2 + cx + d \equiv ay^3 + by^2 + cy + d \equiv P(y) \ (\text{mod. } x - y).$$

Cela signifie exactement que $x - y$ divise $P(x) - P(y)$.

Solution de l'exercice 5 Plaçons nous modulo $y-1$: $y \equiv 1 \pmod{y-1}$, donc $y^{(y^2)} - 2y^{y+1} + 1 \equiv 1^{(y^2)} - 2 \times 1^{y+1} + 1 \equiv 1 - 2 + 1 \equiv 0 \pmod{y-1}$.

Solution de l'exercice 6 On va utiliser le théorème Chinois. Tout d'abord, en se plaçant modulo 5, on observe que $3n - 2 \equiv 0 \pmod 5$ si et seulement si $n \equiv 4 \pmod 5$. De même, en se plaçant modulo 7, on observe que $2n + 1 \equiv 0 \pmod 7$ si et seulement si $n \equiv 3 \pmod 7$.

Notons que 5 et 7 sont premiers entre eux : d'après le théorème de Bézout, il existe des entiers u et v tels que $5u + 7v = 1$. Par exemple, $(u, v) = (3, -1)$ convient. D'après le théorème Chinois, les entiers n tels que $n \equiv 4 \pmod 5$ et $n \equiv 3 \pmod 7$ sont donc les entiers $n \equiv 4(7v) + 3(5u) \equiv -11 \pmod{35}$.

Les entiers recherchés sont donc les entiers de la forme $35k - 11$, où k est entier.

Solution de l'exercice 7 On va, une fois de plus, utiliser le théorème Chinois. Notons que $6 = 2 \times 3$ et que $10 = 2 \times 5$. Dire que $n \equiv 4 \pmod 6$ revient à dire que $n \equiv 4 \pmod 2$ et $n \equiv 1 \pmod 3$. Dire que $n \equiv 8 \pmod{10}$ revient à dire que $n \equiv 8 \pmod 2$ et $n \equiv 8 \pmod 5$.

On cherche donc les entiers n tels que $n \equiv 0 \pmod 2$, $n \equiv 1 \pmod 3$ et $n \equiv 3 \pmod 5$. $n = -2$ est un tel entier. D'après le théorème Chinois, les entiers recherchés sont donc les entiers $n \equiv -2 \pmod{30}$, c'est à dire les entiers de la forme $30k - 2$, où k est entier.

Solution de l'exercice 8 Le problème peut se reformuler comme suit : trouver les entiers a tels que $2a^2 \equiv 2 \pmod 7$. Une telle relation ne dépend que de la congruence de a modulo 7. On vérifie alors à la main que $2 \times 0^2 \equiv 0 \pmod 7$, $2 \times 1^2 \equiv 2 \times 6^2 \equiv 2 \pmod 7$, $2 \times 2^2 \equiv 2 \times 5^2 \equiv 1 \pmod 7$ et $2 \times 3^2 \equiv 2 \times 4^2 \equiv 4 \pmod 7$. Il s'ensuit que $\frac{2a^2-2}{7}$ est un entier si et seulement si a est de la forme $7\ell + 1$ ou $7\ell - 1$.

Solution de l'exercice 9 On veut trouver $a > 0$ et $b > 0$ entiers tels que $a^3b - 1 \equiv 0 \pmod{a+1}$ et $b^3a + 1 \equiv 0 \pmod{b+1}$. Or, $a \equiv -1 \pmod{a+1}$, donc $a^3b - 1 \equiv (-1)^3b - 1 \equiv -(b+1) \pmod{a+1}$. De même, $b \equiv 1 \pmod{b-1}$, donc $b^3a + 1 \equiv 1a + 1 \equiv a + 1 \pmod{b-1}$. En particulier, $b-1$ divise alors $a+1$, qui lui-même divise $b+1$. Donc $b-1$ divise $b+1$ et divise même $(b+1) - (b-1) = 2$. Puisque $b - 1 \geqslant 0$, on en déduit que $b - 1 \in \{1, 2\}$:

1. si $b - 1 = 1$, $a + 1$ divise $b + 1 = 3$ et, puisque $a + 1 > 1$, on en déduit que $a + 1 = 3$;
2. si $b - 1 = 2$, $a + 1$ est pair et divise $b + 1 = 4$ et, puisque $a + 1 > 1$, on en déduit que $a + 1 = 2$ ou $a + 1 = 4$.

Les solutions (a, b) possibles sont donc $(2, 2)$, $(1, 3)$ et $(3, 3)$. On vérifie alors ces solutions donnent respectivement $\frac{a^3b-1}{a+1} = \frac{15}{3}, \frac{2}{2}, \frac{80}{4}$ et $\frac{b^3a+1}{b-1} = \frac{17}{1}, \frac{28}{2}, \frac{82}{2}$. Les couples recherchés sont donc bien $(2, 2)$, $(1, 3)$ et $(3, 3)$.

Solution de l'exercice 10 On pourrait procéder comme ci-dessus, regardant une par une les 35 classes de congruences modulo 35. Cela dit, il y a plus rapide, en utilisant le théorème Chinois.

En effet, puisque $35 = 5 \times 7$, $a^3 \equiv 1 \pmod{35}$ si et seulement si $a^3 \equiv 1 \pmod{5}$ et $a^3 \equiv 1 \pmod{73}$. On vérifie alors à la main que $0^3 \equiv 0 \pmod{7}$, que $1^3 \equiv 2^3 \equiv 4^3 \equiv 1 \pmod{7}$ et que $3^3 \equiv 5^3 \equiv 6^3 \equiv 6 \pmod{7}$; on vérifie également $0^3 \equiv 0 \pmod{53}$, que $1^3 \equiv 1 \pmod{5}$, que $2^3 \equiv 3 \pmod{5}$, que $3^3 \equiv 2 \pmod{5}$ et que $4^3 \equiv 4 \pmod{5}$.

Ainsi, a est solution du problème si et seulement si $a \equiv 1$, 2 ou 4 $\pmod{7}$, et $a \equiv 1 \pmod{5}$. D'après le théorème Chinois, ces conditions reviennent à dire que $a \equiv 1$, 11 ou 16 $\pmod{35}$ Cela signifie que 35 divise $a^3 - 1$ si et seulement si a est de la forme $35\ell + 1$, $35\ell + 11$ ou $35\ell + 16$.

Solution de l'exercice 11 L'astuce est bien sûr de penser à réduire l'équation diophantienne modulo 3. En effet, elle devient $0 \equiv b^2 + 1 \pmod{3}$. Or, b^2 ne peut être congru qu'à 0 ou 1 modulo 3.

Solution de l'exercice 12 Une fois encore, on fait une réduction modulo un certain nombre : ici, on travaille modulo 5. L'équation devient alors $a^4 + b^4 \equiv c^4 + 3 \pmod{5}$. Or, les puissances de 5 sont 0 et 1 modulo 5. Donc $a^4 + b^4$ vaut 0, 1 ou 1, tandis que $c^4 + 3$ vaut 3 ou 4 modulo 5. L'équation n'admet donc, elle non plus, pas de solution en nombres entiers.

Solution de l'exercice 13 Dans ce genre d'exercices, où l'on doit manipuler un grand nombre tel que 2007, il est important de rechercher des simplifications du problème, par exemple en regardant ce qui se passe modulo de petits entiers.

C'est ainsi que l'on en vient tout naturellement, après quelques essais éventuellement infructueux, à considérer l'équation dans $\mathbb{Z}/8\mathbb{Z}$, où elle devient : $a^2 + b^2 + c^2 \equiv 7 \pmod{8}$. Or, les carrés modulo 8 sont 0, 1 et 4.

Pour que l'équation soit vérifiée, il faut donc avoir au moins 2 carrés égaux à 4 modulo 8 (ce sans quoi leur somme vaudra ente 0 et 3 modulo 8), et alors cette somme sera égale au dernier carré, donc différente de 7 (modulo 8). Ainsi, l'équation $a^2 + b^2 + c^2 \equiv 7 \pmod{8}$ n'admet aucune solution. *A fortiori*, l'équation $a^2 + b^2 + c^2 = 2007$ n'admet aucune solution en nombres entiers.

Solution de l'exercice 14 Tout d'abord, on note $d = \text{PGCD}(a, b)$ et $D = \text{PGCD}(n^a - 1, n^b - 1)$: on commence par montrer que $n^d - 1$ divise D. En effet, soit a' et b' deux entiers tels que $a = da'$ et $b = bd'$. Il s'ensuit que $n^a - 1 \equiv (n^d)^{a'} - 1 \equiv 1^{a'} - 1 \equiv 0 \pmod{d}$ et que

$n^b - 1 \equiv (n^d)^{b'} - 1 \equiv 1^{b'} - 1 \equiv 0 \pmod{d}$. En particulier, cela signifie que d divise $n^a - 1$ et $n^b - 1$, donc divise D.

Réciproquement, montrons que D divise $n^d - 1$. Pour ce faire, on va montrer un autre résultat : si $x \geqslant y > 0$, alors $\text{PGCD}(n^x - 1, n^y - 1)$ divise $\text{PGCD}(n^y - 1, n^{x-y} - 1)$. Notons qu'on peut se douter qu'un tel résultat sera vrai, puisque $\text{PGCD}(x, y) = \text{PGCD}(y, x - y)$. Il nous suffit alors de montrer que $\text{PGCD}(n^x - 1, n^y - 1)$ divise $n^{x-y} - 1$, ce qui découle du fait que $n^x - 1 = n^{x-y}(n^y - 1) + (n^{x-y} - 1)$.

En remplaçant l'expression $\text{PGCD}(n^x - 1, n^y - 1)$ par $\text{PGCD}(n^{\min\{x,y\}} - 1, n^{|x-y|} - 1)$, les exposants que l'on obtient sont en fait des termes que l'on trouvera dans l'algorithme d'Euclide (sauf que, quand on a une division Euclidienne $a = bq + r$, on considère tous les couples $(b, r + kq)$ au lieu de passer directement de (a, b) à (b, r)). Ce faisant, on montre bien que $\text{PGCD}(n^a - 1, n^b - 1)$ divise $\text{PGCD}(n^d - 1, n^0 - 1) = n^d - 1$, ce qui conclut l'exercice.

Solution de l'exercice 15 Tout d'abord, en appliquant le principe des tiroirs, il existe deux entiers naturels $u < v$ tels que $a^u \equiv a^v \pmod{n}$. Cela veut dire que n divise $a^v - a^u = a^u(a^{v-u} - 1)$. Or, n est premier avec a, donc avec a^u : par théorème de Gauss, n divise $a^{v-u} - 1$, et il existe donc un plus petit entier $d > 0$ tel que $a^d \equiv 1 \pmod{n}$.

On note alors que, pour tout entier naturel k, $a^{dk} \equiv (a^d)^k \equiv 1^k \equiv 1 \pmod{n}$: si b est un multiple de d, alors n divise $a^b - 1$. Réciproquement, si b n'est pas multiple de d, effectuons la division Euclidienne de b par d : $b = ud + v$, avec $0 < v < d$. Alors $a^b \equiv (a^d)^u a^v \equiv 1^u a^v \equiv a^v \not\equiv 1 \pmod{n}$, par définition de d. Cela montre bien que, si n divise $a^b - 1$, alors d divise b.

Solution de l'exercice 16 Tout d'abord, on note que $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^*$ sont deux ensembles finis. Il nous suffit donc de montrer que la multiplication par a induit une injection de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même, et envoie bien $(\mathbb{Z}/n\mathbb{Z})^*$ sur lui-même.

La première partie se montre comme suit : si $ab \equiv ac \pmod{n}$, alors n divise $a(b - c)$. Puisque n est premier avec a, le théorème de Gauss indique que n divise $b - c$, c'est-à-dire que $b \equiv c \pmod{n}$.

Quant à la deuxième partie, elle découle du fait que, si b est premier avec n, alors ab est premier avec n également : en effet, d'après le théorème de Gauss, ab n'admettra aucun facteur premier p commun avec n, puisqu'un tel p devrait diviser soit n et a, soit n et b.

Solution de l'exercice 17 On utilise ici le fait que la multiplication par a induit une bijection de $(\mathbb{Z}/n\mathbb{Z})^*$ sur lui-même. En effet, $\varphi(n)$ se trouve être exactement le cardinal de l'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$. Notons f cette bijection.

L'idée est alors d'utiliser f pour écrire une égalité de la forme $xa^{\varphi(n)} \equiv x \pmod{n}$, où x est premier avec n : il en résultera bien que $a^{\varphi(n)} \equiv 1 \pmod{n}$. En pratique, on procède en multipliant tous les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$, qui sont en quantité $\varphi(n)$. D'un côté, ce produit est égal à $\prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} u$. De l'autre, en remarquant que $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ est une bijection, ce produit est aussi égal (modulo n) à

$$\prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} f(u) \equiv \prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} au \equiv a^{\varphi(n)} \left(\prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} u \right) \pmod{n}.$$

En posant $x = \prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} u$, on a donc la relation $xa^{\varphi(n)} \equiv x \pmod{n}$. Or, x est un produit d'éléments premiers avec n, donc x est premier avec n également. Il s'ensuit donc bien que $a^{\varphi(n)} \equiv 1 \pmod{n}$.

3 Groupe C : équations fonctionnelles

1 Cours d'équations fonctionnelles

Nous renvoyons au cours de Pierre Bornsztein sur les équations fonctionnelles, disponible sur le site d'Animath.

2 TD d'équations fonctionnelles

- Énoncés des exercices -

Exercice 1 (Périodicité 1) Soit $f : \mathbb{R} \to \mathbb{R}$ telle que pour un certain $a > 0$, pour tout réel x,

$$f(x + a) = \frac{1}{2} + \sqrt{f(x) - f^2(x)}$$

Montrer que f est périodique.
(IMO 1968)

Exercice 2 (Périodicité 2) Soit $f : \mathbb{R} \to \mathbb{R}$ vérifiant pour tout réel x :

$$f(x + 1) + f(x - 1) = \sqrt{2} f(x),$$

montrer qu'elle est périodique.

Exercice 3 (Substitutions 1) Trouver toutes les fonctions de $\mathbb{R} - \{0, 1\}$ dans $\mathbb{R}$ telles que

$$f(x) + f\left(\frac{1}{1 - x}\right) = x.$$

Exercice 4 (Substitutions 2) Trouver les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous $x, y \in \mathbb{R}$, on ait :

$$f(\lfloor x \rfloor y) = f(x) \lfloor f(y) \rfloor$$

(IMO 2010)

Exercice 5 (Constructions dans $\mathbb{R}$) Soit $f : [0, 1] \to \mathbb{R}^+$ telle que $f(1) = 1$ et pour tous x_1, x_2 tels que $x_1 + x_2 \leqslant 1$, $f(x_1 + x_2) \geqslant f(x_1) + f(x_2)$. Montrer que pour tout réel x,

$$f(x) \leqslant 2x$$

et qu'on ne peut pas améliorer cette constante.
(URSS 1974)

Exercice 6 (Points fixes et limites) Trouver toutes les fonctions de $\mathbb{R}_+^* \to \mathbb{R}_+^*$ telles que pour tous $x, y > 0$, $f(xf(y)) = yf(x)$ et $\lim\limits_{x \to +\infty} f(x) = 0$.
(IMO 1983)

Exercice 7 (Polynômes 1) Trouver tous les $P \in \mathbb{R}[X]$ tels que $P(0) = 0$ et

$$P(x^2 + 1) = P(x)^2 + 1$$

pour tout réel x.

Exercice 8 (Injectivité et récurrence) Trouver toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que pour tout naturel n,

$$f(n) + f(f(n)) + f(f(f(n))) = 3n.$$

Exercice 9 (Inéquation dans $\mathbb{N}$) Soit f une fonction de $\mathbb{N}$ dans lui-même. Montrer que si pour tout naturel n,

$$f(n+1) > f(f(n))$$

alors f est l'identité.
(IMO 1977)

Exercice 10 (Constructions dans $\mathbb{N}$ 1) Existe-t-il une fonction $f : \mathbb{N} \to \mathbb{N}$ telle que pour tout entier naturel n,

$$f(f(n)) = n + 2013 \quad ?$$

(IMO 1987 - réactualisé...)

Exercice 11 (Arithmétique des fonctions) Trouver toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ strictement croissantes telles que $f(2) = 2$ et pour tous m, n premiers entre eux, $f(mn) = f(m)f(n)$.

Exercice 12 (Constructions dans $\mathbb{N}$ 2) Existe-t-il une fonction de $\mathbb{N}^*$ dans lui-même, strictement croissante, telle que $f(1) = 2$ et que pour tout n,

$$f(f(n)) = f(n) + n \quad ?$$

(IMO 1993)

- Solutions -

Solution de l'exercice 1 Puisque l'on a $f(x) \geqslant \frac{1}{2}$, posons $g(x) = f(x) - \frac{1}{2}$ En élevant au carré, on obtient : $g(x+a)^2 = \frac{1}{4} - g(x)^2$, ce qui donne aussi $g(x+2a)^2 = \frac{1}{4} - g(x+a)^2$. En sommant les deux relations,

$$g(x)^2 = g(x+a)^2.$$

Or, ces deux quantités sont positives, donc on a $g(x) = g(x+2a)$ pour tout réel x, soit f et g $2a$-périodiques.

Solution de l'exercice 2 On applique à $x, x+1$ et $x-2$ la condition de l'énoncé :

$$\begin{aligned}
\sqrt{2}(f(x+1) + f(x-1)) &= 2f(x) \\
f(x+2) + f(x) &= \sqrt{2}f(x+1) \\
f(x) + f(x-2) &= \sqrt{2}f(x-1)
\end{aligned}$$

Il suffit alors de sommer ces trois équations pour obtenir $f(x+2) = -f(x-2)$ d'où l'on déduit que f est 8-périodique.

Solution de l'exercice 3 On exprime l'équation fonctionnelle avec les valeurs x, $\frac{1}{1-x}$ et $\frac{1}{x}-1$, ce qui donne :

$$\begin{aligned} f(x)+f\left(\frac{1}{1-x}\right) &= x \\ f\left(\frac{1}{1-x}\right)+f\left(1-\frac{1}{x}\right) &= \frac{1}{1-x} \\ f\left(1-\frac{1}{x}\right)+f(x) &= 1-\frac{1}{x} \end{aligned}$$

En sommant les première et troisième lignes puis en soustrayant la deuxième, on trouve

$$f(x)=\frac{1}{2}\left(x+1-\frac{1}{x}-\frac{1}{1-x}\right)$$

Solution de l'exercice 4 Posons $x=0$ dans l'équation, on a $f(0)=f(0)\lfloor f(y)\rfloor$ pour tout réel y ;

- Si $f(0)\neq 0$, alors $f(y)\in[1,2[$ pour tout y réel. Avec $y=0$ dans l'équation, on obtient $f(x)=f(0)$ pour tout $x\in\mathbb{R}$, donc f est constante de valeur $v\in[1,2[$.
- Si $f(0)=0$, on montre que f est la fonction nulle. Si pour un certain $z\in[0,1[$, $f(z)\neq 0$, on obtient avec $x=z$: $0=f(0)=f(z)\lfloor f(y)\rfloor$ donc pour tout réel y, $f(y)\in[0,1[$. Reprenons l'équation initiale avec $x=1$ et $y=z$: on obtient $f(z)=0$, ce qui est une contradiction.

Donc f est nulle sur $[0,1[$. Si maintenant $z\in\mathbb{R}$, il existe un entier $n\in\mathbb{Z}$ tel que $\frac{z}{n}\in[0,1[$. On obtient avec $x=n$ et $y=\frac{z}{n}$:

$$f(z)=f(n)\left\lfloor f(\frac{z}{n})\right\rfloor=0$$

donc f est bien la fonction nulle.
Réciproquement, ces fonctions satisfont toutes l'équation.

Solution de l'exercice 5 Soit f une fonction répondant au problème. Il vient vite $f(0)=0$.
Rappelons-nous la formule de Jensen, qui caractérise les fonctions convexes et concaves. De la même manière qu'on avait montré cette formule, on montre par récurrence sur $n\geqslant 2$ que si $x_1,\cdots,x_n\geqslant 0$ et $\sum x_i\leqslant 1$, alors

$$f(x_1+\cdots+x_n)\geqslant f(x_1)+\cdots+f(x_n)$$

Le lecteur aura soin de poser $y=x_1+x_2$ et d'appliquer la formule de récurrence. En particulier, pour $x\leqslant\frac{1}{n}$,

$$f(nx)\geqslant nf(x)$$

Maintenant, si $x\geqslant\frac{1}{2}$, on a $f(x)\leqslant f(1)-f(1-x)\leqslant f(1)\leqslant 1\leqslant 2x$.
Si $x\in]0,\frac{1}{2}[$, il existe un entier $n\geqslant 2$ tel que $\frac{1}{2}\leqslant nx\leqslant 1$. Par ce qui précède, $nf(x)\leqslant f(nx)\leqslant 2nx$, donc $f(x)\leqslant 2x$.
Ensuite, quelle fonction utiliser pour montrer que la constante 2 ne peut être améliorée ? Prenons $f(x)=0$ si $0\leqslant x\leqslant\frac{1}{2}$ et $f(x)=1$ sinon. On vérifie rapidement qu'elle vérifie l'énoncé. Maintenant, soit $c\in]0,2[$. Il existe $x_0>\frac{1}{2}$ tel que $1>cx_0$, donc $f(x_0)>cx_0$. Ainsi c ne peut convenir comme constante.

Solution de l'exercice 6 Avec $x=y$, on voit que, pour tout $x>0$, $xf(x)$ est un point fixe de f. Si z est point fixe de f, avec $x=1$ et $y=z$, on obtient $z=zf(1)\neq 0$ donc 1 est aussi un point fixe.

De plus, une récurrence rapide montre que pour tout $n \in \mathbb{N}$, a^n est aussi un point fixe de f. La substitution $y = a = \frac{1}{x}$ donne $af(\frac{1}{a}) = f(\frac{1}{a}f(a)) = f(1) = 1$, donc a^{-1} est aussi un point fixe de f. On en déduit que, pour tout $m \in \mathbb{Z}$, $f(a^m) = a^m$. La condition sur la limite en $+\infty$ impose $a = 1$. Donc, pour tout réel strictement positif x, $f(x) = \frac{1}{x}$, qui est réciproquement bien solution du problème.

Solution de l'exercice 7 On trouve $P(1) = 1$, $P(2) = 2$, $P(5) = 5$, etc. On définit alors la suite (a_n) par $a_0 = 0$ et $a_{n+1} = a_n^2 + 1$.
On vérifie sans difficulté qu'elle est strictement croissante, et on montre par récurrence sur n que $P(a_n) = a_n$. Ainsi, le polynôme $Q(X) = P(X) - X$ a une infinité de racines, donc c'est le polynôme nul. Autrement dit, pour tout réel x, $P(x) = x$. Réciproquement, l'identité est solution du problème.

Solution de l'exercice 8 Notons que si $f(n) = f(m)$ alors l'égalité reste vraie en composant par f, donc $3n = 3m$: f est donc injective. Montrons par récurrence forte sur n que $f(n) = n$. On initialise à $n = 0$: on a $f(0), f(f(0)), f(f(f(0))) \in \mathbb{N}$ et leur somme vaut 0, donc $f(0) = 0$.
Supposons que $f(k) = k$ dès lors que $0 \leqslant k \leqslant n$. On a $f(n+1) \geqslant n+1$ par injectivité de f. De même, $f(f(n+1))$ et $f(f(f(n+1)))$ ne peuvent être dans $\{1, \cdots, n\}$. Or,

$$f(n+1) + f(f(n+1)) + f(f(f(n+1))) = 3(n+1),$$

donc $f(n+1) = n+1$ et ceci clôt la récurrence. L'identité est bien l'unique solution du problème (elle convient effectivement).

Solution de l'exercice 9 Montrons d'abord que f est strictement croissante : pour tout $n > 0$, $f(n) > f(f(n-1))$ donc f admet un minimum en 0 (le fait que f soit à valeurs entières et minorée par 0 assure de l'existence d'un minimum), et uniquement en 0. Cherchons la deuxième plus petite valeur de f : pour tout $n > 1$, $f(n) > f(0)$ et $f(n) > f(f(n-1))$ avec $f(n-1) \neq 0$ car $f(n-1) > 0$. Donc la deuxième plus petite valeur de f ne peut être atteinte qu'en 1. On montre en continuant ainsi que f est strictement croissante (le lecteur pourra rédiger la récurrence en question).
Comme $f(0) = 0$, on en déduit que $f(n) \geqslant n$ pour tout n. S'il existe m tel que $f(m) > m$, on a $f(m) \geqslant m+1$ donc par croissance de f, $f(f(m)) \geqslant f(m+1)$, ce qui contredit l'énoncé. Donc pour tout $n \in \mathbb{N}$,

$$f(n) = n$$

Solution de l'exercice 10 Si f est solution, pour tout entier naturel n,

$$f(n + 2013) = f(n) + 2013$$

donc une récurrence immédiate montre pour tous $k, n \in \mathbb{N}$ que $f(n + 2013k) = f(n) + 2013k$. On considère g la fonction induite par f de $\mathbb{Z}/2013\mathbb{Z}$ dans lui-même. D'après l'énoncé, g^2 est l'identité. C'est donc une involution. Or $\mathbb{Z}/2013\mathbb{Z}$ a un cardinal impair, donc il admet un point fixe : il existe deux entiers $n_0 \geqslant 0$ et $m \in \mathbb{Z}$ tels que $f(n_0) = 2013 + m$. Alors

$$n_0 + 2013 = f(f(n_0)) = f(n_0 + 2013m) = f(n_0) + 2013m = n_0 + 2013 \times 2m$$

et $m = \frac{1}{2}$, ce qui est absurde.
On peut faire différemment : on note $f(\mathbb{N})$ l'image de $\mathbb{N}$ par f, $A = \mathbb{N} \setminus f(\mathbb{N})$, et $B = f(A)$.

Notons que, d'après l'énoncé, f est injective. Il s'ensuit que $B = f(\mathbb{N}) \setminus f(f(\mathbb{N}))$. A et B sont donc disjoints, et leur union est $\mathbb{N} - f(f(\mathbb{N})) = \{0, \cdots, 2012\}$, de cardinal 2013, qui est impair. Cependant, f est injective, donc A et B doivent avoir même cardinal, ce qui est absurde.

Solution de l'exercice 11 Par stricte croissance de f, $f(0) = 0$ et $f(1) = 1$. Pour multiplier des nombres premiers entre eux sans utiliser 1, on aimerait bien connaître $f(3)$ par exemple. Posons $f(3) = 3 + k$, $k \geqslant 0$. Par encadrement successifs sur des petites valeurs, on montre que $k = 0$: en effet, $f(6) = 2k+6$ donc $f(5) \leqslant 2k+5$ et $f(10) \leqslant 4k+10$, $f(9) \leqslant 4k+9$, $f(18) \leqslant 8k+18$. Et $f(5) \geqslant 5 + k$ donc $k^2 + 8k + 15 = (3 + k)(5 + k) \leqslant f(15) \leqslant f(18) - 3 \leqslant 8k + 15$; de ceci on déduit $k = 0$.
Maintenant, montrons par récurrence sur n que $f(k) = k$ si $k \leqslant 2^n + 1$. On a vérifié l'initialisation à $n = 1$, et pour l'hérédité :

$$f(2^{n+1} + 2) = f(2)f(2^n + 1) = 2^{n+1} + 2$$

donc les $f(k)$, quand $2^n + 2 \leqslant k \leqslant 2^{n+2} + 2$, sont compris entre $2^n + 2$ et $2^{n+2} + 2$ au sens large ; la stricte croissance de la fonction assure que $f(k) = k$ pour tout $k \leqslant 2^{n+1} + 1$. Ceci clôt la récurrence, et permet d'affirmer que f est l'identité. Réciproquement, cette fonction est évidemment solution du problème.

Solution de l'exercice 12 La question est vicieusement piégeuse : la bonne réponse est un « oui » ingénieux. On procède alors à la construction d'une fonction convenable. Puisqu'on travaille sur les entiers, on peut procéder par récurrence. $f(1) = 2$ et supposons que pour un certain $n \geqslant 1$, on ait construit $f(1) < \cdots < f(n)$. Pour simplifier les notations, on pose $E_n = \{1, 2, \ldots, n\}$.

On va essayer de définir une fonction « réciproque » de f en utilisant la croissance : soit $g(n+1)$ le plus grand entier $m \leqslant n$ tel que $f(k) \leqslant n+1$: une telle fonction existe bien puisque $f(1) = 2 \leqslant n + 1$. Alors on pose $f(n + 1) = g(n + 1) + n + 1$. La croissance de f sur E_n assure que $g(n + 1) \geqslant g(n)$; on en déduit que $f(n + 1) > f(n)$.

Montrons maintenant que la fonction f ainsi définie convient bien. Tout d'abord, f est strictement croissante. En outre, puisque $f(1) > 1$, il s'ensuit que $f(n) > n$ pour tout entier $n \in \mathbb{N}^*$, donc que $g(f(n+1)) = n+1$. Ainsi, $f(f(n+1)) = g(f(n+1))+f(n+1) = f(n+1)+(n+1)$. Le fait que $g(2) = 2$ montre que $f(2) = g(2) + 2 = 1 + 2 = 3$, donc que $f(f(1)) = f(2) = 3 = 2 + 1 = f(1) + 1$, ce qui conclut.

4 Groupe D : inégalités

1 Cours d'inégalites

Donnons pour commencer deux références. Le cours de Pierre Bornztein sur les inégalités est une excellente référence. Il contient un chapitre consacré aux inégalités de convexité. Le lecteur intéressé par la convexité et ayant déjà un bagage mathématique solide pourra consulter l'éternel *Convex Analysis* de Rockafellar.

- Exponentielle et logarithme -

On commence par quelques rappels rapides sur l'exponentielle et le logarithme.

$$\begin{array}{rccc} \exp : & \mathbb{R} & \longrightarrow & \mathbb{R}_+^* \\ & x & \longmapsto & e^x \end{array}$$

$$\begin{array}{rccc} \ln : & \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \ln x \end{array}$$

Résumons dans un tableau leurs principales propriétés. A chaque fois, x et y appartiennent au domaine de définition de la fonction concernée et n est un entier naturel.

exp	ln
strict. croissante	strict. croissante
$\exp'(x) = \exp(x)$	$\ln'(x) = 1/x$
$e^{x+y} = e^x e^y$	$\ln(xy) = \ln x + \ln y$
$e^0 = 1$	$\ln 1 = 0$
$e^{nx} = (e^x)^n$	$\ln(x^n) = n \ln x$
$e^{-x} = 1/e^x$	$\ln(1/x) = -\ln x$
$e^{x/n} = \sqrt[n]{e^x}$	$\ln(\sqrt[n]{x}) = \frac{1}{n} \ln x$

exp et ln sont liées par le fait qu'elles sont inverses l'une de l'autre :

$$\forall x \in \mathbb{R}_+^*,\ e^{\ln x} = x \qquad \text{et} \qquad \forall x \in \mathbb{R},\ \ln(e^x) = x.$$

Pour $a > 0$, une puissance a^x n'étant *a priori* définie que pour $x \in \mathbb{Z}$, on l'étend à tous les x réels de la manière suivante :

$$\forall x \in \mathbb{R}, \quad a^x = e^{x \ln a}.$$

- Convexité -

Définition 4.1. Soit I un intervalle. Une fonction $f : I \longrightarrow \mathbb{R}$ est dite convexe si :

$$\forall x, y \in I,\ \forall \lambda \in [0,1],\ f(\lambda x + (1-\lambda)y) \leqslant \lambda f(x) + (1-\lambda) f(y).$$

On dit que f est concave si $-f$ est convexe.

Théorème 4.2 (Inégalité de Jensen)**.** Soit I un intervalle. Un fonction $f : I \longrightarrow \mathbb{R}$ est convexe si et seulement si pour tout $n \geqslant 1$ et tous $x_1, \ldots, x_n \in I$ et $\lambda_1, \ldots, \lambda_n \in [0,1]$ tels que $\lambda_1 + \cdots + \lambda_n = 1$, l'inégalité suivante est vérifiée :

$$f\left(\sum_{i=1}^{n} \lambda_i x_i\right) \leqslant \sum_{i=1}^{n} \lambda_i f(x_i).$$

Démonstration. Le sens réciproque est acquis, puisqu'il suffit de prendre $n = 2$ pour retomber sur la définition de la convexité. Supposons donc f convexe et démontrons l'inégalité ci-dessus. On raisonne par récurrence sur n. Pour $n = 1$, elle est triviale, et pour $n = 2$ il s'agit de la définition de la convexité. Supposons le résultat acquis jusqu'à $n \geqslant 2$. Si on se donne alors $n+1$ points $x_1, \ldots, x_{n+1}$ ainsi que des coefficients positifs $\lambda_1, \ldots, \lambda_{n+1}$ tels que $\sum_{i=1}^{n+1} \lambda_i = 1$, la combinaison convexe correspondante peut s'écrire :

$$\begin{aligned}\sum_{i=1}^{n+1} \lambda_i x_i &= \sum_{i=1}^{n} \lambda_i x_i + \lambda_{n+1} x_{n+1} \\ &= (1-\lambda_{n+1}) \frac{\sum_{i=1}^{n} \lambda_i x_i}{1-\lambda_{n+1}} + \lambda_{n+1} x_{n+1} \\ &= (1-\lambda_{n+1}) y + \lambda_{n+1} x_{n+1},\end{aligned}$$

où on a posé $y = (1-\lambda_{n+1})^{-1} \sum_{i=1}^{n} \lambda_i x_i$. On est ainsi ramené à une combinaison convexe des deux points y et x_{n+1} associée aux coefficients $(1-\lambda_{n+1})$ et λ_{n+1}. On peut donc y appliquer l'hypothèse de récurrence pour $n = 2$:

$$\begin{aligned}f\left(\sum_{i=1}^{n+1} \lambda_i x_i\right) &= f\left((1-\lambda_{n+1}) y + \lambda_{n+1} x_{n+1}\right) \\ &\leqslant (1-\lambda_{n+1}) f(y) + \lambda_{n+1} f(x_{n+1}).\end{aligned}$$

Occupons-nous maintenant de $f(y)$. y peut être vu comme une combinaison convexe de n points, puisque :

$$y = \frac{1}{1-\lambda_{n+1}} \sum_{i=1}^{n} \lambda_i x_i = \sum_{i=1}^{n} \left(\frac{\lambda_i}{1-\lambda_{n+1}}\right) x_i.$$

y est donc la combinaison convexe des n points $x_1, \ldots, x_n$ associée aux coefficients $\lambda_i/(1-\lambda_{n+1})$ dont la somme vaut bien 1 :

$$\sum_{i=1}^{n} \frac{\lambda_i}{1-\lambda_{n+1}} = \frac{1}{1-\lambda_{n+1}} \sum_{i=1}^{n} \lambda_i = \frac{1}{1-\lambda_{n+1}} (1-\lambda_{n+1}) = 1.$$

On peut donc y appliquer l'hypothèse de récurrence :

$$f(y) \leqslant \sum_{i=1}^{n} \frac{\lambda_i}{1-\lambda_{n+1}} f(x_i).$$

Et finalement :

$$\begin{aligned} f\left(\sum_{i=1}^{n+1}\lambda_i x_i\right) &\leqslant (1-\lambda_{n+1})f(y)+\lambda_{n+1}f(x_{n+1}) \\ &\leqslant (1-\lambda_{n+1})\sum_{i=1}^{n}\frac{\lambda_i}{1-\lambda_{n+1}}f(x_i)+\lambda_{n+1}f(x_{n+1}) \\ &= \sum_{i=1}^{n+1}\lambda_{n+1}f(x_{n+1}). \end{aligned}$$

□

L'inégalité de Jensen n'est guère utile lorsqu'il s'agit de prouver qu'une fonction donnée est convexe. A l'inverse, lorsqu'on a une fonction qu'on sait être convexe, son application est fréquente.

Démontrons à présent une caractérisation qui porte sur les pentes des cordes.

Proposition 4.3. Soit I un intervalle. Une fonction $f : I \longrightarrow \mathbb{R}$ est convexe si et seulement si pour tous $x, y, z \in I$ tels que $x < y < z$:

$$\frac{f(y)-f(x)}{y-x} \leqslant \frac{f(z)-f(x)}{z-x} \leqslant \frac{f(z)-f(y)}{z-y}.$$

Démonstration. Supposons que f est convexe, et donnons-nous trois points $x < y < z$ dans I. y étant strictement compris entre x et z, il existe $\lambda \in]0,1[$ tel que :

$$y = \lambda x + (1-\lambda)z.$$

Par convexité de f, on a

$$f(y) \leqslant \lambda f(x) + (1-\lambda)f(z),$$

ce qui donne, en réarrangeant les termes :

$$\lambda(f(z)-f(x)) \leqslant f(z)-f(y).$$

Remarquons par ailleurs qu'une transformation similaire nous donne $\lambda = (z-y)/(x-z)$. En injectant cette égalité dans l'inégalité précédente, on obitent finalement :

$$\frac{f(z)-f(x)}{z-x} \leqslant \frac{f(z)-f(y)}{z-y}.$$

L'autre inégalité s'obtient de la même manière.

Réciproquement, supposons que les deux inégalités de l'énoncé sont satisfaites pour tous points $x < y < z \in I$ et montrons que f est convexe. Soient $x < z$ deux points de I et $\lambda \in [0,1]$. Si $\lambda = 0$ ou 1, l'inégalité à prouver est triviale. Supposons donc $\lambda \in]0,1[$. On pose $y = \lambda x + (1-\lambda)z$. On a par hypothèse :

$$\frac{f(z)-f(x)}{z-x} \leqslant \frac{f(z)-f(y)}{z-y}.$$

On mène alors les mêmes transformations que précédemment en sens inverse, pour retomber sur l'inégalité souhaitée :

$$f(y) \leqslant \lambda f(x) + (1-\lambda)f(z).$$

□

Voici deux caractérisations pour les fonctions dérivables.

Proposition 4.4. Soient I un intervalle et $f : I \longrightarrow \mathbb{R}$ une fonction dérivable. Les trois propositions suivantes sont équivalentes.

(i) f est convexe sur I.

(ii) f' est croissante sur I.

(iii) Pour tout $x_0 \in I$, la tangente en ce point est tout entière en-dessous de la fonction ; autrement dit :
$$\forall x \in I, \quad f(x_0) + (x - x_0)f'(x_0) \leqslant f(x).$$

Démonstration. (i)$\Longrightarrow$(ii). Supposons f dérivable et montrons que f' est croissante. Soient $x < y$ deux points. Montrons que $f'(x) \leqslant f'(y)$. Pour tout $z > y$, la Proposition 4.3 nous donne :
$$\frac{f(y) - f(x)}{y - x} \leqslant \frac{f(z) - f(y)}{z - y}.$$
En faisant tendre z vers y, on obtient, par passage des inégalités larges à la limite :
$$\frac{f(y) - f(x)}{y - x} \leqslant f'(y).$$
On se donne à présent un $x' \in I$ tel que $x < x' < y$. On a alors :
$$\frac{f(x') - f(x)}{x' - x} \leqslant \frac{f(y) - f(x)}{y - x},$$
et en faisant tendre x' vers x :
$$f'(x) \leqslant \frac{f(y) - f(x)}{y - x}.$$
En combinant les deux inégalités, on a bien $f'(x) \leqslant f'(y)$.

(ii)$\Longrightarrow$(iii). Soit $x_0 \in I$. Montrons que la tangente à f en x_0 est en-dessous du graphe de f. On pose la fonction g définie sur I par $g(x) = f(x) - (f'(x_0)(x - x_0) + f(a))$. Il s'agit donc de montrer que g est positive sur I. g est dérivable et $g'(x) = f'(x) - f'(x_0)$. f' étant croissante, g' est négative pour $x \leqslant x_0$ et positive pour $x_0 \leqslant x$. g est donc décroissante pour $x \leqslant x_0$ et croissante pour $x_0 \leqslant x$. Comme $g(x_0) = 0$, g est bien positive sur I.

(iii)$\Longrightarrow$(i). Suppsons que toutes les tangentes sont en-dessous de la fonction, et montrons que f est convexe. Soient $x, z \in I$ et $\lambda \in [0, 1]$. Notons $y = \lambda x + (1 - \lambda)z$. Notons τ la tangente à f en y :
$$\forall x' \in I, \ \tau(x') = f(y) + f'(y)(x' - y).$$
Par hypothèse, $f(x) \geqslant \tau(x)$ et $f(z) \geqslant \tau(z)$. On a donc :
$$\lambda f(x) + (1 - \lambda)f(z) \geqslant \lambda\tau(x) + (1 - \lambda)\tau(z) = \tau(y) = f(x),$$
où la première égalité se déduit facilement du fait que τ est affine, et la deuxième vient de la définition de τ. f est donc bien convexe. □

Corollaire 4.5. Soient I un intervalle et $f : I \longrightarrow \mathbb{R}$ une fonction deux fois dérivable. Alors f est convexe si, et seulement si, $f'' \geqslant 0$.

Corollaire 4.6.

1. exp est convexe.
2. ln est concave.

Démonstration. Il suffit de calculer les dérivées secondes. $\forall x \in \mathbb{R},\ \exp''(x) = \exp(x) \geqslant 0$, et $\forall x \in \mathbb{R}_+^*,\ \ln''(x) = -1/x^2 \leqslant 0$. □

Exemple 4.7. Donnons trois exemples d'inégalités classiques obtenues par la caractérisation faisant intervenir la tangente.

(i) $\forall x \in \mathbb{R},\ 1 + x \leqslant e^x$.

(ii) $\forall x \in]-1, +\infty[,\ \ln(1+x) \leqslant x$.

(iii) $\forall n \geqslant 1,\ \forall x \in [-1, +\infty[,\ 1 + nx \leqslant (1+x)^n$.

Proposition 4.8. Soit $f : [a, b] \longrightarrow \mathbb{R}$ une fonction convexe. Alors, f atteint son maximum en a ou en b.

Démonstration. Sans perte de généralité, supposons que $f(a) \geqslant f(b)$, et notons γ la corde entre ces deux points :

$$\gamma : x \in I \longmapsto f(a) + \frac{f(b) - f(a)}{b - a}(x - a).$$

On a clairement $\forall x \in I,\ f(x) \leqslant \gamma(x) \leqslant f(a)$. Le maximum de f existe bien et est atteint en a. □

- Exercices -

Exercice 1 Soient α, β, γ les angles d'un triangle Montrer que :

$$\sin\alpha + \sin\beta + \sin\gamma \leqslant \frac{3\sqrt{3}}{2}$$

Solution de l'exercice 1 sin étant concave sur $[0, \pi]$, on peut appliquer l'inégalité de Jensen de la façon suivante :

$$\frac{1}{3}\sin\alpha + \frac{1}{3}\sin\beta + \frac{1}{3}\sin\gamma \leqslant \sin\left(\frac{1}{3}\alpha + \frac{1}{3}\beta + \frac{1}{3}\gamma\right) = \sin\frac{\pi}{3} = \frac{\sqrt{3}}{2},$$

où $\alpha + \beta + \gamma = \pi$ car il s'agit des angles d'un triangle. On conclut en multipliant par 3 de part et d'autre de cette inégalité.

Exercice 2 Soient $a, b, c > 0$ tels que $a + b + c = 1$. Montrer que

$$\left(a + \frac{1}{a}\right)^2 + \left(b + \frac{1}{b}\right)^2 + \left(c + \frac{1}{c}\right)^2 \geqslant \frac{100}{3}.$$

Solution de l'exercice 2 On pose, pour $x > 0$, $f(x) = (x + 1/x)^2$. En calculant la dérivée seconde, on s'aperçoit que cette fonction est convexe. Et donc

$$\begin{aligned}\left(a+\frac{1}{a}\right)^2+\left(b+\frac{1}{b}\right)^2+\left(c+\frac{1}{c}\right)^2 &= 3\left(\frac{f(a)+f(b)+f(c)}{3}\right)\\ &\geqslant 3f\left(\frac{a+b+c}{3}\right) = 3f\left(\frac{1}{3}\right)\\ &= 3\left(\frac{1}{3}+3\right)^2 = \frac{100}{3}.\end{aligned}$$

Exercice 3 Soient $x_1, \dots, x_n > 0$ et $a_1, \dots, a_n \geqslant 0$ non tous nuls. On se donne aussi deux réels $0 < p < q$. Montrer qu'alors :

$$\left(\frac{\sum_{i=1}^n a_i x_i^p}{\sum_{i=1}^n a_i}\right)^{1/p} \leqslant \left(\frac{\sum_{i=1}^n a_i x_i^q}{\sum_{i=1}^n a_i}\right)^{1/q}.$$

Solution de l'exercice 3 Quitte à remplacer a_i par $a_i / \sum_{i=1}^n a_i$, on peut supposer que $\sum_{i=1}^n a_i = 1$. On considère $f(x) = x^{q/p}$ qui est convexe car $q/p \geqslant 1$. En appliquant Jensen aux x_i^p avec les coefficients a_i, on obtient :

$$\left(\sum_{i=1}^n a_i x_i^p\right)^{q/p} \leqslant \sum_{i=1}^n a_i (x_i^p)^{q/p} = \sum_{i=1}^n a_i x_i^q.$$

On conclut en prenant la racine q-ième des deux côtés.

Exercice 4 Soient $0 < a \leqslant b \leqslant c \leqslant d$. Montrer que $a^b b^c c^d d^a \geqslant b^a c^b d^c a^d$.

Solution de l'exercice 4 En passant au logarithme de part et d'autre, il vient :

$$b\ln a + c\ln b + d\ln c + a\ln d \geqslant a\ln b + b\ln c + c\ln d + d\ln a.$$

En réarrangeant les termes, on obtient :

$$\frac{\ln c - \ln a}{c-a} \geqslant \frac{\ln d - \ln b}{d-b}.$$

Cette inégalité se prouve en appliquant l'inégalité des pentes à ln concave aux points (a, b, c) puis (b, c, d).

Exercice 5 Soit $x_1, \dots, x_n$ et $a_1, \dots, a_n$ des réels appartenant à $[0, 1]$ tels que $\sum_{i=1}^n a_i = 1$. Montrer que pour tout $s \in \mathbb{R}$,

$$\ln\left(\sum_{i=1}^n a_i e^{s x_i}\right) \leqslant (e^s - 1)\sum_{i=1}^n a_i x_i.$$

Solution de l'exercice 5 Observons que pour tout $x \in [0,1]$:

$$e^{sx} = e^{xs+(1-x)\cdot 0} \leqslant xe^s + (1-x)e^0 = xe^s + (1-x),$$

par convexité de l'exponentielle. Ainsi :

$$\begin{aligned}\sum_{i=1}^{n} a_i e^{sx_i} &\leqslant \sum_{i=1}^{n} a_i \left(x_i e^s + (1-x_i)\right) \\ &= e^s \sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} a_i - \sum_{i=1}^{n} a_i x_i \\ &= 1 + (e^s - 1) \sum_{i=1}^{n} a_i x_i\end{aligned}$$

car, par hypothèse, $\sum_{i=1}^{n} a_i = 1$. En appliquant l'inégalité $1 + x \leqslant e^x$ à cette dernière expression :

$$1 + (e^s - 1) \sum_{i=1}^{n} a_i x_i \leqslant \exp\left((e^s - 1) \sum_{i=1}^{n} a_i x_i\right).$$

On obtient donc :

$$\sum_{i=1}^{n} a_i e^{sx_i} \leqslant \exp\left((e^s - 1) \sum_{i=1}^{n} a_i x_i\right).$$

On trouve le résultat souhaité en prenant le logarithme des deux côtés de cette inégalité.

Exercice 6 Soient $x_1, \ldots, x_n \geqslant 1$. Montrer que :

$$\frac{1}{x_1+1} + \frac{1}{x_2+1} + \cdots + \frac{1}{x_n+1} \geqslant \frac{n}{1 + (x_1 x_2 \ldots x_n)^{1/n}}.$$

Solution de l'exercice 6 On effectue le changement de variable $x_i = e^{y_i}$. Posons $f(y) = \frac{1}{1+e^y}$ pour $y \geqslant 0$. En dérivant deux fois, on constate que f est convexe sur $\mathbb{R}_+$. Ainsi, l'inégalité demandée revient simplement à appliquer Jensen aux y_i avec coefficients $1/n$.

Exercice 7 Soient $a, b, c \in [0,1]$. Montrer que :

$$\frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c) \leqslant 1.$$

Solution de l'exercice 7 Demandons-nous pour quels $(a,b,c) \in [0,1]^3$ le membre de gauche atteint sa valeur maximale. Pour $b, c \in [0,1]$ fixés, considérons la fonction :

$$f(a) = \frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c).$$

On vérifie aisément que cette fonction est convexe. Cette fonction atteint son maximum en $a = 0$ ou $a = 1$. Avec un raisonnement analogue pour b et c, on voit que nécessairement a, b et c doivent appartenir à $\{0,1\}$ lorsque la quantité considérée est maximale. On conclut en remarquant qu'en chacun des triplets $(a,b,c) \in \{0,1\}^3$, la quantité vaut 1.

Exercice 8

1. Soit $x, y > 0$ et $p, q \in [1, +\infty[$ tels que $1/p + 1/q = 1$. Montrer que :
$$xy \leqslant \frac{x^p}{p} + \frac{y^q}{q}.$$
2. Soient $x_1, \ldots, x_n$ et $y_1, \ldots, y_n$ des réels strictement positifs. On se donne $p, q \in [1, +\infty[$ tels que $1/p + 1/q = 1$. Montrer que :
$$\sum_{i=1}^{n} x_i y_i \leqslant \left(\sum_{i=1}^{n} x_i^p\right)^{1/p} \left(\sum_{i=1}^{n} y_i^q\right)^{1/q}.$$
3. Montrer que :
$$(1 + x^2y + x^4y^2)^3 \leqslant (1 + x^3 + x^6)^2(1 + y^3 + y^6).$$

Solution de l'exercice 8

1. On utilise la convexité de l'exponentielle :
$$\begin{aligned} xy &= \exp(\ln(xy)) = \exp(\ln x + \ln y) \\ &= \exp\left(\frac{1}{p}\ln(x^p) + \frac{1}{q}\ln(y^q)\right) \\ &\leqslant \frac{1}{p}e^{\ln(x^p)} + \frac{1}{q}e^{\ln(y^q)} = \frac{x^p}{p} + \frac{y^q}{q}. \end{aligned}$$
2. On applique la question précédente de la manière suivante :
$$\sum_{i=1}^{n} \frac{x_i}{\left(\sum_{j=1}^{n} x_j^p\right)^{1/p}} \cdot \frac{y_i}{\left(\sum_{j=1}^{n} y_j^q\right)^{1/q}} \leqslant \frac{1}{p}\sum_{i=1}^{n} \frac{x_i^p}{\sum_{i=1}^{n} x_j^p} + \frac{1}{q}\sum_{i=1}^{n} \frac{y_i}{\sum_{j=1}^{n} y_j^q} = \frac{1}{p} + \frac{1}{q} = 1.$$
On conclut en multipliant de part et d'autre par $\left(\sum_{j=1}^{n} x_j^p\right)^{1/p}\left(\sum_{j=1}^{n} y_j^q\right)^{1/q}$.
3. Il s'agit d'une application directe de la question précédente, avec $p = \frac{3}{2}$ et $q = 3$.

2 TD d'inégalités

- Quelques inégalités secondaires, mais utiles -

Proposition 4.9. (Inégalité de Nesbitt) Soient $a, b, c > 0$ des réels. Alors
$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geqslant \frac{3}{2},$$
avec égalité si et seulement si $a = b = c$.

Démonstration. Appelons I le côté gauche de l'inégalité, et $J = a(b+c) + b(c+a) + c(a+b)$. Alors par Cauchy-Schwarz, $IJ \geqslant (a+b+c)^2$. On se ramène donc à montrer
$$\frac{(a+b+c)^2}{2(ab+bc+ca)} \geqslant \frac{3}{2},$$

ce qui est équivalent à

$$2(a^2+b^2+c^2) \geqslant 2(ab+bc+ca),$$

vrai car équivalent à

$$(a-b)^2+(b-c)^2+(c-a)^2 \geqslant 0.$$

Cette dernière inégalité fait aussi apparaître clairement le cas d'égalité. □

Proposition 4.10. (Inégalité de Schur) Soient x, y, z des réels positifs et r un nombre réel. Alors

$$x^r(x-y)(x-z)+y^r(y-x)(y-z)+z^r(z-x)(z-y) \geqslant 0,$$

l'égalité étant atteinte lorsque $x=y=z$, ou bien lorsque deux réels parmi x, y, z sont égaux et le troisième est nul.

Démonstration. L'inégalité étant symétrique en x, y, z, on peut supposer $x \geqslant y \geqslant z$. On peut réécrire le côté gauche sous la forme

$$x^r(x-y)^2+(x^r-y^r+z^r)+z^r(y-z)^2.$$

Le premier et le troisième terme sont positifs. En ce qui concerne le deuxième, si $r \geqslant 0$ alors $x^r \geqslant y^r$ et si $r<0$ alors $z^r \geqslant y^r$, donc il est positif aussi, ce qui conclut. □

Le cas $r=1$ est particulièrement important. Il s'écrit après développement

$$x^3+y^3+z^3-(x^2y+x^2z+y^2x+y^2z+z^2x+z^2y)+3xyz \geqslant 0.$$

Il y a d'autres formes équivalentes, par exemple

$$xyz \geqslant (x+y-z)(y+z-x)(z+x-y). \tag{VI.1}$$

En posant $x+y+z=k$, cela se réécrit

$$xyz \geqslant (k-2x)(k-2y)(k-2z).$$

D'autre part, en remarquant que l'inégalité correspond à la positivité d'un polynôme symétrique en x, y, z, on peut réécrire cela en terme des fonctions symétriques élémentaires :

$$\sigma_1 = x+y+z, \quad \sigma_2 = xy+yz+zx, \quad \sigma_3 = xyz.$$

Un calcul simple montre que $x^3+y^3+z^3 = \sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$ et $x^2y+x^2z+y^2x+y^2z+z^2x+z^2y = \sigma_1\sigma_2-3\sigma_3$. Ainsi, l'inégalité de Schur se réécrit

$$\sigma_1^3-4\sigma_1\sigma_2+9\sigma_3 \geqslant 0,$$

c'est-à-dire

$$(x+y+z)^3+9xyz \geqslant 4(x+y+z)(xy+yz+zx). \tag{VI.2}$$

Il est aussi utile d'avoir en tête la reformulation suivante de Cauchy-Schwarz (parfois appelée inégalité des mauvais élèves, ou lemme de T2), qui facilite l'application de Cauchy-Schwarz dans certains cas.

Proposition 4.11. Soient $a_1, \ldots, a_n$ et $x_1, \ldots, x_n$ des réels strictement positifs. Alors

$$\frac{a_1^2}{x_1} + \ldots + \frac{a_n^2}{x_n} \geqslant \frac{(a_1 + \ldots + a_n)^2}{x_1 + \ldots + x_n},$$

avec égalité lorsque les vecteurs $(a_1, \ldots, a_n)$ et $(x_1, \ldots, x_n)$ sont colinéaires.

Exercice 1 (IMO 1995) Soient $a, b, c > 0$ tels que $abc = 1$. Montrer que

$$\frac{1}{a^3(b+c)} + \frac{1}{b^3(c+a)} + \frac{1}{c^3(a+b)} \geqslant \frac{3}{2}.$$

- Inégalités avec condition sur le produit des variables -

De nombreuses inégalités olympiques font intervenir des variables $a_1, \ldots, a_n$ soumises à une condition du type $a_1 \ldots a_n = 1$. Une méthode très utile pour aborder ce genre d'inégalités consiste à se débarrasser de cette contrainte en opérant un changement de variables du type

$$a_1 = \left(\frac{x_2}{x_1}\right)^\alpha, \ a_2 = \left(\frac{x_3}{x_2}\right)^\alpha, \ldots, a_n = \left(\frac{x_1}{x_n}\right)^\alpha,$$

où α est un réel à choisir, souvent pris égal à 1.

Exemple 4.12. Soient a, b, c des réels positifs tels que $abc = 1$. Montrer que

$$\frac{a}{ab+1} + \frac{b}{bc+1} + \frac{c}{ca+1} \geqslant \frac{3}{2}.$$

La substitution la plus simple $a = \frac{x}{y}$, $b = \frac{y}{z}$, $c = \frac{z}{x}$ (obtenue en prenant par exemple $x = 1 = abc$, $y = bc$, $z = c$) transforme le côté gauche en

$$\frac{\frac{x}{y}}{\frac{x}{z}+1} + \frac{\frac{y}{z}}{\frac{y}{x}+1} + \frac{\frac{z}{x}}{\frac{z}{y}+1} = \frac{zx}{xy+yz} + \frac{xy}{yz+zx} + \frac{yz}{zx+xy}.$$

On applique l'inégalité de Nesbitt pour conclure.

Remarque 4.13. Puisque les substitutions de ce genre peuvent compliquer sensiblement l'inégalité à prouver, on a tout intérêt, pour gagner en clarté, à effectuer la substitution la plus judicieuse possible. Par exemple, ici, même si dans ce cas cela ne changeait pas grand chose à la lisibilité de l'inégalité, on aurait pu choisir la substitution de sorte à ce que a et ab soient automatiquement réduits au même dénominateur, à savoir $a = \frac{y}{x}$, $b = \frac{z}{y}$, $c = \frac{x}{z}$, ce qui donnait l'inégalité de Nesbitt directement.

Exercice 2 (Russie 2004) Montrer que si $n > 3$ et $x_1, \ldots, x_n$ sont des réels strictement positifs de produit 1, alors

$$\frac{1}{1+x_1+x_1x_2} + \frac{1}{1+x_2+x_2x_3} + \ldots + \frac{1}{1+x_n+x_nx_1} > 1.$$

Exercice 3 Soient $a, b, c > 0$ avec $abc = 1$. Montrer que

$$3 + \frac{a}{b} + \frac{b}{c} + \frac{c}{a} \geqslant a + b + c + \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

Exercice 4 Soient $a, b, c, d > 0$ avec $abcd = 1$. Montrer que

$$\frac{1}{a(1+b)} + \frac{1}{b(1+c)} + \frac{1}{c(1+d)} + \frac{1}{d(1+a)} \geqslant 2.$$

Exercice 5 Soit $n \geqslant 3$ et soient $x_1, \ldots, x_n > 0$ tels que $x_1 \ldots x_n = 1$. Montrer que

$$\frac{1}{x_1^2 + x_1x_2} + \frac{1}{x_2^2 + x_2x_3} + \ldots + \frac{1}{x_n^2 + x_nx_1} \geqslant \frac{n}{2},$$

lorsque n vaut 3 ou 4.

- Autres inégalités -

Les exercices suivants tournent autour de la transformation de Ravi, de l'inégalité de Schur, de l'inégalité de Cauchy-Schwarz, et de la manipulation de racines carrées.

Exercice 6 (Olympiades indiennes 1989) Soient a, b, c les longueurs des côtés d'un triangle. Prouver que

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} < 2.$$

Exercice 7 (APMO 1996) Soient a, b, c les longueurs des côtés d'un triangle. Démontrer que

$$\sqrt{a+b-c} + \sqrt{b+c-a} + \sqrt{c+a-b} \leqslant \sqrt{a} + \sqrt{b} + \sqrt{c}.$$

Exercice 8 Soient $a, b, c > 0$ tels que $abc = 1$. Montrer que

$$\sqrt{\frac{1+a^2b}{1+ab}} + \sqrt{\frac{1+b^2c}{1+bc}} + \sqrt{\frac{1+c^2a}{1+ca}} \geqslant 3.$$

Exercice 9 Soient a, b, c les longueurs des côtés d'un triangle. Montrer que

$$\sqrt{3(\sqrt{ab} + \sqrt{bc} + \sqrt{ca})} \geqslant \sqrt{a+b-c} + \sqrt{b+c-a} + \sqrt{c+a-b}.$$

Exercice 10 (APMO 2004) Soient $a, b, c > 0$. Montrer que

$$(a^2+2)(b^2+2)(c^2+2) \geqslant 9(ab+bc+ca)$$

- Solutions des exercices -

Solution de l'exercice 1 On applique Cauchy-Schwarz de la manière suivante (en s'aidant éventuellement de la proposition 4.11 ci-dessus).

$$\frac{1}{a^2}\frac{1}{a(b+c)}+\frac{1}{b^2}\frac{1}{b(c+a)}+\frac{1}{c^2}\frac{1}{c(a+b)}\geqslant\frac{\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)^2}{a(b+c)+b(c+a)+c(a+b)}.$$

En simplifiant et en utilisant $abc=1$, le côté droit devient

$$\frac{(ab+bc+ca)^2}{2(ab+bc+ca)}\geqslant\frac{1}{2}(ab+bc+ca)\geqslant\frac{3}{2}(abc)^{\frac{2}{3}}=\frac{3}{2}$$

où la dernière inégalité vient de l'IAG.

Solution de l'exercice 2 On utilise les substitutions $x_1=\frac{a_2}{a_1}$, $x_2=\frac{a_3}{a_2},\ldots,x_n=\frac{a_1}{a_n}$ (qui ont l'avantage de mettre x_i et x_ix_{i+1} au même dénominateur pour tout i automatiquement). Alors on obtient :

$$\frac{a_1}{a_1+a_2+a_3}+\ldots+\frac{a_n}{a_n+a_1+a_2}>\sum_{i=1}^{n}\frac{a_i}{a_1+\ldots+a_n}=1.$$

Solution de l'exercice 3 Ici, pour n'avoir aucun carré au dénominateur, ce qui va faciliter la mise au même dénominateur ultérieure, on va prendre $a=\frac{y}{x}$, $b=\frac{z}{y}$, $c=\frac{x}{z}$, ce qui donne

$$3+\frac{y^2}{xz}+\frac{z^2}{yx}+\frac{x^2}{zy}\geqslant\frac{y}{x}+\frac{z}{y}+\frac{x}{z}+\frac{x}{y}+\frac{y}{z}+\frac{z}{x}.$$

On multiplie par xyz des deux côtés pour obtenir

$$x^3+y^3+z^3+3xyz\geqslant y^2z+z^2x+x^2y+x^2z+xy^2+yz^2,$$

qui est juste l'inégalité de Schur.

Solution de l'exercice 4 De même, on essaye de se débrouiller pour que a et ab soient au même dénominateur. La substitution qu'on choisit est donc

$$a=\frac{y}{x},\ \ b=\frac{z}{y},\ \ c=\frac{t}{z},\ \ d=\frac{x}{t}.$$

L'inégalité devient donc

$$\frac{x}{y+z}+\frac{y}{z+t}+\frac{z}{t+x}+\frac{t}{x+y}\geqslant 2.$$

Puis, on a applique Cauchy-Schwarz pour obtenir

$$\frac{x}{y+z}+\frac{y}{z+t}+\frac{z}{t+x}+\frac{t}{x+y}\geqslant\frac{(x+y+z+t)^2}{xy+xz+yz+yt+zt+zx+tx+ty}.$$

Il reste donc à prouver

$$(x+y+z+t)^2\geqslant 2(xy+xz+yz+yt+zt+zx+tx+ty),$$

ce qui est équivalent à

$$x^2 + y^2 + z^2 + t^2 \geqslant 2(xz + yt),$$

qui à son tour est équivalent à

$$(x - z)^2 + (y - t)^2 \geqslant 0.$$

Solution de l'exercice 5 Cette fois-ci, histoire d'avoir le moins de carrés possible, et d'avoir x_i^2 et $x_i x_{i+1}$ au même dénominateur, nous allons poser

$$x_1 = \sqrt{\frac{a_2}{a_1}},\ x_2 = \sqrt{\frac{a_3}{a_2}}, \ldots, x_n = \sqrt{\frac{a_1}{a_n}}.$$

L'inégalité devient alors

$$\frac{a_1}{a_2 + \sqrt{a_1 a_3}} + \frac{a_2}{a_3 + \sqrt{a_2 a_4}} + \ldots + \frac{a_n}{a_1 + \sqrt{a_n a_1}} \geqslant \frac{n}{2}.$$

D'après l'IAG, on a $\sqrt{a_i a_{i+2}} \leqslant \frac{a_i + a_{i+2}}{2}$, ce qui nous conduit à montrer

$$\frac{a_1}{2a_2 + a_1 + a_3} + \frac{a_2}{2a_3 + a_2 + a_4} + \ldots + \frac{a_n}{2a_1 + a_n + a_2} \geqslant \frac{n}{4}.$$

En appliquant Cauchy-Schwarz, cela revient à prouver

$$\frac{(a_1 + \ldots + a_n)^2}{a_1(a_1 + 2a_2 + a_3) + a_2(a_2 + 2a_3 + a_4) + \ldots + a_n(a_n + 2a_1 + a_2)} \geqslant \frac{n}{4}.$$

Distinguons maintenant suivant si $n = 3$ ou $n = 4$. Si $n = 4$, l'inégalité se réécrit

$$(a_1+a_2+a_3+a_4)^2 \geqslant a_1^2+2a_1a_2+a_1a_3+a_2^2+2a_2a_3+a_2a_4+a_3^2+2a_3a_4+a_3a_1+a_4^2+2a_4a_1+a_4a_2,$$

et on constate que c'est en fait même une égalité. Si $n = 3$, on doit prouver

$$4(a_1 + a_2 + a_3)^2 \geqslant 3(a_1^2 + 2a_1a_2 + a_1a_3 + a_2^2 + 2a_2a_3 + a_2a_1 + a_3^2 + 2a_3a_1 + a_3a_2),$$

ce qui est équivalent à

$$a_1^2 + a_2^2 + a_3^2 \geqslant a_1a_2 + a_2a_3 + a_3a_1,$$

qui découle directement de l'inégalité du réordonnement.

Solution de l'exercice 6 On applique la transformation de Ravi : $a = x + y$, $b = y + z$, $c = z + x$, où $x, y, z > 0$. On a donc

$$\frac{x+y}{x+2y+z} + \frac{y+z}{y+2z+x} + \frac{z+x}{z+2x+y} < \frac{x+y}{x+y+z} + \frac{y+z}{y+z+x} + \frac{z+x}{z+x+y} = 2.$$

Solution de l'exercice 7 Après avoir appliqué la transformation de Ravi, on obtient

$$\sqrt{2x} + \sqrt{2y} + \sqrt{2z} \leqslant \sqrt{x+y} + \sqrt{y+z} + \sqrt{z+x}.$$

Par concavité de la fonction racine carrée, on a $\sqrt{\frac{x+y}{2}} \geqslant \frac{\sqrt{x}+\sqrt{y}}{2}$, et de même avec y et z, puis avec z et x. En sommant ces trois inégalités, on obtient inégalité cherchée.

Solution de l'exercice 8 En utilisant la condition sur abc, on peut réécrire l'inégalité sous la forme

$$\sqrt{\frac{a+b}{a+1}} + \sqrt{\frac{b+c}{b+1}} + \sqrt{\frac{c+a}{c+1}} \geqslant 3$$

En appliquant l'IAG, on se ramène à

$$(a+b)(b+c)(c+a) \geqslant (a+1)(b+1)(c+1).$$

Pour démontrer cette inégalité, il existe deux méthodes.

Première méthode : on fait la substitution $a = \frac{x}{y}$, $b = \frac{y}{z}$, $c = \frac{z}{x}$, ce qui donne

$$(y^2+xz)(z^2+xy)(x^2+yz) \geqslant xyz(x+y)(x+z)(y+z).$$

On applique Cauchy-Schwarz sous la forme

$$\left(1+\frac{y}{z}\right)(x^2+yz) \geqslant (x+y)^2$$
$$\left(1+\frac{z}{x}\right)(y^2+xz) \geqslant (y+z)^2$$
$$\left(1+\frac{x}{y}\right)(z^2+xy) \geqslant (x+z)^2.$$

On a le résultat en multipliant les trois inégalités.

Deuxième méthode : on pose $p = a+b+c$, $q = ab+bc+ca$. On remarque que

$$pq = (a+b+c)(ab+bc+ca) = (a+b)(b+c)(c+a)+1,$$

donc l'inégalité cherchée revient à

$$pq - 1 \geqslant 1 + p + q + 1,$$

c'est-à-dire $pq \geqslant p+q+3$. D'autre part, l'IAG donne $p \geqslant 3$ et $q \geqslant 3$, donc on a

$$pq = \frac{pq}{2} + \frac{pq}{2} \geqslant \frac{3p}{2} + \frac{3q}{2} \geqslant p+q+\frac{p+q}{2} \geqslant p+q+3.$$

Solution de l'exercice 9 On effectue une transformation de Ravi et on met tout au carré. On obtient

$$3\sqrt{(x+y)(y+z)}+3\sqrt{(y+z)(z+x)}+3\sqrt{(z+x)(x+y)} \geqslant 2(x+y+z)+4(\sqrt{xy}+\sqrt{yz}+\sqrt{zx}).$$

Par Cauchy-Schwarz, $\sqrt{(x+y)(y+z)} \geqslant (y+\sqrt{xz})$, et de même pour les deux autres termes. On doit alors prouver

$$3(x+y+z)+3(\sqrt{xy}+\sqrt{yz}+\sqrt{zx}) \geqslant 2(x+y+z)+4(\sqrt{xy}+\sqrt{yz}+\sqrt{zx}),$$

c'est-à-dire

$$x+y+z \geqslant \sqrt{xy}+\sqrt{yz}+\sqrt{zx}.$$

Or l'IAG appliquée trois fois nous donne

$$\frac{x+y}{2}+\frac{y+z}{2}+\frac{z+x}{2}\geqslant\sqrt{xy}+\sqrt{yz}+\sqrt{zx},$$

ce qui conclut.

Solution de l'exercice 10 Quand on développe tout, cela donne

$$(abc)^2+2(a^2b^2+b^2c^2+c^2a^2)+4(a^2+b^2+c^2)+8\geqslant 9(ab+bc+ca).$$

On va essayer de faire ressembler ça à la variante (VI.2) de l'inégalité de Schur, réécrite sous la forme

$$9\frac{xyz}{x+y+z}\geqslant 4(xy+yz+zx)-(x+y+z)^2.$$

En particulier, nous allons faire disparaître les termes en a^2b^2 grâce à l'inégalité

$$2(a^2b^2+b^2c^2+c^2a^2)+6\geqslant 2(a^2b^2+1)+2(b^2c^2+1)+2(c^2a^2+1)\geqslant 4(ab+bc+ca)$$

obtenue à partir de l'IAG. D'autre part $3(a^2+b^2+c^2)\geqslant 3(ab+bc+ca)$, et il nous reste donc à prouver

$$(abc)^2+2\geqslant 2(ab+bc+ca)-(a^2+b^2+c^2).$$

Pour obtenir ça, on applique l'IAG deux fois, puis la variante (VI.2) de l'inégalité de Schur telle qu'elle est écrite ci-dessus :

$$\begin{aligned}(abc)^2+2=(abc)^2+1+1&\geqslant 3(abc)^{\frac{2}{3}}\\&\geqslant 9\frac{abc}{a+b+c}\\&\geqslant 4(ab+bc+ca)-(a+b+c)^2\\&=2(ab+bc+ca)-(a^2+b^2+c^2).\end{aligned}$$

VII. Test de fin de parcours

Contenu de cette partie

1 Groupe A

1 Énoncés

Exercice 1 Soient A et B les intersections de deux cercles Γ_1 et Γ_2. Soient $[CD]$ une corde de Γ_2, et E et F les secondes intersections respectives des droites (CA) et (BD) avec Γ_1. Montrer que les droites (CD) et (EF) sont parallèles.

Exercice 2 Montrer que 24 divise $p^2 - 1$ pour tout nombre premier $p \geqslant 5$.

Exercice 3 Soit ABC un triangle. On note Γ son cercle inscrit et Γ_A son cercle exinscrit en A. Γ touche $[BC]$ en I, et Γ_A touche $[BC]$ en J. Soit K le point d'intersection de Γ avec (AJ) le plus proche de A.

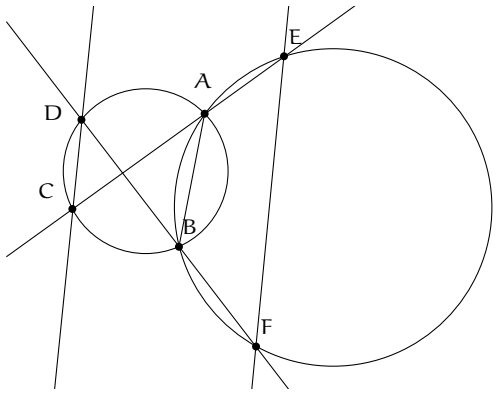
Montrer que IJK est rectangle en I.

Remarque. Le cercle exinscrit en A au triangle ABC est le cercle tangent au segment $[BC]$, à la demi-droite $[AB)$ au-delà de B et à la demi-droite $[AC)$ au-delà de C.

Exercice 4 Trouver tous les entiers positifs ou nuls x, y, z tels que $x^3 + 4y^3 = 16z^3 + 4xyz$.

2 Solutions

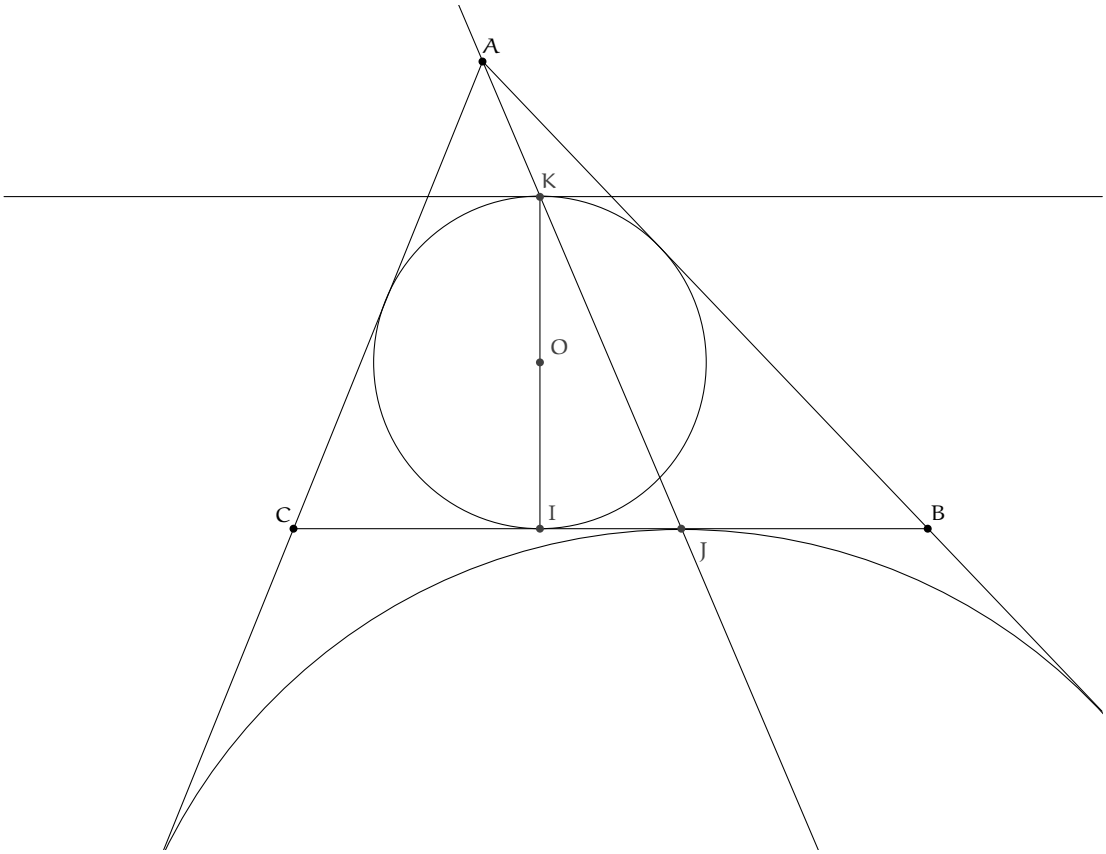
Solution de l'exercice 1



Chassons les angles. Par cocyclicité, on a $\widehat{AEF} = 180° - \widehat{ABF} = \widehat{ABD} = 180° - \widehat{ACD}$. Donc les droites (CD) et (EF) sont parallèles.

Solution de l'exercice 2 On remarque que $24 = 3 \times 8$. Or, 3 et 8 sont premiers entre eux. Il nous suffit donc de prouver que 3 et 8 divisent $p^2 - 1$. Or, p est premier, différent de 3, et donc $p^2 \equiv 1\,[3]$, donc 3 divise bien $p^2 - 1$. On factorise maintenant $p^2 - 1 = (p-1)(p+1)$ et on remarque que $p - 1$ et $p + 1$ sont deux nombres pairs consécutifs (car p est différent de 2, en particulier il est impair). Or, parmi deux pairs consécutifs, l'un des deux est divisible par 4, donc $(p-1)(p+1)$ est divisible par 8. On a terminé.

Solution de l'exercice 3



A est l'intersection des tangentes communes extérieures à Γ et Γ_A, donc c'est le centre de l'homothétie positive h qui envoie Γ_A sur Γ. $h(J)$ est sur (AJ) et sur le cercle $h(\Gamma_A) = \Gamma$, donc $h(J) = K$. La tangente à Γ en K est donc parallèle à (BC). Soit donc O le centre de Γ : (OK) est perpendiculaire à la tangent, donc à (BC), donc $K \in (OI)$ et (IK) est perpendiculaire à (BC), d'où le résultat.

Solution de l'exercice 4 Soit x, y, z une solution. On remarque que $4y^3$, $16z^3$ et $4xyz$ sont pairs, donc x^3 doit être pair, donc x aussi. On pose $x' = x/2$. L'équation devient $8x'^3 + 4y^3 = 16z^2 + 8x'yz$, autrement dit $2x'^3 + y^3 = 4z^2 + 2x'yz$. On remarque que y est pair : on écrit $y = 2y'$, et l'équation devient $x'^3 + 4y'^3 = 2z^2 + 2x'y'z$. On remarque que x' est pair : on écrit $x' = 2x''$, et l'équation devient $4x''^3 + 2y'^3 = z^2 + 2x''y'z$. On remarque que z est pair : on écrit $z = 2z'$, et l'équation devient $2x''^3 + y'^3 = 4z'^2 + 2x''y'z'$. On remarque que cette cinquième équation est identique à la seconde ! On a ainsi prouvé que, si (x', y, z) est solution de l'équation $2x'^3 + y^3 = 4z^2 + 2x'yz$, que nous appellerons (E), alors $(x'/2, y/2, z/2)$ est aussi solution. Par principe de descente infinie, la seule solution de l'équation (E) est $(0, 0, 0)$. Or on avait que, si (x, y, z) est solution de l'équation de départ, $(x/2, y, z)$ est solution de (E). Ainsi, $(x/2, y, z) = (0, 0, 0)$, puis $x = y = z = 0$ comme demandé.

2 Groupe B

1 Énoncés

Exercice 1 Soit ABC un triangle, soient P, Q et R les points de tangence du cercle inscrit du triangle ABC avec les côtés BC, CA et AB du triangle. Montrer que les droites AP, BQ et CR sont concourantes.

Exercice 2 Soit a, b et c des entiers relatifs tels que $a \wedge b = 1$. Montrer que $a \wedge (bc) = a \wedge c$.

Exercice 3 Soit $ABCD$ un parallélogramme, P un point à l'intérieur de $ABCD$, tel que $\widehat{APB} + \widehat{DPC} = 180°$. Montrer que $\widehat{ADP} = \widehat{PBA}$.

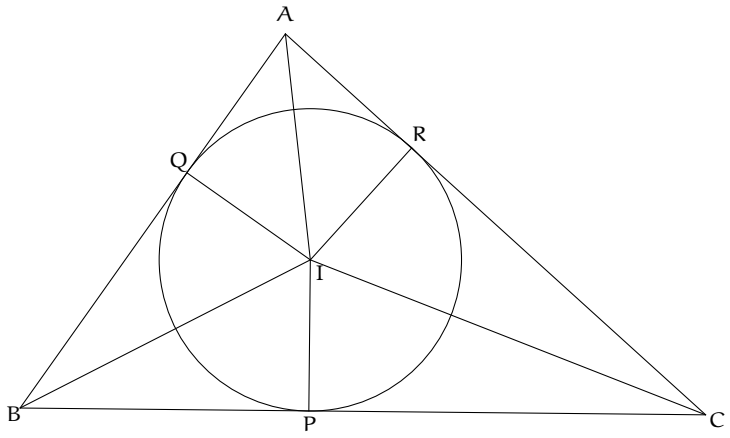
Exercice 4 Soit p et q deux entiers naturels premiers entre eux. Pour tout entier n, on note $r_p(n)$ (respectivement, $r_q(n)$) le reste dans la division euclidienne de n par p (respectivement q). Montrer que $\sum_{n=0}^{pq-1} (-1)^{r_p(n)+r_q(n)}$ vaut 0 si pq est pair, et 1 si pq est impair.

2 Solutions

Solution de l'exercice 1 Soit I le centre du cercle inscrit dans ABC. On remarque que $PB = QB$ (par exemple car $PB^2 = IB^2 - IP^2 = IB^2 - IQ^2 = PC^2$. Symétriquement, on a $RC = PC$ et $QA = RA$. Donc,

$$\begin{aligned}\frac{\overline{PB}}{\overline{PC}} \cdot \frac{\overline{RC}}{\overline{RA}} \cdot \frac{\overline{QA}}{\overline{QB}} &= -\frac{PB}{PC} \cdot -\frac{RC}{RA} \cdot -\frac{QA}{QB} \\ &= -\frac{PB}{QB} \cdot -\frac{RC}{PC} \cdot -\frac{QA}{QB} = -1.\end{aligned}$$

Le théorème de Céva dit donc que AP, BQ et CR sont alignés.



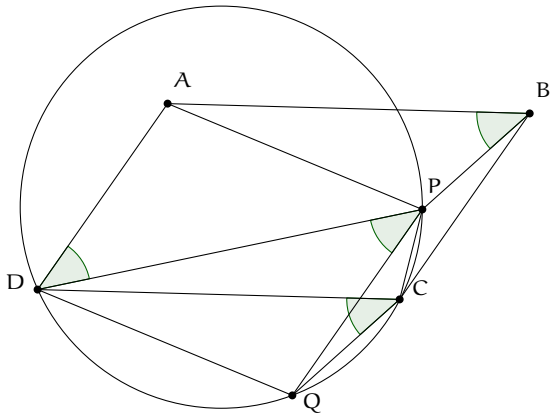
Solution de l'exercice 2 On note $d = a \wedge c$ et $D = a \wedge (bc)$. En outre, puisque $a \wedge b = 1$, le théorème de Bézout indique qu'il existe des entiers relatifs u et v tels que $au + bv = 1$.

Tout d'abord, par définition, d divise a et c : en particulier, d divise bc ; il s'ensuit que d divise D.

Réciproquement, D divise a et bc. D divise donc $a(cu) + (bc)v = c(au + bv) = c$. Puisque D divise a et c, il s'ensuit que D divise d.

d et D se divisent mutuellement et sont positifs ou nuls, donc $d = D$.

Solution de l'exercice 3



Soit Q le point tel que $APQD$ soit un parallélogramme. Alors, $\widehat{DQC} = \widehat{APB} = 180° - \widehat{CPD}$. Donc $PCQD$ sont cocycliques. Ainsi, $\widehat{ADP} = \widehat{QPD}$ (angles alternes-internes), puis $\widehat{QPD} = \widehat{QCD}$ (théorème de l'angle inscrit). Or, (AB) est parallèle à (DC), (PB) est parallèle à (QC), donc $\widehat{QCD} = \widehat{PBA}$. On a terminé.

Solution de l'exercice 4 p et q sont deux entiers premiers entre eux. D'après le théorème Chinois, pour toute paire d'entiers a et b tels que $0 \leqslant a < p$ et $0 \leqslant b < q$, il existe un unique entier k tel que $0 \leqslant k < pq$, $k \equiv a \pmod{p}$ et $k \equiv b \pmod{q}$.

Soit S_{pq} la somme $\sum_{n=0}^{pq-1} (-1)^{r_p(n)+r_q(n)}$. La remarque ci-dessus nous permet de réécrire S sous la forme

$$S_{pq} = \sum_{a=0}^{p-1}\sum_{b=0}^{q-1}(-1)^{a+b} = \sum_{a=0}^{p-1}\sum_{b=0}^{q-1}(-1)^a(-1)^b = \left(\sum_{a=0}^{p-1}(-1)^a\right)\left(\sum_{b=0}^{q-1}(-1)^b\right).$$

Or, en regroupant les termes de la somme $S_p = \sum_{a=0}^{p-1}(-1)^a$ deux par deux, on se rend compte que $S_p = 1$ si p est impair et $S_p = 0$ si p est pair. De même, la somme $S_q = \sum_{b=0}^{q-1}(-1)^b$ vaut $S_q = 1$ si q est impair et $S_q = 0$ si q est pair. Ainsi, $S_{pq} = S_pS_q$ vaut $S_{pq} = 1$ si pq est impair, et vaut $S_{pq} = 0$ si pq est pair.

3 Groupe C

1 Énoncés

Exercice 1 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y :

$$f(x - f(y)) = 1 - x - y.$$

Exercice 2 Soit n et k deux entiers naturels premiers entre eux, $1 \leqslant k \leqslant n-1$ et M l'ensemble $\{1, 2, \ldots, n-1\}$. On colorie les éléments de M de deux couleurs. On suppose que pour tout i dans M, i et $n - i$ ont la même couleur, et si $i \neq k$, i et $|i - k|$ ont la même couleur. Montrer que tous les éléments de M sont de la même couleur.

Exercice 3 Soit $n > 1$ un entier et $a_1, \cdots, a_n > 0$ des réels, on note s leur somme. Montrer :

$$\sum_{i=1}^{n} \frac{a_i}{s - a_i} \geqslant \frac{n}{n-1}.$$

Exercice 4 Soit $a < b < c < d$ des entiers naturels impairs tels que $ad = bc$, $a + d$ et $b + c$ sont des puissances de 2. Montrer que $a = 1$.

2 Solutions

Solution de l'exercice 1 Pour $y = 0$, on trouve et $x = z + f(0)$, on trouve $f(z) = f(x - f(y)) = 1 - x - y = 1 - z - f(0)$. En outre, si $z = 0$, alors $f(0) = 1 - f(0)$, donc $f(0) = \frac{1}{2}$. Réciproquement, la fonction

$$x \to \frac{1}{2} - x$$

est bien solution du problème.

Solution de l'exercice 2 On voit M comme étant $\mathbb{Z}/n\mathbb{Z} - \{0\}$. La première condition donne alors que, dans $\mathbb{Z}/n\mathbb{Z}$, i et $-i$ sont de la même couleur. On peut alors à partir de la seconde condition écrire que i et $i - k$ sont de la même couleur si aucun des deux n'est 0 (on peut enlever la valeur absolue car i et $-i$ sont de même couleur). Par une récurrence immédiate, on obtient que $k, 2k, \ldots, (n-1)k$ sont de la même couleur, aucun n'étant nul modulo n car k est inversible modulo n. De plus, ces éléments sont deux à deux distincts car si $ik \equiv jk[n]$, $i \equiv j[n]$ donc $i = j$ car $1 \leqslant i, j < n$. Ce sous-ensemble de M est donc de cardinal $n - 1$ donc égal à M, donc tous les éléments de M sont de la même couleur.

Solution de l'exercice 3 Première solution, avec Cauchy-Schwarz :

$$\sum_{i=1}^{n} a_i(s - a_i) \sum_{i=1}^{n} \left(\frac{a_i}{s - a_i} \right) \geqslant \left(\sum_{i=1}^{n} a_i \right)^2 \geqslant s^2$$

De plus, on a aussi $\left(\sum_{i=1}^{n} 1\right)\left(\sum_{i=1}^{n} a_i^2\right) \geqslant \left(\sum_{i=1}^{n} a_i\right)^2 \geqslant s^2$, d'où :

$$\sum_{i=1}^{n} a_i(s-a_i) = s^2 - \sum_{i=1}^{n} a_i^2 \leqslant s^2 - \frac{s^2}{n}$$

De là :

$$\sum_{i=1}^{n} \left(\frac{a_i}{s-a_i}\right) \geqslant \frac{s^2}{s^2 - \frac{s^2}{n}} \geqslant \frac{n}{n-1}$$

Seconde solution, avec Tchebycheff cette fois-ci : $a_1 \geqslant \cdots \geqslant a_n$ sans perte de généralité, donc $\frac{1}{s-a_1} \geqslant \cdots \geqslant \frac{1}{s-a_n}$. L'inégalité du cours donne, en notant S la somme de l'énoncé :

$$S \geqslant \sum_{i=1}^{n} \frac{a_{i+k}}{s-a_i}$$

pour $1 \leqslant k \leqslant n-1$ (en notant $a_q = a_p$ pour tous entiers p, q lorsque $n|p-q$). Or, pour tout i entre 1 et n, $s - a_i = \sum_{k=1}^{n-1} a_{i+k}$. En sommant les $n-1$ inégalités de Tchebycheff, on obtient :

$$(n-1)S \geqslant n,$$

ce qu'on voulait.

Solution de l'exercice 4 Le nerf de la guerre est de trouver des factorisations adéquates, pour avoir des relations de divisibilité.

On pose $a+d = 2^k$ et $b+c = 2^l$. On a alors $a(2^k-a) = b(2^l-b)$, identité dans laquelle on voit apparaître deux carrés. Il faut penser immédiatement à faire apparaître leur différence : $b^2 - a^2 = (b-a)(b+a) = 2^l b - 2^k a$. Pour factoriser les puissances de deux, il faut savoir laquelle est la plus grande. On sait qu'on doit trouver $k > l$ car si $a = 1$, $d = bc$ et $d+1$ est supérieur à $b+c$.

Pour le vérifier, on considère $2^k - 2^l$, et on fait apparaître le produit ad en multipliant par a : $a(2^k-2^l) = a(a+d-b-c) = ad - ba + a^2 - ac = bc - ba + a(a-c) = (b-a)(c-a) > 0$, d'où $k > l$.

On reprend l'équation précédente : $(b-a)(b+a) = 2^l(b-2^{k-l}a)$. En particulier, 2^l divise $(b-a)(b+a)$. Or, a et b étant impairs, l'un des deux facteurs est congru à 2 modulo 4, donc 2^{l-1} divise $b-a$ ou $b+a$. Ainsi, $2^{l-1} \leqslant b+a < b+c = 2^l$, donc 2^{l-1} est égal au facteur qu'il divise. En particulier, a et b sont premiers entre eux, car si p premier les divisait tous deux, il diviserait leur somme et leur différence donc 2^{l-1}, d'où $p = 2$, ce qui est impossible puisque a et b sont impairs.

On obtient de même que a et c sont premiers entre eux. Or, a divise bc. Donc $a = 1$.

4 Groupe D

1 Énoncés

Exercice 1 Les 62 stagiaires du stage Animath prennent chacun une boule de glace parmi 5 parfums proposés. On sait que
- la glace goût malabar a été au moins aussi populaire que la glace goût tabasco ;
- le nombre d'élèves qui ont choisi une glace au cactus est un multiple de 6 ;
- au plus 5 élèves ont dégusté une glace citron basilic ;
- au plus un élève a opté pour la glace au foie gras.

Lorsqu'Igor passe commande auprès du marchand de glaces, il lui communique, par ordre alphabétique des parfums, le nombre d'élèves ayant choisi chaque parfum. Combien de listes de nombres différentes a-t-il pu prononcer ?

Exercice 2

1. Soient $x_1, \dots, x_n$ et $y_1, \dots, y_1$ des réels strictement positifs tels que

$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i = 1.$$

Montrer que :

$$\sum_{i=1}^{n} x_i \ln \frac{x_i}{y_i} \geqslant 0,$$

et en déduire que :

$$-\sum_{i=1}^{n} x_i \ln x_i \leqslant \ln n.$$

2. Soient $x_1, \dots, x_n$ et $y_1, \dots, y_n$ des réels strictement positifs. On note x la somme des x_i et y celle des y_i. Montrer que :

$$\sum_{i=1}^{n} x_i \ln \frac{x_i}{y_i} \geqslant x \ln \frac{x}{y}.$$

Exercice 3 Montrer que pour tout entier positif n, on a l'égalité

$$\sum_{k=0}^{n} 2^k \binom{n}{k} \binom{n-k}{\lfloor \frac{n-k}{2} \rfloor} = \binom{2n+1}{n}.$$

Exercice 4 Soit $f : \mathbb{N} \longrightarrow \mathbb{Z}$ une fonction telle que
- Pour tous entiers $n > m \geqslant 0$, $n - m$ divise $f(n) - f(m)$.
- Il existe un polynôme P tel que pour tout $n \in \mathbb{N}$, $|f(n)| < P(n)$. Montrer qu'il existe un polynôme Q tel que $f(n) = Q(n)$ pour tout entier naturel n.

2 Solutions

Solution de l'exercice 1 Il s'agit de compter le nombre de manières d'écrire 62 sous la forme $r+t+6a+b+c$ où r, t, a, b, c sont des entiers naturels, $r \leqslant t$, $b \leqslant 5$ et $c \leqslant 1$. Puisqu'on veut $r \leqslant t$, on peut écrire $t = r + s$ avec $s \in \mathbb{N}$. Il suffit donc de compter le nombre de manières d'écrire 62 sous la forme $2r+s+6a+b+c$ avec r, s, a, b, c des entiers naturels, $b \leqslant 5$ et $c \leqslant 1$. Cela correspond au coefficient de degré 62 de la série génératrice

$$\left(\sum_{r\geqslant 0} x^{2r}\right)\left(\sum_{s\geqslant 0} x^{s}\right)\left(\sum_{a\geqslant 0} x^{6a}\right)(1+x+\ldots+x^5)(1+x).$$

En utilisant la forme close de la série géométrique, cette série se réécrit sous la forme

$$\frac{1}{1-x^2}\frac{1}{1-x}\frac{1}{1-x^6}\frac{1-x^6}{1-x}(1+x) = \frac{1}{(1-x)^3}.$$

Cette dernière fraction rationnelle est la dérivée de $\frac{1}{2}\frac{1}{(1-x)^2}$, donc son développement en série est $\sum_{n\geqslant 2}\frac{n(n-1)}{2}x^{n-2}$, obtenu en dérivant $\frac{1}{2}\sum_{n\geqslant 1} nx^{n-1}$. Par conséquent, le coefficient de degré 62 cherché est $\frac{64\times 63}{2} = 2016$.

Solution de l'exercice 2

1. $$\begin{aligned}\sum_{i=1}^{n} x_i \ln\frac{x_i}{y_i} &= -\sum_{i=1}^{n} x_i \ln\frac{y_i}{x_i}\\ &\geqslant -\ln\left(\sum_{i=1}^{n} x_i\frac{y_i}{x_i}\right) = -\ln 1 = 0,\end{aligned}$$

   où on a utilisé la concavité de ln. Voici une solution alternative :

   $$\begin{aligned}\sum_{i=1}^{n} x_i \ln\frac{x_i}{y_i} &= -\sum_{i=1}^{n} x_i \ln\frac{y_i}{x_i}\\ &\geqslant -\sum_{i=1}^{n} x_i\left(\frac{y_i}{x_i}-1\right) = -\sum_{i=1}^{n} y_i + \sum_{i=1}^{n} x_i\\ &= -1+1 = 0,\end{aligned}$$

   où on a utilisé l'inégalité $\ln x \leqslant x-1$ ($x > 0$). Pour la deuxième inégalité, l'égalité s'obtient lorsqu'on choisit $y_i = 1/n$, la somme des y_i étant alors bien égale à 1.
2. On pose $f(x) = x\ln x$ ($x > 0$). En dérivant deux fois, on voit que cette fonction est convexe. On écrit ensuite :

   $$\begin{aligned}\sum_{i=1}^{n} x_i \ln\frac{x_i}{y_i} &= \sum_{i=1}^{n} y_i f\left(\frac{x_i}{y_i}\right) = y\sum_{i=1}^{n}\frac{y_i}{y} f\left(\frac{x_i}{y_i}\right)\\ &\geqslant y f\left(\sum_{i=1}^{n}\frac{y_i}{y}\frac{x_i}{y_i}\right) = y f\left(\frac{1}{y}\sum_{i=1}^{n} x_i\right)\\ &= y f\left(\frac{x}{y}\right) = x\ln\frac{x}{y}.\end{aligned}$$

Solution de l'exercice 3 On procède par double-comptage en calculant de deux façons différentes le nombre de parties à n éléments d'un ensemble à $2n+1$ éléments. Ce nombre est égal à

$$\binom{2n+1}{n}$$

En observant le membre de gauche, on observe un un terme 2^k, qui correspond à k choix binaires, et un terme $\binom{n}{k}$, correspondant à un choix de k éléments. Cela conduit à procéder de la manière suivante.

Groupons nos $2n+1$ éléments en n paires, et mettons le dernier élément à part. Choisissons k de ces paires ($\binom{n}{k}$ choix). Le nombre k correspond au nombre de paires contenant exactement un élément de notre ensemble à n éléments : dans chacune de ces k paires, choisissons un des deux éléments (2^k choix). Nous avons sélectionné k éléments, il nous reste à en choisir $n-k$ pour aboutir à un ensemble à n éléments. Ces $n-k$ éléments doivent être regroupés dans $\lfloor (n-k)/2 \rfloor$ paires, et si $n-k$ est impair, pour compléter, on rajoute à notre ensemble l'élément n'appartenant à aucune paire. on voit immédiatement que l'on construit ainsi une fois chaque ensemble à n éléments et qu'il y a exactement

$$\sum_{k=0}^{n} 2^k \binom{n}{k} \binom{n-k}{\lfloor (n-l)/2 \rfloor}$$

façons de procéder ainsi. Cela conclut.

Solution de l'exercice 4 Soit d le degré du polynôme P. Par la formule d'interpolation de Lagrange, il existe un polynôme Q de degré $\leqslant d$ tel que $Q(i) = q_i$ pour $0 \leqslant i \leqslant d$. On veut montrer que pour tout entier naturel, $Q(n) = f(n)$, car si f est polynômiale, son degré est inférieur ou égal à d et le polynôme correspondant est solution du même problème d'interpolation que Q.

Quitte à multiplier Q et f par le dénominateur commun des coefficients de Q, on peut supposer que Q est à coefficients entiers, de manière à vérifier $n-m \mid Q(n)-Q(m)$. En particulier, en posant $g(n) = Q(n) - f(n)$, on a $n-m \mid g(n) - g(m)$, et il existe un polynôme R de degré $\leqslant d$ majorant $g(n)$ (tel que $|g(n)| \leqslant R(n)$) car c'est le cas pour Q et f. On s'est en fait ramené au cas de l'énoncé où les $d+1$ premières valeurs de la fonction sont nulles, et on souhaite montrer qu'alors la fonction est nulle.

On a pour $n > d$ et $0 \leqslant i \leqslant d$, $n-i \mid g(n) - g(i) = g(n)$ donc $g(n)$ est divisible par $\mathrm{ppcm}(n, n-1, \ldots, n-d)$. Pour n assez grand, $\mathrm{ppcm}(n, n-1, \ldots, n-d) > R(n)$, ce qui entraîne $g(n) = 0$.

En effet,

$$\mathrm{ppcm}(n, n-1, \ldots, n-d) \geqslant \frac{\prod_{0 \leqslant i \leqslant d} (n-i)}{\prod_{0 \leqslant i < j \leqslant d} \gcd(n-i, n-j)}$$

(regarder les décompositions en facteurs premiers, l'idée étant que la contribution de $n-i$ au ppcm provient des facteurs premiers « nouveaux » ou à une puissance plus élevée qu'il contient. On en déduit $\mathrm{ppcm}(n, n-1, \ldots, n-d) \geqslant \frac{\prod_{0 \leqslant i \leqslant d}(n-i)}{\prod_{0 \leqslant i < j \leqslant d}(j-i)}$ or $\prod_{0 \leqslant i \leqslant d}(X-i)$ est de degré $d+1$ d'où l'existence d'un entier N tel que pour tout $n > N$, $\mathrm{ppcm}(n, n-1, \ldots, n-d) > R(n)$ et donc $g(n) = 0$.

Il reste à vérifier $g(n) = 0$ pour $n \leqslant N$, or pour tout entier naturel $m > N$, $n - m \mid g(n) - g(m) = g(n)$ donc $g(n)$ est divisible par des entiers arbitrairement grands, donc $g(n) = 0$, ce qui conclut.

VIII. Dernière période

Le but des séances de la dernière période était de présenter de belles mathématiques, n'ayant pas forcément un rapport direct avec le programme des olympiades de mathématiques.

Voici le programme :

Contenu de cette partie

1 Groupe A

1 Théorie des graphes

Pour certaines définitions et certains résultats, ainsi qu'un cours plus complet sur les graphes, nous renvoyons vers l'excellent polycopié de P. Bornsztein.

- Notion de graphe -

Un *graphe* c'est
- des *sommets* ;
- des *arêtes* reliant des sommets.

Imaginons par exemple que les sommets du graphe représentent des personnes, et qu'il y a une arête entre deux personnes si ces dernières ont échangé une poignée de main. Nous allons travailler avec des graphes *simples*, c'est-à-dire tels que deux sommets ne sont jamais reliés par plus d'une arête, et *finis*, c'est-à-dire ayant un nombre fini de sommets et d'arêtes. Pour tout n, on note K_n le graphe *complet* à n sommets, c'est-à-dire le graphe à n sommets tel que chacun de ses sommets est relié à tous les autres.

Exercice 1 Dessiner les graphes K_1, K_2, K_3, K_4, K_5. Combien ont-ils de sommets ? D'arêtes ?

Exercice 2 Trois maisons doivent être reliées chacune à l'eau, au gaz, et à l'électricité. Dessiner un graphe pour illustrer une configuration possible. Pensez-vous qu'on puisse se débrouiller pour que les différentes conduites ne se croisent pas ?

Un *chemin* entre deux sommets A et B est une suite d'arêtes reliant A et B. Un graphe est dit *connexe* si deux sommets quelconques peuvent toujours être reliés par un chemin. Autrement dit, pour tous sommets A et B, une fourmi placée en A peut atteindre B en ne se promenant que suivant des arêtes du graphe. Un chemin qui parcourt au moins trois arêtes distinctes et qui revient sur lui-même s'appelle un *cycle*. Un *arbre* est un graphe connexe sans cycle.

Exercice 3 Dessiner quelques arbres. Combien d'arêtes au moins faut-il enlever au graphe K_4 pour qu'il devienne un arbre ?

- Degré d'un sommet, lemme des poignées de mains -

Le *degré* d'un sommet est le nombre d'arêtes partant de ce sommet. Si on fait la somme des degrés de tous les sommets, chaque arête compte double, vu qu'elle relie toujours deux sommets. Nous avons donc le résultat suivant :

Lemme 1.1. (Lemme des poignées de main) La somme des degrés de tous les sommets d'un graphe G est égale au double du nombre d'arêtes du graphe.

Exercice 4 Chaque stagiaire du stage d'Animath serre la main d'un certain nombre d'autres stagiaires. Montrer que le nombre de stagiaires ayant serré un nombre impair de mains est pair.

Exercice 5 Parmi les 30 élèves d'une classe, certains sont amis, et d'autres ne le sont pas. Montrer qu'il y a deux élèves ayant le même nombre d'amis.

- Graphes planaires -

Un graphe est dit *planaire* si on peut le dessiner sans que ses arêtes se coupent (ailleurs qu'en les sommets, bien évidemment). Une telle manière de le dessiner s'appelle une *représentation planaire*. On voit donc que la question posée dans l'exercice 2 revient à celle de savoir si le graphe intervenant dans l'exercice est planaire. Attention : ce n'est pas parce qu'une des représentations du graphe n'est pas planaire qu'il est impossible de le dessiner de manière planaire.

Soit un graphe planaire. Alors ses arêtes délimitent des régions du plan que nous appellerons *faces*.

Théorème 1.2. (Formule d'Euler, 1758) Soit G un graphe qui est simple, planaire et connexe. Supposons qu'une représentation planaire de G possède s sommets, a arêtes et f faces. Alors

$$s - a + f = 2.$$

Remarque 1.3. Attention, si le graphe est fini, l'une des faces du graphe est infinie !

Un peu d'histoire des mathématiques : Leonhard Euler (1707- 1783) était un grand mathématicien et physicien suisse. Il a fait de nombreuses découvertes dans à peu près tous les domaines des mathématiques de son temps, en particulier en théorie des graphes et en arithmétique. Bien qu'originaire de Bâle en Suisse, il a passé une grande partie de sa vie à Saint Petersbourg en Russie, où il a contribué à l'émergence de l'école mathématique russe, et à Berlin en Prusse. Malgré de grands problèmes de vue qui ont fini par évoluer vers une cécité quasi-totale, il a été extrêmement prolifique tout au long de sa vie, laissant derrière lui une œuvre mathématique colossale, qui a inspiré des générations de mathématiciens.

Revenons aux graphes. On sent bien que, si un graphe a trop d'arêtes par rapport à son nombre de sommets, on va avoir du mal à le dessiner sans que ses arêtes se croisent. Plus précisément, nous aurons :

Proposition 1.4. Soit G un graphe connexe simple planaire à s sommets et a arêtes. Alors

$$a \leqslant 3s - 6.$$

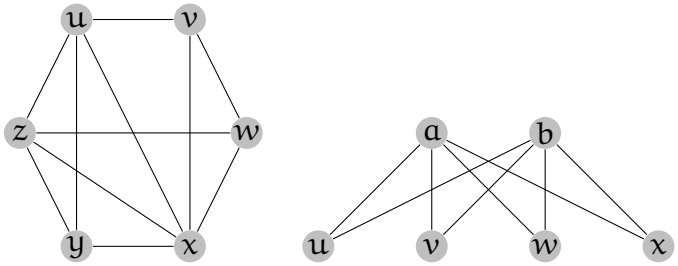
Démonstration. Puisque G est simple, chaque face utilise au moins trois arêtes. D'autre part, chaque arête appartient à deux faces. Donc nous avons que $3f \leqslant 2a$. En utilisant la formule d'Euler, on a $2 + a = s + f \leqslant s + \frac{2}{3}a$, d'où $a \leqslant 3s - 6$. □

Cette proposition nous fournit une manière de montrer qu'un graphe n'est pas planaire : s'il ne vérifie pas l'inégalité, il ne peut être planaire. Par contre, il faut faire attention au fait qu'un graphe peut très bien vérifier l'inégalité, et tout de même ne pas être planaire (autrement dit, la réciproque de ce résultat n'est pas vraie).

Exercice 6

1. Montrer que le graphe complet K_4 est planaire, et que le graphe complet K_5 ne l'est pas. Vérifier la formule d'Euler pour K_4.

2. Montrer que les graphes suivants



   sont planaires. Vérifier la formule d'Euler pour ces derniers.
3. Résoudre la deuxième question de l'exercice 2.

- Coloriages -

Un *coloriage* du graphe G est une manière d'attribuer une couleur à chacun de ses sommets. On dit qu'un coloriage est *propre* si deux sommets reliés par une arête ont des couleurs différentes.
Exercice 7 Montrer que tout graphe fini admet un coloriage propre.

Ainsi, on peut définir le *nombre chromatique* $\chi(G)$ d'un graphe fini G comme le plus petit nombre n tel que G puisse être colorié avec n couleurs.
Exercice 8 À quoi ressemble un graphe de nombre chromatique 1 ?

Exercice 9

1. Quel est le nombre chromatique du graphe complet K_4 ? Plus généralement, quel est le nombre chromatique du graphe complet K_n ?
2. Quel est le nombre chromatique d'un carré ? Proposer un coloriage optimal.
3. Déterminer les nombres chromatiques des arbres obtenus dans la solution de l'exercice 3.

Exercice 10

1. Soit G un graphe simple et planaire, ayant un nombre fini de sommets. Montrer que G possède au moins un sommet de degré ne dépassant pas 5.
2. Montrer le théorème des 6 couleurs : Tout graphe simple et planaire G ayant un nombre fini de sommets a un nombre chromatique inférieur ou égal à 6.

L'algorithme glouton Il existe beaucoup d'algorithmes pour trouver un coloriage propre d'un graphe fini. Nous allons présenter ici le plus connu, l'algorithme glouton (appelé ainsi probablement en référence au fait qu'il cherche toujours le sommet qui a le plus grand degré). Cet algorithme se déroule de la manière suivante.

1. On choisit un sommet non encore colorié de degré maximal et on le colorie d'une nouvelle couleur.

2. On colorie de cette même couleur, par ordre décroissant des degrés, tous les sommets non encore coloriés qui ne sont pas reliés à ce sommet, ni reliés entre eux. Plus précisément, on colorie un sommet de degré maximal non colorié et non relié au sommet colorié dans l'étape 1. Ensuite on colorie un sommet de degré maximal et non relié ni au sommet qu'on vient de colorier, ni au sommet colorié dans l'étape 1, et ainsi de suite.
3. S'il reste encore des sommets à colorier, on reprend à l'étape 1.

Cette procédure termine forcément puisque le nombre de sommets coloriés augmente au moins d'un à chaque fois.

Exercice 11 Montrer grâce à l'algorithme glouton que le nombre chromatique $\chi(G)$ d'un graphe fini G vérifie

$$\chi(G) \leqslant D(G) + 1,$$

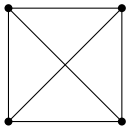
où $D(G)$ est le degré maximal d'un sommet de G.

Remarque 1.5. Il faut faire attention au fait que l'algorithme glouton ne permet pas nécessairement de calculer le nombre chromatique d'un graphe : il propose un certain coloriage propre, qui n'est pas nécessairement minimal.

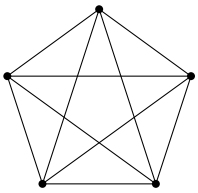
Exercice 12 A l'aide de l'algorithme glouton, proposer un coloriage du premier graphe intervenant dans l'exercice 6 (ou plutôt de sa version planaire, plus lisible, disponible dans la solution de ce dernier exercice). En déduire son nombre chromatique.

- Solutions des exercices -

Solution de l'exercice 1 Le graphe K_1 est simplement un point (un sommet, 0 arêtes), K_2 est un segment (2 sommets, 1 arête), K_3 est un triangle (3 sommets, 3 arêtes), K_4 est un carré dont on a dessiné également les diagonales :

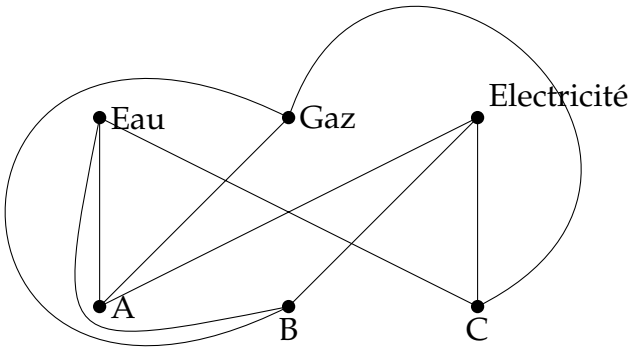


Il a donc 4 sommets et $\binom{4}{2} = 6$ arêtes. Le graphe K_5 est un pentagone dont on a dessiné toutes les diagonales :



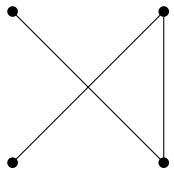
Il a 5 sommets et $\binom{5}{2} = \frac{5\times4}{2} = 10$ arêtes.

Solution de l'exercice 2 On peut par exemple dessiner les choses de la manière suivante :

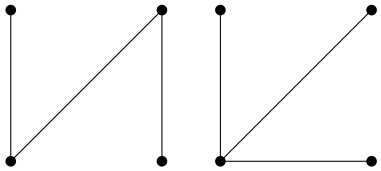


Pour la deuxième question, nous renvoyons vers le chapitre sur les graphes planaires.

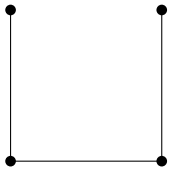
Solution de l'exercice 3 Il faut enlever au moins un côté car si on garde les quatre côtés, ça fait un cycle. Ensuite, si on garde les deux diagonales, il faut enlever encore deux côtés. En effet, si on garde deux côtés adjacents, ils vont former un triangle avec l'une des diagonales, ce qui donne un cycle. Si on garde deux côtés opposés, ils forment un cycle avec les deux diagonales. Dans ce cas, il faut donc enlever 3 arêtes au total pour obtenir un arbre. On obtient, à rotation près :



Si on enlève l'une des diagonales, mais qu'on garde trois côtés, on aura un triangle formé par la diagonale restante et deux des côtés restants. On doit donc enlever un des côtés, On obtient, à rotation près, l'un des dessins suivants :



Si on enlève les deux diagonales, on obtient, à rotation près :



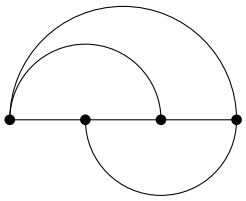
Ainsi, 3 est le nombre minimal d'arêtes qu'il faut enlever. Remarquons qu'à déformation près, on n'a obtenu que deux types d'arbres différents.

Solution de l'exercice 4 On considère un graphe dont les sommets sont les stagiaires, et où il y a une arête entre deux stagiaires s'ils se sont serré la main. Alors le degré d'un sommet correspond au nombre de mains que le stagiaire représenté par ce sommet a serrées. Soit p le nombre total de poignées de main (qui est aussi le nombre d'arêtes du graphe). Alors $2p$ est la somme de tous les degrés de tous les sommets. La somme des degrés des sommets de degré pair est paire. Donc la somme des degrés des sommets de degré impair est une différence de deux nombres pairs, et est par conséquent paire.

Solution de l'exercice 5 Chaque élève a un nombre d'amis compris entre 0 et 29. Si deux élèves n'ont jamais le même nombre d'amis, alors, forcément, pour tout i entre 0 et 29, il existe un élève qui a i amis. Autrement dit, un élève a 0 ami, un autre en a 1, un troisième en a 2, ..., et le dernier en a 29. Mais alors ce dernier est ami avec tout le monde, et en particulier, il est ami avec celui qui n'est ami avec personne, ce qui constitue une contradiction.

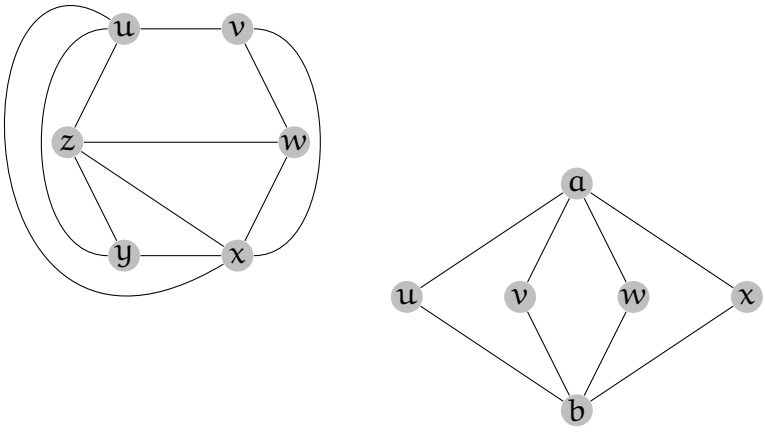
Solution de l'exercice 6

1. Une représentation planaire de K_4 est donnée par le dessin suivant :



   Il y a donc 4 sommets, 6 arêtes, et 4 faces (en comptant la face infinie) : on vérifie bien que $4-6+4=2$. Pour ce qui est de K_5, souvenons-nous qu'il a 5 sommets et 10 arêtes. Or $3\times5-6=9<10$, donc l'inégalité de la proposition 1.4 n'est pas satisfaite, et K_5 n'est pas planaire.

2. Voici des représentations planaires possibles :



   On vérifie en outre que le premier graphe a 6 sommets, 9 arêtes et 7 faces, et $6-9+7=2$. Le deuxième graphe a 6 sommets, 8 arêtes et 4 faces, et $6-8+4=2$.

3. Nous avons $s=6$ et $a=9$, donc d'après la formule d'Euler, si le graphe considéré était planaire, on devrait avoir $f=2+a-s=5$. D'autre part, aucune des faces n'est un

triangle. En effet, si on prend trois sommets du graphe, deux d'entre eux sont nécessairement soit des maisons, soit des usines, et ne sont donc pas reliés. Ainsi, chaque face (et la face infinie également) est délimitée par au moins quatre arêtes. Puisque chaque arête appartient à deux faces, on a $4f \leqslant 2a$, d'où $f \leqslant \frac{9}{2} < 5$, contradiction. Les différentes conduites se croiseront donc nécessairement.

Solution de l'exercice 7 Il suffit de colorier tous les sommets avec des couleurs différentes.

Solution de l'exercice 8 Soit un graphe de nombre chromatique 1. Alors on obtient un coloriage propre en coloriant tous ses sommets avec la même couleur. Mais alors on ne peut avoir aucune arête dans le graphe, puisque deux points reliés par une arête doivent être de couleurs différentes. Ainsi, le graphe en question est juste une collection de points.

Solution de l'exercice 9

1. Le graphe K_4 est complet, c'est-à-dire que chaque sommet est relié à tous les autres. Ainsi, tous les sommets doivent être de couleurs différentes, donc le nombre chromatique de K_4 est 4. De même, celui de K_n est n.
2. Il faut au moins deux couleurs. D'autre part, en coloriant deux sommets opposés en jaune, et les deux autres en rouge, on obtient un coloriage propre. Donc le nombre chromatique d'un carré est 2.
3. Trois des arbres obtenus dans l'exercice 3 peuvent aussi être dessinés sous la forme

Ce dernier peut être colorié à l'aide de deux couleurs, donc son nombre chromatique est 2. De même, l'autre arbre obtenu peut être colorié à l'aide de deux couleurs, donc son nombre chromatique est 2.

Solution de l'exercice 10

1. Supposons que le degré de chaque sommet est supérieur à 6. De chaque sommet partent au moins 6 arêtes, et chaque arête relie deux sommets, donc nous avons $6s \leqslant 2a$, c'est-à-dire $3s \leqslant a$. Or nous savons que $a \leqslant 3s - 6$, contradiction. Donc il existe un sommet de degré au plus égal à 5.
2. Nous allons raisonner par récurrence sur n. Pour $n = 1$, c'est clair. Supposons que c'est vrai pour $n - 1$. Soit un graphe à n sommets, simple et planaire. D'après la première question, il existe un sommet M de degré plus petit que 5. Si on l'enlève, lui ainsi que les arêtes qui partent de lui, on obtient un graphe à $n-1$ sommets que l'on peut colorier avec 6 couleurs. Si on remet M où il était, il n'est relié qu'au plus à 5 autres sommets, donc il y a au moins une couleur parmi les 6 couleurs utilisées avec laquelle nous pouvons le colorier.

Solution de l'exercice 11 Soit M le dernier sommet colorié. Si M n'a pas été colorié avant, c'est qu'à chaque étape, l'un de ses voisins a été colorié. Ainsi, le nombre de couleurs utilisées avant de colorier M ne peut dépasser le degré $d(M)$ de M. Le nombre total des couleurs utilisées (en tenant compte de la couleur de M) ne peut donc pas dépasser $d(M) + 1$. On a donc par définition du nombre chromatique

$$\chi(G) \leqslant \text{ nombre total de couleurs utilisées } \leqslant d(M) + 1 \leqslant D(G) + 1.$$

Solution de l'exercice 12 Le sommet x est de degré maximal 5, on commence donc par le colorier, par exemple en jaune. Le seul sommet auquel il n'est pas relié est u, donc nous pouvons colorier ce dernier en jaune aussi. Ensuite, on recommence le processus : z est de degré maximal 4, donc on le colorie par exemple en bleu. Il est relié à tous les sommets non encore coloriés sauf v, donc on colorie v en bleu également. Ensuite, y est de degré maximal 3, donc on le colorie par exemple en rouge. Il reste à colorier w en rouge. On a donc un coloriage avec trois couleurs. D'autre part, on ne peut espérer avoir un coloriage avec seulement deux couleurs, vu que le graphe contient un triangle (par exemple le triangle xyz), autrement dit un graphe complet à 3 sommets, qui ne peut être colorié qu'avec 3 couleurs. Le nombre chromatique cherché est donc égal à 3.

2 Combinatoire

- Combinatoire : bijections et double-comptage -

Exercice 1 Démontrer par un double-comptage les identités suivantes :

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n} = 2^n$$

Solution de l'exercice 1 $\binom{n}{k}$ est le nombre de sous-ensembles de $[\![1, n]\!]$ de cardinal k, donc la somme est le nombre de sous-ensembles de $[\![1, n]\!]$ de cardinal compris entre 0 et n, c'est-à-dire le nombre total de sous-ensembles.
Pour choisir un sous-ensemble, il suffit de choisir si on prend 1, puis si on prend 2 etc..., donc le nombre de sous-ensembles de $[\![1, n]\!]$ vaut aussi 2.

Exercice 2 Par un double comptage, calculer la somme :

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + ... + n\binom{n}{n}$$

Solution de l'exercice 2 $k\binom{n}{k}$ est le nombre de manières de choisir $A \subset [\![1, n]\!]$ de cardinal k et $x \in A$, donc la somme est égale au nombre de couples (x, A) avec $x \in A \subset [\![1, n]\!]$.
D'autre part, pour choisir un tel couple, on peut d'abord choisir x (il y a n choix possibles), puis A (pour chaque choix de x, il y a 2^{n-1} sous-ensembles de A possibles). La somme vaut donc $n2^{n-1}$.

Exercice 3 n personnes sont autour d'une table et, pour tout k, on note p_k le nombre de manières de changer ces personnes de place où exactement k personnes restent à leur place.
Montrer que $p_1 + 2p_2 + 3p_3 + ... + np_n = n!$.

Solution de l'exercice 3 On utilise la même technique que ci-dessus : kp_k est le nombre de manière de choisir une personne x et une permutation σ telle que k personnes dont x restent à leur place, donc la somme est égale au nombre de manière de choisir x et σ telle que x reste à sa place.
Or, il y a n manières de choisir x puis, ensuite, il reste à choisir une permutation des $n-1$ personnes restantes. Il y a $(n-1)!$ manières de le faire, soit $n!$ au total.

Exercice 4 Montrer par des bijections les identités suivantes :

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - ... + (-1)^n \binom{n}{n} = 0$$

et :

$$\binom{n}{k} = \binom{n}{n-k}$$

Solution de l'exercice 4 On veut que les nombres soient les cardinaux d'ensembles, donc soient positifs. On passe donc les termes négatifs de l'autre côté, et on veut montrer qu'il y a autant de sous-ensembles de $[\![1, n]\!]$ de cardinal pair que de cardinal impair.
Pour cela, on considère la fonction qui à A associe A privé de 1 si $1 \in A$, et A avec 1 en plus si $1 \notin A$. On vérifie que cette fonction est une bijection entre les sous-ensembles de cardinal pair et ceux de cardinal impair.
Pour la deuxième, on montre que la fonction qui à un sous-ensemble associe son complémentaire est une bijection.

Exercice 5 On considère un grand rectangle de taille m sur n, découpé en petits carrés de côté 1.
Combien y a-t-il de manières d'aller du coin inférieur gauche au coin supérieur droit en se déplaçant uniquement sur le quadrillage, et seulement vers le haut ou la droite ?

Solution de l'exercice 5 Il faut faire m pas vers la droite et n pas vers la droite, soit un total de $m+n$ pas, qu'on peut numéroter de 1 à $m+n$ en suivant le chemin. On considère la fonction qui à un chemin associe l'ensemble des numéros des pas vers la droite : c'est un sous-ensemble de $[\![1, m+n]\!]$ de cardinal n, donc le nombre de chemins vaut $\binom{m+n}{n}$.

Exercice 6 On considère cette fois un grand carré de côté n découpé en petits carrés de côté 1. Combien y a-t-il de manières d'aller du coin inférieur gauche au coin supérieur droit en restant au-dessus de la diagonale principale ?

Solution de l'exercice 6 Astuce : plutôt que de compter les chemins qui marchent, on va compter ceux qui ne marchent pas : un mauvais chemin passe forcément par la droite (d) juste en-dessous de la diagonale principale. On peut regarder ce qu'il se passe si on réfléchit par rapport à (d) la partie du chemin avant de rencontrer (d) pour la première fois : si on choisit le coin en bas à gauche comme origine, on obtient un chemin du point de coordonnées $(1, 0)$ vers le coin supérieur droit. C'est une bijection, donc il y a $\binom{2n}{n+1}$ mauvais chemins, et un peu de calcul montre qu'il y en a $\frac{1}{n+1}\binom{2n}{n}$ bons.

Remarque 1.6. Les nombres obtenus (les $\frac{1}{n+1}\binom{2n}{n}$) sont appelés nombres de Catalan, et permettent de compter des objets combinatoires très variés, à l'aide de bijections avec les chemins de l'exercice. Voici quelques exemples :

- Les parenthésages corrects, i.e les manières de placer n parenthèses ouvrantes et n fermantes de manière à n'avoir jamais plus de parenthèses fermantes qu'ouvrantes. Par exemple, (()()) marche mais pas ())((.
- Les manières de relier deux à deux par des segments $2n$ points d'un cercle sans que deux segments se coupent.
- Les manières d'aller d'un point à lui-même en restant sur une demi-droite issue de ce point et en faisant $2n$ pas de 1 mètre vers la droite ou vers la gauche.
- Les arbres généalogiques à n sommets décrivant la descendance d'une personne.

2 Groupe B

1 Fonctions

La notion de fonction est relativement récente en mathématiques, puisqu'elle est due à Leonhard Euler (1707 - 1783). La plupart des théorèmes que vous étudierez au lycée sont antérieurs, y compris ceux utilisés pour l'étude des variations d'une fonction, comme le théorème de Rolle. Car avant Euler, on savait étudier comment une "quantité" variait en fonction d'une autre quantité.

L'idée originale d'Euler est d'introduire un objet mathématique "fonction" qui associe une valeur à une variable. C'est une notion très générale : la variable et la valeur associée ne sont pas obligatoirement des nombres. Et les fonctions ainsi définies n'ont pas de propriétés a priori, c'est l'hypothèse qui permet de leur définir des propriétés en rapport avec le problème posé. La plupart des fonctions que vous manipulerez sont des "bonnes fonctions", comme les fonctions polynômes ou la fonction exponentielle par exemple. Mais quand vous devrez résoudre un problème très général sur les fonctions, par exemple une équation fonctionnelle (environ 10% des problèmes d'Olympiades sont des équations fonctionnelles), même si, en définitive, la solution est une fonction très élémentaire, vous ne pourrez pas utiliser, dans la démonstration, le présupposé que vous cherchez une "bonne fonction".

Exercice 1

Soit $E = \{a, b, c, d\}$ un ensemble. Combien existe-t-il de fonctions f de E dans E vérifiant, pour tout x appartenant à E, $f(f(f(x))) = x$?

Solution de l'exercice 1

L'identité, définie pour tout x par $f(x) = x$, est évidemment solution. Si l'un des éléments a une image distincte de lui-même, par exemple $f(x) = y$, à quoi peut être égal $f(y)$? Si l'on avait $f(y) = x$, on aurait : $f(f(f(x))) = f(f(y)) = f(x) = y$, la relation de l'hypothèse ne serait pas vérifiée. De même si l'on avait $f(y) = y$. Il en résulte que $f(y) = z$ distinct de x et y, et $f(z) = f(f(f(x))) = x$. La fonction permute circulairement trois des éléments x, y, z de l'ensemble, et laisse invariant le dernier t. En effet, si l'on avait $f(t) \in \{x, y, z\}$, on aurait également $f(f(f(t))) \in \{x, y, z\}$ ce qui contredirait $f(f(f(t))) = t$. Pour définir une de ces fonctions, il suffit de déterminer son "point fixe" (élément t tel que $f(t) = t$, puis le sens de la permutation circulaire des trois autres éléments, ce qui donne $4 \times 2 = 8$ fonctions, plus l'identité, soit 9 en tout.

Exercice 2

Existe-t-il une fonction f de $\mathbb{N}$ dans $\mathbb{N}$ telle que, pour tout entier naturel n, $f(f(n)) = n + 1$?

Solution de l'exercice 2

Etudions quelques valeurs de la fonction, en appelant a la valeur de $f(0)$: $f(a) = f(f(0)) = 1$ par hypothèse, $f(1) = f(f(a)) = a + 1$, et ainsi de suite.

x	0	a	1	$a+1$	2	$a+2$	3	$a+3$	$\ldots$
$f(x)$	a	1	$a+1$	2	$a+2$	3	$a+3$	4	$\ldots$

On remarque dans ce tableau que pour tout $n \geqslant 0$, $f(n) = n + a$. Démontrons-le par récurrence. C'est vrai pour $n = 0$ (initialisation), et si c'est vrai pour n, $f(n + a) = f(f(n)) = n + 1$, $f(n + 1) = f(f(n + a)) = n + a + 1$, ce qui prouve que la relation est encore vraie pour $n + 1$, elle est donc vraie pour tout $n \in \mathbb{N}$. Elle est en particulier vraie pour $n = a$: $f(a) = 2a$.

Mais par ailleurs, on sait que $f(a) = 1$. On doit donc avoir : $2a = 1$, ce qui est impossible vu que a est entier. Donc une telle fonction n'existe pas.

A propos de deux fonctions particulières : partie entière et valeur absolue

On notera $[x]$ la partie entière du réel x, c'est-à-dire le plus grand entier inférieur ou égal à x.

Exercice 3

a) Montrer que pour tout entier $n \geqslant 0$, $[\sqrt{n} + \sqrt{n+2}] = [\sqrt{4n+1}]$

b) Trouver un réel x tel que $[\sqrt{x} + \sqrt{x+2}] \neq [\sqrt{4x+1}]$

Solution de l'exercice 3

a) $[\sqrt{4n+1}]$ est le plus grand entier i dont le carré soit inférieur ou égal à $4n+1$, et $\left[\sqrt{n} + \sqrt{n+2}\right]$ le plus grand entier j inférieur ou égal à $\sqrt{n}+\sqrt{n+2}$. j^2 est donc le plus grand carré parfait inférieur ou égal à $\left(\sqrt{n} + \sqrt{n+2}\right)^2 = n + (n+2) + 2\sqrt{n(n+2)}$. Or $(n+1)^2 = n^2+2n+1 > n(n+2)$, donc $n < \sqrt{n(n+2)} < n+1$, et $4n+2 < \left(\sqrt{n} + \sqrt{n+2}\right)^2 < 4n+4$. Le plus grand entier inférieur ou égal à $\left(\sqrt{n} + \sqrt{n+2}\right)^2$ peut être soit $4n+2$, soit $4n+3$, mais le plus grand carré parfait ? On utilise un résultat d'arithmétique, à savoir que ni $4n+2$ ni $4n+3$ ne peuvent être des carrés parfaits, donc le plus grand carré parfait inférieur ou égal à $4n+3$ est inférieur ou égal à $4n+1$: c'est i^2 d'après sa définition ci-dessus. En d'autres termes, on a bien $i = j$, c'était la relation à démontrer.

b) Nous avons utilisé des propriétés arithmétiques des carrés parfaits. Dès lors qu'on choisit x parmi les réels, nous n'avons plus le même résultat. Par exemple pour $x = \frac{1}{4}$, $[\sqrt{x} + \sqrt{x+2}] = 2$ alors que $[\sqrt{4n+1}] = 1$.

Exercice 4

Montrer que pour tout réel x et tout entier $p \geqslant 2$, $\sum_{k=0}^{p-1} \left[\frac{x+k}{p}\right] = [x]$

Solution de l'exercice 4

Posons $[x] = pn + r$, avec $0 \leqslant r < p$. Cela signifie que $pn + r \leqslant x < pn + r + 1$. Donc si $k \leqslant p - (r+1)$, $n \leqslant \frac{x+k}{n} < n+1$, d'où $[\frac{x+k}{n}] = n$, alors que si $k \geqslant p - r$, $[\frac{x+k}{n}] = n+1$. Les termes de la somme prendront donc $(p-r)$ fois la valeur n et r fois la valeur $n+1$, donc la somme vaudra bien $pn + r = [x]$.

Exercice 5

On considère une fonction f de $\mathbb{Z}$ dans $\mathbb{R}$ vérifiant, pour tout entier n,

$$f(n+1) = |f(n)| - f(n-1)$$

a) On suppose $f(1) = 3$ et $f(2) = 2$. Calculer $f(12)$ et $f(0)$.

b) Montrer que pour tout entier n, l'une au moins des trois valeurs $f(n)$, $f(n+1)$, $f(n+2)$ est positive ou nulle.

c) Montrer que pour tout entier n, l'une au moins des quatre valeurs $f(n)$, $f(n+1)$, $f(n+2)$, $f(n+3)$ est négative ou nulle.

d) Montrer qu'il existe un entier k tel que : $0 \leqslant k \leqslant 4$, $f(k) \leqslant 0$ et $f(k+1) \geqslant 0$.

e) On suppose que $f(0) = -a \leqslant 0$ et $f(1) = b \geqslant 0$. Calculer $f(9)$ et $f(10)$.

f) Montrer que pour tout entier n, $f(n+9) = f(n)$

Solution de l'exercice 5

a) Si $f(1) = 3, f(2) = 2, f(3) = -1, f(4) = -1, f(5) = 2, f(6) = 3, f(7) = 1, f(8) = -2, f(9) = 1, f(10) = 3, f(11) = 2, f(12) = -1 \cdots$. Par ailleurs, la relation de l'hypothèse peut s'écrire : $f(n-1) = |f(n)| - f(n+1)$ donc $f(0) = 1$: à partir de deux valeurs consécutives de f, on peut calculer toutes les autres valeurs, dans un sens et dans l'autre. On remarque que $f(0) = f(9), f(1) = f(10), f(2) = f(11)$ et $f(3) = f(12)$: le but du problème est précisément de généraliser ce résultat.

b) D'après l'hypothèse, pour tout n : $f(n+2) + f(n) = |f(n+1)| \geqslant 0$, donc l'une au moins des valeurs $f(n+2)$ ou $f(n)$ est positive ou nulle.

Notons que, la fonction identiquement nulle vérifiant les conditions de l'énoncé, il ne sera jamais possible, dans tout ce problème, de remplacer "positive ou nulle" par "strictement positive" ni "négative ou nulle" par "strictement négative".

c) Non seulement $f(n+2) + f(n) = |f(n+1)|$, mais $f(n+3) + f(n+1) = |f(n+2)|$, donc : $f(n) + f(n+1) + f(n+2) + f(n+3) = |f(n+1)| + |f(n+2)|$. Si $f(n+1)$ et $f(n+2)$ sont tous deux positifs, on en déduit : $f(n) + f(n+3) = 0$, donc l'une des deux valeurs $f(n)$ ou $f(n+3)$ est négative ou nulle.

d) Parmi les quatre valeurs $f(0), f(1), f(2), f(3)$, on vient de voir que l'une au moins, $f(i)$, est négative ou nulle. $f(i+2) = |f(i+1)| - f(i) \geqslant 0$. Dès lors, de deux choses l'une : soit $f(i+1) \geqslant 0$ et $k = i$ répond à la question. Soit $f(i+1) < 0$ et $k = i+1$ répond à la question.

e) Si $f(0) = -a \leqslant 0$ et $f(1) = b \geqslant 0$, $f(2) = b + a \geqslant 0$, $f(3) = a \geqslant 0$, $f(4) = -b \leqslant 0$, $f(5) = b - a$, dont on ne connaît pas le signe, $f(6) = |b-a| + b \geqslant 0$, $f(7) = |b-a| + a \geqslant 0$, $f(8) = a - b$, dont on ne connaît pas le signe (mais on remarque, conformément à la question c, que $f(8) = -f(5)$). $f(9) = -a = f(0) \leqslant 0$ et $f(10) = b = f(1) \geqslant 0$.

f) D'après la question d, quelle que soit la fonction f vérifiant la condition de l'énoncé, il existe k compris entre 0 et 4 tel que $f(k) = -a \leqslant 0$ et $f(k+1) = b \geqslant 0$. D'après la question e, on aura donc $f(k+9) = -a = f(k)$ et $f(k+10) = b = f(1)$. Mais on a vu à l'occasion de la question a que deux valeurs consécutives de la fonction suffisent à définir toutes les autres, tant dans un sens que dans l'autre. Donc la relation $f(n+9) = f(n)$ se prolonge à toutes les valeurs de n, $f(n)$ étant d'ailleurs explicitement calculé dans la question e. Notre fonction f est périodique de période 9.

Ce problème m'a été proposé par Gilbert Rebel en 1997, sous le nom "Rêve d'absolus". Cela ne fait-il pas rêver d'écrire, en calculant explicitement $f(10)$ à partir de $f(0) = b$ et $f(1) = a$:

"Quels que soient les réels a et b, $|||||||||a| - b| - a| - |a| + b| - ||a| - b| + a| - |||a| - b| - a| + |a| - b| - ||||a| - b| - a| - |a| + b| + ||a| - b| - a| - |||||a| - b| - a| - |a| + b| - ||a| - b| + a| + |||a| - b| - a| - |a| + b| - ||||||a| - b| - a| - |a| + b| - ||a| - b| + a| - |||a| - b| - a| + |a| - b| + ||||a| - b| - a| - |a| + b| - ||a| - b| + a| - |||||||a| - b| - a| - |a| + b| - ||a| - b| + a| - |||a| - b| - a| + |a| - b| - ||||a| - b| - a| - |a| + b| + ||a| - b| - a| + |||||a| - b| - a| - |a| + b| - ||a| - b| + a| - |||a| - b| - a| + |a| - b = a|$" ?

Ce même problème a été posé peu après au Concours Général (destiné aux meilleurs élèves de terminale).

2 Théorie des graphes

Voir le cours de théorie des graphes page 350.

3 Groupe C

1 Compter l'infini

Le but de cette séance d'ouverture est d'essayer de compter jusqu'à l'infini, en vous introduisant à la théorie des cardinaux, une des révolutions majeures de l'histoire des mathématiques, développée par Cantor autour de la fin du 19° siècle. Nous donnerons, quand c'est possible, les définitions précises de ces quantités infinies, puis nous essaierons de les comparer, et de dénombrer certains ensembles infinis usuels.

- Cardinaux : définitions -

On commence par un rappel :

Définition 3.1. Une application $f : E \longrightarrow F$ est dite
- *injective* si deux éléments distincts de E ont des images distinctes par F (i.e. f "sépare" les éléments de E)
- *surjective* si tout élément de F a un antécédent par f (i.e. f "recouvre" F tout entier)
- *bijective* si elle est injective et surjective (i.e. f "couple" les éléments de E avec ceux de F).

J'ai 7 poules. Que se passe-t-il quand je compte mes poules ? Je choisis une poule, je décrète que c'est la poule numéro 1, puis je prends une autre poule, qui sera la poule numéro 2, et ainsi de suite jusqu'à 7. Implicitement, j'ai donc construit une bijection entre mon ensemble de poules et l'ensemble $\{1, \dots, 7\}$. D'où la définition :

Définition 3.2. Soit n un entier non nul. On dit qu'un ensemble E a n éléments s'il est en bijection avec $\{1, \dots, n\}$. On dit alors que le cardinal de E est n, et on note cela $|E| = n$. (On dit qu'un ensemble est de cardinal 0 s'il est en bijection avec l'ensemble vide, c'est-à-dire s'il est vide).

L'avantage de ce point de vue est qu'il s'étend sans efforts aux ensembles infinis ! Ainsi :

Définition 3.3. Soient E et F deux ensembles (potentiellement infinis).
- Si E et F sont en bijection, on dit qu'ils ont même *cardinal*, on note cela $|E| = |F|$.
- S'il existe une injection de E dans F, on dit que le cardinal de E est plus petit que celui de F, on note cela $|E| \leqslant |F|$.
- S'il existe une surjection de E vers F, on dit que le cardinal de E est plus grand que celui de F, on note cela $|E| \geqslant |F|$.

La notation $\leqslant$ n'est pas innocente, et on voit d'ailleurs que cette relation vérifie plusieurs des propriétés naturelles d'une relation de comparaison, par exemple $|E| \leqslant |F|, |F| \leqslant |G| \Rightarrow |E| \leqslant |G|$ en composant les injections. Le théorème suivant regroupe plusieurs résultats montrant que notre relation vérifie toutes les propriétés naturelles d'une relation de comparaison, et on peut donc la manipuler comme un ordre classique.

Théorème 3.4. Soient E et F deux ensembles (potentiellement infinis).
- S'il existe une injection de E dans F, et une injection de F dans E, alors E et F sont en bijection, autrement dit : $|E| \leqslant |F|, |F| \leqslant |E| \Rightarrow |E| = |F|$.

- Il existe une injection de E dans F si et seulement s'il existe une surjection de F dans E, autrement dit : $|E| \leqslant |F| \Leftrightarrow |F| \geqslant |E|$.
- Il existe toujours soit une injection de E dans F, soit une injection de F dans E, autrement dit : $|E| \leqslant |F|$ ou $|F| \leqslant |E|$.

Démonstration. Je vais juste prouver la première propriété, connue sous le nom de théorème de Cantor-Bernstein. Cette preuve est un peu technique et peut tout à fait être sautée. On cherche à construire une bijection φ de E dans F. Soit f l'injection de E dans F et g celle de F dans E. Une idée est de partir de f. On décrète que φ vaut f sur E. Il existe alors des points de B non atteints par φ : les points y hors de $f(E)$, pour eux on a envie de se servir de g, par exemple dire que, $\varphi(g(y)) = y$. Le problème, c'est qu'après cette modification le point $f(g(y))$ n'est plus atteint par φ, il faudrait donc trouver un moyen de répéter à volonté le processus.

Une façon de faire cela proprement est d'introduire des « chaînes ». Soit x dans E, on définit la chaîne de x comme étant la suite (x_n) définie par récurrence par $x_{2k+1} = f(x_{2k})$ et $x_{2k} = g(x_{2k-1})$. Si cette suite revient sur x, on dit que la chaîne de x est une boucle. Si ce n'est pas une boucle, on l'étend le plus possible sur les entiers négatifs : si x a un antécédent y par g, il n'en a qu'un, et on pose $x_{-1} = y$. Puis on cherche un antécédent de x_{-1} par f, et ainsi de suite. Si ce processus bloque au bout d'un moment (si on tombe sur un élément n'ayant pas d'antécédent), on dit que la chaîne a une origine, sinon on dit qu'elle est infinie.

On va définir φ directement sur les chaînes : si la chaîne de x est une boucle ou est infinie, on prend pour $\varphi(x)$ l'élément suivant x dans la chaîne (c'est-à-dire $f(x)$). Si la chaîne a une origine et que cette origine est dans E, on prend pour $\varphi(x)$ l'élément suivant x dans la chaîne, mais si l'origine de la chaîne est dans F, on prend pour $\varphi(x)$ l'élément précédent x dans la chaîne (si on ne faisait pas cela, l'origine de la chaîne n'aurait pas d'antécedent par φ). On vérifie qu'une telle définition fonctionne. □

Les deux propriétés qui restent sont plus méchantes car elles nécessitent de faire appel à l'axiome du choix.

- Petite digression : l'axiome du choix -

Les axiomes sont le point de départ de toute théorie mathématique : ce sont des propriétés basiques et naturelles que l'on admet et dont on se sert ensuite pour déduire toute la théorie. Un exemple célèbre est l'axiome des parallèles de la géométrie euclidienne : par tout point passe une unique parallèle à une droite donnée. Quand on fait de la théorie des ensembles, et que l'on dispose d'un ensemble non vide E, on a bien sûr le droit de se fixer un élément $x \in E$, puis de travailler dessus. L'axiome du choix affirme que l'on peut faire une infinité de tels choix simultanément :

Axiome 2. Soit $(E_i)_{i \in I}$ une famille d'ensembles. Alors il existe une fonction f, appelée fonction de choix, associant à chaque i un élément de E_i.

Cela paraît totalement évident, à tel point que les mathématiciens ont mis longtemps à se rendre compte que cette propriété était indépendante de tous les axiomes usuels de la théorie des ensembles, et méritait donc d'être érigée en axiome. Pourtant, quand on y réfléchit, la situation est loin d'être aussi claire.

Supposons que les E_i soient des parties de $\mathbb{N}$. Dans ce cas, nul besoin de faire appel à l'axiome du choix : on peut définir une fonction de choix explicite, par exemple la fonction "plus petit élément". Ainsi, dans ce cas, l'axiome du choix se déduit des axiomes de base.

La situation se complique quand on travaille avec des ensembles plus compliqués, comme par exemple celui des réels. Supposez que les E_i soient biscornus, et essayez de trouver une fonction de choix universelle, "canonique". Celle utilisée pour les entiers, "plus petit élément", ne marche plus, un E_i n'ayant pas forcément de plus petit élément ! On se convainc rapidement qu'un choix "canonique" est impossible. Obtenir une fonction de choix nécessite alors de faire une infinité de choix totalement arbitraires, une chose qu'il n'est pas possible de faire avec les autres axiomes. Faire appel à l'axiome du choix, en quelque sorte, c'est introduire une grande quantité d'arbitraire dans les mathématiques.

Du coup, l'axiome du choix a un statut un peu à part parmi les autres axiomes. Quand on l'utilise, on se retrouve avec des objets vraiment moches, non explicites, et donc non manipulables par un ordinateur. Un exemple d'objet ainsi construit est une solution non continue de l'équation de Cauchy $f(x+y) = f(x)+f(y)$. Les mathématiciens modernes utilisent régulièrement l'axiome du choix, notamment en analyse, ou comme ici en théorie des ensembles, mais essayent dès que possible de s'en passer, afin que les mathématiques restent accessibles d'un point de vue algorithmique.

- Ensembles dénombrables -

Un ensemble ayant un cardinal entier est appelé un ensemble fini. Cette section est consacrée à l'étude de ce qu'il se passe juste après les cardinaux entiers. On montre en effet que :

Définition 3.5. Le cardinal de $\mathbb{N}$ est le plus petit cardinal infini. Un ensemble ayant même cardinal que $\mathbb{N}$ (i.e. en bijection avec $\mathbb{N}$, i.e. dont on peut énumerer les éléments) est appelé un ensemble *dénombrable*.

Démonstration. Soit E un ensemble infini. Il s'agit de montrer que $\mathbb{N}$ s'injecte dans E. Soit x_1 un élément de E. Comme E est infini, $E\backslash\{x_1\}$ est non vide : soit x_2 dans $E\backslash\{x_1\}$. On repète le procédé : supposons $\{x_1, \dots, x_n\}$ construits, alors on prend pour x_{n+1} un élément de l'ensemble non vide $E\backslash\{x_1, \dots, x_n\}$. L'application $i \mapsto x_i$ est alors l'injection recherchée.

Il y a une subtilité. Dire « on repète le procédé » n'a pas vraiment de sens dans le cadre de la théorie des ensembles. En fait, une des formes de l'axiome du choix, appelée axiome des choix dépendants, dit précisément qu'une telle construction est possible. (On choisit une infinité de x_i à la fois, il est donc naturel de devoir faire appel à l'axiome du choix). □

Ainsi, beaucoup d'ensembles qui pourraient sembler à première vue plus petits que $\mathbb{N}$, par exemple l'ensemble des nombres pairs, celui des nombres premiers, ou celui des puissances de 2, sont en fait dénombrables, et donc de même taille que $\mathbb{N}$. Le phénomène inverse est vrai : beaucoup d'ensemble paraissant plus gros que $\mathbb{N}$ sont en fait dénombrables.

Théorème 3.6. Les ensembles suivants sont dénombrables : $\mathbb{Z}$, $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$, $\mathbb{Q}$.

Démonstration. Une énumération des éléments de $\mathbb{Z}$ est facile à trouver : prendre par exemple $(0, 1, -1, 2, -2, \dots)$. On peut la traduire en une bijection explicite : $n \mapsto (-1)^{n+1}\lfloor (n+1)/2 \rfloor$.

Pour $\mathbb{N}^2$, on énumère les couples d'entiers diagonales par diagonales :

$$((0,0),(0,1),(1,0),(0,2),(1,1),(2,0),(0,3),(1,2),(2,1),(3,0),(0,4),\dots).$$

On peut à nouveau expliciter la bijection : la diagonale de $\mathbb{N}^2$ des points (m, n) tels que $m+n = k$ contient $k+1$ points. Ainsi, les diagonales en dessous de celle contenant le point (m, n) contiennent au total $1 + 2 + \ldots + (m + n)$ points, et la bijection est donnée par $(m, n) \mapsto (m + n)(m + n + 1)/2 + m + 1$.

Pour $\mathbb{Q}$, il est plus difficile d'obtenir une bijection explicite. On peut par contre remarquer que $\mathbb{Q}$ s'injecte dans l'ensemble $\mathbb{N}^2$ (par l'application associant à un rationnel son numérateur et son dénomniateur, lorsque la fraction est sous forme réduite). Ainsi, le cardinal de $\mathbb{Q}$ est infini, mais plus petit que celui d'un ensemble dénombrable, et le résultat précédent dit que $\mathbb{Q}$ est dénombrable.

Pour ceux que cela intéresse, le livre "Raisonnements divins" donne des exemples de bijection explicite entre $\mathbb{Q}$ et $\mathbb{N}$. Par exemple, considérons la fonction

$$f \mapsto \frac{1}{\lfloor x \rfloor + 1 - \{x\}},$$

et définissons une suite par $x_0 = 1$, et $x_{n+1} = f(x_n)$. Alors $n \mapsto x_n$ est une bijection de $\mathbb{N}$ dans $\mathbb{Q}$. Une autre façon de le voir est de considérer l'arbre binaire dont la racine est étiquetée par le rationnel $1/1$ (écrit sous cette forme), et dont les deux fils d'un sommet étiqueté par a/b sont étiquetés par $a/(a + b)$ et $(a + b)/b$. Alors, quand on parcourt l'arbre de gauche à droite puis de bas en haut, on retrouve la suite précédente. Les preuves ne sont pas très difficiles à faire, et constituent un exercice amusant. □

L'argument utilisé pour prouver que $\mathbb{Q}$ est dénombrable permet en outre d'obtenir le résultat suivant, très utile en pratique, et dont nous donnons immédiatement un exemple d'application :

Lemme 3.7. Toute union dénombrable d'ensembles dénombrables est dénombrable.

Démonstration. Soit $(U_i)_{i\in A}$ une famille dénombrable d'ensembles dénombrables, et soit f une bijection de A dans $\mathbb{N}$ et $(f_i)_{i\in\mathbb{N}}$ une famille de bijections de $\mathbb{N}$ dans U_i (pour construire cette famille, on a utilisé l'axiome du choix). Il s'agit de prouver que

$$U := \cup_{i\in A} U_i$$

est dénombrable. Or, cet ensemble s'injecte dans $\mathbb{N}^2$ par l'application envoyant un élément x de U sur le couple $(f_i(x), f(i))$, où i est l'élément de A tel que x appartienne à U_i et que $f(i)$ soit minimal. □

Proposition 3.8. L'ensembles des nombres algébriques, c'est-à-dire des réels racines d'une équation polynomiale à coefficients dans $\mathbb{Q}$, est dénombrable.

Démonstration. L'ensemble des polynômes de degré d à coefficients dans $\mathbb{Q}$ est dénombrable (il est en bijection avec $\mathbb{Q}^{d+1}$), donc par le lemme l'ensemble des polynômes de degré quelconque à coefficients dans $\mathbb{Q}$ est lui aussi dénombrable. L'ensemble des racines d'un tel polynôme est fini, donc l'ensemble des nombres algébriques est une union dénombrable d'ensembles finis, et la preuve du lemme s'adapte sans difficultés pour prouver qu'un tel ensemble est dénombrable. □

Remarques 3.9. Le lemme admet une généralisation bien plus puissante : si E et F sont des ensembles tels que $|F| < |E|$ (et tel que F soit non vide), alors $|E^F| = |E|$, où E^F est l'ensemble des applications de F dans E.

- Au delà de l'infini -

La question qui vient ensuite est la suivante : y'a-t-il des ensembles plus gros que celui des entiers ? La réponse est oui, et pas besoin de chercher bien loin pour les trouver. Le résultat suivant de Cantor, qui ne ressemblait à aucun autre résultat connu à l'époque, a eu l'effet d'un coup de tonnerre dans la communauté mathématique.

Théorème 3.10. $|\mathbb{R}| > |\mathbb{N}|$.

Démonstration. Nous allons montrer que $\mathbb{N}$ ne peut pas se surjecter dans $[0,1[$, et on aura ainsi $|\mathbb{N}| < |[0,1[| \leqslant |\mathbb{R}|$. Soit donc f allant de $\mathbb{N}$ dans $[0,1[$. Rappelons que tout réel de $[0,1[$ admet un unique développement décimal propre, c'est-à-dire un développement ne se terminant pas par une infinité de 9. On écrit les développements décimaux propres de tous les $f(i)$, et on cherche à exhiber un réel n'apparaissant pas dans cette liste. Une façon naturelle de le faire est de choisir un réel ayant un développement décimal propre différent de tous ceux des $f(i)$. Une telle construction est donnée par ce que l'on appelle un argument diagonal :

Soit x_i un entier de $\{0,\dots,8\}$, différent de la i-ième décimale du développement décimal propre de $f(i)$. Alors $0,x_1x_2\dots$ est le développement propre d'un réel x, et x est différent de chacun des $f(i)$, puisque les i-èmes décimales de leurs uniques développements propres sont différentes. Ainsi, x n'est pas dans l'image de f, et f n'est pas surjective. □

L'ensemble des réels est donc strictement plus gros que celui des entiers. On se demande donc s'il existe un ensemble de taille intermédiaire entre ces deux ensembles. Et bien, étrangement, cette propriété, connue sous le nom d'"hypothèse du continu", est indépendante de tous les axiomes de la théorie des ensembles, et il est donc impossible de répondre à cette question. Contrairement à l'axiome du choix, la véracité ou non de l'hypothèse du continu n'a que peu d'influence sur le reste des mathématiques, et il n'y a donc pas besoin d'introduire un nouvel axiome.

Voici un autre résultat de même nature que le précédent :

Proposition 3.11. Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble des parties de E. Alors $|\mathcal{P}(E)| > |E|$. (remarque : $\mathcal{P}(E)$ est en bijection avec 2^E.)

Démonstration. Tout d'abord, E s'injecte dans $\mathcal{P}(E)$ par l'application associant à l'élément x le singleton $\{x\}$. Ainsi, $|\mathcal{P}(E)| \geqslant |E|$. Supposons maintenant l'existence d'une surjection f de E dans $\mathcal{P}(E)$. Définissons

$$U := \{x \in E | x \notin f(x)\}.$$

Comme f est surjective, on peut trouver u tel que $f(u) = U$. Cet élément u est-t-il dans U ? S'il l'était, u ne serait pas dans $f(u)$, donc dans U, ce qui est absurde, mais s'il ne l'était pas, alors cela voudrait dire que u est dans $f(u)$, c'est-à-dire U. Nous arrivons donc à un paradoxe, cela contredit l'existence de la surjection. □

- Conséquences de la non dénombrabilité de $\mathbb{R}$ -

Une conséquence importante est qu'une partie dénombrable de $\mathbb{R}$ ne peut être égale à $\mathbb{R}$ tout entier. Ainsi, il existe des réels qui ne sont pas algébriques ! On appelle un tel réel un nombre transcendant. L'existence de ces réels n'est pas une question facile : il est déjà relativement difficile d'expliciter de tels réels, il est encore plus difficile de prouver qu'un

réel donné est transcendant. Encore aujourd'hui, on ne sait le faire que pour peu de réels. Et pourtant, le résultat de Cantor nous dit en deux lignes qu'il existe des nombres transcendants, et même pire que cela, qu'il en existe une infinité non dénombrable ! On peut aller plus loin.

En théorie des probabilités, on définit une quantité appelée la mesure de Lebesgue, notée λ, de telle sorte que, si on tire un réel au hasard dans $]0,1[$, ce réel est dans l'ensemble A avec probabilité $\lambda(A)$. Cette mesure vérifie les propriétés que l'on espère : par exemple, si $0 \leqslant a \leqslant b \leqslant 1$, alors $\lambda(]a,b[) = b - a$; λ est croissante pour l'inclusion ; la mesure de l'union disjointe de A et B est égale à la somme des mesures de A et de B.

On vérifie alors qu'un sous-ensemble E dénombrable de $]0,1[$ est toujours de mesure nulle ! n effet, admettons qu'il soit mesurable. Soit alors ϵ un réel strictement positif, et soit $(e_1, e_2, \ldots)$ une énumération des éléments de E. Pour tout i, on inclut e_i dans un intervalle ouvert de $]0,1[$ de mesure $\frac{\epsilon}{2^i}$. Alors, E sera inclus dans une réunion d'intervalles ouverts, de mesure totale inférieure à

$$\frac{\epsilon}{2^1} + \frac{\epsilon}{2^2} + \frac{\epsilon}{2^3} + \ldots = \epsilon.$$

Ainsi, la mesure de E est inférieure à ϵ, et ce pour tout ϵ, donc E est de mesure nulle.

Ainsi, un réel choisi au hasard dans $]0,1[$ sera transcendant avec probabilité 1 ! On pourrait montrer, comme on l'a fait avec les nombres algébriques, que l'ensemble des réels constructibles à la règle et au compas, ou que l'ensemble des réels définissables par une phrase (ou, si vous préférez , l'ensemble des réels calculables par un ordinateur) sont eux aussi dénombrables. Ainsi, un réel choisi au hasard sera avec probabilité 1 transcendant, non constructible et non calculable ! (Un bémol toutefois : comment chosir un réel au hasard ?) Cantor a ainsi réussi à prouver, par sa théorie des cardinaux, que la majorité des nombres réels seraient à tout jamais hors de portée des mathématiciens et, ce faisant, a ébranlé de manière irréversible la conception idéaliste qu'avaient alors les gens envers la portée des mathématiques, une révolution qui serait achevée des années plus tard par Gödel, mais c'est une autre histoire…

2 Automates

Ce cours a vocation à présenter aux élèves le concept d'automates finis, ainsi que le concept voisin de transducteurs finis. Un automate peut être vu comme une machine, ou bien un programme informatique, qui représente un ensemble : ce programme décide si, oui ou non, un mot donné appartient à l'ensemble en question. De même, un transducteur peut être vu comme un programme informatique, qui représente une fonction transformant les mots en d'autres mots : le programme permet de calculer explicitement cette fonction.

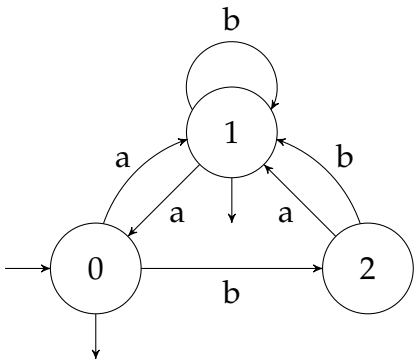
- Automates -

Qu'est-ce qu'un automate ? Alors qu'il existe bien des types d'automates (permettant de travailler sur mots ou bien des arbres, qu'ils soient finis ou infinis), nous nous concentrerons ici sur un type d'automates bien particulier : les automates traitant de **mots finis**.

En clair, comment tout cela fonctionne-t-il ? Tout d'abord, on décide de se fixer un alphabet (ensemble de lettres) fini $\mathcal{A}$. Un **mot fini** est une suite finie d'éléments de $\mathcal{A}$, et c'est sur de tels mots que l'on va travailler ; on note couramment $\mathcal{A}^*$ l'ensemble de ces mots finis dont les lettres appartiennent à $\mathcal{A}$. Un automate peut être vu comme un graphe orienté fini $\mathcal{G}$, un peut spécial :

– il admet une ou plusieurs arêtes **entrantes**, qui viennent de nulle part et arrivent en un sommet de $\mathcal{G}$;
– il admet des arêtes **sortantes**, qui partent d'un sommet de $\mathcal{G}$ et n'aboutissent nulle part ;
– il admet des arêtes **normales**, permettant d'aller d'un sommet de $\mathcal{G}$ à un autre ; de surcroît, chacune de ces arêtes normales est étiquetée par une lettre, c'est-à-dire un élément de $\mathcal{A}$.

Voici un exemple d'automate $\mathcal{G}$ pour l'alphabet $\mathcal{A} = \{a, b\}$:



Automate $\mathcal{G}$

Le graphe $\mathcal{G}$ admet une arête entrante (qui arrive au sommet 0), deux arêtes sortantes (qui partent des sommets 0 et 1) et six arêtes normales. Notons d'ailleurs que le graphe $\mathcal{G}$, s'il est orienté, n'est pas nécessairement **simple** : il peut tout à fait contenir des boucles (l'arête b qui relie le sommet 1 à lui-même) et des arêtes multiples (les arêtes a et b qui vont du sommet 2 au sommet 1).

Cependant, on a dit plus haut qu'un tel graphe pouvait être vu comme un programme informatique, voire comme un **ensemble** de mots : il nous faut donc décrire maintenant pourquoi. Considérons un mot fini $\mathbf{u} = u_1 u_2 \dots u_n$, de longueur n. Un **chemin acceptant** pour le mot $\mathbf{u}$ sera une suite de sommets $s_0 s_1 \dots s_n$ (de longueur $n+1$) telle que

– il existe une arête entrante qui arrive au sommet s_0 ;
– pour tout entier $k \in \{1, 2, \dots, n\}$, il existe une arête normale, étiquetée par la lettre u_k, qui part du sommet s_{k-1} et arrive au sommet s_k ;
– il existe une arête sortante qui part du sommet s_n.

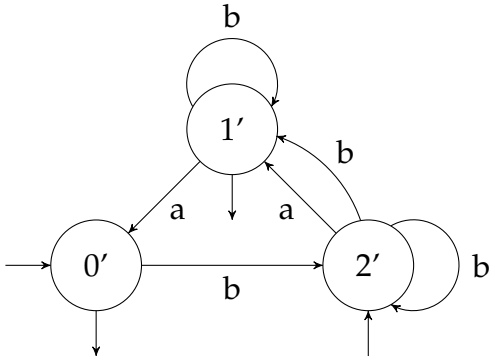
On dira que l'automate $\mathcal{A}$ **accepte** le mot $\mathbf{u}$ s'il contient un tel chemin acceptant pour $\mathbf{u}$.

Concrètement, regardons ce que cela donne si on s'intéresse au graphe $\mathcal{G}$ ci-dessus et aux mots $\mathbf{u} = bbaa$ et $\mathbf{v} = abab$. Dans le premier cas, $\mathcal{G}$ accepte bien le mot $\mathbf{u}$; en effet, la suite de sommets 02101 est bien un chemin acceptant pour $\mathbf{u}$. Au contraire, dans le second cas, $\mathcal{G}$ n'accepte pas le mot $\mathbf{v}$; en effet, un chemin acceptant éventuel devrait nécessairement commencer par le sommet 0, puis se poursuivre avec les sommets $1, 1, 0, 2$, mais nulle arête sortante ne part du sommet 2.

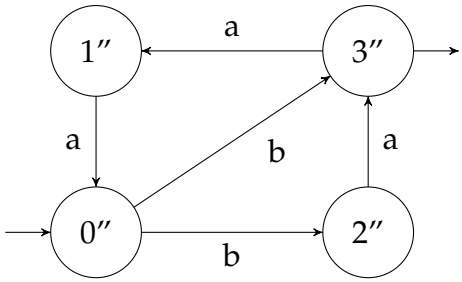
Automates non déterministes, non complets Le lecteur avisé aura remarqué qu'il était très facile de tester si un mot était accepté par l'automate $\mathcal{G}$ présenté ci-dessus : en effet, il n'existe qu'une seule arête entrante et, pour chaque sommet s et chaque lettre λ de l'alphabet, il existe exactement une arête qui part de s et qui est étiquetée par la lettre λ. On n'a donc jamais de choix à faire, le début du seul chemin acceptant éventuel nous est imposé, et il nous suffit

juste de nous promener dans le graphe en suivant un tel début de chemin avant de constater si, oui ou non, on aboutit sur un sommet d'où part une arête sortante.

Cependant, il existe d'autres automates finis moins gentils, tels que les graphes $\mathcal{G}'$ et $\mathcal{G}''$ ci-dessous :



Automate $\mathcal{G}'$



Automate $\mathcal{G}''$

En effet, observons attentivement le graphe $\mathcal{G}'$:

1. depuis le sommet 0, si on veut suivre une arête étiquetée par la lettre a, on est bloqué ;
2. $\mathcal{G}'$ contient deux arêtes entrantes, vers les sommets 0 et 1 ;
3. depuis le sommet 2, en suivant une arête étiquetée par la lettre b, on peut soit aller vers le sommet 1, soit boucler et revenir au sommet 2.

Le point 1 n'est pas trop gênant si le but est simplement de tester si $\mathcal{G}'$ accepte un mot : dans le pire des cas, si on teste un chemin acceptant potentiel et qu'on souhaite prendre une arête qui n'existe pas, c'est juste que notre chemin n'était en fait pas acceptant. Un tel automate est dit **non complet** : c'est un automate où il existe un sommet s et une lettre $\lambda \in \mathcal{A}$ tels que nulle arête étiquetée par λ ne part du sommet s.

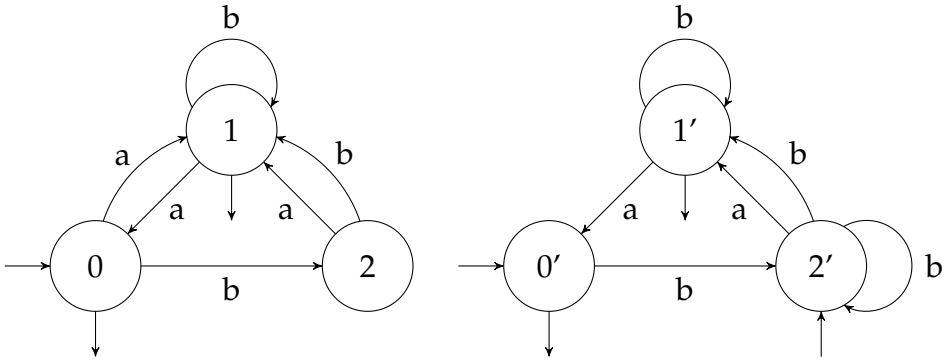
Au contraire, les points 2 et 3 impliquent que l'utilisateur doit tester plusieurs chemins acceptants potentiels : dès l'entrée dans le graphe (point 2) ou à certains moments ultérieurs du parcours (point 3), s'il veut étendre un début de chemin acceptant potentiel, il est obligé de faire des choix a priori entre plusieurs arêtes, sans savoir si un tel choix serait avisé. Notre automate est alors dit **non déterministe** : c'est un automate qui contient

- plusieurs arêtes entrantes, ou bien
- un sommet s et une lettre $\lambda \in \mathcal{A}$ tels qu'il existe plusieurs arêtes étiquetées par λ qui partent du sommet s (et qui vont vers des sommets différents).

De tels automates sont évidemment moins faciles à utiliser, puisque l'on devra parfois s'y reprendre à plusieurs fois pour tester si un mot donné est accepté : peut-être se rendra-t-on compte que le mot est en effet accepté, mais après avoir dû tester un grand nombre de chemins acceptants potentiels ; peut-être devra-t-on, au contraire, tester beaucoup de tels chemins avant de se rendre compte que le mot n'est en fait pas accepté.

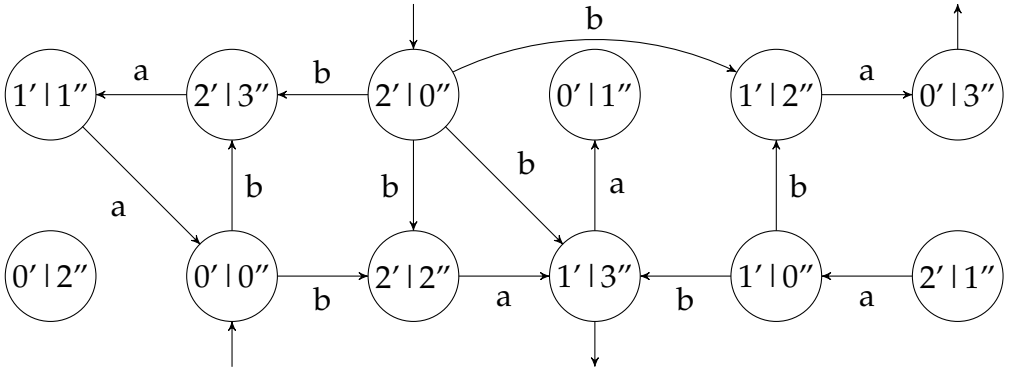
Jouer sur les automates et les ensembles associés Pourquoi avoir été chercher des automates a priori aussi peu utilisables que les automates non complets et non déterministes ? Tout simplement parce qu'ils nous permettent de réaliser facilement des opérations assez naturelles sur les ensembles qu'ils représentent.

Par exemple, supposons que l'on dispose de deux automates $\mathcal{G}$ et $\mathcal{G}'$, associés à deux ensembles de mots $E_{\mathcal{G}}$ et $E_{\mathcal{G}'}$. On souhaite savoir s'il existe un automate associé à la réunion $E_{\mathcal{G}} \cup E_{\mathcal{G}'}$; si oui, on veut également construire un tel automate. Or, rappelons-nous qu'un mot **u** est accepté par un automate si et seulement si cet automate contient un chemin acceptant pour **u**. Il nous suffirait donc de construire un automate $\mathcal{G} \cup \mathcal{G}'$ dont les chemins acceptants peuvent être identifiés soit à un chemin acceptant de $\mathcal{G}$, soit à un chemin acceptant de $\mathcal{G}'$. Construire un tel automate est donc facile : il suffit de placer côte à côte les deux automates $\mathcal{G}$ et $\mathcal{G}'$ et de prétendre qu'ils forment maintenant, à eux deux, un nouvel automate (non déterministe, puisqu'il contient au moins deux arêtes entrantes).



Automate $\mathcal{G} \cup \mathcal{G}'$

De même, on peut construire un automate $\mathcal{G}' \cap \mathcal{G}''$ dont l'ensemble associé sera l'intersection $E_{\mathcal{G}'} \cap E_{\mathcal{G}''}$. Pour ce faire, il faut que tout chemin acceptant dans $\mathcal{G}' \cap \mathcal{G}''$ corresponde **simultanément** à **deux** chemins acceptants : l'un dans $\mathcal{G}'$, l'autre dans $\mathcal{G}''$. Il nous faut alors recourir à une ruse, en introduisant un automate **produit** : on imagine que l'on parcourt ces deux chemins en parallèle, et on enregistre, à chaque étape, les états s et s' dans lesquels on se trouve dans notre visite des automates $\mathcal{G}'$ et $\mathcal{G}''$. Tout sommet de l'automate $\mathcal{G}' \cap \mathcal{G}''$ correspond donc à une paire de sommets, et on autorise une arête du type $(s_0|s'_0) \to^{\lambda} (s_1|s'_1)$ uniquement si les deux arêtes $s_0 \to^{\lambda} s_1$ et $s'_0 \to^{\lambda} s'_1$ existent.



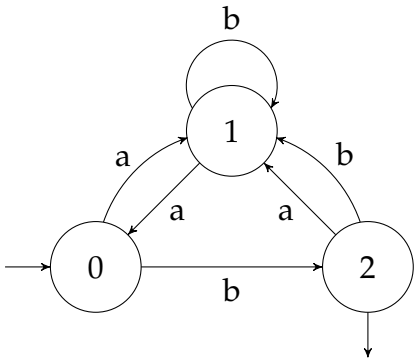
Automate $\mathcal{G}' \cap \mathcal{G}''$

Continuant sur cette voie, on peut réaliser d'autres opérations sur les automates et les ensembles associés. Par exemple, si $\mathcal{G}$ et $\mathcal{G}'$ sont deux automates, on peut construire un automate

$\mathcal{G} \cdot \mathcal{G}'$ dont l'ensemble associé est la **concaténation** des deux ensembles $E_{\mathcal{G}}$ et $E_{\mathcal{G}'}$: plus précisément, il s'agit de l'ensemble $E_{\mathcal{G}} \cdot E_{\mathcal{G}'} = \{u_1u_2 \dots u_k v_1 v_2 \dots v_n : u_1u_2 \dots u_k \in E_{\mathcal{G}}, v_1v_2 \dots v_n \in E_{\mathcal{G}'}\}$.

Exercice 1 Construire un automate $\mathcal{G} \cdot \mathcal{G}'$, où $\mathcal{G}$ et $\mathcal{G}'$ sont les deux automates mentionnés en début de cours.

Cependant, il est très difficile de réussir à créer, dans le cas général, un automate $\neg\mathcal{G}$ qui va représenter le complémentaire de l'ensemble $E_{\mathcal{G}}$ dans l'ensemble $\mathcal{A}^*$ (c'est-à-dire qui accepte un mot **u** si et seulement si $\mathcal{G}$ n'accepte pas **u**). Un espoir est néanmoins que créer un tel automate $\neg\mathcal{G}$ est très facile si $\mathcal{G}$ est déterministe complet. En effet, on a dit, au tout début du cours, qu'on pouvait tester si $\mathcal{G}$ acceptait un mot **u** rien qu'en suivant le seul début de chemin acceptant potentiel pour **u**, puis en vérifiant si, oui ou non, il existe une arête sortante qui part du dernier état dans lequel on est arrivé. Dans ces conditions, pour créer l'automate $\neg\mathcal{G}$, il suffit de considérer l'ensemble S des sommets depuis lesquels part une arête sortante de $\mathcal{G}$, puis de supprimer toute arête sortante partant d'un sommet de S et de rajouter une arête sortante à tout sommet n'appartenant pas à S.

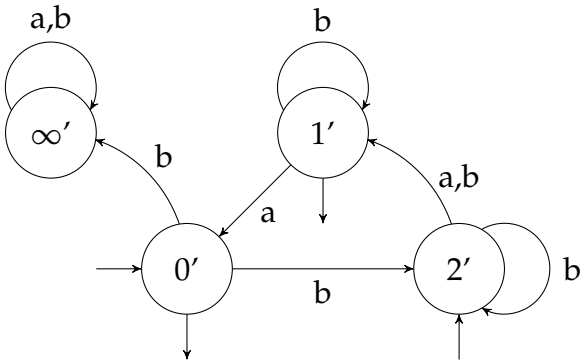


Automate $\neg\mathcal{G}$

Dans ces conditions, être capable de transformer tout automate en un automate déterministe complet équivalent (c'est-à-dire qui est associé au même ensemble de mots) est doublement important :

- cela nous permet d'obtenir des automates avec lesquels il est facile de travailler, par exemple pour tester si un mot est accepté ;
- cela nous permet également de construire un automate associé au complémentaire d'un ensemble $E_{\mathcal{G}}$ quelconque.

Obtenir un automate déterministe complet Montrons d'abord comment, à partir d'un automate $\mathcal{G}$ non complet, on peut obtenir un automate complet $\overline{\mathcal{G}}$ tel que $E_{\mathcal{G}} = E_{\overline{\mathcal{G}}}$. Pour ce faire, c'est assez simple : si on se trouve dans un état s d'où ne part aucune arête étiquetée par la lettre $\lambda \in \mathcal{A}$, il suffit de rajouter une telle arête qui partira vers un état s_∞ par lequel ne peut passer aucun chemin acceptant. Et créer un tel "état poubelle" s_∞ est aisé : pour toute lettre $\lambda \in \mathcal{A}$, on se contente de créer une arête étiquetée par λ, qui part de s_∞ et qui reboucle sur l'état s_∞ lui-même. En outre, notons que, si $\mathcal{G}$ était déjà déterministe, alors $\overline{\mathcal{G}}$ le sera tout autant : une telle remarque ne saurait trop s'apprécier quand on voudra rendre un automate déterministe, puis le rendre complet.



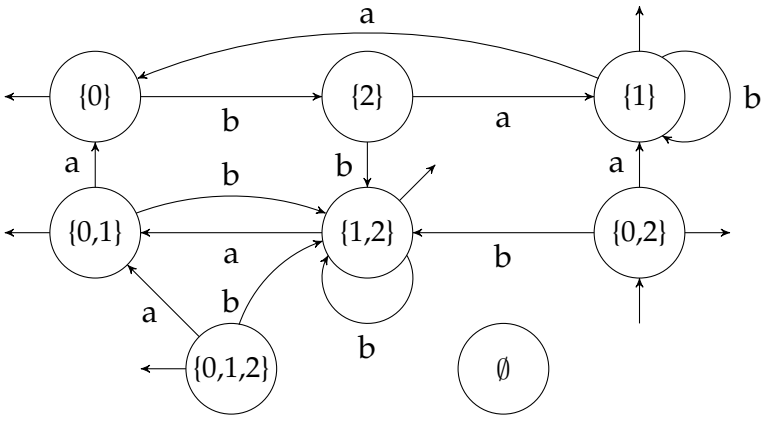
Automate $\overline{\mathcal{G}'}$

Notons d'ailleurs ici que, pour des raisons de lisibilité, on a décidé de fusionner plusieurs arêtes du graphe $\overline{\mathcal{G}'}$ quand on l'a dessiné : il s'agit des arêtes allant du sommet $1'$ au sommet $2'$, et de celles bouclant sur le sommet ∞'. C'est une pratique courante, dont il ne faut donc pas s'émouvoir outre mesure.

Enfin, reste à savoir comment on peut **déterminiser** un automate $\mathcal{G}$ non déterministe. Une idée est que, quand on veut tester si $\mathcal{G}$ accepte un mot **u**, il nous faudrait tester tous les débuts de chemins acceptants potentiels. Cependant, au lieu de faire tous ces tests séquentiellement, l'un après l'autre, rien n'empêche de les faire *en parallèle*. En particulier, si un début de chemin nous amène dans un état s de l'automate, et qu'il nous reste le suffixe $u_k u_{k+1} \dots$ à lire, le fait qu'on ait une chance d'aboutir à un chemin acceptant ne dépend pas du tout des lettres qu'on a déjà lues : seul le fait qu'on ait lu $k-1$ lettres et qu'on soit arrivé dans l'état s est important.

L'idée de la déterminisation est donc de retenir, quand on a lu ces $k-1$ lettres, **l'ensemble des états** de $\mathcal{G}$ dans lesquels on est susceptible de se trouver. Si on aboutit à un ensemble dont un sommet contient une arête sortante, alors $\mathcal{G}$ accepte notre mot **u** ; si on est bloqué par l'absence d'une arête ou si nulle arête sortante ne part d'un sommet de notre ensemble d'arrivée, alors $\mathcal{G}$ n'accepte pas **u**. Cette simple remarque nous permet de construire l'automate des **parties** de $\mathcal{G}$: cet automate déterministe , noté $\det(\mathcal{G})$, est lui aussi associé à l'ensemble $E_{\mathcal{G}}$.

En outre, notons que, si $\mathcal{G}$ est complet, alors $\det(\mathcal{G})$ est lui-aussi complet. Cependant, si on part d'un automate quelconque $\mathcal{G}$, l'automate $\overline{\det(\mathcal{G})}$ obtenu en déterminisant puis en complétant $\mathcal{G}$ contient généralement moins de sommets et d'arêtes que l'automate $\det(\overline{\mathcal{G}})$ obtenu en complétant puis en déterminisant $\mathcal{G}$.



Automate $\det(\mathcal{G}')$

Conclusion On pourrait évidemment se poser bien d'autres questions sur les automates finis. En voici une, non exhaustive :

- tout ensemble de mots est-il associé à un automate ?
- peut-on tester si deux automates sont associés au même ensemble de mots ?
- étant donné un automate $\mathcal{G}$, existe-t-il un unique automate déterministe complet $\mathcal{G}'$ tel que $E_{\mathcal{G}} = E_{\mathcal{G}'}$ et tel que $\mathcal{G}'$ ait un nombre minimal de sommets ?
- et si l'on enlève la contrainte "déterministe complet" ?
- la procédure indiquée ici pour obtenir le complémentaire d'un ensemble est assez compliquée : y a-t-il plus simple ?
- existe-t-il d'autres opérations naturelles sur les ensembles de mots, que l'on pourrait réaliser plus ou moins facilement avec des automates ?

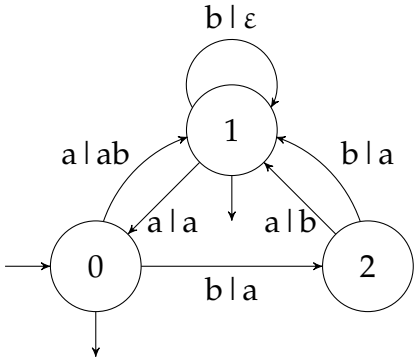
Certaines de ces questions se traitent relativement facilement, si tant est qu'on ait les bonnes idées (ce qui est bien sur la partie difficile du travail). D'autres, au contraire, nécessitent d'utiliser des outils assez lourds. Si vous voulez vous y essayer, et quitte à chercher dans la littérature pour vous aider dans votre quête, n'hésitez pas !

- Transducteurs -

Qu'est-ce qu'un transducteur ? De même qu'il existe de multiples sortes d'automates, il existe bien des sortes de transducteurs. Comme lors de notre étude des automates, nous travaillerons sur une petite partie d'entre eux : les transducteurs traitant de **mots finis**.

Comment un transducteur fonctionne-t-il ? Cette fois, on se fixe deux alphabets : un alphabet $\mathcal{A}$ **d'entrée**, et un alphabet $\mathcal{B}$ **de sortie**. Un transducteur ressemble à un automate, sauf que ses étiquettes ne sont plus de simples lettres $\lambda \in \mathcal{A}$. Il s'agit de paires $\lambda|\mathbf{b}$, où λ est une lettre appartenant à $\mathcal{A}$ et $\mathbf{b}$ est un mot fini constitué de lettres de $\mathcal{B}$.

Voici un exemple de transducteur $\mathcal{T}$ pour l'alphabet d'entrée $\mathcal{A} = \{a, b\}$ et l'alphabet de sotie $\mathcal{B} = \{a, b\}$. Notons que $\mathcal{A} = \mathcal{B}$ dans ce cas précis, mais que $\mathcal{A}$ et $\mathcal{B}$ n'ont a priori rien à voir l'un avec l'autre :



Transducteur $\mathcal{T}$

Pourquoi un tel transducteur représente-t-il une fonction ? Considérons un mot fini $\mathbf{u} = u_1u_2\dots u_n$, de longueur n, Un **chemin acceptant** pour le mot **u** sera une suite de sommets $s_0s_1\dots s_n$ (de longueur $n+1$) telle que

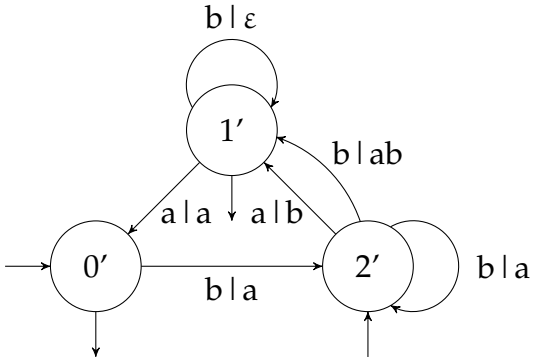
- il existe une arête entrante qui arrive au sommet s_0 ;
- pour tout entier $k \in \{1, 2, \dots, n\}$, il existe une arête normale, étiquetée par une paire $u_k|b_k$ (b_k est un mot quelconque dont les lettres appartiennent à $\mathcal{B}$), qui part du sommet s_{k-1} et arrive au sommet s_k ;
- il existe une arête sortante qui part du sommet s_n.

Le mot **u** sera alors associé à la concaténation de mots $b_1 \cdot b_2 \cdot \dots \cdot b_n$.

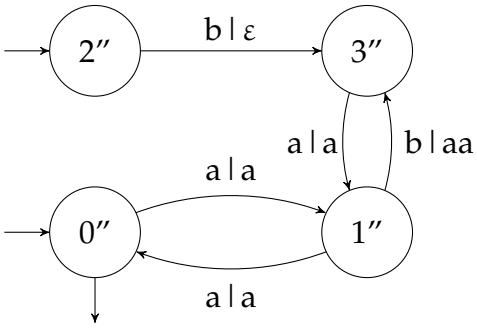
Concrètement, regardons ce que cela donne si on s'intéresse au transducteur $\mathcal{T}$ ci-dessus et aux mots $\mathbf{u} = bbaab$ et $\mathbf{v} = abab$. **u** a un unique chemin acceptant dans le transducteur $\mathcal{T}$: ce chemin est la suite de sommets 021011, obtenue en suivant des arêtes d'étiquettes $b|a$, $b|a$, $a|a$, $a|ab$, $b|\varepsilon$. On associe dont à **u** le mot $aaaab$ (le symbole ε est couramment utilisé pour désigner le mot vide, c'est-à-dire le mot qui ne compte aucune lettre). Par contre, **v** n'a aucun chemin acceptant, ce qui signifie qu'il n'appartient pas au domaine de définition de la fonction associée à $\mathcal{T}$: on voit déjà là une difficulté, qui est que cette fonction n'est pas nécessairement définie sur $\mathcal{A}^*$ tout entier !

Transducteurs non déterministes, non complets De même qu'il existe des automates non déterministes et non complets, on peut concevoir des transducteurs non déterministes et non complets. La partie "complète" du transducteur se traite aisément : il nous suffit de recréer un état poubelle s_∞, auquel mènent les transitions manquantes du type $\lambda|\varepsilon$.

Cependant, le non déterminisme pose davantage de problèmes : en effet, tout d'abord, à un mot **u** doit être associé zéro (s'il n'est pas dans le domaine de définition de la fonction) ou un mot de $\mathcal{B}^*$, mais des chemins acceptants différents peuvent, a priori, donner des mots de $\mathcal{B}^*$ différents. C'est le problème que posent le transducteur $\mathcal{T}'$ suivant, alors même que le transducteur $\mathcal{T}''$ n'est pas touché :



Transducteur $\mathcal{T}'$



Transducteur $\mathcal{T}''$

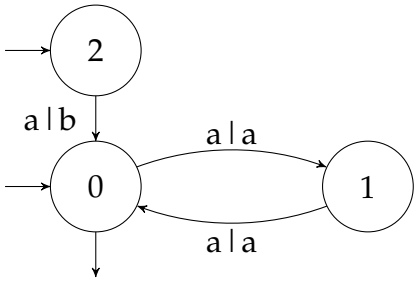
Exercice 2 Trouver un mot $\mathbf{v} \in \mathcal{A}^*$ auquel le transducteur $\mathcal{T}'$ pourrait associer plusieurs mots **différents**.

On pourrait naturellement concevoir que le transducteur $\mathcal{T}'$ représente en fait une fonction qui, à tout mot $\mathbf{u} \in \mathcal{A}^*$, associe un **ensemble** de mots $\mathbf{b} \in \mathcal{B}^*$, cet ensemble étant éventuellement vide. Toutefois, puisque nous nous intéressons simplement aux fonctions $f : \mathcal{A}^* \to \mathcal{B}^*$, nous n'étudierons pas ce cas ici ; nous préférerons nous concentrer sur les transducteurs **fonctionnels**, c'est-à-dire les transducteurs qui représentent effectivement une fonction $f : \mathcal{A}^* \to \mathcal{B}^*$ (dont le domaine de définition n'est pas nécessairement $\mathcal{A}^*$ tout entier).

Une fois cette décision prise, une question se pose :

- peut-on tester a priori si un transducteur non déterministe $\mathcal{T}$ est fonctionnel ?
- si oui, peut-on construire un transducteur déterministe $\det(\mathcal{T})$ qui représente la même fonction ?

Il se trouve que la réponse à la première question est **oui**, mais est assez compliquée à expliquer (bien plus que la déterminisation !). Cependant, la réponse à la deuxième question est **non**, comme l'illustre le contre-exemple suivant, pour l'alphabet de départ $\mathcal{A} = \{a\}$ et l'alphabet d'arrivée $\mathcal{B} = \{a, b\}$:



Transducteur $\mathcal{U}$

En effet, la fonction $f_{\mathcal{U}}$ associée au transducteur $\mathcal{U}$ est telle que $f_{\mathcal{U}}(a^{2k}) = a^{2k}$ et que $f_{\mathcal{U}}(a^{2k+1}) = ba^{2k}$. Ainsi, pour tout mot $\mathbf{u} \in \mathcal{A}^*$, avant d'écrire ne serait-ce que la première lettre de son image $f_{\mathcal{U}}(\mathbf{u})$, il faut déjà connaître la longueur $|\mathbf{u}|$ (mod. 2). Cela fait, il nous faudra alors écrire un mot de longueur $|\mathbf{u}|$, alors même que l'on aura déjà lu toutes les lettres de $\mathbf{u}$. Il nous faut donc savoir combien de lettres écrire, c'est-à-dire retenir la longueur $|\mathbf{u}|$ elle-même. Mais toute notre mémoire à ce moment-là dépendra uniquement de l'état dans lequel on sera. Un transducteur ayant un nombre fini d'états, on ne peut donc distinguer qu'un nombre fini

de longueurs de mots, et non pas traiter correctement des mots qui peuvent avoir un nombre arbitrairement grand de longueurs différentes.

Composition des transducteurs Si l'on veut travailler de manière sereine, il faut donc se restreindre à travailler uniquement sur des transducteurs déterministes, ou bien être prêt à renoncer à jamais à tous les avantages que pourrait nous offrir le déterminisme ! Cela dit, quoi qu'il en soit, une des propriétés principales des fonctions est que l'on peut les **composer**.

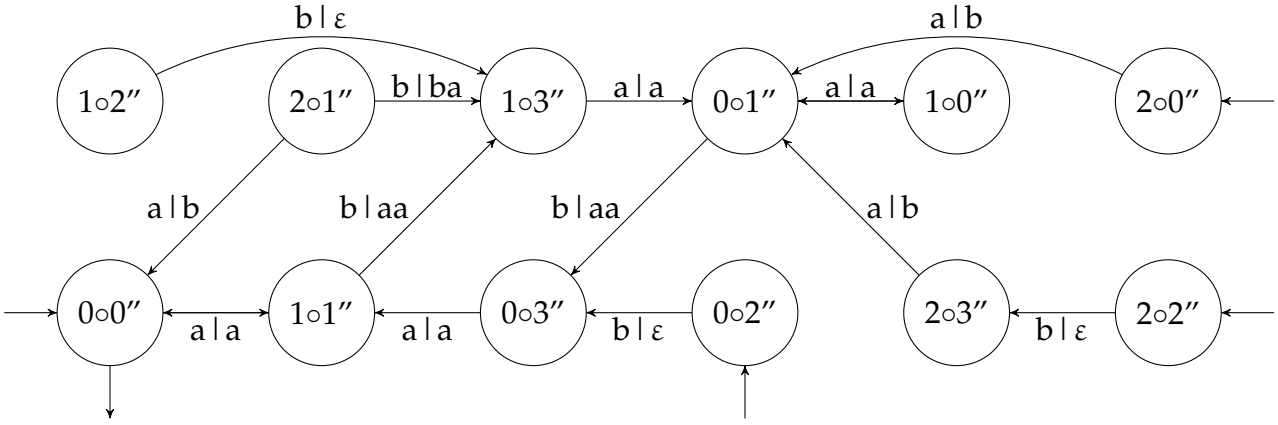
On cherche donc, étant donnés
- un transducteur $\mathcal{T}$ qui représente une fonction $f_{\mathcal{T}} : \mathcal{B}^* \to \mathcal{C}^*$ et
- un transducteur $\mathcal{T}'$ qui représente une fonction $f_{\mathcal{T}'} : \mathcal{A}^* \to \mathcal{B}^*$,

à construire un transducteur $\mathcal{T} \circ \mathcal{T}'$ qui représente la fonction composée $f_{\mathcal{T}} \circ f_{\mathcal{T}'}$.

On procède alors comme suit : supposons que l'on dispose d'un mot $\mathbf{u} = u_1 u_2 \dots u_n \in \mathcal{A}^*$ et que l'on veut calculer $f_{\mathcal{T}} \circ f_{\mathcal{T}'}(\mathbf{u})$. Puisque $\mathcal{T}'$ est fonctionnel, on peut directement se concentrer sur le cas où $\mathcal{T}'$ contient un chemin acceptant $s_0, s_1, \dots, s_n$ pour $\mathbf{u}$, où l'on transite par des arêtes d'étiquettes $u_1|b_1, u_2|b_2, \dots, u_n|b_n$. En outre, $\mathcal{T}$ est fonctionnel lui aussi, donc on se concentre sur le cas où $\mathcal{T}$ contient un chemin acceptant $s'_0, s_1, \dots, s'k$ pour $f_{\mathcal{T}'}(\mathbf{u}) = \beta_1 \dots \beta_k$, où l'on transite par des arêtes d'étiquettes $\beta_1|c_1, \beta_2|c_2, \dots, \beta_n|c_n$. Notons qu'il faut faire attention, car les b_i sont des mots de longueur a priori quelconque, tandis que les β_i ne sont que des lettres : en particulier, dans le cas général, $\beta_i \neq b_i$.

Au lieu de parcourir les deux transducteurs $\mathcal{T}'$ puis $\mathcal{T}$ l'un après l'autre, on peut alors parcourir les deux transducteurs simultanément, en parallèle : c'est une ruse analogue à celle utilisée pour faire l'intersection de deux automates. Cependant, alors que l'on parcourt une arête du transducteur $\mathcal{T}'$, on peut être amené à créer un nombre quelconque de lettres du "mot intermédiaire " $f_{\mathcal{T}'}(\mathbf{u}) = b_1 \cdot b_2 \cdot \dots \cdot b_n$. Il nous faut donc parcourir d'un seul coup plusieurs arêtes (ou aucune) du transducteur $\mathcal{T}'$; une fois cette subtilité prise en compte, plus aucun problème ne se pose.

C'est ainsi que l'on peut obtenir le transducteur $\mathcal{U} \circ \mathcal{T}''$ suivant :



Transducteur $\mathcal{U} \circ \mathcal{T}''$

Conclusion Tout ce qui n'est bien sur qu'une introduction au monde très vaste des transducteurs, qu'il convient d'ailleurs d'étudier conjointement avec leurs cousins les automates. Une fois encore, on pourrait se poser mille et une questions qui n'ont pas été abordées ici, et donc voici quelques unes parmi tant d'autres tout aussi intéressantes :

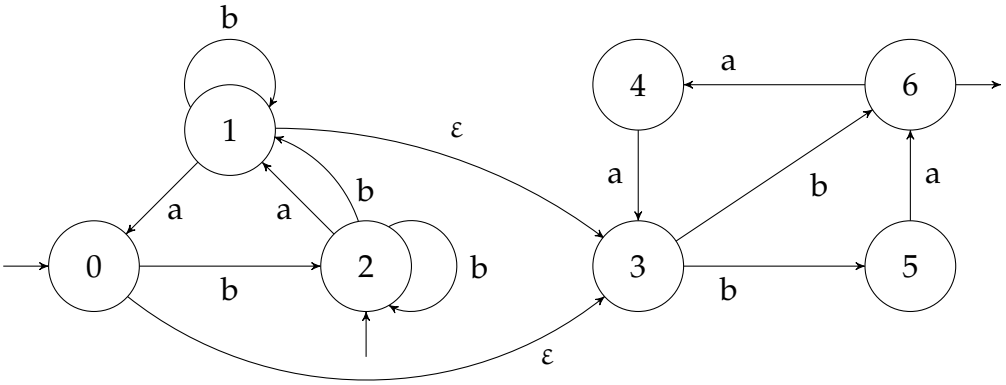
- étant donnés deux transducteurs fonctionnels $\mathcal{T}$ et $\mathcal{T}'$, sont-ils associés à la même fonction ?
- peut-on tester si $f_{\mathcal{T}}(\mathbf{u}) = f_{\mathcal{T}'}(\mathbf{u})$ pour tout mot $\mathbf{u}$?
- si $\mathcal{T}$ est déterministe, existe-t-il un unique transducteur déterministe complet $\mathcal{U}$ tel que $f_{\mathcal{T}} = f_{\mathcal{U}}$ et tel que $\mathcal{U}$ ait un nombre minimal de sommets ?
- et si l'on enlève la contrainte "déterministe complet" ?
- existe-t-il d'autres opérations naturelles sur les fonctions, que l'on pourrait réaliser plus ou moins facilement avec des transducteurs ?

De nouveau, certaines de ces questions trouvent facilement une réponse, tandis que d'autres sont probablement ouvertes à l'heure actuelle (selon le moment auquel vous lirez ce texte) : dans tous les cas, faciles ou difficiles, elles n'attendent que vous pour être résolues !

- Solutions des exercices -

Solution de l'exercice 1 Un mot $\mathbf{u}$ est accepté par l'automate $\mathcal{G} \cdot \mathcal{G}'$ si et seulement si on peut décomposer $\mathbf{u}$ sous la forme $\mathbf{u} = \mathbf{v} \cdot \mathbf{w}$ de sorte que $\mathbf{v}$ soit accepté par $\mathcal{G}$ et $\mathbf{w}$ soit accepté par $\mathcal{G}'$. Cela revient à dire que $\mathcal{G}$ contient un chemin acceptant pour $\mathbf{v}$ puis que $\mathcal{G}'$ contient un chemin acceptant pour $\mathbf{w}$.

Une idée, pour tester l'existence de tels chemins acceptants, est de se « téléporter » depuis une arête sortante de $\mathcal{G}$ vers une arête entrante de $\mathcal{G}'$ au moment où on arrive à la fin du préfixe $\mathbf{v}$. Cette notion de téléportation est transcrite par ce que l'on appelle des « ε-transitions ». Informellement, on pourrait considérer les automates avec ε-transitions comme de automates non-déterministes usuels, où l'on a rajouté à l'alphabet $\mathcal{A}$ une lettre ε : on peut alors suivre n'importe quelle arête étiquetée par ε, sans avoir besoin de lire une lettre du mot $\mathbf{u}$.

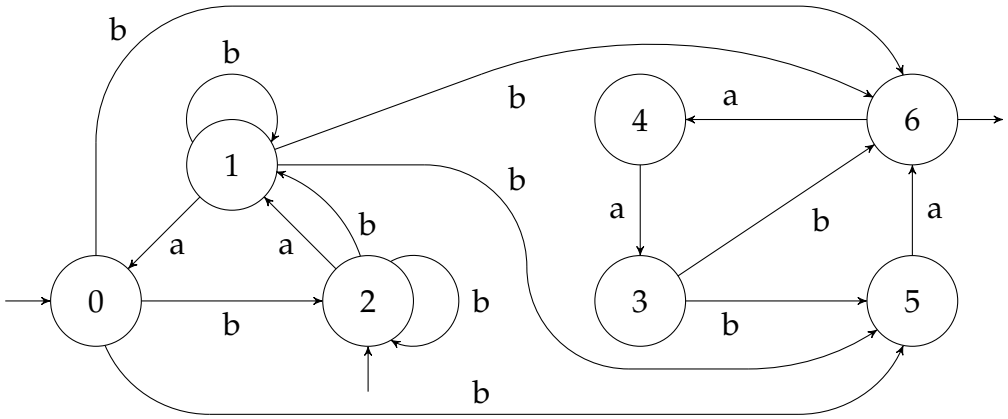


Automate $\mathcal{G} \cdot \mathcal{G}'$, avec ε-transitions

Toutefois, dans le cadre de ce cours, on préfère travailler avec des automates sans ε-transition. Il nous faut donc ôter les deux transitions que l'on vient de rajouter. Pour ce faire, on simule l'exécution d'une ε-transition : après tout, un chemin constitué de ε-transitions n'est qu'un moyen de se déplacer d'un sommet à un autre avant de suivre soit une arête normale, soit une arête sortante. On peut alors remplacer

- un chemin $s_1 \to^{\varepsilon} s_2 \to^{\varepsilon} \cdots \to^{\varepsilon} s_n \to^{\lambda} s_{n+1}$, par une arête $s_1 \to^{\lambda} s_{n+1}$ normale ;
- un chemin $s_1 \to^{\varepsilon} s_2 \to^{\varepsilon} \cdots \to^{\varepsilon} s_n$ menant à une arête sortant de s_n par une arête sortant directement de s_1.

Dans notre cas, cela donne l'automate $\mathcal{G} \cdot \mathcal{G}'$ ci-dessous, ce qui conclut l'exercice :



Automate $\mathcal{G} \cdot \mathcal{G}'$, sans ε-transition

Solution de l'exercice 2 Le mot $\mathbf{v} = \mathtt{bb}$ est associé aux chemins acceptants $0'2'1'$, $2'2'1'$ et $2'1'1'$ au sein du transducteur $\mathcal{T}'$. À ces chemins respectifs correspondent plusieurs images possibles pour $\mathbf{v}$, à savoir les mots $\mathtt{aab}$, $\mathtt{aab}$ et $\mathtt{ab}$.

4 Groupe D

1 Théorie de Galois

2 Probabilités

Nous avons défini la notion de probabilité sur un ensemble probabilisé dénombrable, calculé la probabilité d'extinction d'un processus de Galton–Watson et étudié la percolation par arêtes sur $\mathbb{Z}^2$.

IX. Les soirées

Contenu de cette partie

1 Conférence : la cryptographie, de vraies maths ! (Razvan)

Voici le résumé de la conférence. La cryptographie est apparue quand Jules César voulait communiquer avec ses armées. En effet, les soldats qui transmettaient ses instructions pouvaient à tout moment tomber prisonniers et être torturés. Il fallait donc chiffrer les messages. La solution a consisté à échanger un secret avec ses généraux avant qu'ils partent en mission. Aujourd'hui on ne peut pas échanger de secret avec tous les ordinateurs avec lesquels on communique sur internet (Facebook, Gmail, etc.). En échange, on utilise une technique inventée en 1976 par Diffie et Hellman. Pour cela, on utilise les propriétés de l'ensemble $(\mathbb{Z}/p\mathbb{Z})^*$ pour p premier. On aperçoit des vraies applications de l'arithmétique. Mais le meilleur de la cryptographie est dans le futur...

2 Présentation de compétitions mathématiques diverses

Depuis vingt ou trente ans, un certain nombre de compétitions mathématiques ont été créées, et nous nous efforçons de prendre en compte leurs palmarès dans le repérage d'élèves à qui l'on propose le test de sélection de notre stage olympique. En premier lieu, les Olympiades, académiques (en France) et internationales, auxquelles nous consacrerons toute une soirée. Le concours Kangourou, que la majorité d'entre vous ont passé, questionnaire à choix multiple à résoudre en temps très limité, corrigé électroniquement par des lecteurs optiques. Le championnat de la Fédération Française des Jeux Mathématiques, qui se déroule en plusieurs temps : quarts de finale, demi-finale, finale régionale et finale internationale, à laquelle certains d'entre vous participeront - elle a lieu cette année juste après notre stage, les 29 et 30 août 2013. Enfin des compétitions régionales, comme le rallye d'Alsace, le rallye du Centre, le tournoi du Limousin... La publication *Panoramath* recense ces différentes compétitions, et nous nous efforcerons de compléter la liste pour la faire figurer sur notre site **www.animath.fr**.

Mais la présente soirée est consacrée avant tout à un tournoi différent de toutes ces compétitions, puisqu'il ne s'agit pas d'une épreuve en temps limité, mais de problèmes ouverts (dont nul ne connaît la solution complète) sur lesquels différentes équipes de lycéens travaillent pendant plusieurs mois : ITYM, tournoi international des jeunes mathématiciens, et le TFJM, tournoi français des jeunes mathématiciens.

Le TFJM[2] est un tournoi est destiné aux élèves de lycée. Il se distingue d'autres compétitions comme les olympiades en proposant des problèmes ouverts et en étant organisé par équipes. Guidés par des encadrantes et encadrants, les équipes auront plus d'un mois et demi pour réfléchir aux problèmes exposés. Pendant le tournoi, les élèves participants présenteront leurs résultats partiels ou intermédiaires sous forme de débats avec quatre rôles : défenseur, opposant, rapporteur et observateur.

Les principaux objectifs du tournoi sont :
- stimuler l'intérêt pour les mathématiques et leurs applications,
- développer la pensée scientifique des élèves, leurs talents de communication, et leur capacité à
- travailler en équipe, permettre l'échange d'expérience entre enseignants et étudiants.

Les équipes gagnantes sont invitées au tournoi international des jeunes mathématiciens (ITYM).

En 2014, Le 4e Tournoi Français des Jeunes Mathématiciennes et Mathématiciens aura lieu du 18 au 21 Avril 2014. Pour plus d'informations, voir http://www.tfjm.org et http://www.itym.org.

À titre d'exemple, les pages suivantes sont constituées de la solution de exercice présentée par l'équipe gagnante France 2 à l'ITYM.

5th ITYM — Problem 5: Congruent Polygons

Team France 2

Abstract:
We solve completely the questions 1 and 4, and find a near-complete solution to questions 2, 3 and 5 — as only finitely many cases have not been treated.

1. We prove that a convex pentagon must be regular if and only if it has at least 5 isometric sides and 3 isometric diagonals, or 3 isometric sides and 5 isometric diagonals.
2. We prove that no regular n-gon has more than n isometric diagonals, and that, for all values of n except finitely many (in particular, as soon as $n \geq 74$), even having n isometric sides and n isometric diagonals is not enough to force a convex n-gon to be regular.
3. We prove that, if $n \geq 9$, a regular and a convex n-gons must be congruent if and only if they have at most either 0 side and $2n-5$ diagonals, 1 side and $n-3$ diagonals, or $n-2$ diagonals that are not isometric to their corresponding edges.
4. We prove that two convex pentagons with 5 sides and 3 diagonals, 4 sides and 4 diagonals, or even 5 sides and only 2 diagonals that are isometric to their corresponding edges must be congruent.
5. We prove that, if $n \geq 9$, two convex n-gons must be congruent if and only if they have at most either 0 side and $2n-5$ diagonals, 1 side and $n-3$ diagonals, or $n-2$ diagonals that are not isometric to their corresponding edges.

Contents

1 Must these convex pentagons be regular?

1.1 5 sides and 3 diagonals have the same length

Theorem 1:
If a convex pentagon has 5 isometric sides and 3 isometric diagonals, this pentagon is regular. ■

Proof of Theorem 1:
We can distinguish 2 cases. Let A, B, C, D and E be the vertices of the pentagon. We know that $AB = BC = CD = DE = EA$. Since a pentagon has 5 diagonals, if 3 have the same length, at least 2 will have a common vertex. We can therefore suppose that $AC = AD$. The third diagonal either has a common vertex with AC or AD — we assume that this diagonal will be CE — or not – this diagonal must be EB.

1st case: Here we assume that $AC = AD = CE$. Thick lines represent segments of same length, and dotted lines represent segments whose length is unknown *a priori*.

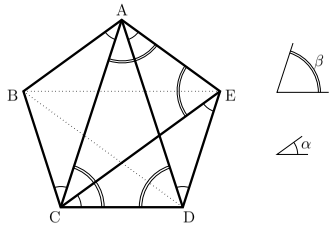


Figure 1: AC=AD=CE

In the triangles ECD isosceles in D, we have : $\widehat{DEC} = \widehat{DCE} = \alpha$.
In the triangle DEA isosceles in E, we have : $\widehat{ADE} = \widehat{DAE} = \alpha$.
In the triangle ABC isosceles in B, we have : $\widehat{BAC} = \widehat{BCA} = \alpha$.
In the triangle ACD isosceles in A, we have : $\widehat{ACD} = \widehat{ADC} = \beta$.
In the triangle ACE isosceles in C, we have : $\widehat{CAE} = \widehat{CEA} = \beta$.
Triangles BCD, ABE and CDE are therefore isometric, since they have 2 sides ($BC = CD = DE = EA = AB$) and 1 angle ($\widehat{BCD} = \widehat{EAB} = \widehat{CDE} = \alpha + \beta$) in common.
Therefore, their third sides have same length, i.e. $DB = BE = CE$.
Finally, all the diagonals have the same length and the pentagon is regular.

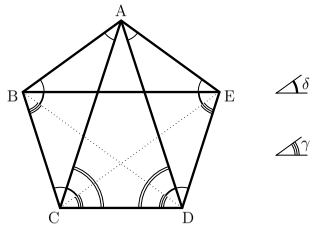


Figure 2: AC = AD = EB

2nd case: Let's suppose now that $AC = AD = EB$.
In the isosceles and isometric triangles ABE, ADE and ABC, we have : $\widehat{BAC} = \widehat{BCA} = \widehat{ADE} = \widehat{DAE} = \widehat{ABE} = \widehat{AEB} = \alpha$.
In the triangle ACD isosceles in A, we have : $\widehat{ACD} = \widehat{ADC} = \beta$.
Therefore, in DEC and CDB : $\widehat{CDE} = \widehat{BCD} = \alpha + \beta$. So DEC et CDB are isometric, as they have 1 angle and 2 sides in common. We can thus write : $\widehat{DCE} = \widehat{DEC} = \widehat{CDB} = \widehat{CBD} = \gamma$, as well as $BD = CE$.
Therefore, DEB, CBE, DAB and CEA are isometric (their 3 sides match), so : $\widehat{DBE} = \widehat{CEB} = \widehat{BDA} = \widehat{ACE} = \delta$.
Then, $\alpha = \widehat{ACD} = \widehat{ACE} + \widehat{ECD} = \gamma + \delta$, so that $\widehat{DEB} = \widehat{CBE} = \gamma + \delta = \alpha$.
Therefore, in DEB and CDA, where $DE = DC$, $DA = EB$ and $\widehat{DEB} = \widehat{CDA} = \alpha$, $DB = AC$. Since we saw above that $CE = BD$, the 5 diagonals have the same length, and the pentagon is regular. □

1.2 4 sides and 4 diagonals have the same length

Theorem 2:
There exists an irregular convex pentagon with 4 isometric sides and 4 isometric diagonals. ■

Proof of Theorem 2:
We just need to consider the following pentagon:

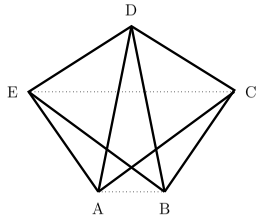


Figure 3: Irregular pentagon

Let ABD be a triangle isoceles in A with $BD > 2AB$, and C — respectively, E — be the intersection of the mediator of $[BD]$ — respectively, $[AD]$ — and of the circle of center A — respectively, B — and of radius AD.
The mediator of $[AB]$ is an axis of symmetry of the pentagon $ABCDE$, and therefore $DE = CD$. Moreover, $BC = CD$ and $AE = DE$. Therefore, $ABCD$ has 4 isometric sides.
In addition, $BD = AD = AC = BE$, and $ABCD$ has 4 isometric diagonals.
Finally, note that $ABCDE$ is convex and that, since $2AB < BD \leq BC + CD = 2BC$, $ABCDE$ is not regular. □

1.3 3 sides and 5 diagonals have the same length

Theorem 3:
If a convex pentagon has 3 isometric sides and 5 isometric diagonals, this pentagon is regular. ■

Proof of Theorem 3:
We can distinguish 2 cases, depending on if the sides that don't have the same length are adjacent or not.

1st case : Let us assume that $BC = CD = DE$.

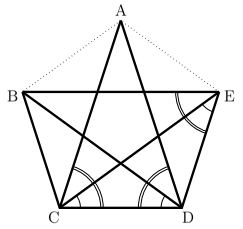


Figure 4: BC=CD=DE

In the isosceles and isometric triangles BCD and DEC, we have : $\widehat{BDC} = \widehat{DCE} = \widehat{DEC} = \alpha$.
In the isosceles and isometric triangles DAC and BDE, we have : $\widehat{CDA} = \widehat{ACD} = \widehat{BED} = \beta$.
Therefore, $\widehat{CEB} = \widehat{DEB} - \widehat{DEC} = \beta - \alpha$, $\widehat{BDA} = \widehat{CDA} - \widehat{BDC} = \beta - \alpha$ and $\widehat{ACE} = \widehat{ACD} - \widehat{ECD} = \beta - \alpha$. Thus, $\widehat{CEB} = \widehat{BDA} = \widehat{ACE}$, which implies that $BA = CB = AE$ and that the pentagon is regular.

2nd case : Let us assume that $BC = CD = EA$.

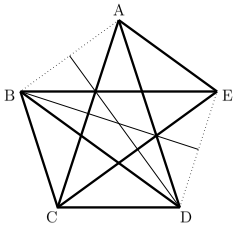


Figure 5: BC=CD=EA

Since BEA and CBA are isometric, the points C and E are symmetric with respect to the mediator of $[AB]$. Moreover, ABD is isosceles in D, so that D belongs to this mediator. Therefore, $CD = DE$.
Similarly, the mediator of $[DE]$ is an axis of symmetry of $ABCDE$, and $AB = BC$.
This proves that the $ABCDE$ has 5 sides of the same length and must be regular. □

1.4 5 sides and 2 diagonals have the same length

Theorem 4:
There exists an irregular convex pentagon with 5 isometric sides and 2 isometric diagonals. ■

Proof of Theorem 4:
We just need to consider the following pentagon:

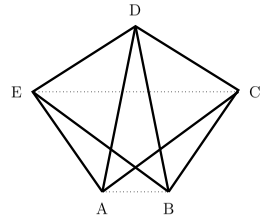


Figure 6: Irregular pentagon

Let CDE be an equilateral triangle, and $ABCD$ a square. $AC = BD$, so that $ABCDE$ has 2 isometric diagonals, and $DA = AB = BC = CD = DE = EC$, so that $ABCDE$ has 5 isometric diagonals.
$ABCDE$ is convex. Moreover, since C is the circumcenter of the triangle BDE, the pentagon $ABCDE$ is not cocyclic, and therefore not regular. □

2 For which triples (s, d, n) must a convex n-gon with s isometric sides and d isometric diagonals be regular?

Proposition 5:
No regular n-gon to has more than n isometric diagonals. ■

Proof of Proposition 5:
Consider a n-gon with at least $n+1$ isometric diagonals. Each diagonal joins 2 of the n vertices, so there exists at least one vertex A that belongs to at least 3 of the diagonals mentioned before: let AB, AC and AD be such diagonals.
Then, A is the circumcenter of the triangle BCD and our n-gon is not cocyclic, hence not regular. □

Theorem 6:
Let $n \geq 5$ be a composite integer. There exists an irregular convex n-gon with n isometric sides and n isometric diagonals. ■

Proof of Theorem 6:
We treat separately 2 cases: when n is divisible by 4 — which is the case of all powers of 2 — and when n has a proper odd prime factor — which is the case of all other composite integers $n \geq 6$.

- If 4 divides n:

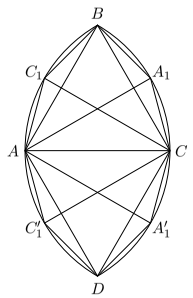


Figure 7: Irregular octogon

Let ABC and ACD be 2 equilateral triangles such that the segments $[AC]$ and $[BD]$ intersect. We divide the arc of circle $\overline{BC}$ of center A and radius $AB = AC$ in $\frac{n}{4}$ isometric small arcs of circle $\overline{A_0A_1}, \overline{A_1A_2}, \ldots, \overline{A_{\frac{n}{4}-1}A_{\frac{n}{4}}}$, with $A_0 = B$ and $A_{\frac{n}{4}} = C$.

Similarly, we divide the arc of circle $\overline{DC}$ — respectively, $\overline{BC}$ and $\overline{DC}$ — of center A — respectively, C and C — and radius AB in $\frac{n}{4}$ isometric small arcs of circle $\overline{A'_iA_{i+1}}$ — respectively, $\overline{C_iC_{i+1}}$ and $\overline{C'_iC_{i+1}}$ — with $C_0 = B$, $A'_0 = C'_0 = D$, $A'_{\frac{n}{4}} = C$ and $C_{\frac{n}{4}} = C'_{\frac{n}{4}} = B$.

Consider now the n-gon

$$\mathcal{P} = AC_{\frac{n}{4}-1}C_{\frac{n}{4}-2}\ldots C_1BA_1A_2\ldots A_{\frac{n}{4}-1}CA'_{\frac{n}{4}-1}A'_{\frac{n}{4}-2}\ldots A'_1DC'_1C'_2\ldots C'_{\frac{n}{4}-1}.$$

$\mathcal{P}$ is convex and, by construction, its n sides are isometric. In addition, the n diagonals AA_i, AA'_i, CC_i and CC'_i with $\frac{n}{4} > i \geq 0$ are all isometric to AC. By counting the diagonal AC itself, $\mathcal{P}$ has actually $n+1$ isometric diagonals.

Finally, note that A is the circumcenter of the triangle BCD, hence that $\mathcal{P}$ is not cocyclic.

- If $n = ab$ where a is and odd prime number and $b \geq 2$:

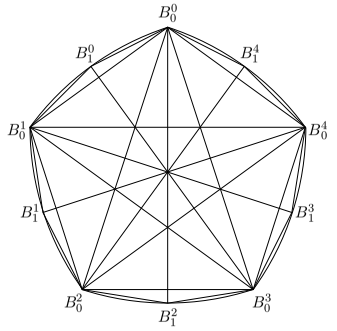


Figure 8: Irregular decagon

Let $A_0A_1\ldots A_{a-1}$ be a regular a-gon — below, we consider the indices modulo a. Like above, we divide each arc of circle $\overline{A_iA_{i+1}}$ of center $A_{i+\frac{a+1}{2}}$ and radius

$A_iA_{i+\frac{a+1}{2}} = A_{i+1}A_{i+\frac{a+1}{2}}$ in b isometric small arcs of circle $\overline{B_0^iB_1^i}, \overline{B_1^iB_2^i}, \dots, \overline{B_{b-1}^iB_b^i}$, with $B_0^i = A_i$ and $B_b^i = A_{i+1}$.

Consider now the n-gon

$$\mathcal{P} = B_0^0B_1^0 \dots B_{b-1}^0B_0^1B_1^1 \dots B_{b-1}^1 \dots B_0^{a-1}B_1^{a-1} \dots B_{b-1}^{a-1}.$$

$\mathcal{P}$ is convex and, by construction, its n sides are isometric. In addition, the n diagonals $B_0^{i+\frac{a+1}{2}}B_j^i = A_{i+\frac{a+1}{2}}B_j^i$ with $0 \leq i < a$ and $0 \leq j < b$ are all isometric: $\mathcal{P}$ has actually n isometric diagonals.

Finally, note that $B_0^{i+\frac{a+1}{2}} = A_{i+\frac{a+1}{2}}$ is the circumcenter of the triangle $B_0^iB_1^iB_2^i$, hence that $\mathcal{P}$ is not cocyclic.

□

Proposition 7:
Let $n \geq 8$ be an integer not divisible by 3. There exists an irregular convex n-gon with $n-1$ isometric sides and n isometric diagonals. ■

Proof of Proposition 7:

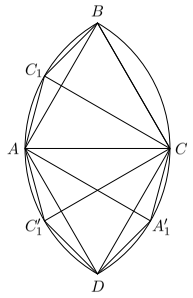


Figure 9: Irregular heptagon

We consider the biggest integer $k \geq 1$ such that $4 + 3k \leq n$: since 3 cannot divide n, $4 + 3k \in \{n-1, n\}$. We build an n-gon as follows:

Build the $4(k+1)$-gon built in the first part of the proof of Theorem 6. Then, if $4 + 3k = n - 1$ — respectively, if $4 + 3k = n$ — remove the vertices $A_1, \dots, A_{k-1}$ — respectively, the vertices $A_1, A_2, \dots, A_k$. The n-gon we obtain has $n-1$ isometric sides — all the sides except the side A_0A_k or A_0A_{k+1}, depending on how many vertices we removed — and n isometric diagonals — all the diagonals AA_i, AA_i', CC_i and CC_i' that remain in our n-gon. Moreover, since C is still the circumcenter of the vertices A, B, D, our n-gon is not cocyclic, hence not regular. □

Theorem 8:
Let n be a prime number such that either:

- $n \equiv 1$ (mod. 4) and $n \geq 85$;
- $n \equiv 3$ (mod. 4) and $n \geq 29$.

. There exists an irregular convex n-gon with n isometric sides and n isometric diagonals. ■

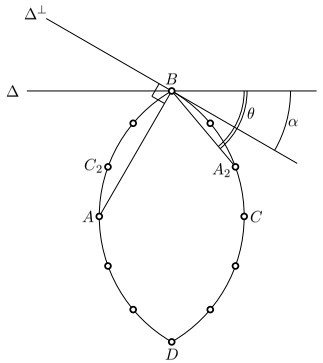


Figure 10

Proof of Theorem 8:
Consider the integer $m = \left\lceil \frac{n}{4} \right\rceil$: we start from the convex $(4m)$-gon built in the first part of the proof of Theorem 6 and want to obtain a convex n-gon by removing 1 vertex — respectively, 3 vertices — if $n \equiv 3$ (mod. 4) — respectively, if $n \equiv 1$ (mod. 4). However,

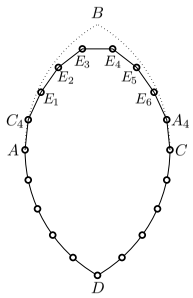


Figure 11: Adding Points $E_1, \dots, E_{7k-1}$

we cannot proceed as directly as in Proposition 7, since we want to have n isometric sides and not only $n-1$.
Since (BD) is an axis of symmetry of the $(4m)$-gon, the distance between the vertices A_i and C_i is

$$\begin{aligned} A_iC_i &= A_iB\cos(\theta) + C_iB\cos(\theta) \\ &\leq 2iA_0A_1\cos(\theta) \text{ by triangular inequality} \\ &\leq 2iA_0A_1\cos(\alpha), \end{aligned}$$

where:

- Δ is the parallel to (AC) going through B,
- $\Delta^\perp$ is the tangent in B to the circle of center A and radius AB,
- α is the angle between Δ and $\Delta^\perp$, and
- θ is the angle between (A_0A_i) and Δ,

as shown on Figure 10.
Note that $\Delta^\perp$ is in fact orthogonal to (AB), so that $\alpha = 30°$ and $\cos(\alpha) = \frac{\sqrt{3}}{2}$. In particular, note that $8\cos(\alpha) = \sqrt{48} < 7 = 8-1$, and thus that $24\cos(\alpha) < 21 = 24-3$. In particular, let $k = 4m-n$ be the number of vertices we have to remove to go from a $(4m)$-gon to an n-gon. We just proved above that there exist $7k-1$ points $E_1, \dots, E_{7k-1}$ such that

- $C_{4k}E_1 = E_1E_2 = \dots = E_{7k-1}A_{4k}$;

- the vertices $E_1, \dots, E_{7k-1}$ belong to the polygon $C_{4k}C_{4k-1}\dots C_1BA_1A_2\dots A_{4k}$;
- the polygon $C_{4k}E_1, \dots, E_{7k-1}A_{4k}$ is convex.

Then, the n-gon that we wanted to build is the n-gon

$$\mathcal{P}_n = C_{4k}E_1E_2\dots E_{7k-1}A_{4k}A_{4k+1}\dots A_{m-1}CA'_{m-1}A'_{m-2}\dots A'_1DC'_1C'_2\dots C'_{m-1}AC_{m-1}C_{m-2}\dots C_{4k+1}.$$

Indeed, each diagonal $[A_iA'_{m-i}]$ is obtained from the diagonal $[BC]$ by a rotation of center A and angle $\frac{i}{m}60°$ clockwise. Similarly, each diagonal $[C_iC'_{m-i}]$ is obtained from the diagonal $[AB]$ by a rotation of center B and angle $\frac{i}{m}60°$ counterclockwise.
Therefore, we know that $A_iA'_{m-i} = C_iC'_{m-i} = AC$ for all integers $i \leq m$. In particular:

- by construction, the n sides of $\mathcal{P}_n$ are isometric;
- $\mathcal{P}_n$ has at least $\mathbf{d} = 6m-16k+1$ distinct diagonals isometric to AC:
  - the $2(m-4k)$ diagonals AA_i and CC_i with $4k \leq i < m$;
  - the $2m$ diagonals AA'_i and CC'_i with $0 < i \leq m$;
  - the $2(m-4k)$ diagonals $A_iA'_{m-i}$ and $C_iC'_{m-i}$ with $4k \leq i < m$;
  - the diagonal AC itself.

We know that $k = 1$ if $n \equiv 3 \pmod 4$ and that $k = 3$ if $n \equiv 1 \pmod 4$. Moreover,

$$\mathbf{d} - n = 6m-16k+1-n = 6m-16k+1-(4m-k) = 2m-15k+1.$$

Therefore,

- if $n \equiv 1 \pmod 4$ and $n \geq 85$, then $k = 3$ and $m \geq 22$, so $\mathbf{d} - n \geq 44-45+1 \geq 0$;
- if $n \equiv 3 \pmod 4$ and $n \geq 29$, then $k = 1$ and $m \geq 7$, so $\mathbf{d} - n \geq 14-15+1 \geq 0$.

In all cases, $\mathcal{P}_n$ has indeed $\mathbf{d} \geq n$ isometric diagonals, which completes the proof. □

Overall, all these results give us a near-complete solution, as summarized here:

Theorem 9:
Let n be an integer:

- if $n \in \{7, 11, 13, 17, 19, 23, 29, 37, 41, 53, 61, 73\}$, then even having $n-1$ isometric sides and n isometric diagonals does not guarantee being regular;
- if $n \geq 9$ and $n \notin \{7, 11, 13, 17, 19, 23, 29, 37, 41, 53, 61, 73\}$, then even having n isometric sides and n isometric diagonals does not guarantee being regular.

■

In particular, although we have not *completely* solved the problem, we have only a finite number of cases to treat left. And, in these cases, we have already obtained partial results.

Corollary 10:
There exists only finitely many triples (s, d, n) such that having s isometric sides and d isometric diagonals forces an n-gon to be regular. ■

3 For which triples (s, d, n) must a convex and a regular n-gons with s isometric corresponding sides and d isometric corresponding diagonals be congruent?

We first identify triples (s, d, n) such that there exists an irregular convex and a regular n-gons with s isometric corresponding sides and d isometric corresponding diagonals. Then, we will show that all convex n-gons with enough isometric sides and diagonals must be congruent.

3.1 Triples (s, d, n) such that a convex and a regular n-gons with s sides and d diagonals isometric to their corresponding edges may not be congruent

Definition 11:
Consider two convex n-gons $\mathcal{P}$ and $\mathcal{P}'$. We say that an edge P_iP_j of the $\mathcal{P}$ — be it a side or a diagonal — that is not isometric to the corresponding edge $P'_iP'_j$ of $\mathcal{P}'$ is *missing*. ■

Proposition 12:
If $n \geq 4$, then there exists a regular n-gon $\mathcal{P}$ and an irregular convex n-gon $\mathcal{P}'$ such that $2n - 6$ diagonals of $\mathcal{P}$ are missing. ■

Proof of Proposition 12:

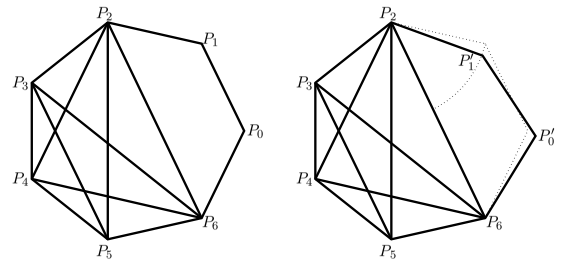


Figure 12: Non-congruent heptagons

We first consider a regular n-gon $P_0P_1P_2P_3P_4 \dots P_{n-1}$, then some point P'_1 inside the polygon $P_0P_1P_2P_{n-1}$ such that $P_1P_2 = P'_1P_2$. We finally define P'_0 to be the point such

that $P_0'P_1' = P_0'P_{n-1} = P_0P_1$, and such that the segment $[P_0P_2]$ and the line $(P_{n-1}P_1')$ intersect.
If P_1' is chosen close enough to P_1, then P_0' will be arbitrarily close to P_0, so that the n-gons $\mathcal{P} = P_0P_1 \dots P_{n-1}$ and $\mathcal{P}' = P_0'P_1' \dots P_{n-1}$ are convex. Moreover, they are not congruent, since $\mathcal{P}$ is regular but not $\mathcal{P}'$, whose angles are not all equal.
Finally, note that $2n-6$ diagonals are missing, which completes the proof. □

Proposition 13:
If $n \geq 3$, then there exists a regular n-gon $\mathcal{P}$ and an irregular convex n-gon $\mathcal{P}'$ such that 1 side and at most $n-3$ diagonals of $\mathcal{P}$ are missing. ■

Proof of Proposition 13:

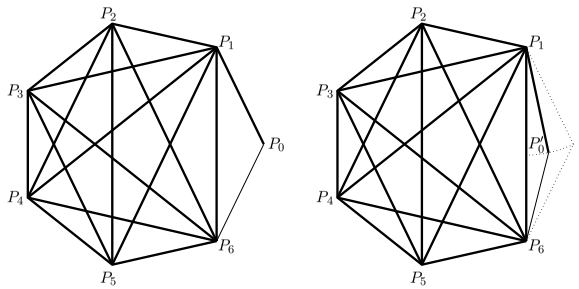


Figure 13: Non-congruent heptagons

We first consider a regular n-gon $P_0P_1P_2P_3P_4 \dots P_{n-1}$, then some point P_0' inside the triangle $P_0P_1P_{n-1}$ such that $P_0P_1 = P_0'P_1$.
The n-gons $\mathcal{P} = P_0P_1 \dots P_{n-1}$ and $\mathcal{P}' = P_0'P_1 \dots P_{n-1}$ are convex and not congruent, as their areas are different.
Finally, note that 1 side and $n-3$ diagonals are missing, which completes the proof. □

Proposition 14:
If $n \geq 4$, then there exists a regular n-gon $\mathcal{P}$ and an irregular convex n-gon $\mathcal{P}'$ such that 2 sides and at most $n-4$ diagonals of $\mathcal{P}$ are missing. ■

Proof of Proposition 14:

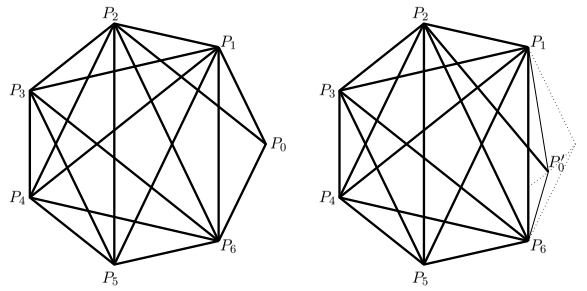


Figure 14: Non-congruent heptagons

We first consider a regular n-gon $P_0P_1P_2P_3P_4 \dots P_{n-1}$, then some point P_0' inside the triangle $P_0P_1P_{n-1}$ such that $P_0P_2 = P_0'P_2$.
The n-gons $\mathcal{P} = P_0P_1 \dots P_{n-1}$ and $\mathcal{P}' = P_0'P_1 \dots P_{n-1}$ are convex and not congruent, as their areas are different.
Finally, note that 2 sides and $n-4$ diagonals are missing, which completes the proof. □

3.2 Triples (s, d, n) such that a convex and a regular n-gons with s sides and d diagonals isometric to their corresponding edges must be congruent

Having found triples (s, d, n) that provide no guarantee at all for being congruent, we focus now on triples (s, d, n) that guarantee congruence. However, we do not directly do so, and first introduce the notion of *strong congruence*, then prove a lemma that will appear very useful, allowing us to consider congruence problems as graph problems.
We focus here on convex n-gons $\mathcal{P}$ and $\mathcal{P}'$ with s isometric corresponding sides and d isometric corresponding diagonals, such that:

- if no side is missing, at most $2n-7$ diagonals are missing;
- if 1 side is missing, at most $n-4$ diagonals are missing;
- if 2 sides are missing, at most $n-5$ diagonals are missing.

Definition 15:
We say that two convex n-gons $P_0P_1\dots P_{n-1}$ and $P'_0P'_1\dots P'_{n-1}$ are *strongly congruent* if the lengths P_iP_j and $P'_iP'_j$ are equal for all integers $i \neq j$. ■

Remark:
This definition implicitly depends on the order in which we consider the vertices P_i and P'_i. In particular, note that a triangle ABC may be strongly congruent to another triangle $A'B'C'$ but not to $B'C'A'$. Therefore, whenever we will speak of strongly congruent polygons, one should pay attention to the order in which the vertices are enumerated.

Lemma 16:
Let $\mathcal{P} = P_0P_1\dots P_{n-1}$ and $\mathcal{P}' = P'_0P'_1\dots P'_{n-1}$ be convex n-gons, and I the collection of sets $\{P_{s_1}, P_{s_2}, \dots, P_{s_k}\} \subseteq \{P_0, P_1, \dots, P_{n-1}\}$ such that $P_{s_1}P_{s_2}\dots P_{s_k}$ is strongly congruent to $P'_{s_1}P'_{s_2}\dots P'_{s_k}$ — with $s_1 < s_2 < \dots s_k$.
Then:

- for every set $S \in I$ and every subset T of S, $T \in I$;
- for all $u, v, w \in \{P_0, P_1, \dots, P_{n-1}\}$, if $\{u, v\}, \{v, w\}, \{u, w\} \in I$, then $\{u, v, w\} \in I$;
- for all sets $A, B \in I$ such that $|A \cap B| \geq 2$, $A \cup B \in I$.

■

Proof of Lemma 16:
The first two assertions are obvious, and therefore we focus on proving the third one. Then, since it is enough for us to prove that $P_uP_v = P'_uP'_v$ whenever $P_u \in A$ and $P_v \in B$, we can focus on the special case where $A = \{P_s, P_t, P_u\} \in I$ and $B = \{P_s, P_t, P_v\} \in I$.
In that case, $\widehat{P_sP_tP_u} = \widehat{P'_sP'_tP'_u}$ and $\widehat{P_sP_tP_v} = \widehat{P'_sP'_tP'_v}$. Since $\mathcal{P}$ and $\mathcal{P}'$ are convex, it follows that $\widehat{P_vP_tP_u} = \widehat{P_sP_tP_u} + \widehat{P_sP_tP_v} = \widehat{P'_sP'_tP'_u} + \widehat{P'_sP'_tP'_v} = \widehat{P'_vP'_tP'_u}$.
Then, since $P_vP_t = P'_vP'_t$ and $P_uP_t = P'_uP'_t$, it follows that $P_uP_v = P'_uP'_v$, which completes the proof.

□

Lemma 17:
Let I be the set described in Lemma 16. The biggest element X of I is a set whose size $|X|$ verifies the following inequality :

$$(n - |X|)(|X| - 1) \leq 2n - 5.$$

■

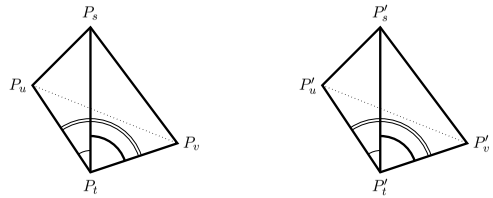


Figure 15: Congruent polygons

Proof of Lemma 17:
Suppose that some vertex $P_v \notin X$ belongs to 2 distinct edges — sides or diagonals — P_vP_s and P_vP_t such that $P_s, P_t \in X$ and $\{P_s, P_v\}, \{P_t, P_v\} \in I$. Then, Lemma 16 indicates that $\{P_s, P_t\} \in I$, that $\{P_s, P_t, P_v\} \in I$ and thus that $X \cup \{P_v\} \in I$, which is impossible since X is the biggest element of I.
Therefore, each vertex $P_v \notin X$ belongs to at most 1 edge P_vP_s such that $P_s \in X$. In particular, P_v belongs to at least $|X| - 1$ missing edges P_vP_t with $P_t \in X$. Since $n - |X|$ vertices do not belong to X and since the edges mentioned above must be pairwise different, it follows that at least $(n - |X|)(|X| - 1)$ edges are missing.
Finally, note that at most $2n - 5$ edges are missing:

- if no side is missing, then at most $2n - 7$ diagonals are missing;
- if 1 side is missing, then at most $n - 4$ diagonals are missing;
- if 2 sides at least are missing, then at most $n - 5$ diagonals are missing.

It follows that $(n - |X|)(|X| - 1) \leq 2n - 5$. □

Proposition 18:
If $n \geq 9$, then $|X| \geq n - 2$. ■

Proof of Proposition 18:
If $n \geq 9$, then $2n - 5 \leq 3n - 15 < 3n - 12$. Therefore, Lemma 17 indicates that $(n - |X|)(|X| - 1) < 3n - 12$, i.e. that

$$(n - |X|)(|X| - 1) - 3n + 12 = (n - 3 - |X|)(|X| - 4) < 0.$$

Suppose now that $|X| < 4$. The polygon $\mathcal{P}$ has $\frac{n(n-1)}{2}$ edges, among which at most $2n - 5$ are missing. Therefore, since each edge contains exactly 2 vertices of $\mathcal{P}$, there must exist some vertex P_u of $\mathcal{P}$ such that the set $\mathcal{V} = \{P_v : P_uP_v = P'_uP'_v\}$ is of size at least $\left\lceil \frac{n(n-1)-2(2n-5)}{n} \right\rceil \geq n - 5$.

Now, let $\mathcal{C}$ be the collection of all sets $S \subseteq \{P_0, P_1, \dots, P_{n-1}\} \backslash \{P_u\}$ such that $\{P_u\} \cup S \in I$. Since $|X| < 4$, the elements of $\mathcal{C}$ are all of size at most 2.
However, Lemma 16 indicates that, if $S, S' \in \mathcal{C}$ intersect each other, then $S \cup S' \in \mathcal{C}$. In addition, by definition of $\mathcal{V}$, we know that $\{P_v\} \in \mathcal{C}$ for every element P_v of $\mathcal{V}$. Therefore, the elements of $\mathcal{C}$ that are maximal for the inclusion relation form a partition of $\mathcal{V}$, and if S, S' are two such elements, we know that the edge $P_s P_{s'}$ is missing whenever $P_s \in S$ and $P_{s'} \in S'$.
If the partition is composed of k sets of size 2 and $|\mathcal{V}|-2k$ singletons, then exactly k edges are not missing among those whose endpoints are in $\mathcal{V}$ — these edges not missing are the edges $P_v P_w$ such that $\{P_v, P_w\}$ is a maximal element of $\mathcal{S}$ for the inclusion relation. In addition, remember that, by definition of P_u and of $\mathcal{V}$, each of the $n-|\mathcal{V}|$ vertices outside of $\mathcal{V}$ belongs to at least $n-1-|\mathcal{V}|$ missing edges. Therefore, at least $\frac{(n-|\mathcal{V}|)(n-1-|\mathcal{V}|)}{2}$ missing edges do not have both their endpoints in $\mathcal{V}$.
Overall, and since $2k \leq |\mathcal{V}|$, at least

$$\frac{(n-|\mathcal{V}|)(n-1-|\mathcal{V}|)}{2} + \frac{|\mathcal{V}|(|\mathcal{V}|-1)}{2} - k \geq \frac{n(n-1)}{2} + |\mathcal{V}|^2 - \frac{2n+1}{2}|\mathcal{V}| = f_n(|\mathcal{V}|)$$

edges are missing, where $f_n(x) = \frac{n(n-1)}{2} + x^2 - \frac{2n+1}{2}x$.
Since $f_n'(x) = \frac{4x-(2n+1)}{2}$, we know that $f_n(|\mathcal{V}|) \geq f_n\left(\frac{2n+1}{4}\right)$. Therefore, $f_n\left(\frac{2n+1}{4}\right) \leq 2n-5$. However, note that

$$f_n\left(\frac{2n+1}{4}\right) = \frac{4n^2-12n-1}{16} = (2n-5) + \frac{(n-2)(n-9)}{4} + \frac{7}{16}.$$

Hence, we must have $(n-2)(n-9) < 0$, which is impossible since $n \geq 9$.
Consequently, we know that $|X| \geq 4$, and even — based on the first inequality in this proof — that $|X| \geq n-2$. □

Theorem 19:
If $n \geq 9$, then the two n-gons $\mathcal{P}$ and $\mathcal{P}'$ are congruent. ■

Proof of Theorem 19:
Our goal is to prove that $|X| = n$ as soon as $|X| \geq n-2$.
First, we know that only those edges with at least one endpoint outside of X may be missing. Second, we also know that at least $(n-|X|)(|X|-1)$ edges must be missing.
We distinguish now 2 cases:

- If $|X| = n-2$, then at least $2n-6$ edges must be missing. Therefore, we know that at least 2 sides are missing, then that at most $n-5$ diagonals are missing, and therefore that at least $n-1$ edges must be missing. However, at most 4 edges do not have both their endpoints outside of X, so that at most 4 edges may be missing.

  Since $n \geq 9$, this is impossible.

- If $|X| = n-1$, consider the only vertex $P_v \notin X$, and the sides $P_s P_v$, $P_t P_v$ it belongs to. Since $P_v \notin X$, at least one of $P_s P_v$ and $P_t P_v$ must be missing; without loss of generality, we suppose that this is the case of $P_s P_v$.

  If $P_t P_v$ is missing as well, then exactly 2 sides are missing, and at most $n-5$ diagonals may be missing; if $P_t P_v$ is not missing, then exactly 1 side is missing, and at most $n-4$ diagonals are missing. Therefore, in all cases, at most $n-3$ edges are missing.

  Since at least $n-2$ edges must be missing, this is impossible as well.

Since Proposition 18 already shows that $|X| \geq n-2$, we have proved that $|X| = n$, i.e. that $\mathcal{P}$ and $\mathcal{P}'$ are congruent. □

3.3 Conclusion

Theorem 20:
Whenever $n \geq 4$, there exists a regular n-gon $\mathcal{P}$ and an irregular convex n-gon $\mathcal{P}'$ with s isometric corresponding sides and d isometric corresponding diagonals, with either:

- $s = n$ and $d \leq \frac{(n-4)(n-3)}{2}$;
- $s = n-1$ and $d \leq \frac{(n-2)(n-3)}{2}$;
- $s \leq n-2$ and $d \leq \frac{(n-4)(n-3)}{2} + 1$.

Conversely, whenever $n \geq 9$, a two convex n-gons $\mathcal{P}$ and $\mathcal{P}'$ with s isometric corresponding sides and d isometric corresponding diagonals must be congruent as soon as either:

- $s = n$ and $d > \frac{(n-4)(n-3)}{2}$;
- $s = n-1$ and $d > \frac{(n-2)(n-3)}{2}$;
- $s \leq n-2$ and $d > \frac{(n-4)(n-3)}{2} + 1$.

■

Proof of Theorem 20:
There are $\frac{n(n-3)}{2}$ diagonals in a n-gon. Therefore, the first part of Theorem 20 is proved by Propositions 12, 13 and 14, while the second part of Theorem 20 is proved by Theorem 19. □

4 Must these convex pentagons be congruent?

4.1 5 corresponding sides and 3 corresponding diagonals have the same length

Theorem 21:
If two convex pentagons have 5 corresponding isometric sides and 3 corresponding isometric diagonals, these pentagons are congruent. ■

To prove this theorem, we first introduce a notion that is slightly stronger than just being congruent, then prove a lemma that we will use both here and later in the document.

Proof of Theorem 21:
Let $\mathcal{P} = P_0P_1P_2P_3P_4$ and $\mathcal{P}' = P'_0P'_1P'_2P'_3P'_4$ be pentagons as in Theorem 21, and set I the set described in Lemma 16.
A pentagon has 5 diagonals, and therefore there must be 2 diagonals in $\mathcal{P}$ that share a vertex and that are isometric to their corresponding diagonals. Thus, without loss of generality, we assume that these diagonals are P_0P_2 and P_0P_3. This means that

$$\{0,1\},\{1,2\},\{2,3\},\{3,4\},\{0,4\},\{0,2\},\{0,3\} \in I.$$

Therefore, by Lemma 16, $\{0,1,2\},\{0,2,3\},\{0,3,4\} \in I$, and even $\{0,1,2,3,4\} \in I$, which completes the proof.

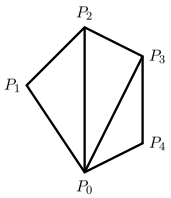


Figure 16: Isometric segments in the pentagon

□

4.2 4 corresponding sides and 4 corresponding diagonals have the same length

Theorem 22:
If two convex pentagons have 4 corresponding isometric sides and 4 corresponding isometric diagonals, these pentagons are congruent. ■

Proof of Theorem 22:
Let $\mathcal{P} = P_0P_1P_2P_3P_4$ and $\mathcal{P}' = P'_0P'_1P'_2P'_3P'_4$ be such pentagons, and I the set described in Lemma 16. Without loss of generality, we assume that $P_iP_{i+1} = P'_iP'_{i+1}$ when $0 \leq i \leq 3$. Moreover, there is at most one diagonal not isometric to its corresponding diagonal.
Therefore, and since P_4P_0 is not a diagonal, at least one of the vertices P_0 and P_4 has its 2 diagonals isometric to their corresponding diagonals. Without loss of generality, we assume that P_0 is such a vertex. This means that $P_0P_2 = P'_0P'_2$ and $P_0P_3 = P'_0P'_3$ or, in other words, that

$$\{0,1\},\{1,2\},\{2,3\},\{3,4\},\{0,2\},\{0,3\} \in I.$$

Therefore, by Lemma 16, $\{0,1,2\},\{0,2,3\} \in I$, which implies that $\{0,1,2,3\} \in I$ and even that $\{1,3\} \in I$.
Then, either $\{1,4\} \in I$ or $\{2,4\} \in I$. In the first case — respectively, in the second case — $\{1,3,4\} \in I$ — respectively, $\{2,3,4\} \in I$ — and thus $\{0,1,2,3,4\} \in I$, which completes the proof.

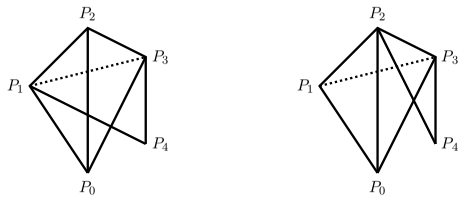


Figure 17: Isometric segments in the pentagon

□

4.3 5 corresponding sides and 2 corresponding diagonals have the same length

Theorem 23:
If two convex pentagons have 5 corresponding isometric sides and 2 corresponding isometric diagonals, these pentagons are congruent. ■

Proof of Theorem 23:
Let $\mathcal{P} = P_0P_1P_2P_3P_4$ and $\mathcal{P}' = P'_0P'_1P'_2P'_3P'_4$ be such pentagons, and I the set described in Lemma 16.
We distinguish 2 cases, depending on whether the 2 diagonals not missing have a common vertex.

1. If they have no common vertex, we assume, without loss of generality, that these diagonals are P_0P_2 and P_1P_3. Then,

   $$\{0,1\},\{1,2\},\{2,3\},\{0,2\},\{1,3\} \in I.$$

   Thus, by Lemma 16, $\{0,1,2\},\{1,2,3\} \in I$. Hence, $\{0,1,2,3\} \in I$, and even $\{0,3\} \in I$: we are in fact in the second case.

2. If they have a common vertex, we assume, without loss of generality, that these diagonals are P_0P_2 and P_0P_3. Then,

   $$\{0,1\},\{1,2\},\{2,3\},\{3,4\},\{0,4\}\{0,2\},\{0,3\} \in I.$$

   Thus, by Lemma 16, $\{0,1,2\},\{0,2,3\},\{0,3,4\} \in I$. Hence, $\{0,1,2,3,4\} \in I$, which completes the proof.

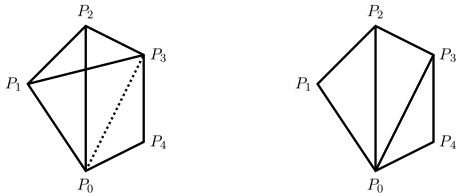


Figure 18: Isometric segments in the pentagon

□

5 For which triples (s,d,n) must two convex n-gons with s isometric corresponding sides and d isometric corresponding diagonals be congruent?

Theorem 20 still applies here, as all regular n-gons are convex. In particular, each triple (s,d,n) that forces convex n-gons to be congruent forces, *a fortiori*, a regular and a convex n-gon to be congruent, while the converse direction is false *a priori*.

However, we have not yet found triples (s,d,n) that would force a regular and a convex n-gons to be congruent but not two convex n-gons in general. Therefore, if such triples (s,d,n) exist, Theorem 20 proves that we must have $n \leq 8$, as it provides a complete characterization of the case $n \geq 9$, which does not depend on whether we choose one regular n-gon.

3 Présentation des différentes olympiades

Créée en 1998, l'Association Animath vise à développer les activités mathématiques périscolaires, qu'il s'agisse des clubs de mathématiques, des compétitions, de la culture mathématique ou encore des journées filles pour encourager les filles à rivaliser avec les garçons en mathématiques et dans les études scientifiques plus généralement.

Les compétitions sont un centre d'intérêt important d'Animath : tout d'abord les Olympiades et leur préparation dont on vous parlera plus longuement après cette introduction. Animath organise chaque année deux stages olympiques dont celui-ci. Mais également les clubs olympiques (à Lyon, Orsay, Strasbourg notamment). Cette année, Bodo Lass n'est pas présent pour présenter son club de mathématiques discrètes, à Lyon, mais celui-ci ne s'adresse pas uniquement aux Lyonnais : certains viennent de très loin pour suivre, un dimanche sur deux, l'enseignement de Bodo Lass et ses collaborateurs (Theresia Eisenkoelbl...). Citons en outre les concours de projets scientifique, comme C.Génial, portant sur toutes les disciplines scientifiques, et où plusieurs projets mathématiques ont été primés cette année. Enfin, les tournois ITYM et TFJM dont on vous a parlé mercredi dernier.

Mais les stages ne sont pas tous olympiques. En particulier, les stages Math C2+ sont davantage orientés vers une initiation à la recherche, en partenariat avec des universitaires notamment. Ils ont lieu en dehors des temps scolaires, pendant des week-ends ou des petites vacances ; en dehors des lieux scolaires, par exemple à l'université ; sur un thème non scolaire : ce n'est ni du soutien ni de la préparation à une compétition. Signalons également le tutorat pour les lycéens, qui s'adresse essentiellement aux élèves des banlieues défavorisées, ainsi que plusieurs séminaires sur certains sujets extra-scolaires et non orientés compétitions. Enfin, l'école d'été qui s'appelle actuellement MOMISSS mais a déjà changé de nom, où des mathématiciens prestigieux présentent des cours de haut niveau à des lycéens de première à math spé, sélectionnés sur dossier.

Animath vous propose également de rencontrer des mathématiciens professionnels au cours de « promenades mathématiques » coorganisées par la Société Mathématique de France. Des universitaires viennent dans des classes de lycées et collèges pour exposer un sujet de recherche. Le cycle de quatre conférences « un texte, un mathématicien », chaque année à la Bibliothèque de France, accueille un grand public de plusieurs centaines de personnes, parmi lesquelles des classes de lycée qui ont été préparés à la conférence par une promenade mathématique préalable dans leur classe sur ce même sujet.

Mais pour prouver que les mathématiques ne servent pas seulement à devenir chercheur ou enseignant en mathématiques, Animath invite également des professionnels à expliquer en quoi les mathématiques leur servent dans leurs diverses professions. C'est le programme « Les maths, ça sert ! ».

Enfin, Animath a pour ambition de chapeauter les diverses activités mathématiques périscolaires, auxquelles travaillent différentes autres associations partenaires. C'est aujourd'hui une grosse association, avec trois salariées, car c'est elle qui administre la subvention de 3 millions d'euros sur cinq ans accordée récemment pour financer des projets visant l'égalité des chances. Vous aurez toutes informations sur le site d'Animath ainsi que celui de Cap'Maths. De manière très générale, nous nous efforçons de mettre en ligne le maximum d'informations et de liens sur notre site vous permettant de suivre tout ce qui se passe en France concernant les activités mathématiques périscolaires : consultez régulièrement notre site **www.animath.fr** pour vous tenir informé.

Les Olympiades Académiques de Mathématiques

Compétition française créée en 2001, les Olympiades Académiques de Mathématiques s'adressent à tous les lycéens de première, et pas seulement ceux des sections scientifiques : il y a eu 17 331 candidats en 2013, dont 3 000 de l'étranger (lycées français à l'étranger, dans 70 pays). La proportion de filles était 36%.

L'épreuve dure quatre heures et comprend quatre exercices, chacun structuré en plusieurs questions de difficultés inégales, contrairement aux Olympiades Internationales où un problème consiste en une seule question brève. Les premières questions d'un exercice sont faciles et en principe faisables par tout le monde. Deux exercices sont nationaux (identiques quelle que soit l'Académie), deux autres sont académiques (choisis par l'Académie et différents d'une Académie à l'autre). L'énoncé précise quels exercices sont nationaux.

L'épreuve a lieu en mars. Chaque Académie établit son propre classement et organise sa propre remise des prix, à des dates diverses. Puis elle envoie au jury national quelques unes de ses meilleures copies. Début mai, le jury national examine les copies ainsi reçues en prenant en compte uniquement les deux exercices nationaux. Il élabore son propre classement, indépendant du classement académique (un élève cinquième dans son Académie peut être second au palmarès national par exemple, s'il a moins bien réussi un exercice académique). Enfin, les lauréats nationaux sont convoqués pour une cérémonie officielle de remise des prix au Ministère de l'Éducation Nationale, début juin, parfois en présence du Ministre. C'est Animath qui gère les prix décernés aux lauréats ainsi que l'organisation matérielle de cette cérémonie (remboursement des frais de voyage notamment).

Plus récemment, à l'initiative de l'Académie de Versailles (Monsieur Michalak), une autre Olympiade a été créée pour les collégiens de quatrième. Cette Olympiade n'existe que dans quelques Académies : Versailles, Rouen, Amiens, Lyon, Corse, et elle peut encore s'étendre. Les palmarès de cette Olympiade sont pris en compte dans le repérage que nous organisons (élèves à qui l'on propose le test de sélection du stage olympique).

La plupart des élèves de première à qui l'on a proposé le test de sélection pour le présent stage olympique ont été repérés grâce aux palmarès académiques et nationaux de l'Olympiade Académique. Mais nous n'avions pas tous les palmarès Académiques. Nous avons aussi utilisé les palmarès d'autres compétitions.

Olympiades internationales

La France participe à quatre compétitions olympiques internationales :
- Les Olympiades Internationales de Mathématiques (IMO)
- Les Olympiades Balkaniques de Mathématiques (BMO)
- Les Olympiades Balkaniques de Mathématiques Junior (JBMO)
- Les Olympades Européennes de Mathématiques pour Filles (EGMO)

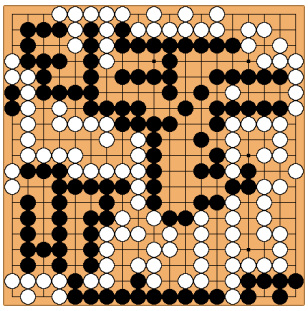
Pour plus d'informations, nous renvoyons aux liens suivants sur le site d'Animath :
- http://www.animath.fr/spip.php?rubrique1
- http://www.animath.fr/spip.php?rubrique296

4 Conférence : La théorie des jeux combinatoires (Louis)

Les tranparents de la conférence commencent à la page suivante.

Pourquoi une théorie ?

- Une position d'un jeu combinatoire est soit gagnante, soit perdante, soit nulle.
- Un ordinateur peut déterminer la nature d'une position.



Jeux combinatoires ?

Deux types de théorie des jeux

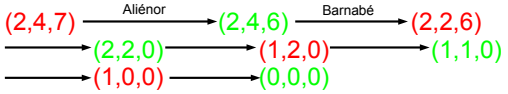
- Théorie « classique » : jeux à information partielle, par exemple jeux de dés, ou pierre-feuille-ciseau. Crée par John Nash.
- Théorie combinatoire : jeux à information totale, par exemple morpion, échecs, go. Crée par John Conway (et autres).

Non.

- Les problèmes de jeux sont TRÈS difficiles d'un point de vue algorithmique.
- La théorie sert à simplifier ces algorithmes, ou à prouver que ce n'est pas possible .

Exemples de jeux impartiaux

Nim : se joue avec des tas de jetons, à son tour un joueur enlève d'une pile un certain nombre de jetons.



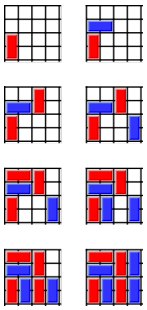
Aliénor gagne !

Définition

Nous allons nous restreindre aux jeux

- Où deux joueurs (disons Alice et Bob) jouent successivement
- Finis (dont l'arbre des possibilités est fini)
- Où l'on perd si l'on ne possède plus de coups légaux
- Impartiaux : quelle que soit la position, Alice à le droit de jouer les mêmes coups que Bob .

Cram



Bowling (Kayles)

Jeu des carrés

- C'est Nim à un seul tas, en enlevant à chaque fois un nombre carré de jetons.

  G: gagnant pour celui dont c'est le tour

  P: perdant pour celui dont c'est le tour

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P	G	P		G	P				G							G	

Jeu des carrés

- C'est Nim à un seul tas, en enlevant à chaque fois un nombre carré de jetons.

  G: gagnant pour celui dont c'est le tour

  P: perdant pour celui dont c'est le tour

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P	G			G					G							G	

Jeu des carrés

- C'est Nim à un seul tas, en enlevant à chaque fois un nombre carré de jetons.

  G: gagnant pour celui dont c'est le tour

  P: perdant pour celui dont c'est le tour

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P	G	P	G	G	P	G	P		G	P	G			G		G	

Jeu des carrés

- C'est Nim à un seul tas, en enlevant à chaque fois un nombre carré de jetons.

  G: gagnant pour celui dont c'est le tour

  P: perdant pour celui dont c'est le tour

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P	G	P	G	G	P	G			G		G			G		G	

Et Nim ?

- Une position à un tas non vide est G.
- Une position à deux tas non vide est G si et seulement si les tailles sont différentes : on égalise les tas, puis on joue symétriquement.
- (1,2,3) est P.
- (50,45,20) est G, le seul coup gagnant étant vers (50,38,20).

Jeu des carrés

- C'est Nim à un seul tas, en enlevant à chaque fois un nombre carré de jetons.

  G: gagnant pour celui dont c'est le tour

  P: perdant pour celui dont c'est le tour

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P	G	P	G	G	P	G	P	G	G	P	G	P	G	G	P	G	P

- Les positions perdantes sont précisément celles de nimbre *0 ! En effet :

- Quand on joue dans une position de nimbre *0, on change le nimbre
- Dans une postion de nimbre différent de *0, il existe toujours un coup vers une position de nimbre *0.

- On associe à chaque position un nombre, appelé son « nimbre » en faisant des « additions en binaire sans retenue ».

  Par exemple

```
50 =  1 1 0 0 1 0
45 =  1 0 1 1 0 1
20 =    1 0 1 0 0
-----------------
      0 0 1 0 1 1 = 11
```

- Le nimbre de (50,45,20) sera donc 11. On le note *11.

• Autre exemple : Soustraction(1,2,3,4).

- C'est le jeu de Nim où on ne peut pas retirer plus de 4 jetons.
- Les positions où 5 divise les tailles de tas sont perdantes.
- On regarde les tailles des tas modulo 5, et on joue comme dans le vrai jeu de Nim
- Une subtilité : un coup peut augmenter la taille d'un tas. Ça ne change rien puisque la partie est finie.

Par exemple, N(50,38,20) = *0. Si Aladdin est dans cette position et joue vers (24,38,20), alors

```
24 =    1 1 0 0 0
38 =  1 0 0 1 1 0
20 =    1 0 1 0 0
-----------------
    1 0 1 0 1 0 = 42
```

Pour annuler cette somme, il faut remplacer 100110 par 1100. Bergamote répond donc en jouant vers (24,12,20), de nimbre *0.

Nombre de Grundy

- On le définit récursivement
- Le nombre de Grundy du jeu où personne ne peut jouer est 0.
- Celui d'un jeu quelconque est le mex des nombres de Grundy des positions accessibles depuis ce jeu.

Mex

- Le mex d'un ensemble (abbréviation de minimum exclu), est l'entier minimal n'appartenant pas à cet ensemble.
- Par exemple :

  mex(3,0,4,2,8,11) = 1

  mex(6,8,2,0,1,7,18,42,3,57) = 4

Nombre de Grundy et nimbre

- Par récurrence, pour le jeu de Nim à un tas, G(n) = n, or N(n) = *n.
- Le symbole ⊕ désigne « l'addition en binaire sans retenues ». Par récurrence, G(m,n) = m⊕n, or par définition N(m,n) = *m⊕n.
- Ainsi, le nombre de Grundy est une généralisation du nimbre.

Exemple sur le jeu des carrés

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	1	0	1	2	0	1	0	1	2	0	1	0	1	2	0	1	0

- On ne le voit pas sur ce court exemple, mais la suite est très irrégulière. Elle peut prendre des valeurs plus grandes : pour 25 on obtient 3.
- On remarque que les positions perdantes sont celles de nombre de Grundy 0.

- Quand on sait jouer à Nim, on sait donc jouer à tout jeu impartial !

Comment jouer un jeu impartial ? Exemple du jeu des carrés.

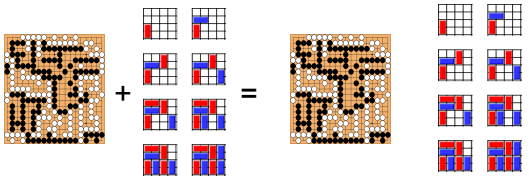
- Partons de la position (14,13,7,12,1)
- On calcule les nombres de Grundy de chaque tas : (2,1,0,0,1)
- On cherche un coup gagnant dans le jeu de Nim correspondant : il n'y en a qu'un :

  $(2,1,0,0,1) \longrightarrow (0,1,0,0,1)$

- On choisit son coup de telle sorte qu'il fasse le même effet sur les nombres de Grundy : par exemple $(14,13,7,12,1) \longrightarrow (5,13,7,12,1)$

Somme de jeux.

- C'est le jeu obtenu en mettant deux positions côte-à-côte. Par exemple



- Dans les slides suivantes, nous ne nous restreindront plus aux jeux impartiaux.

- Soit G un jeu quelconque, et X un jeu tel que le joueur jouant en second puisse toujours gagner X (i.e., si Antoine commence Bodo gagne, et si Bodo commence Antoine gagne).

- Alors G+X aura toujours la même issue que G ! Par exemple, si Antoine gagne G en commençant, il gagne G+X en commençant par le coup gagnant dans G, puis en jouant toujours dans le même jeu que Bodo.

Cette somme est « gentille »

- Elle est commutative : G + H = H + G
- Elle est associative : (G + H) + I = G + (H + I)

Cela permet d'étendre cette notion à un nombre quelconque de jeux, par exemple un jeu de Nim à k tas est la somme de k jeux de Nim à 1 tas.

Opposé d'un jeu

Définition : L'opposé du jeu G, noté - G, est le jeu obtenu en renversant la position de Alexandra et Béatrice .

G = 

- G = 

Égalité de jeux

Définition : On dit que deux jeux X et Y sont égaux si, quel que soit le jeu G, G+X a la même issue que G+Y.

- Par exemple, si le second joueur gagne toujours X, X sera égal au jeu vide (ou personne n'a le droit de jouer). On note le jeu vide ***0.***

Proposition : X = Y $\Leftrightarrow$ X – Y = ***0***

Démonstration :

- Si X = Y, X - Y a même issue que Y – Y, donc X-Y = ***0***
- Si X-Y = ***0***, soit G un jeu quelconque, G + Y a même issue que G + Y + (X – Y), qui est égal à G + X + (Y – Y), donc a même issue que G+X.

Proposition : G + (- G) = ***0***

Démonstration : Le second joueur joue de façon symétrique.

On remarque que si G est un jeu impartial, alors G = -G.

Théorème de Sprague-Grundy

Nous venons de prouver :

Théorème : Tout jeu impartial est égal à un jeu de Nim.

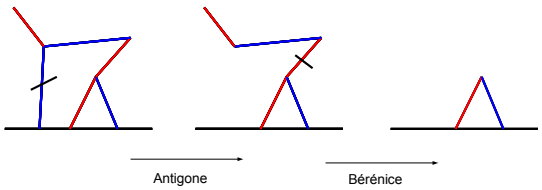
Retour à Nim

- Soit G un jeu impartial de nombre de Grundy n.
- Soit N le jeu de Nim à un tas à n jetons.

D'après notre discussion sur les jeux impartiaux, le jeu G – N = G + N est gagnant pour le second joueur. Donc G – N = 0. Donc G = N !

Hackenbush

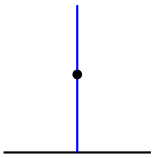
- On joue sur un buisson. À son tour, Antigone découpe une branche bleue, et Bérénice découpe une branche rouge. On enlève ensuite toutes les branches non reliées au sol.



La suite ?

- Trouver des méthodes pour calculer les nombres de Grundy. La récurrence avec le mex est très puissante, mais pas suffisante. Par exemple, si G est un jeu du même style que « bowling », et G(k) la suite des nombres de Grundy des positions à k quilles consécutives. On conjecture que cette suite est périodique.
- Traiter le jeu de « qui perd gagne ».

- On vérifie que ***1*** + ***1*** est égal au jeu suivant, que l'on appellera ***2*** :



Ainsi, on appellera ***n*** le jeu à une tige à n branches bleues, et -***n*** le jeu à une tige à n branches rouges.

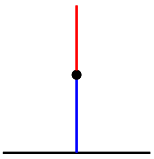
- On appelle ***1*** le jeu ou il n'y a qu'une branche bleue et ***-1*** son opposé.

1 =  ***-1*** = 

L'intuition derrière cette définition est que, dans le jeu ***1***, Anémone a un coup d'avance, et que dans le jeu ***-1*** Basile a un coup d'avance .

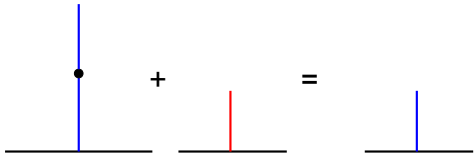
Jeu mystère

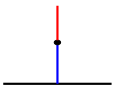
Que vaut

 ?

Jeux entiers

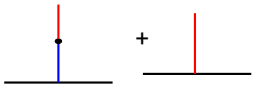
L'addition fonctionne bien sur les jeux entiers : le somme des jeux ***m*** et ***n*** est le jeu associé à l'entier m+n. Par exemple.



Revenons à G = 

Astérix gagne G quel que soit le joueur qui commence. Autrement dit, G > ***0***.

Par contre, c'est Bonemine qui gagne G – ***1,*** quel que soit le joueur qui commence, donc G < ***1***.

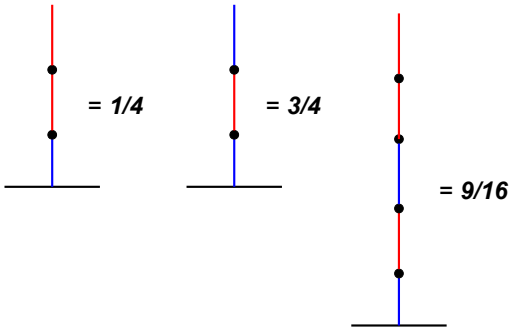
G - ***1*** = 

Comparaison de jeux

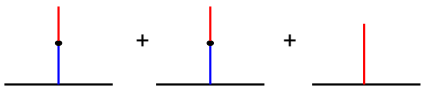
Définition : Soient G et H deux jeux. On dit que G ≤ H si, quel que soit le jeu X, l'issue de H+X est au moins aussi bonne que celle de G+X pour Alfred (qu'il commence ou non)

C'est équivalent au fait que H - G soit positif, c'est-à-dire au fait que Alfred gagne H – G en jouant en second.

On pourrait continuer :



- En fait, le second joueur gagne toujours le jeu G + G – ***1***



On décrète donc que G = ***½*** !

En un sens, Apollon a un demi coup d'avance dans G.

Rationnels et nimbres

- Ainsi, l ' « ensemble » des jeux contient celui des rationnels diadiques.
- Il contient aussi l'ensemble $*\mathbb{N}$ celui des jeux de nim, et l'addition des jeux coïncide, sur cet ensemble avec $\oplus$.
- On pourrait montrer que si N est un jeu de nim et G un rationnel strictement positif, on a N<G, on dit que les jeux de Nim sont infinitésimaux.

On pourrait montrer que :

- Chaque rationnel diadique correspond à une tige de Hackenbush,
- Réciproquement, que chaque position de Hackenbush correspond à un diadique,
- Que cette correspondance est compatible avec l'addition des rationnels.
- Il existe de nombreuses astuces facilitant le calcul de la valeur associée à une position donnée (mais le problème reste difficile).

Fin ?

- La théorie telle que présentée ici ne s'applique pas à de nombreux jeux populaires. Par exemple le go est un jeu à score, autorisant les répétitions de coup. Il faut trouver des astuces pour contourner cela.
- L' « ensemble » des jeux contient encore BEAUCOUP d'autres choses, dont de nombreux jeux intervenant dans de nombreux cas pratiques. La théorie est là pour étudier ces autres jeux, et regarder comment ils se comportent vis à vis de l'addition.

X. La Muraille

Une muraille de 127 exercices était affichée dans la salle commune. Les exercices 1 à 35 sont dits de NIVEAU 1. Les exercices 36 à 80 sont dits de NIVEAU 2. Les exercices au delà de 81 sont dits de de NIVEAU 3

Un exercice est décoré de n étoiles lorsque il est resté sans solution à la muraille de n stages.

Les élèves du groupe A cherchent les exercices de NIVEAU 1 (ou au-dessus). Les élèves du groupe B cherchent les exercices de NIVEAU 2 et les exercices étoilés de niveau NIVEAU 1 (ou au-dessus). Les élèves du groupe C cherchent les exercices de NIVEAU 3 et les exercices étoilés de niveau NIVEAU 2 (ou au-dessus). Les élèves du groupe D cherchent les exercices de NIVEAU 3 (mais pas au-dessus, vu qu'il n'y en a pas).

Une fois un exercice résolu, la solution devait être rédigée et donnée à une animatrice ou un animateur. La première solution correcte d'un exercice est reproduite dans ce polycopié. Il était possible de résoudre les exercices à plusieurs. Le but était d'avoir tout résolu à la fin du stage !

Tous les deux exercices résolus (individuellement ou bien par équipe d'au plus deux personnes), une glace est offerte !

À la fin du stage, quatre Grand Prix Mystère seront décernés aux quatre élèves ayant obtenu le plus de points en résolvant des exercices de la Muraille dans chacun des quatre groupes A, B, C, D.

À la fin du stage, un autre Grand Prix Mystère sera décerné à l'équipe (constituée d'au moins deux élèves et d'au plus quatre élèves) ayant obtenu le plus de points en résolvant des exercices de la Muraille.

BARÈME : Un exercice à x étoiles résolu rapporte $x + 1$ points (sauf pour les élèves du groupe B qui résolvent des exercices étoilés de NIVEAU 1 et les élèves du groupe C qui résolvent des exercices étoilés de NIVEAU 2, pour lesquels un exercice à x étoiles rapporte x points).

Exercice 1 Considérons 3 piles de jetons, contenant 51, 49 et 5 jetons. Une étape consiste à fusionner deux piles, ou à séparer en deux piles égales une pile contenant un nombre pair de jetons. Est-il possible d'obtenir, au bout d'un certain nombre d'étapes, 105 piles de 1 jeton ?

Exercice 2 (*) p filles et q garçons se mettent en cercle. On note a le nombre de paires de filles se tenant côte à côté, b le nombre de paires de garçons se tenant côte à côte. Montrer que $a - b = p - q$.

Exercice 3 (*) De combien de manières peut-on mettre 10 pièces de monnaie dont 5 sont identiques et 5 autres différentes dans 5 poches numérotées de 1 à 5 ?

Exercice 4 Soit ABC un triangle de centre de gravité G. On note A_1, B_1, C_1 les milieux respectifs des segments $[BC], [CA], [AB]$. La droite parallèle à BB_1 passant par A_1 coupe (B_1C_1) en F. Prouver que les triangles ABC et FA_1A sont semblables si, et seulement si, les quatre points A, B_1, G, C_1 sont cocycliques.

Exercice 5 Le nombre 10^{2013} est écrit au tableau. Alexandra et Béatrice jouent au jeu suivant à tour de rôle, où à chaque tour il est permis de faire l'une des deux opérations suivantes :

- remplacer un nombre x écrit au tableau par deux entiers $a, b > 1$ tels que $ab = x$.
- choisir deux nombres égaux x et y écrits au tableau, et effacer soit x, soit x et y.

Celle qui ne peut plus jouer a perdu.

Alexandra joue en premier. Est-elle sure de gagner ?

Exercice 6 Montrer qu'il existe une infinité de nombres premiers dont le dernier chiffre n'est pas 1.

Exercice 7 (*) Montrer que pour tout entier $n \geqslant 1$, $3^{6n} - 2^{6n}$ est divisible par 35.

Exercice 8 (*) Soit k un entier supérieur ou égal à 2. Trouver tous les entiers x et y tels que :

$$y^k = x^2 + x.$$

Exercice 9 (*) Soit $[EF]$ un segment inclus dans le segment $[BC]$ tel que le demi-cercle de diamètre $[EF]$ est tangent à $[AB]$ en Q et à $[AC]$ en P. Prouver que le point d'intersection K des droites (EP) et (FQ) appartient à la hauteur issue de A du triangle ABC.

Exercice 10 Soit $ABCD$ un carré, et $PQRS$ un petit carré placé à l'intérieur de $ABCD$ de telle sorte que les segments $[AP], [BQ], [CR], [DS]$ ne s'intersectent pas entre eux, et n'intersectent pas $PQRS$. Prouver que la somme des aires des quadrilatères $ABQP$ et $CDSR$ est égale à la somme des aires des quadrilatères $BCRQ$ et $DAPS$.

Exercice 11 Trouver tous les entiers a, b et m tels que

$$4a^b + 1 = m^2.$$

Exercice 12 (**) On considère un nombre fini de segments sur la droite réelle tels que, quels que soient deux de ces segments, ils aient un point commun. Montrer qu'il existe un point appartenant à tous ces segments.

Exercice 13 Montrer que $\sqrt{2}+\sqrt{5}+\sqrt{13}$ est irrationnel.

Exercice 14 Existe-t-il un polyèdre à 2013 faces dont toutes les faces soient des pentagones ?

Exercice 15 (*) On a un polyèdre convexe, dont les faces sont des triangles. Les sommets du polyèdre sont coloriés avec trois couleurs.

Montrer que le nombre de triangles dont les sommets ont trois couleurs distinctes est pair.

Exercice 16 Trouver tous les entiers strictement positifs n tels que $2^n + 12^n + 2011^n$ soit un carré parfait.

Exercice 17 (*) Soit n un entier naturel. À un stage de mathématiques, $2n+1$ élèves se réunissent, chacun étant muni d'un pistolet à eau. On suppose que les distances entre élèves sont deux à deux distinctes. À midi précises, chaque élève tire sur son plus proche voisin. Montrer qu'il existe au moins un élève qui restera sec.

Exercice 18 Trouver tous les nombres naturels n tels que $n^3 + 1 = 2n$.

Exercice 19 (*) Les nombres naturels $n_1, n_2, \ldots, n_{2012}$ satisfont l'équation

$$n_1^2 + \ldots + n_{2011}^2 = n_{2012}^2.$$

Montrer qu'au moins deux nombres sont pairs.

Exercice 20 Six amis, Alice, Bob, Céline, Damien, Elisabeth et Frédéric décident de nager un 30km en eau libre. Sachant qu'il peut y avoir éventuellement des ex-aequo, combien y a-t-il d'arrivées possibles ?

Exercice 21 Trouver les entiers strictement positifs a et b tels que $\frac{a^{2b+1}b-1}{a+1}$ et $\frac{b^a a+1}{b-1}$ soient des entiers.

Exercice 22 On considère $ab+1$ condylures (avec a, b des entiers positifs) telles que si l'on considère 2 quelconques d'entre eux, alors soit l'un descend de l'autre, soit ils n'ont aucune lien de parenté. Montrer que l'on peut en trouver $a+1$ qui descendent les uns des autres ou bien $b+1$ qui n'ont aucun lien de parentré entre eux.

Exercice 23 Soient m, n des entiers positifs. À quelle condition existe-t-il un entier positif N tel que pour tout entier $r \geqslant N$ il existe deux entiers positifs a et b tels que $r = am + bn$? Estimer la valeur minimale de N aussi précisément que possible.

Exercice 24 (*) Trouver tous les entiers naturels n tels que l'écriture décimale de n^2 se termine par n.

Exercice 25 (*) Soit $x_0, x_1, x_2, \ldots$ une suite de nombres réels. On dit que la suite $x_0, x_1, \ldots$ est convexe si :

$$\text{pour tout entier } n \geqslant 0, \frac{x_{n-1}+x_{n+1}}{2} \geqslant x_n$$

et qu'elle est log-convexe si :

$$\text{pour tout entier } n \geqslant 0, x_{n+1}x_{n-1} \geqslant x_n^2$$

On suppose que pour tout nombre réel $a > 0$, la suite $x_0, ax_1, a^2x_2^2, a^3x_3^3, \ldots$ est convexe. Prouver que la suite $x_0, x_1, \ldots$ est log-convexe.

Exercice 26 On considère des entiers naturels dont la somme vaut 2013. Quelle est la valeur maximale de leur produit ?

Exercice 27 (⋆) Soit ABC un triangle isocèle en C. On considère un point P sur le cercle circonscrit au triangle ABC situé entre A et B, tels que les segments $[AB]$ et $[PC]$ sont sécants. Soit D un point de la droite (PB) tel que les droites (CD) et (PB) soient perpendiculaires. Prouver que $PA + PB = 2 \cdot PD$.

Exercice 28 (⋆) Soient $x, y > 0$, et soit $s = \min(x, y + 1/x, 1/y)$. Quelle est la valeur maximale possible de s ? Pour quels x, y est-elle atteinte ?

Exercice 29 (⋆) Trouver les nombres premiers p pour lesquels il existe des entiers positifs x et y tels que :

$$x(y^2 - p) + y(x^2 - p) = 5p.$$

Exercice 30 (⋆⋆) On place $2n$ points dans le plans et on trace $n^2 + 1$ segments entre ces points.
Montrer que l'on peut trouver 3 points reliés deux à deux.

Exercice 31 (⋆) Soit $\mathcal{P} = A_1 \dots A_{2n}$ un $2n-$gone convexe dans le plan. Soit P un point intérieur à $\mathcal{P}$, non situé sur une diagonale. Prouver que P est contenu dans un nombre pair de triangles à sommets parmi les A_i.

Exercice 32 (⋆) Soit $n > 0$ un entier. On considère un entier A constitué de $2n$ chiffres qui sont tous des 4, et un entier B constitué de n chiffres, qui sont tous des 8. Prouver que l'entier $A + 2B + 4$ est un carré parfait.

Exercice 33 (⋆) Soit ABC un triangle isocèle en A tel que $\widehat{BAC} < 60°$. Les points D et E sont des points du côté $[AC]$ tels que $EB = ED$ et $\widehat{ABD} = \widehat{CBE}$. Soit O le point d'intersection des bissectrices des angles $\widehat{BDC}$ and $\widehat{ACB}$. Trouver la valeur de l'angle $\widehat{COD}$.

Exercice 34 (⋆) Trouver tous les entiers positifs a, b, c tels que

$$2^a 3^b + 9 = c^2.$$

Exercice 35 (⋆) Soit ABC un triangle dont tous les angles sont aigus. On note Γ son cercle circonscrit. On suppose que la tangente en A à Γ coupe la droite (BC) en un point P. Soit M le milieu de $[AP]$ et soit R le deuxième point d'intersection de la droite (BM) avec le cercle Γ. La droite (PR) recoupe le cercle Γ en S.

Prouver que les droites (AP) et (CS) sont parallèles.

Exercice 36 (⋆) Trouver tous les nombres naturels n tels que $n2^{n+1} + 1$ soit un carré parfait.

Exercice 37 (⋆) Soit ABC un triangle isocèle en A tel que $\widehat{BAC} = 20°$. Soit X le point sur le segment $[AB]$ avec $\widehat{XCA} = 20°$ et soit Y le point sur le segment $[AC]$ avec $\widehat{ABY} = 30°$.

Déterminer la valeur de l'angle $\widehat{CXY}$.

Exercice 38 (⋆) Considérons un polynôme :

$$f(x) = x^{2012} + a_{2011}x^{2011} + ... + a_1 x + a_0.$$

Albert Einstein et Homer Simpson jouent au jeu suivant. Tour à tour, ils choisissent un des coefficients a_0, a_1, ..., a_{2011}, et lui assignent une valeur réelle. Une fois qu'une valeur est assignée à un coefficient, elle ne peut plus être changée. C'est Albert qui commence. Le but d'Homer est de rendre $f(x)$ divisible par un polynôme $m(x)$, fixé à l'avance, et le but d'Albert est de l'en empêcher. Quel joueur à une stratégie gagnante si :

$$a) \quad m(x) = x - 2012 \qquad\qquad b) \quad m(x) = x^2 + 1?$$

(On rappelle que le polynôme $m(x)$ *divise* le polynôme $f(x)$ s'il existe un polynôme $g(x)$ tel que $f(x) = m(x) \cdot g(x)$).

Exercice 39 Considérons un triangle ABC tel que $AB = BC$ et $\widehat{ABC} = 80^\circ$. Soit P le point de l'intérieur de ABC tel que $\widehat{PAC} = 40^\circ$ et $\widehat{PCA} = 30^\circ$. Calculer l'angle $\widehat{BPC}$.

Exercice 40 (*) Soit $n > 2$ un entier naturel, T la transformation $\mathbb{R}^n \to \mathbb{R}^n, (x_1, \ldots, x_n) \mapsto (\frac{x_1+x_2}{2}, \frac{x_2+x_3}{2}, \ldots, \frac{x_{n-1}+x_n}{2}, \frac{x_n+x_1}{2})$. On part d'un $n-$uplet $(a_1, \ldots, a_n)$ d'entiers deux à deux distincts. Prouver que pour $k \in \mathbb{N}$ assez grand, $T^k(a_1, \ldots, a_n) \notin \mathbb{N}^n$.

Exercice 41 On considère un triangle acutangle ABC avec $\widehat{A} = 60^\circ$. Déterminer les points $M \in (AB)$ et $N \in (AC)$ qui minimisent la somme $|CM| + |MN| + |BN|$.

Exercice 42 Soit a et b deux entiers naturels non nuls. Montrer que a divise $b^{a!} - b^{2a!}$.

Exercice 43 On considère un cube constitué de 2013^3 petits cubes. On considère un plan perpendiculaire à une grande diagonale du cube et passant par son centre. Combien de petits cubes coupe-t-il ?

Exercice 44 (*) Soit P un point à l'intérieur d'un polygone régulier à n côtés tel que, pour tout côté du polygone, P se projette orthogonalement sur l'intérieur du côté. Ces n projections orthogonales partagent les n côtés du polygône en $2n$ segments. On numérote ces segments de 1 à $2n$, en commençant par un segment arbitraire, puis en tournant dans le sens direct le long du polygone. Prouver que la somme des longueurs des segments de numéros pairs est égale à la somme des longueurs des segments de numéros impairs.

Exercice 45 On sait que parmi 10 stagiaires quelconques, au moins 3 habitent dans la même ville. Prouver qu'au moins 15 des 60 stagiaires habitent dans la même ville.

Exercice 46 La fonction $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 6^x - 2 \cdot 3^x - 9 \cdot 2^x + 19$ est-elle injective ?

Exercice 47 Soit ABC un triangle, D le milieu de $[AB]$, M le milieu de $[AD]$. On suppose que les droites (BM) et (AC) sont sécantes, en un point que l'on nomme N. Enfin, soit Γ le cercle circonscrit au triangle BCN. Montrer que AB est tangente à Γ si et seulement si

$$\frac{BM}{MN} = \frac{(BC)^2}{(BN)^2}.$$

Exercice 48 Soit n un entier relatif, montrer qu'il existe un unique polynôme P à coefficients dans $\{0, 1\}$ tel que $P(-2) = n$.

Exercice 49 (*) Si A est un ensemble d'entiers naturels non vide, on note $PGCD(A)$ le plus grand diviseur commun à tous les éléments de A.

Trouver le plus petit entier naturel non nul n vérifiant la propriété suivante : pour toute partie A de $\{1, 2, ..., 2012\}$, il existe une partie B de A de cardinal inférieur ou égal à n telle que $\mathrm{PGCD}(B) = \mathrm{PGCD}(A)$.

Exercice 50 (**) De combien de manières différentes peut-on écrire 2^n comme somme de quatre carrés de nombres strictement positifs ?

Exercice 51 (**) Soit A le point d'intersection de deux cercles Γ_1 et Γ_2 de rayons p et q. Soient respectivement B et C deux points de Γ_1 et Γ_2 tels que (BC) est tangente aux deux cercles.

Prouver que $pq = R^2$, où R est le rayon du cercle circonscrit au triangle ABC.

Exercice 52 (**) Montrer que parmi les réels positifs $a, 2a, \ldots, (n-1)a$, l'un au moins est à distance au plus $1/n$ d'un entier positif, pour tout $a > 0$.

Exercice 53 * Résoudre dans $\mathbb{N}$ l'équation :

$$3^x - 5^y = z^2.$$

Exercice 54 On considère un rectangle de format $2 \times N$. De combien de façons différentes peut-on le paver avec des rectangles de taille 1×1, 1×2 ou 2×1 ?

Exercice 55 On appelle I l'ensemble des points du plan tels que leur abscisse et leur ordonnée soient des nombres irrationnels, et R celui des points dont les deux coordonnées sont rationnelles. Combien de points de R au maximum peuvent se situer sur un cercle de rayon irrationnel dont le centre appartient à I ?

Exercice 56 Soit $f : \mathbb{R} \to \mathbb{R}$ un fonction telle que pour tous $x, y \in \mathbb{R}$, on a

$$f(x+y) = \frac{f(x) + f(y)}{1 - f(x)f(y)}.$$

Montrer que $f(x) \cdot f(2x) \cdot f(3x) + f(x) + f(2x) - f(3x) = 0$ pour tout $x \in \mathbb{R}$.

Exercice 57 Si n est un entier, on note $S(n)$ la somme de ses chiffres en base 10. Trouver quatre entiers distincts m, n, p, q tels que

$$m + S(m) = n + S(n) = p + S(p) = q + S(q).$$

Exercice 58 Sur chaque ticket d'un loto sont écrits tous les entiers de 1 à 100. Quand on achète un ticket, on choisit 10 de ces entiers, et on les coche. À la fin de la journée, 10 entiers distincts sont tirés au hasard. Un ticket est gagnant si aucun des nombres cochés n'a été tiré. Combien faut-il acheter de tickets au minimum, et comment faut-il les cocher, pour être sûr d'avoir au moins un ticket gagnant ?

Exercice 59 Étant donné un cube $ABCDA'B'C'D'$, montrer qu'il existe une sphère S qui passe par A, B, C et D et qui est tangente au plan $(A'B'C'D')$.

Exercice 60 (*) Soient ABC un triangle, H le pied de la hauteur issue de B, M le milieu de $[AB]$ et N le milieu de $[BC]$. Les cercles circonscrits aux triangles AHN et CHM se recoupent au point P. Prouver que la droite (PH) coupe le segment $[MN]$ en son milieu.

Exercice 61 On considère trois nombres réels x, y, z qui ne sont pas tous égaux. On suppose que

$$x + \frac{1}{y} = y + \frac{1}{z} = z + \frac{1}{x} = k.$$

Trouver toutes les valeurs possibles de k.

Exercice 62 Trouver tous les entiers positifs n et m tels que $2^n = 3^m + 7$.

Exercice 63 Montrer que si $3n + 1$ et $4n + 1$ sont des carrés alors n est un multiple de 7.

Exercice 64 Une droite passant par un point A coupe un cercle $\mathcal{C}$ en B et C. On suppose que B est situé entre A et C. Les deux tangentes à $\mathcal{C}$ passant par A sont tangentes à $\mathcal{C}$ en S et en T. On note P le point d'intersection de (ST) et (AC). Montrer que $\frac{AP}{PC} = 2\frac{AB}{BC}$

Exercice 65 (**) Un cercle passant par les sommets A et C d'un triangle ABC coupe le côté $[AB]$ en son milieu D et le côté $[BC]$ en E. Le cercle tangent à (AC) en C et passant par E recoupe la droite (DE) en F. Soit K le point d'intersection des droites (DE) et (AC).

Prouver que les droites (CF), (AE) et (BK) sont concourantes.

Exercice 66 (*) Une ampoule est placée sur chaque case d'un échiquier 2011×2012. Initialement, 4042111 ampoules sont allumées. On a le droit d'éteindre une ampoule si elle appartient à un bloc 2×2 dont les trois autres ampoules sont éteintes. Peut-on éteindre toutes les ampoules ?

Exercice 67 Soit ABC un triangle dont le cercle inscrit est noté ω. Soient I le centre de ω et P un point tel que les droites (PI) et (BC) soient perpendiculaires et les droites (PA) et (BC) parallèmes. Soient finalement Q et R deux points tels que $Q \in (AB)$, $R \in (AC)$, les droites (QR) et (BC) soient parallèles et finalement (QR) soit tangente à ω.

Prouver que $\widehat{QPB} = \widehat{CPR}$.

Exercice 68 (*) Soit p un nombre premier congru à 2 modulo 3 et a et b des entiers tels que p divise $a^2 + ab + b^2$. Montrer que p divise a et b.

Exercice 69 Trouver tous les polynômes $P(x)$ à coefficients réels tels que

$$xP\left(\frac{y}{x}\right) + yP\left(\frac{x}{y}\right) = x + y$$

pour tous nombres réels non nuls x, y.

Exercice 70 (*) Soit n un entier non nul. Montrer que

$$\lfloor \sqrt{n} \rfloor + \lfloor \sqrt[3]{n} \rfloor + \ldots + \lfloor \sqrt[n]{n} \rfloor = \lfloor \log_2 n \rfloor + \lfloor \log_3 n \rfloor + \ldots + \lfloor \log_n n \rfloor.$$

On rappelle que $\lfloor x \rfloor$ désigne le plus grand entier inférieur ou égal à x, et que $\lfloor \log_k n \rfloor$ est égal au plus grand exposant a tel que $k^a \leqslant n$.

Exercice 71 Trouver tous les nombres premiers p, q tels que $p^2 - pq - q^3 = 1$.

Exercice 72 (*) Soit $ABCD$ un carré, E un point sur $[BC]$ et F un point sur $[DC]$, tels que le périmètre de ECF soit égal au double du côté du carré. Trouver l'angle $\widehat{EAF}$.

Exercice 73 (**) Soit ABC un triangle isocèle en A, les points M et N sont pris sur les côtés AB et AC respectivement. Les droites (BN) et (CM) se coupent en P.

Montrer que les droites (MN) et (BC) sont parallèles si, et seulement si, $\widehat{APM} = \widehat{APN}$.

Exercice 74 Trouver tous les couples (p, n), où p est un nombre premier et n un entier strictement positif, tels que p^n divise $(p-1)! + 1$.

Exercice 75 Trouver tous les réels x, y tels que $x + y = 3$ et $x^5 + y^5 = 33$.

Exercice 76 Trouver tous les entiers positifs a et b tels que

$$\sqrt{a} + \sqrt{b} = \sqrt{2009}.$$

Exercice 77 Trouver tous les entiers positifs x, y tels que

$$x^3y + x + y = xy + 2xy^2.$$

Exercice 78 On considère un cercle $\mathcal{C}_1$ du plan, d'équation $(x-4)^2 + y^2 = 1$, ainsi qu'une droite l de pente positive qui passe par l'origine et qui est tangente à $\mathcal{C}_1$ en P. Le cercle $\mathcal{C}_2$ est tangent à l'axe des abscisses en P_2, passe par P_1 et son centre appartient à l.

Le cercle $\mathcal{C}_3$ est tangent à l en P_3, passe par P_2 et son centre appartient à l'axe des abcisses. Le cercle $\mathcal{C}_4$ est tangent à l'axe des abscisses en P_4, passe par P_3 et son centre appartient à l.

On construit de la même manière les cercles $\mathcal{C}_5, \mathcal{C}_6$, etc. Pour $n \geqslant 1$, on note S_n l'aire du cercle $\mathcal{C}_n$.

Lorsque N tend vers l'infini, vers quoi converge la somme

$$\sum_{n=1}^{N} S_n \qquad ?$$

Exercice 79 (*) Soit $n \geqslant 0$ un entier naturel. Montrer qu'il existe un disque dans le plan contenant exactement n points à coordonnées entiéres.

Exercice 80 (**) Montrer que si n points du plan ne sont pas tous colinéaires, il y a au moins n droites distinctes passant par deux d'entre eux.

Exercice 81 Trouver tous les polynômes P à coefficients réels tels que

$$P(x^2)P(x^3) = P(x)^5$$

pour tous nombres réels x.

Exercice 82 (*) Un nombre est dit « varié » s'il a 9 chiffres, tous distincts et non nuls (par exemple, 782319564 ou 678123954). Montrer que le nombre de paires de nombres variés dont la somme est 987654321 est impair.

Exercice 83 Trouver tous les polynômes p à coefficients réels tels que

$$(x+1) \cdot p(x-1) + (x-1) \cdot p(x+1) = 2x \cdot p(x).$$

Exercice 84 Montrer qu'il existe une infinité d'entiers a tels que $a^a + b$ divise $b^b + a$ pour au moins un entier $b > a$.

Exercice 85 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$y^2 f(x) + x^2 f(y) + xy = xyf(x+y) + x^2 + y^2$$

pour tous réels x, y.

Exercice 86 Soient k, m des entiers strictement positifs tels que $k > m$ et le tels que $k^3 - m^3$ divise $km(k^2 - m^2)$. Prouver que $(k-m)^3 > 3km$.

Exercice 87 Soit ABC un triangle dont le cercle circonscrit est noté ω, le centre du cercle inscrit ω_1 est noté I et le centre du cercle exinscrit ω_2 tangent au côté $[BC]$ est noté I_A. Les cercles ω_1 et ω_2 sont tangents à $[BC]$ respectivement en D et en E. Soit finalement M le milieu de l'arc (BC) qui ne contient pas A. On considère un cercle tangent à ω en un point T et à la droite (BC) en D. Soit S l'intersection de (TI) avec Ω. Prouver que les droites (SI_A) et (ME) se coupent sur ω.

Exercice 88 Soient a, b, c des réels strictement positifs tels que

$$a + b + c = a^{1/7} + b^{1/7} + c^{1/7}.$$

Prouver que

$$a^a b^b c^c \geqslant 1.$$

Exercice 89 (**) Alice et Bob jouent sur un échiquier plan infini. Alice commence par choisir une case et la colorie en rouge, puis Bob choisit une case non encore coloriée et la colorie en vert, et ainsi de suite. Alice gagne la partie si elle réussi à colorier en rouge quatre cases qui dont les centre forment les sommets d'un carré de côtés parallèles à ceux des cases.

a) Prouver qu'Alice possède une stratégie gagnante.

b) Qu'en est-il si Bob a, lui, le droit de colorier deux cases en vert à chaque coup ?

Exercice 90 Soit $x, y, z \geqslant 1$ des nombres réels tels que

$$\frac{1}{x^2-1} + \frac{1}{y^2-1} + \frac{1}{z^2-1} = 1.$$

Montrer que

$$\frac{1}{x+1} + \frac{1}{y+1} + \frac{1}{z+1} \leqslant 1.$$

Exercice 91 Trouver tous les entiers strictement positifs $a, b > 1$ tels que a divise $b+1$ et b divise $a^3 - 1$.

Exercice 92 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$f(xy) = \max\{f(x+y), f(x)f(y)\}$$

pour tous $x, y \in \mathbb{R}$.

Exercice 93 Soit $ABCD$ un quadrilatère tel que $AC = BD$. Soit P le point d'intersection des diagonales (AC) et (BD). On note ω_1 le cercle circonscrit de ABP. Soit O_1 le centre de ω_1. On note ω_2 le cercle circonscrit de CDP. Soit O_2 le centre de ω_2. On note S et T les intersections respectives de ω_1 et ω_2 avec $[BC]$ (autres que B et C). Soient M et N les milieux respectifs des arcs (SP) (ne contenant pas B) et (TP) (ne contenant pas C). Prouver que les droites (MN) et (O_1O_2) sont parallèles.

Exercice 94 (*) Soient a, b, c, d des réels positifs tels que $a + b + c + d = 2$. Montrer que :

$$\frac{a^2}{(a^2+1)^2} + \frac{b^2}{(b^2+1)^2} + \frac{c^2}{(c^2+1)^2} + \frac{d^2}{(d^2+1)^2} \leqslant \frac{16}{25}.$$

Exercice 95 (**) L'ensemble $\{1, 2, \ldots, 3n\}$ est partitionné en trois ensembles A, B et C de n éléments chacun.

Montrer qu'il est possible de choisir un élément dans chacun de ces trois ensembles, tels que la somme de deux d'entre eux soit égale au troisième.

Exercice 96 Soit P(X) un polynôme de degré 3, à coefficients rationnels. On suppose que le graphe de P admet un point de tangence avec l'axe des abscisses. Montrer que les racines de P sont rationnelles.

Exercice 97 (***) Les élèves d'une classe sont allés se chercher des glaces par groupe d'au moins deux personnes. Il y a eu $k > 1$ groupes en tout. Deux élèves quelconques sont partis ensemble exactement une fois

Prouver qu'il n'y a pas plus de k élèves dans la classe.

Exercice 98 (**) Soient a, b, c, d les longueurs des côtés consécutifs d'un quadrilatère convexe $ABCD$. Soient m et n les longueurs de ses diagonales.

Prouver que :

$$m^2n^2 = a^2c^2 + b^2d^2 - 2abcd\cos(\widehat{A} + \widehat{C}).$$

Exercice 99 Trouver toutes les fonctions $f : \mathbb{R}_+ \to \mathbb{R}_+$ telles que pour tous $a > b > c > d > 0$ vérifiant $ad = bc$ on ait

$$f(a + d) + f(b - c) = f(a - d) + f(b + c).$$

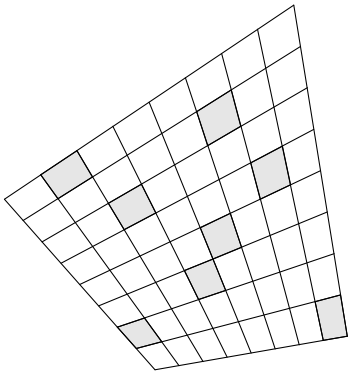
Exercice 100 Soient $n \geqslant 2$ un entier et $a_1, \ldots, a_n$ des entiers relatifs. Montrer que

$$\prod_{i<j}(a_i - a_j)$$

est divisible par

$$\prod_{i<j}(i - j).$$

Exercice 101 (*) On prend un quadrilatère convexe $ABCD$, et on divise chacun de ses côtés en N portions égales. On relie ensuite ces différentes portions de façon à former un quadrillage $N \times N$, comme sur la figure. On sélectionne ensuite N quadrilatères de ce quadrillage, de telle sorte qu'il n'y en ait pas deux sur la même ligne ou sur la même colonne du quadrillage. Calculer l'aire totale de tous ces quadrilatères.



Exercice 102 (**) Une suite croissante $(s_n)_{n\geqslant 0}$ est dite super-additive si pour tout couple (i,j) d'entiers on a $s_{i+j} \geqslant s_i + s_j$. Soient (s_n) et (t_n) deux telles suites super-additives. Soit (u_n) la suite croissante d'entiers vérifiant qu'un nombre apparaît autant de fois dans (u_n) que dans (s_n) et (t_n) combinées.

Montrer que (u_n) est elle aussi super-additive.

Exercice 103 (**) Soit ABC un triangle, soit $A'B'C'$ un triangle directement semblable à ABC de telle sorte que A appartienne au côté $B'C'$, B au côté $C'A'$ et C au côté $A'B'$. Soit O le centre du cercle circonscrit à ABC, H son orthocentre et H' celui de $A'B'C'$.

Montrer qu'on a $OH = OH'$.

Exercice 104 (*) On considère un nombre fini de segments sur la droite réelle tels que, pour tout sous-ensemble de k segments, on puisse trouver deux segments de ce sous-ensemble ayant un point commun. Montrer qu'il existe un ensemble de $k-1$ points tel que tout segment contienne l'un de ces points.

Exercice 105 Trouver toutes les fonctions $f : \mathbb{R} \longrightarrow \mathbb{R}$ telles que, pour tout réel x,

$$f(f(x)) = x^2 - 1996.$$

Exercice 106 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$(x+y)(f(x) - f(y)) = (x-y)f(x+y)$$

pour tous réels x, y.

Exercice 107 On considère un échiquier 8×8 rempli de lampes (éteintes ou allumées), on autorise les opérations consistant à inverser toutes les cases :

- d'une même ligne
- d'une même colonne
- d'une même diagonale ou parallèle à une diagonale (y compris les parallèles à une case, ie les coins)

Dans la position initiale, toutes les cases sont allumées, sauf la quatrième case de la première ligne.

Peut-on se retrouver dans la position ou toutes les lampes sont éteintes ?

Exercice 108 (*) Soit $n, k \in \mathbb{N}$. Déterminer le nombre de $k-$uplets $(T_1, \ldots, T_k)$ de parties de l'ensemble $\{1, \ldots, n\}$ tel que $T_1 \subseteq T_2 \supseteq T_3 \subseteq T_4 \supseteq T_5 \subseteq \cdots T_k$.

Exercice 109 Montrer que, parmi un groupe de 100 personnes, il en existe toujours deux ayant un nombre pair d'amis communs.

Exercice 110 Trouver toutes les fonctions strictement croissantes $f : \mathbb{N}^* \to \mathbb{N}^*$ telles que $nf(f(n)) = f(n)^2$ pour tout entier strictement positif n.

Exercice 111 (**) On considère un ensemble de $2n+1$ droites du plan, deux jamais parallèles ni perpendiculaires et trois jamais concourantes. Trois droites forment donc toujours un triangle non-rectangle.

Déterminer le nombre maximal de triangles aigus qui puissent ainsi être formés.

Exercice 112 Soit n un entier. Dans les lignes d'un tableau de 2^n lignes et n colonnes on place tous les n-uplets formés de 1 et de -1. Ensuite, on efface certains de ces nombres, et on les remplace par des 0. Prouver que l'on peut trouver un ensemble de lignes dont la somme est nulle (i.e., tel que, pour tout i, la somme des nombres appartenant à la colonne i d'une ligne de notre ensemble soit nulle).

Exercice 113 (**) Soient A, B, C_2, C_1 des points d'un cercle Γ dans cet ordre. Soit γ un cercle tangent à $[AC_2]$, $[BC_1]$ et Γ. On note M_2 le point de contact entre γ et $[AC_2]$ et par N_1 le point de contact entre γ et $[BC_1]$.

Prouver que le centres des cercles inscrits à ABC_1 et ABC_2 sont sur $[M_2N_1]$

Exercice 114 Soit a, b, c des nombres réels strictement positifs. Prouver que

$$1 \leqslant (1-a)^2 + (1-b)^2 + (1-c)^2 + \frac{2\sqrt{2}abc}{\sqrt{a^2+b^2+c^2}}.$$

Exercice 115 (*) Soit ABC un triangle, et O un point à l'intérieur de ce triangle. Quel est le point M minimisant la quantité $AM + BM + CM + OM$?

Exercice 116 Soient a, b, c des réels positifs tels que $abc = 1$. Prouver que

$$\frac{1}{1+a+b} + \frac{1}{1+b+c} + \frac{1}{1+c+a} \leqslant 1.$$

Exercice 117 (***) Soit E un ensemble de $n \geqslant 2$ points du plan. On désigne respectivement par D et d la plus grande et la plus petite distance entre deux points distincts de E.

Prouver que :

$$D \geqslant \frac{\sqrt{3}}{2}(\sqrt{n}-1)d.$$

Exercice 118 Dans une compétition de lancer de moutons, la cible est divisée en deux zones, appelées zone 1 et zone 2. Si le mouton tombe dans la zone 1, on gagne 10 points ; s'il tombe dans la zone 2, on gagne 5 points ; et si le mouton tombe en dehors des deux zones on ne gagne pas de points. Chaque participant lance 16 moutons.

À l'issue de la compétition, on s'aperçoit que strictement plus de 50% des moutons ont atterri en zone 2, et le nombre de moutons ayant atterri en zone 1 est égal au nombre de moutons ayant atterri en dehors des zones.

Sachant qu'il y a 30 concurrents, prouver qu'il existe deux participants ayant obtenu le même score.

Exercice 119 (**) Soit S un ensemble infini de points du plan tel que si A, B et C sont trois points quelconques dans S, la distance de A à la droite (BC) soit un entier.

Prouver que les points de S sont tous alignés.

Exercice 120 (*) Soient $a, b, c > 0$ des nombres réels tels que $a + b + c = 3$. Prouver que :

$$\frac{ab}{b^3+1} + \frac{bc}{c^3+1} + \frac{ca}{a^3+1} \leqslant \frac{3}{2}.$$

Exercice 121 (***) Trouver toutes les fonctions continues $f : \mathbb{C} \to \mathbb{C}$ vérifiant :

$$f(x+y)f(x-y) = f(x)^2 - f(y)^2.$$

Exercice 122 Soient $a_1, a_2, \ldots$ et $b_1, b_2, \ldots$ des suites de nombres entiers définies par $a_1 = 1, b_1 = 0$ et, pour $n \geqslant 1$:

$$a_{n+1} = 7a_n + 12b_n + 6, \qquad b_{n+1} = 4a_n + 7b_n + 3.$$

Prouver que a_n^2 est la différence de deux cubes consécutifs.

Exercice 123 Soient P, Q deux polynômes non nuls à coefficients entiers tels que $\deg P > \deg Q$. On suppose que le polynôme $p \cdot P + Q$ possède une racine rationnelle pour une infinité de nombre premiers p. Montrer qu'au moins une racine de P est rationelle.

Exercice 124 (*) Soient P et Q deux polynômes à coefficients entiers, premiers entre eux. Pour tout entier n, posons $u_n = \mathrm{PGCD}(P(n), Q(n))$. Montrer que la suite (u_n) est périodique.

Exercice 125 Trouver tous les couples d'entiers $m \leqslant n$ tels que la quantité suivante soit entière :

$$\frac{1}{m} + \frac{1}{m+1} + \ldots + \frac{1}{n}.$$

Exercice 126 (**) On veut colorier certains des points de l'ensemble $E_n = \{(a, b) \mid a, b \text{ entiers et } 0 \leqslant a, b \leqslant n\}$ de sorte que tout carré $k \times k$ dont les sommets sont dans E_n contienne au moins un point colorié sur son bord. On note $m(n)$ le nombre minimum de points à colorier pour que la condition désirée soit satisfaite.

Prouver que

$$\lim_{n \to +\infty} \frac{m(n)}{n^2} = \frac{2}{7}.$$

Exercice 127 (***) Soit $E = \{M_1, M_2, \ldots, M_n\}$ un ensemble de $n \geqslant 3$ points appartenant à un même cercle Γ. Pour $i = 1, \ldots n$, on désigne par G_i l'isobarycentre des $n-1$ points de $E \backslash \{M_i\}$, et par Δ_i la droite passant par G_i et perpendiculaire à la tangente à Γ en M_i.

Prouver que les droites $\Delta_1, \Delta_2, \ldots, \Delta_n$ sont concourantes.

XI. Solutions de la Muraille

Solution de l'exercice 1 (Résolu par Louis Charnavel)
Remarquons que si d est un diviseur du nombre de jetons de chaque pile, il le reste si on fusionne deux piles, et il le reste si on sépare une pile en deux autres, à condition qu'il soit premier avec 2, donc impair.
Or depuis la configuration du départ, $(5, 49, 51)$, on ne peut obtenir que les configurations suivantes : $(100, 5)$, $(56, 49)$, et $(54, 51)$, et on peut prendre respectivement $d = 5$, $d = 7$ et $d = 3$. Donc toutes les piles auront toujours un nombre de jetons divisible par d, donc on ne peut aboutir à 105 piles de 1 jeton.

Solution de l'exercice 3 (Résolu par Eva Philippe)
Pour placer 5 pièces distinctes : chaque pièce peut avoir une des 5 places différentes, donc 5^5 possibilités.
Pour placer 5 pièces identiques, on regarde le nombre de poches occupées par des pièces. S'il n'y en a qu'une, il y a 5 possibilités.
S'il y en a deux, soit on a une répartition 3 pièces - 2 pièces, avec $5 \times 4 = 20$ choix des poches, soit 4 pièces - 1 pièce, avec encore 20 choix. Donc 40 choix au total.
S'il y en a trois, la répartition $3-1-1$ donne $5 \times \binom{4}{2} = 30$, et la répartition $2-2-1$ aussi, d'où 40 possibilités.
S'il y en a quatre, la répartition en $2-1-1-1-1$ donne 5 possibilités.
Et s'il y en a cinq, il n'y a qu'une possibilité : une pièce par poche.
Ainsi, au total pour les 5 pièces identiques, il y a 126 possibilités.
Donc pour l'ensemble des pièces, il y a $5^5 \times 126 = 393750$ répartitions possibles.

Solution de l'exercice 7 (Résolu par Baptiste Collet)
On a pour a et b réels $a^n - b^n = (a-b)(a^{n-1} + ba^{n-2} + \cdots + b^{n-1})$, donc $3^{6n} - 2^{6n}$ est divisible par $3^6 - 2^6 = 665$, lui-même multiple de 35.

Solution de l'exercice 12 (Résolu par Louis Charnavel)
On considère le segment dont l'extrémité droite est la plus à gauche. Avec tout autre segment, il a des points communs, et son extrémité droite en fait nécessairement partie : ce point est commun à tous les segments.

Solution de l'exercice 17 (Résolu par Louis Charnavel)
Les deux élèves reliés par la distance la plus courte vont s'entretremper. Parmi les $2n-1$ élèves restants, il y en a de nouveau deux à distance la plus courte. Soit l'un deux tire sur un des deux autres, auquel cas il reste $2n-2$ tirs pour mouiller les $2n-1$ autres élèves, donc l'un reste sec, soit ils se tirent l'un l'autre dessus, et on considère les $2n-3$ élèves restants, etc.
Note du Typographe : cette formulation par itération de la solution cache bien sûr une récurrence (qui n'avait pas encore été vue en cours par l'élève concerné). Le lecteur pourra se

donner le plaisir de l'écrire.

Solution de l'exercice 18 (Résolu par Thibaut Fay de Lestrac et Henry Bambury)
Pour $n > 2$, $n^3 + 1 > n^2 > 2n$ donc il faut étudier les cas $n = 1$ ou $n = 2$. Seul le premier donne une solution.

Solution de l'exercice 19 (Résolu par Ilyes Hamdi)
On sait qu'un carré ne peut être congru qu'à 0 ou 1 modulo 4. Si $n_1, \cdots, n_{2011}$ sont impairs, alors $n_1^2 \equiv \cdots \equiv n_{2011}^2 \equiv 1 \bmod [4]$ et $n_{2012}^2 \equiv 2011 \equiv 3 \bmod [4]$, ce qui est impossible.
Si un seul des n_i ($1 \leqslant i \leqslant 2011$) est pair, alors il en va de même de leurs carrés, et $n_{2012}^2 \equiv 2010 + 0 = 0 \bmod [2]$, donc n_{2012} est pair, donc il y a deux nombres pairs au total.
Conclusion : il y a au moins 2 nombres pairs.

Solution de l'exercice 32 (Résolu par Morine Delhelle, Julies Devaux et Lauquin)
Posons $S = A + 2B + 4$. On a

$$\begin{aligned}
S &= 4\sum_{k=0}^{2n-1} 10^k + 2 \times 8\sum_{k=0}^{n-1} 10^k + 4) \\
S &= 4\left(\sum_{k=0}^{2n-1} 10^k + 4\sum_{k=0}^{n-1} 10^k + 1\right) \\
S &= 4\left(\frac{10^{2n}-1}{10-1} + \frac{4(10^n-1)}{9} + \frac{9}{9}\right) \\
S &= \frac{4}{9}(10^{2n} + 4 \times 10^n + 4) \\
S &= \frac{4}{9}(10^n + 2)^2 \\
S &= \left(\frac{2(10^n+2)}{3}\right)^2
\end{aligned}$$

Et $10^n + 2$ est multiple de 3 donc S est bien le carré d'un entier.

Solution de l'exercice 36 (Résolu par Romain Fouilland et Vincent Bouis)
Soit $n \in \mathbb{N}$ tel qu'il existe $a \in \mathbb{N}$ vérifiant $n2^{n+1} = a^2 - 1 = (a-1)(a+1)$. Pour $n \leqslant 3$, seuls 0 et 3 sont solutions. Maintenant, $n \geqslant 4$. Le membre de gauche est pair, donc a ne l'est pas, $a = 2a' + 1$, d'où $n2^{n-1} = a_1(a_1 + 1)$.
Si a_1 est pair, $2^{n-1} | a_1$ et donc $a_1 + 1 \leqslant n$, donc $2^{n-1} \leqslant n - 1$. On montre aisément que c'est faux par récurrence sur $n \geqslant 0$. On procède de manière analogue si c'est $a_1 + 1$ qui est pair.
Donc 0 et 3 sont les seules solutions.

Solution de l'exercice 37 (Résolu par Sébastien Baumert)
On construit M du côté de (XB) tel que MYC soit équilatéral. On a $\widehat{ABC} = 80°$ donc $\widehat{YBC} = 50° = \widehat{BYC}$ (en remarquant que $\widehat{AYB} = 130°$). Donc $BC = YC = MC$ et BMC est isocèle en C. On a $\widehat{MCB} = \widehat{ACB} - \widehat{YCM} = 80° - 60° = 20°$ donc on trouve $\widehat{MBC} = 80° = \widehat{ABC}$, donc $M \in [AB]$.
Or, $\widehat{BXC} = 180° - \widehat{BCX} - \widehat{XBC} = 180° - 60° - 80° = 40°$ et $\widehat{XCM} = \widehat{YCM} - \widehat{YCX} = 60° - 20° = 40°$, donc XMC isocèle en M et $XM = MC = YM$. Donc est le M centre du cercle circonscrit à XCY, et par le théorème de l'angle inscrit :

$$\widehat{YMC} = 2 \times \widehat{CXY}$$

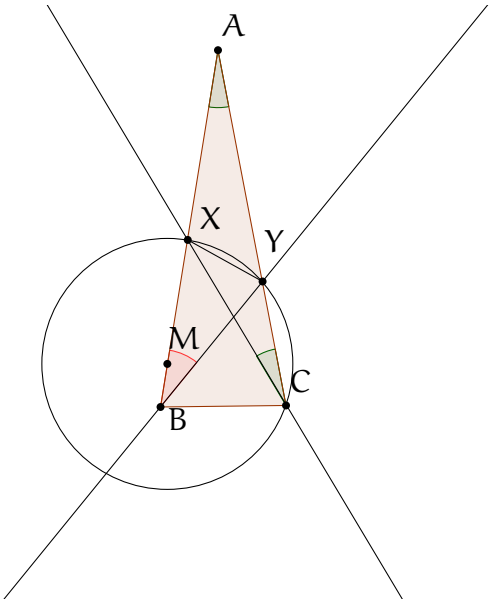


FIGURE 1 – Figure de l'exercice 37

donc

$$\widehat{CXY} = 30°.$$

Solution de l'exercice 38 (Résolu par Paul Lobie et Matthieu Dolbeaut)

a Albert commence, donc Homer choisi le 2012-ème et dernier coefficient. Pour Homer, il suffit que 2012 soit racine de f. Il faut vérifier la relation

$$\sum_{i=1}^{2012} 2012^i a_i = 0$$

qui est linéaire en les a_i, dont aucun coefficient n'est nul, donc Homer pourra toujours choisir le dernier a_i pour annuler la somme, donc il a une stratégie gagnante.

b Soit $f = g + h$ où g est la partie paire (somme des monômes de degré pair) et h la partie impaire de f. Soustraire x^2+1 ne peut affecter que des monômes de même parité, donc soit g soit h mais pas les deux simultanément. g et h ont 1006 coefficients à fixer, et de même qu'en a), si Albert joue sur un des deux polynômes g ou h, Homer joue sur le même et termine les deux polynômes. Et, $h(x) = xH(x^2)$ et $g(x) = G(x^2)$ où H et G ont 1006 coefficients devant être choisis, et devant avoir -1 comme racine (pour être divisibles par $x+1$, de sorte que g et h le soient par x^2+1). Comme en a), c'est encore Homer qui gagne.

Solution de l'exercice 45 (Résolu par Louis Charnavel)
S'il y a au moins 9 villes, on prend un stagiaire par ville, puis un dixième : trois d'entre eux ne sont jamais dans la même ville, contradiction avec l'énoncé. Donc il y a au plus 8 villes.
S'il y a au plus 4 villes, d'après le principe des tiroirs, au moins 15 élèves sont citadins d'une même agglomération.
Avec 5 villes, pour éviter de pouvoir obtenir $2-2-2-2-2$ lors d'un tirage de dix stagiaires,

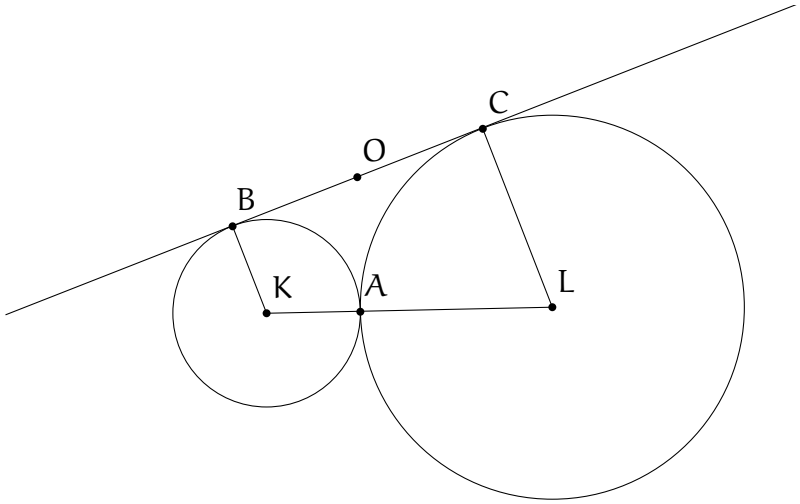


FIGURE 2 – Figure de l'exercice 51

il est nécessaire qu'une ville n'aie qu'un seul élève, auquel cas il reste 59 élèves pour 4 villes et le principe des tiroirs permet de conclure de même.
Avec 6 villes, on montre de même qu'au moins 3 villes ne sont le lieu de résidence que d'un seul élève, et il reste 57 élèves pour les 3 autres.
Avec 7 et 8 villes, on procède de la même manière, d'où la conclusion.

Solution de l'exercice 46 (Résolu par Pierre Bras)
On constate que $f(1) = f(2) = 1$ donc f n'est pas injective.

Solution de l'exercice 51 (Résolu par Cédric Ollivier)

Soit L le centre de Γ_1 et K celui de Γ_2, on pose $\widehat{BKA} = x$, donc $\widehat{KAB} = 90^\circ - \frac{x}{2}$ (car KAB est isocèle en K). Et, $\widehat{KBC} = \widehat{BCL} = 90^\circ$ donc $\widehat{ALC} = 180^\circ - x$, donc $\widehat{LAC} = \frac{x}{2}$, donc ABC est rectangle en A, et

$$R = \frac{BC}{2}$$

Soit S l'aire de ABC. Par la formule d'Al-Kashi dans ABK et ALC, en utilisant $\cos(180^\circ - x) = -\cos x$,

$$S = \frac{AB \times AC}{2} = \frac{\sqrt{(2p^2 + 2p^2\cos x)(2q^2 - 2q^2\cos x)}}{2}$$

Donc $S = \sqrt{p^2q^2 - p^2q^2\cos^2 x} = pq\sin x$ (cette quantité est bien positive).
Et, si O est le milieu de [BC], AOC est isocèle en O, et on trouve $\widehat{COA} = x$. Si S' est l'aire de COA,

$$S' = \frac{R^2 \sin x}{2} = \frac{S}{2}$$

donc $pq = R^2$.

Solution de l'exercice 52 (Résolu par Vincent Bouis)
On pose $A_k = [\frac{k}{n}; \frac{k+1}{n}[$ pour $0 \leqslant k \leqslant n-1$. Si l'un des $n-1$ réels considérés a sa partie décimale dans A_1 ou A_n, on a fini. Sinon, deux d'entre eux sont dans le même A_i par le principe des tiroirs, donc sont distant de moins de $\frac{1}{n}$, notons ua et va avec $u > v$. Alors $(u-v)a$ a sa partie décimale dans A_1 ou A_n.

Solution de l'exercice 54 (Résolu par Eva Philippe)
On note u_n le nombre de manières de paver un rectangle $2 \times n$. En tâtonnant, $u_0 = 1$, $u_1 = 2$ et $u_2 = 7$.
On cherche une formule de récurrence. On peut remplir le dernier rectangle 1×2 de 2 manières. Sinon, le dernier rectangle 2×2 peut être rempli de 2 manières. Pour $k \geqslant 3$, pour remplir le dernier rectangle $k \times 2$ sans remplir le $(k-1) \times 2$, il y a deux manières de procéder (en « décalant » des dominos dans le sens de la longueur). Donc pour $n \geqslant 3$,

$$u_n = 2u_{n-1} + 3u_{n-2} + 2u_{n-3} + \cdots + 2u_0$$

En exprimant ainsi $u_n - u_{n-1}$, on trouve l'équation de récurrence :

$$u_n = 3u_{n-1} + u_{n-2} - u_{n-3}.$$

L'équation caractéristique associée est $X^3 - 3X^2 - X + 1 = 0$. Soit $P(X) := X^3 - 3X^2 - X + 1$. On a $P(-1), P(1)$ strictement négatifs et $P(0), P(4)$ strictement positifs, donc le polynôme a trois racines réelles distinctes a, b, c. On peut vérifier qu'aucune des trois n'est rationnelle. Calculer leur expression explicite est assez fastidieux et laissé aux capacités du lecteur cultivé maîtrisant la méthode de Tartaglia. Il existe alors trois réels $\alpha_1, \alpha_2, \alpha_3$ tels que pour tout $n \in \mathbb{N}$,

$$u_n = \alpha_1 a^n + \alpha_2 b^n + \alpha_3 c^n$$

et on trouve ces trois constantes en utilisant les valeurs de u_0, u_1, u_3.

Solution de l'exercice 56 (Résolu par Pierre Bras)
En posant $y = 2x$, on trouve

$$f(3x) - f(x)f(2x)f(3x) = f(x) + f(2x),$$

d'où le résultat.

Solution de l'exercice 57 (Résolu par Charles Madeline-Dérou)
On exhibe un quadruplet solution du problème, en posant $a = 10^{1\,111\,111\,111\,127}$ et $b = 10^{13}$:

$$m = a - 9,\ n = a + b - 1,\ p = a + b + 98,\ q = a + b + 107$$

Solution de l'exercice 58 (Résolu par Louis Charnavel)
On va montrer que le minimum est 13 tickets. Il est clair qu'il faut acheter au moins 10 tickets. Si on en achète 11, par le théorème des tiroirs, il existe un numéro appartenant à 2 tickets différents. S'il est tiré, il suffit de tirer un numéro dans chacun des 9 autres tickets, et tous les tickets auront subi une perte. Si on en achète 12, on pioche le numéro qui touche le plus de tickets. S'il en touche au moins 3, on fait comme précédemment. S'il en touche 2 seulement, on cherche un autre numéro qui intersecte deux autres tickets. Soit n ce numéro, les 10 autres

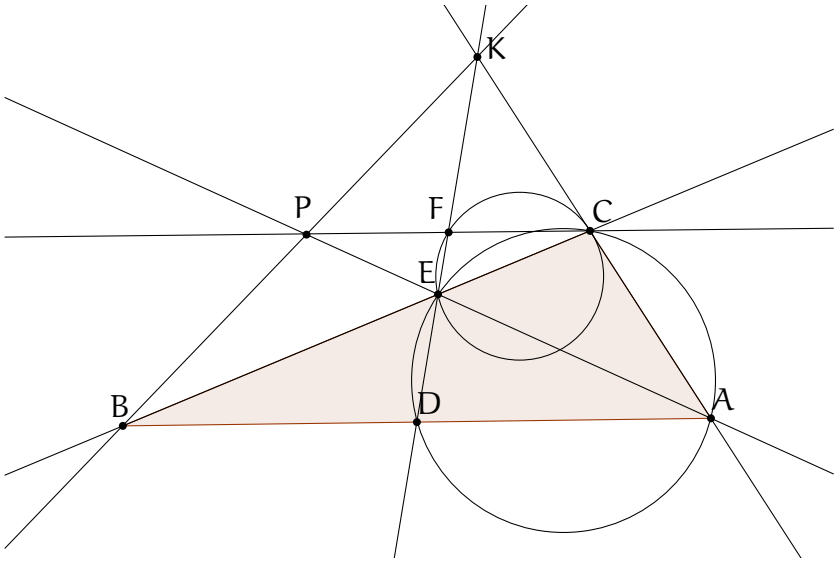


FIGURE 3 – Figure de l'exercice 65

tickets ne peuvent le toucher, et ne peuvent se toucher entre eux : or ils n'ont que 99 emplacements disponibles pour 100 numéros, ce qui n'est pas possible.
Et, avec 13 tickets, on peut réussir : on prend les 6 ensembles $1-10$, $16-25$, $6-15$, $21-30$, $1-5 \cup 11-15$ et $16-20 \cup 26-30$ ($a-b$ désignant les entiers $a, \cdots, b$). Il est assez simple de se convaincre qu'il faut tirer au moins quatre tickets pour bloquer les 6 ensembles. Il suffit alors de compléter par les 7 ensembles $10a+1-10(a+1)$ avec $a \in \{3,9\}$, qui nécéssitent sept autres tickets.

Solution de l'exercice 59 (Résolu par Paul Laubie et Antoine Séré)

Soit M et M' les centres de $ABCD$ et $A'B'C'D'$. Soit $K \in [MM']$ tel que $MK = \frac{MM'}{4}$. K est équidistant de A, B, C et D. On trouve avec Pythagore dans AKM :

$$AK = \sqrt{\frac{MM'^2}{2} + \frac{MM'}{16}} = \frac{3MM'}{4} = KM'.$$

La sphère de centre K et de rayon KM' est clairement tangente au plan $(A'B'C'D')$, et passe par A (donc B, C, D). Ceci résout l'exercice.

Solution de l'exercice 65 (Résolu par Sébastien Baumert)
Soit P l'intersection de (BK) et (CF). Il suffit de montrer que (AP), (DK) et (AP) sont concourantes en E. Si $\widehat{ACE} = \beta$, par cocyclicité, $\widehat{ADE} = 180° - \beta$ et donc $\widehat{BDE} = \beta$. Et de même, selon la formule de l'angle inscrit, $\widehat{EFC} = \beta$. Par propriété des angles alternes-internes, (CP) est parallèle à (AB). Donc par le théorème de Thalès, $\frac{KC}{CA} \times \frac{BP}{PK} = 1$. Comme $AD = DB$, on a, en longueurs algébriques,

$$\frac{KC}{CA} \times \frac{BP}{PK} \times \frac{AD}{DB} = 1$$

donc le théorème de Ménélaüs permet d'affirmer que (AP), (DK) et (AP) sont concourantes, ce qui termine la preuve.

Solution de l'exercice 72 (Résolu par Tobias Parker)

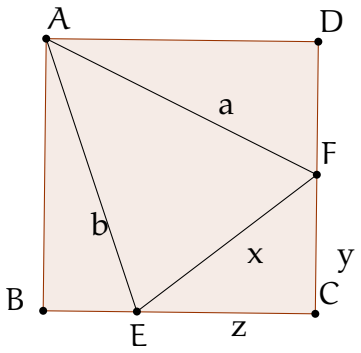


FIGURE 4 – Figure de l'exercice 72

Posons $x = EF$, $y = FC$ et $z = EC$, et notons M, N, P, Q les aires des triangles ADF, FCE, ABE et AFE respectivement. On a $AB = 1$ et $x + y + z = 2$. Posons de plus $a = AF$ et $b = AE$. Montrons d'abord $x = ab\cos\alpha$. On a par Pythagore : $a = \sqrt{2 + y^2 - 2y}$ et $b = \sqrt{2 + z^2 - 2z}$. Puis par Pythagore et Al-Kashi,

$$x^2 = y^2 + z^2 = a^2 + b^2 - 2ab\cos\alpha$$

En développant, on trouve :

$$y + z + \sqrt{y^2 - 2y + 2}\sqrt{z^2 - 2z + 2} = 2 = x + y + z$$

Et on obtient bien $x = ab\cos\alpha$.
En calculant les aires des quatre triangles (dont la somme vaut 1), on trouve

$$Q = \frac{y + z - yz}{2}$$

Calculons un peu :

$$\begin{aligned}
&(x + y + z)^2 = 4\\
&y^2 + z^2 + xy + yz + zx = 2\\
&2y + z(x + z) = x + y + z\\
&2y + 2z - yz = x + y + z\\
&x = y + z - yz = 2Q
\end{aligned}$$

Or par la loi des sinus, $ab\sin\alpha = 2Q$, donc :

$$x = ab\cos\alpha = ab\sin\alpha$$

Or α est entre 0 et 90 degrés, donc vaut 45 degrés.

Solution de l'exercice 73 (Résolu par Charles Madeline-Dérou)

Notons O le point d'intersection de (AP) et (BC).
Si (MN) et (BC) sont parallèles, MNCB est un trapèze « isocèle » (MB = NC), et P est l'intersection de ses diagonales. (PO) est alors la médiatrice de [BC], et PBC isocèle en P. Et

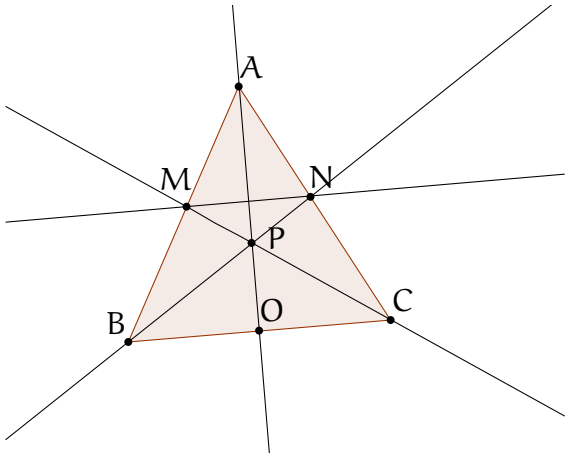


FIGURE 5 – Figure de l'exercice 73

$NC = MB$ donc $MP = NP$. Et, $AM = AN$, les triangles APM et APN sont isométriques et $\widehat{APM} = \widehat{APN}$.
Réciproquement, si $\widehat{APM} = \widehat{APN}$, notons que $\widehat{APB} = \widehat{APC}$ et que les triangles ABP et ACP sont isométriques. Donc PBC est isocèle en P. Par la propriété des angles opposés, $\widehat{BPO} = \widehat{CPO}$, (BO) est la bissectrice issue de P donc médiatrice de $[BC]$, le triangle étant isocèle. C'est alors également la bissectrice de $\widehat{BAC}$, ABC étant isocèle en A. Alors APM et APN sont isométriques. Donc $MP = NP$, et comme $PB = PC$, la réciproque du théorème de Thalès dans MPN et BPC montre que (MN) est parallèle à (BC).

Solution de l'exercice 75 (Résolu par Matthieu Dolbeaut)
On remarque que

$$x^5 + y^5 = (x+y)^5 - 5xy(x+y)^3 + 5x^2y^2(x+y) = 33$$

Posons $P = xy$. Alors $243 - 135P + 15P^2 - 33 = 0$, donc :

$$P^2 - 9P + 14 = 0$$

Les solutions de l'équation sont $P = 2$ et $P = 7$, cette dernière menant à l'équation $x^2 - 3x + 7 = 0$, qui n'a pas de solution réelle. Pour $P = 2$, $x = 1$ et $y = 2$, ou l'inverse. Réciproquement, les couples $(1, 2)$ et $(2, 1)$ sont solution du problème.

Solution de l'exercice 77 (Résolu par Charles Madeline-Dérou et Edwige Cyffers)
On a $x + y = xy(2y^2 - x^2 + 1)$. On vérifie aisément que si $x = 0$ alors $y = 0$ et réciproquement, et le couple $(0, 0)$ est solution du problème.
D'après notre équation, $\frac{x+y}{xy} = \frac{1}{x} + \frac{1}{y}$ est un entier. Si $x = 1$, nécessairement $y = 1$. Si $x \geqslant 2$, alors $y \leqslant 2$, et la seule possibilité est $x = y = 2$. En réinjectant ces deux couples dans l'équation initiale, ils sont solution. On en déduit que $(0, 0)$, $(1, 1)$ et $(2, 2)$ sont les trois uniques couples cherchés.

Solution de l'exercice 80 (Résolu par Louis Charnavel)
Soit P un point, « aligné » avec au plus x autres points (si $x < 2$, on choisit arbitrairement un autre point). On trace les $n - x - 1$ droites passant par P et un point hors de l'alignement, ainsi que la droite de l'alignement de P. Cela fait bien $n - x$ droites distinctes. Puis, on prend

un point hors de l'alignement et on le relie avec chacun des x points de l'alignement de P qui n'est pas P. Cela donne bien n droites distinctes.

Solution de l'exercice 81 (Résolu par Yassine Hamdi)
Soit $P(X) = a_n X^n + \cdots + a_0$, $a_n \neq 0$ solution du problème, on a

$$(a_n X^n + \cdots + a_0)^5 = (a_n X^{2n} + \cdots + a_0)(a_n X^{3n} + \cdots + a_0)$$

En s'intéressant au terme en X^{5n}, on trouve $a_n^5 = a_n^2$ et $a_n \in \mathbb{R}^*$ donc $a_n = 1$. Montrons maintenant par récurrence sur $k \in \mathbb{N}^*$ que $a_{n-k} = 0$. Pour l'initialisation, le terme en X^{5n-1} est $5a_n a_{n-1}$ à gauche et 0 à droite, donc $a_{n-1} = 0$.
Supposons le rang k, $k \geqslant 1$, par hypothèse de récurrence :

$$\begin{aligned}(a_n X^n + a_{n-k-1} X^{n-k-1} + \cdots + a_0)^5 &= (a_n X^{2n} + a_{n-k-1} X^{2(n-k-1)} + \cdots + a_0) \\ &\quad \times (a_n X^{3n} + a_{n-k-1} X^{3(n-k-1)} + \cdots + a_0)\end{aligned}$$

Le terme en X^{5n-k-1} est $5a_{n-k-1}$ à gauche et 0 à droite donc $a_{n-(k+1)} = 0$. Ceci clôt la récurrence. On en conclut que $P(X) = X^n$, et réciproquement ces polynômes sont solution pour tout $n \in \mathbb{N}$.

Solution de l'exercice 85 (Résolu par Raphaël Ruimy et Moïse Blanchard)

$$y^2 f(x) + x^2 f(y) + xy = xy f(x+y) + x^2 + y^2 \Leftrightarrow y^2(f(x)-1) + x^2(f(y)-1) = xy(f(x+y)-1) \quad \text{(XI.1)}$$

Soit $g : x \to (x) - 1$. D'où :

$$y^2 g(x) + x^2 g(y) = xy g(x+y) \quad \text{(XI.2)}$$

Pour $y = 1$, $g(x) + x^2 g(1) = x g(x+1)$ Ainsi si $x \neq 0$,

$$g(x+1) = x g(1) + g(x)/x \quad \text{(XI.3)}$$

Pour $x = 0$, quelque soit y, $y^2 g(0) = 0$. Donc $g(0) = 0$.

Posons $g(1) = a$. Alors :

$$g(1+1) = g(1) + g(1) = 2a$$

$$g(2+1) = 2g(1) + \frac{g(2)}{2} = 3a$$

Par récurrence rapide, $g(n) = an$ avec (3). Grâce à (2) et toujours par récurrence, on prouve que $g(\frac{1}{2^n}) = \frac{a}{2^n}$. Soit $(p, q) \in \mathbb{N}^2$. En prenant $x = \frac{1}{2^p}$ et $y = \frac{1}{2^q}$ on trouve

$$g\left(\frac{1}{2^p} + \frac{1}{2^q}\right) \times \frac{1}{2^p} \times \frac{1}{2^q} = \frac{1}{2^{2q}} \times \frac{a}{2^p} + \frac{1}{2^{2p}} \times \frac{a}{2q} \Leftrightarrow g\left(\frac{1}{2^p} + \frac{1}{2^q}\right) = a\left(\frac{1}{2^p} + \frac{1}{2^q}\right) \quad \text{(XI.4)}$$

Or, tout rationnel r dans $[0, 1]$ peut s'écrire sous la forme : $r = \sum_{i=1} a_i \frac{1}{2^i}$. En répétant (4), on trouve donc $g(r) = r$. $\mathbb{Q}$ étant dense sur $[0, 1]$ on a $g(x) = ax$ sur $[0, 1]$. En écrivant tout réel positif comme la somme de sa partie entière et de sa partie décimale : $x = n + r$, on trouve

$$g(n+r) * n * r = n^2 g(r) + r^2 g(n) = n^2 ar + r^2 an \Leftrightarrow g(n+r) = a(n+r)$$

Enfin avec $y = -x$ dans (2), on trouve $g(-x) = -g(x) = a(-x)$. Réciproquement, la fonction g marche.

Finalement, $\forall x \in \mathbb{R}$, $g(x) = ax$ donc $f(x) = ax - 1$.

Solution de l'exercice 86 (Résolu par Yassine Hamdi)
Soit $k = xd$ et $m = yd$ avec $pgcd(x, y) = 1$. On a

$$x^2 + xy + y^2 | xyd(x + y)$$

Soit p un diviseur premier de $x^2 + xy + y^2$. Si $p|x$, $p|y^2$ donc $p|y$, ce qui est absurde. De même si $p|x$. Si $p|(x + y)$, $x(x + y)$ est multiple de p et donc $p|y^2$, $p|y$ et finalement, $p|x$, d'où une contradiction. Ainsi, $x^2 + xy + y^2 | d$ par le lemme de Gauss, et $d \geqslant x^2 + xy + y^2 \geqslant 3xy$. Or, on veut montrer $(x - y)^3 d > 3xy$. Et $k > m$ donc $x > y$. Il reste à montrer qu'on ne peut avoir $x - y = 1$. Alors on a $d = x^2 + xy + y^2 > 3xy$ car $x \neq y$. Ainsi, on a bien toujours

$$(k - m)^3 > 3km.$$

Solution de l'exercice 90 (Résolu par Clément Lezane)
On raisonne par l'absurde et on pose $a = x + 1$, $b = y + 1$ et $c = z + 1$. On suppose alors

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 > 0$$

On remplace 1 par $\frac{1}{a(a-2)} + \frac{1}{b(b-2)} + \frac{1}{c(c-2)}$ pour aboutir à

$$3\left(\frac{1}{a(a-2)} + \frac{1}{b(b-2)}\right) < \frac{1}{a-2} + \frac{1}{b-2} + \frac{1}{c-2}$$

et donc en faisant de nouveau cette substitution :

$$\frac{1}{a-2} + \frac{1}{b-2} + \frac{1}{c-2} > 3.$$

Donc :

$$\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right)\left(\frac{1}{a-2} + \frac{1}{b-2} + \frac{1}{c-2}\right) > 3$$

et les suites $\frac{1}{a}, \frac{1}{b}, \frac{1}{c}$ et $\frac{1}{a-2}, \frac{1}{b-2}, \frac{1}{c-2}$ sont rangées dans le même ordre, donc par l'inégalité de Tchebychev,

$$\frac{1}{a(a-2)} + \frac{1}{b(b-2)} + \frac{1}{c(c-2)} > 1$$

ce qui contredit l'énoncé. On en déduit le résultat.

Solution de l'exercice 91 (Résolu par Yassine Hamdi)
On a $b = ak - 1$, $a^3 = bl + 1$ avec $k, l \geqslant 1$. Donc $a^3 = akl - (l - 1)$ donc $l = am + 1$, $m \geqslant 0$. Donc $a^3 = ak(am + 1) - am$ et

$$a^2 - kma + (m - k) = 0$$

a étant un entier, le discriminant de l'équation $X^2 - kmX + (m - k)$ l'est aussi. Donc il existe $d \geqslant 0$ tel que

$$4(m - k) = (km - d)(km + d)$$

Distinguons deux cas :

- Si $k = m$, $a^2 - ak^2 = 0$, $a = k^2$ et $b + 1 = k^3$. On vérifie que pour tout $k \geqslant 2$, les couples $(k^2, k^3 - 1)$ sont solution du problème.
- Si $k \neq m$, on trouve $km \leqslant km + d \leqslant 4|m - k|$. De nouveau, deux cas sont à distinguer.
  - Si $m > k$, $km \leqslant 4m - 4k \leqslant 4m$ donc $k \in \{1, 2, 3\}$. Si $k = 1$, $b = a - 1$ et on vérifie que pour $a \geqslant 2$, le couple $(a, a - 1)$ convient. Si $k = 2$, $a = (b + 1)/2$, et $b|a^3 - 1$ donne $8b|(b + 1)^3 - 8$. Or, $(b + 1)^3 - 8 \equiv -7 \bmod b$ donc $b|7$ et $b = 7$, $a = 4$, de la forme $(k^2, k^3 - 1)$, déjà trouvé dans un cas précédent. Si $k = 3$, on trouve de même $b|26$ et la solution $(9, 26)$, toujours de la forme $(k^2, k^3 - 1)$.
  - Si $m < k$, $km \leqslant 4k - 4m \leqslant 4k$ donc $m \in \{0, 1, 2, 3, 4\}$. Le cas $m = 0$ donne $K = a^2$ et $b = a^3 - 1$. Pour $a \geqslant 2$, les couples a, $a^3 - 1$ sont bien solution. Les quatre autres cas n'apportent aucune solution nouvelle.

Conclusion : les solutions sont les couples $(a, a - 1)$ et $(a^p, a^3 - 1)$ avec $a \geqslant 2$ et $p \in \{1, 2\}$.

Solution de l'exercice 92 (Résolu par Arthur Nebout)
f est constante sur $\mathbb{R}^-$. En effet, si x et y sont négatifs, l'équation $X^2 - yX + x = 0$ a deux solutions réelles a et b (discriminant positif), avec $ab = x$ et $a + b = y$. Donc $f(x) \geqslant f(y)$. De même, on montre $f(y) \geqslant f(x)$, donc $f(x) = f(y)$. Avec $(0, z)$ on obtient que si $f(0)$ est strictement négatif, $f(z)$ et $f(0)f(z)$ aussi, ce qui n'est pas possible.
Si $f(0) = 0$, $0 = \max(f(z), 0)$ donc f est négative. Avec $z = ab$, $f(z) \geqslant f(a)f(b) \geqslant 0$ donc f est la fonction nulle.
Si $f(0) > 0$, on prend $x = 0$, on a

$$f(0) = \max(f(z), f(0)f(z)) = \max(f(-z), f(0)f(-z))$$

et on en déduit $f(z) = f(-z)$ donc f, qui était constante sur $\mathbb{R}^-$, l'est sur $\mathbb{R}$.
On vérifie aisément alors que f est solution si et seulement si elle est constante avec $0 \leqslant f(0) \leqslant 1$.

Solution de l'exercice 96 (Résolu par Yassine Hamdi et Antoine Dupuis)
Soit P le polynôme à coefficients rationnels considéré. Il a une racine réelle double a, l'abscisse du point de tangence (car $P(a) = P'(a) = 0$). Donc on peut écrire

$$P(X) = k(X - a)^2(X - b)$$

et b est également réel, et k est rationnel.
Si $a = b$, alors en développant, $3ka \in \mathbb{Q}$ donc $a \in \mathbb{Q}$.
Sinon, $2a + b$, $a^2 + 2ab$ et a^2b sont rationnels (toujours en développant). Donc $(2a + b)^2 - 3(a^2 + 2ab) = (a - b)^2 =: q \in \mathbb{Q}$. Supposons $a - b = \sqrt{q}$ (le cas $a - b = -\sqrt{q}$ se traite de manière semblable. Posons $r := 2a + b \in \mathbb{Q}$. On a $b = \frac{r - 2\sqrt{q}}{3}$ et $a = \frac{r + \sqrt{q}}{3}$. En calculant a^2b, on trouve que $r^3 - 3rq - 2q\sqrt{q} \in \mathbb{Q}$ donc $\sqrt{q} \in \mathbb{Q}$, d'où la conclusion.
Note du typographe : Il existe une méthore plus simple. Avec une division euclidienne de P par P', le quotient et le reste, ô miracle, sont dans $\mathbb{Q}[X]$! Et ils sont de degré 1, et a est racine du reste, donc est rationnel. On en déduit la rationnalité de b.

Solution de l'exercice 98 (Résolu par Antoine Séré, Matthieu Dolbeaut et Christian Michon)
On se place dans le plan complexe, et on peut prendre $\alpha = 0$ et $\beta = 1$ pour les affixes de A et

B. Notons γ et δ celles de C et D. On pose $a = AB$, $b = BC$, etc. On calcule et on trouve :

$$\begin{aligned} m^2n^2 &= \gamma\overline{\gamma}(\delta-1)(\overline{\delta}-1) \\ a^2c^2 &= (\gamma-\delta)(\overline{\gamma}-\overline{\delta}) \\ b^2d^2 &= \delta\overline{\delta}(\gamma-1)(\overline{\gamma}-1) \end{aligned}$$

On sait également exprimer $2abcd$, reste $\cos(\widehat{A}+\widehat{C})$. Notons que

$$\frac{\delta-\alpha}{\beta-\alpha}\times\frac{\beta-\gamma}{\delta-\gamma}+\frac{\overline{\delta}-\overline{\alpha}}{\overline{\beta}-\overline{\alpha}}\times\frac{\overline{\beta}-\overline{\gamma}}{\overline{\delta}-\overline{\gamma}} = \frac{bd}{ac}(e^{i(\widehat{A}+\widehat{C})}+e^{-i(\widehat{A}+\widehat{C})})$$

et $2\cos(\widehat{A}+\widehat{C}) = e^{i(\widehat{A}+\widehat{C})}+e^{-i(\widehat{A}+\widehat{C})}$. En remplaçant les longueurs a, b, c, d par leurs expressions complexes, on trouve

$$2abcd\cos(\widehat{A}+\widehat{C}) = \delta(\gamma-1)(\overline{\gamma}-\overline{\delta})+\overline{\delta}(\overline{\gamma}-1)(\gamma-\delta)$$

Et en sommant cette égalité avec les trois trouvées avant, on obtient le résultat voulu.
Note du typographe : pour une preuve alternative (et beaucoup plus facile à lire), voir le cours de géométrie du groupe D portant sur les inversions.

Solution de l'exercice 105 (Résolu par Florent Noisette)
Posons $g = f^2$ (f composée par elle-même) et cherchons ses points fixes. Ils sont solutions de $x^2-x-1996=0$, équation ayant deux racines réelles distinctes a et b. Si on note $f(a) = a'$ et $f(b) = b'$, alors $a', b' \in \{a, b\}$.
Et, $g^2(x) - x = x^4 - 2\times 1996x^2 - x + 1996\times 1995$. Ce polynôme a a et b comme racines. Notons que seuls a et b peuvent alors être points fixes de f. Montrons qu'il en a quatre, toutes distinctes : g^2 change (strictement de signe) entre $-10^6, -\sqrt{1995}, 0, \sqrt{1995}, 10^6$, et le théorème des valeurs intermédiaires garantit l'existence de 4 racines : une dans $]-10^6, -\sqrt{1995}[$, etc. Et, ce polynôme ne peut en avoir d'autres car il est de degré 4.
Soit c une des deux racines différentes de a et b, et posons $c' = f(c)$. On voit facilement que $f(c)$ est un point fixe de g^2, et $f^2(c)$ aussi. Or, c est distinct de a et b. Donc $f^2(c) \neq c$, et $f(c) \neq c$. Si $f(c) = f^2(c)$, alors $f(c) \in \{a, b\}$, et on aurait $f^4(c) \neq c$, ce qui est absurde. Donc les trois quantités $c, f(c), f^2(c)$ sont distinctes entre elles. Par le même argument, aucun itéré de c par f ne peut être dans $\{a, b\}$. On a alors trouvé cinq points fixes distincts pour g, ce qui est absurde. Donc aucune fonction f ne remplit les conditions de l'énoncé.

Solution de l'exercice 106 (Résolu par Adrien Lemercier)
Avec $(x, 1)$, $(x, 2)$ et $(x+1, 1)$, on obtient :

$$\begin{aligned} (x+1)(f(x)-f(1)) &= (x-1)f(x+1) \\ (x+2)(f(x)-f(2)) &= (x-2)f(x+2) \\ (x+2)(f(x+1)-f(1)) &= xf(x+2) \end{aligned}$$

On a alors pour, tout réel x, et en supprimant astucieusement les termes en $f(x+1)$ et $f(x+2)$:

$$x(x+2)(f(x)-f(2))(x-1) = (x-2)(x+2)((x+1)(f(x)-f(1))-(x-1)f(1))$$

Donc :

$$f(x) = \frac{f(2)}{2}(x^2-x)-(x^2-2x)f(1)$$

Donc f est un polynôme de degré 2 sur $\mathbb{R}$, de terme constant nul : $f(x) = ax^2+bx$. En réinjectant ceci dans l'équation fonctionnelle, on vérifie réciproquement que ces fonctions sont solutions.

Solution de l'exercice 107 (Résolu par Florent Noisette)
On associe 1 à une lampe allumée et -1 à une lampe éteinte. Le produit des cases du bord exceptées les quatre coins est un invariant. Or il doit passer de -1 à 1, ce qui est impossible. On ne peut éteindre toutes les lampes.

Solution de l'exercice 109 (Résolu par Florent Noisette et Colin Davalo)
Si une personne A a un nombre impair d'amis, soit G le graphe dont les sommets sont les amis de A, et les arêtes leurs relations d'amitiés éventuelles. Ce graphe ayant un nombre impair de sommets, au moins l'un d'eux, A', a un nombre pair d'arêtes, et A et A' ont un nombre pair d'amis communs.
Si tout le monde a un nombre pair d'amis, on prend une personne A. On note B l'ensemble des amis de A, et C celui des non amis de A. Si un élément de C a un nombre pair d'amis dans B, c'est fini.
Montrons par l'absurde que le contraire est impossible. Soit g le graphe représentant les 100 personnes et leurs liens d'amitié. On note $2k$ le nombre d'amis de A, l le nombre d'arêtes du sous-graphe B, et $2m+1$ le nombre d'arêtes reliant un sommet de B et un de C (nombre impair, car le cardinal de C est impair, et chacun a un nombre impair d'amis dans B par hypothèse). Soit $d(x)$ le degré du sommet x. On a

$$\sum_{x\in B} d(x) = 2m + 1 + 2l + 2k$$

qui est donc impair, or $d(x)$ est supposé pair pour tout x, donc cette somme devrait être paire, ce qui est la contradiction (ardemment) souhaitée.

Solution de l'exercice 110 (Résolu par Antoine Dupuis)
On a $2|f(2)^2$ donc $f(2)$ est pair, notons $f(2) = 2c$, $c \geqslant 1$. On montre aisément par récurrence que $f(2c^k) = 2c^{k+1}$ pour $k \in \mathbb{N}$.
Soit $x \geqslant 2$ un entier, $f(x) = mx$ avec $m > 0$ un réel. La même récurrence que précédemment montre $f(xm^k) = xm^{k+1}$ pour $k \in \mathbb{N}$.
On va alors encadrer x pour montrer que $m = c$ nécessairement.
On prend $l \in \mathbb{N}$ tel que $2^l \leqslant x < 2^{l+1}$. La croissance stricte de la fonction implique pour tout naturel n :

$$2c^{l+n} \leqslant m^n x < 2c^{l+n+1}$$

Lorsque n tend vers $+\infty$, l'inégalité de gauche devient fausse pour $m < c$, et sinon c'est le cas de celle de droite pour $m > c$, donc $m = c$. Ainsi, pour tout $n \geqslant 2$, on a $f(n) = cn$ où $c \in \mathbb{N}^*$.
Si $f(1) \neq 1$, on a $f(f(1)) = cf(1) = f(1)^2$ donc $f(1) = c$. Donc $f(1) = 1$ ou $f(1) = c$.
Réciproquement, les fonctions $x \to cx$ pour $x \geqslant 2$ et $f(1) = c$ ou $f(1) = 1$ sont solutions du problème.

Solution de l'exercice 116 (Résolu par Antoine Dupuis et Adrien Lemercier)
L'énoncé se ramène à

$$\sum_{cyc}(1+a+b)(1+a+c) \leqslant (1+a+b)(1+b+c)(1+a+c)$$

En développant et simplifiant, il reste à montrer

$$2(a+b+c) \leqslant a^2c + ac^2 + ab^2 + a^2b + b^2c + bc^2$$

Avec $abc = 1$, on peut prendre $a = x/y$, $b = y/z$ et $c = z/x$ avec $x, y, z > 0$ pour obtenir

$$2\sum_{cyc} x^3y^2z \leqslant \sum_{cyc} x^3y^3 + \sum_{cyc} x^4yz \tag{XI.5}$$

Or, $\sum_{cyc} x^3y^3 = \sum_{cyc} \frac{x^3z^3}{3} + \frac{2x^3y^3}{3} \geqslant \sum_{cyc} x^3y^2z$ par l'inégalité arithmético-géométrique. On procède de même pour l'autre somme cyclique de (5).

Solution de l'exercice 118 (Résolu par Clément Lezane)
On martyrise 480 moutons, donc au moins 241 d'entre eux s'écrasent en zone 2. Divisons par cinq : la zone 1 vaut 2 points et la zone 2, 1 points. On peut donc faire 33 scores différents. On veut montrer que moins de 30 scores sont réalisés. Supposons par l'absurde que ce ne soit pas le cas, et que 30 exactement soient réalisés, donc que 3 scores ne soient pas atteints, a, b et c.
Maximisons le nombre de moutons en zone 2 : si un participant lance un mouton en zone 1 et un hors-zone, disons qu'il en a lancé deux en zone 2, ce qui ne change pas son score.
Si on note k un score en points, il y a au plus $16 - |16 - k|$ moutons en zone 2, et la différence du nombre de moutons en zone 1 moins le nombre de ceux hors-zone est alors $k-16$. Or il y a autant de moutons hors-zone que dans la zone 1, et $\sum_{k=0}^{32} k-16 = 0$, donc $a-16+b-16+c-16 = 0$ donc

$$a + b + c = 48.$$

En zone 2, le nombre de victimes est

$$1 + \cdots + 15 + 16 + 15 + \cdots + 1 - (16 - |16 - a|) - (16 - |16 - b|) - (16 - |16 - c|)$$

soit

$$256 - 48 + |16 - a| + |16 - b| + |16 - c|$$

Une petite étude de cas permet de voir que $|16 - a| + |16 - b| + |16 - c| \leqslant 32$, donc il y aura au plus 240 moutons en zone 2, ce qui est impossible.
On en conclut que deux personnes au moins font le même score.

Solution de l'exercice 125 (Résolu par Florent Noisette)
On a $\frac{1}{m} + \cdots + \frac{1}{2m-1} < m \times \frac{1}{m} \leqslant 1$ donc nécessairement, $n \geqslant 2m$. (sauf si $m = 1$, auquel cas $n = 1$).
Dans ce cas, soit r tel que $m \leqslant 2^r \leqslant n < 2^{r+1}$. La valuation 2-adique des entiers de m à n est alors maximale uniquement en 2^r, ce qui montre que la somme ne peut être entière. La seule solution est donc $m = n = 1$.

Solution de l'exercice 127 (Par Félix Breton) Soit B l'isobarycentre de M_1, ..., M_n et h l'homothétie de centre B et de rapport $-\frac{1}{n-1}$. Pour tout i, comme G est le barycentre de M_i avec un poids 1 et G_i avec un poids $n-1$, on a $h(M_i) = G_i$.
Soient Γ' le cercle $h(\Gamma)$ et O le centre de Γ' : les points G_i sont alors cocycliques sur Γ'. Pour tout i, Δ_i est perpendiculaire à la tangente à Γ en M_i, et donc à son image par h qui est la tangente à Γ' en G_i. Or, elle passe par G_i donc $\Delta_i = (OG_i)$, d'où la concourance en O de toutes les droites Δ_i.

XII. Test de sélection du 4 juin 2013

270 candidat-e-s ont composé le test de sélection pour le stage olympique de Montpellier 2013 du 19 au 29 août 2013. 62 élèves (23%) ont participé au stage olympique de Montpellier, dont 12 filles : la liste des stagiaires est publiée sur notre site www.animath.fr. Nous avons admis une plus grande proportion d'élèves de seconde et troisième, d'une part parce que ceux qui bénéficient de plusieurs années pour préparer les Olympiades peuvent progresser sensiblement d'une année sur l'autre, d'autre part car nous avons besoin de jeunes nés en 1999 ou plus tard pour les Olympiades Balkaniques Junior 2014 ainsi que de filles pour les Olympiades Européennes de Filles 2014. Mais j'espère que celles et ceux qui n'ont pas été admis-es ne se décourageront pas : un certain nombre d'entre elles et eux peuvent participer au(x) prochain(s) stage(s).

Voici la solution des différents exercices.

Exercice 1

Trouver tous les quadruplets d'entiers strictement positifs (a, b, c, d) tels que $a+b+c+d = 2013$ et tels que chacun des nombres a, b, c, d divise 2013.

Solution de l'exercice 1

La première difficulté est de bien comprendre l'énoncé : en effet, *quadruplet* signifie quatre éléments non nécessairement distincts mais ordonnés. En ce qui concerne la divisibilité, il s'agit d'une relation entre nombres **entiers** et il ne faut pas oublier que 1 et 2013 divisent 2013, tandis que 0 ne le divise pas.

Beaucoup ont cherché les diviseurs de 2013 : la méthode la plus simple pour les nombres de cette taille reste de chercher la décomposition en facteurs premiers. Cette décomposition vise à écrire 2013 comme produit d'entiers n'ayant comme diviseurs que 1 et eux-mêmes (1 exclu), les diviseurs de 2013 s'obtenant alors en réalisant des combinaisons de ces facteurs. Or, les critères de divisibilité par 3 (somme des chiffres $2+0+1+3$ divisible par 3) et par 11 ($2-0+1-3$ divisible par 11) sont classiques. On obtient : $2013 = 3 \times 11 \times 61$, donc tous les diviseurs de 2013 sont :

$$\{1, 3, 11, 33, 61, 183, 671, 2013\}$$

On ne sait pas encore s'il existe ou non des solutions, et on va finalement prouver qu'il n'en existe pas. Pour ce faire, soit on commence par supposer par l'absurde l'existence d'une solution pour ensuite aboutir à une contradiction, soit on traite **méthodiquement** tous les quadruplets pris dans l'ensemble ci-dessus.

1ère Méthode Soit une solution (a,b,c,d). Puisque a divise 2013, un nombre impair, a est lui-même impair (pour ceux qui ont fait un peu de logique, c'est la contraposée du fait qu'un multiple d'un entier pair est pair), de même b,c,d sont impairs, donc $a+b$ et $c+d$ sont pairs, d'où $a+b+c+d$ est pair, il y a donc une contradiction. Par conséquent, il n'existe pas de quadruplet solution.

2ème Méthode Soit un quadruplet (a,b,c,d) parmi les diviseurs de 2013, on pose sans perdre de généralité $a \geqslant b \geqslant c \geqslant d$. Si $a = 2013$, alors, comme $b \geqslant 1$, la somme dépasse 2013. On traite donc les cas où $a \leqslant 671$, soit $671 \geqslant a \geqslant b \geqslant c \geqslant d$. Si $c \leqslant 183$, alors on a $a+b+c+d \leqslant 671+671+183+183 = 1708$. Il nous reste les cas où $a = b = c = 671$, mais alors $d \geqslant 1$ implique que la somme dépasse 2013. On a traité tous les cas sans trouver de solutions : il n'en existe donc pas.

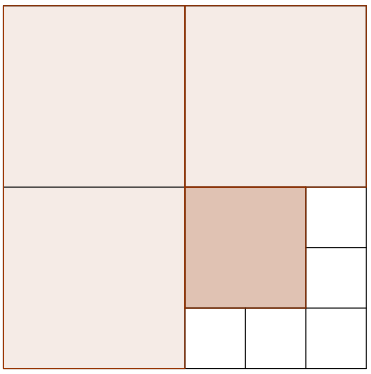
Exercice 2

Est-il possible découper un carré en neuf carrés et d'en colorer un en blanc, trois en gris et les cinq restants en noir de sorte que des carrés de couleur identique soient de même taille et des carrés de couleurs différentes aient des tailles différentes ?

Solution de l'exercice 2

Pour cet exercice il n'y avait pas grand chose à dire. Il y avait bien une solution. Juste un conseil : certains ont essayé de prouver que ce n'était pas possible. Ils ont dû se rendre compte que c'était difficile et fastidieux d'écrire une telle démonstration (d'autant plus qu'elle était forcément fausse). Généralement, dans des cas pareils, cela signifie qu'il existe bien une solution (surtout pour les exercices supposés faciles).

Pour faciliter la lecture de la figure, les couleurs ont été modifiées.

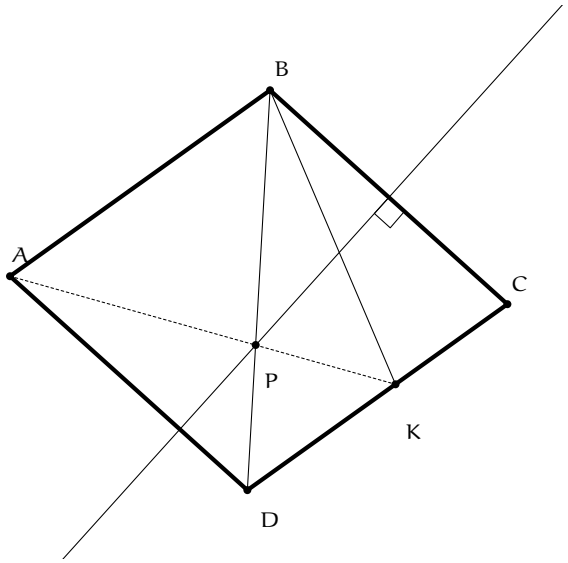


Exercice 3

Soit $ABCD$ un losange. Soit K un point de la droite (CD), autre que C et D, tel que $AD = BK$. Soit P le point d'intersection de la droite (BD) avec la médiatrice de $[BC]$. Prouver que les points A, K et P sont alignés.

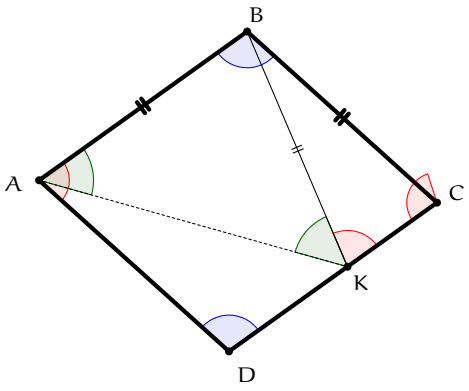
Solution de l'exercice 3

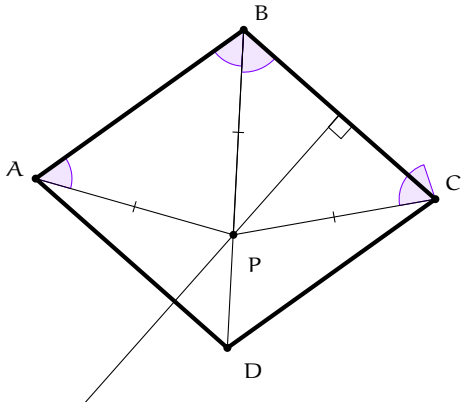
Commençons par faire la figure :



Nous allons simplement faire une chasse aux angles pour calculer les angles $\widehat{BAP}$ et $\widehat{BAK}$ dans notre figure. Si ces deux angles sont égaux, nous aurons démontré que les trois points sont alignés.

Notons $\widehat{BAD} = \widehat{DCB} = \alpha$ et $\widehat{CBA} = \widehat{ADC} = \beta$. Comme la somme des quatre angles d'un quadrilatère fait 360°, on sait que $\alpha + \beta = 180°$.





Calculons $\widehat{BAK}$. Par hypothèse, $BK = AD$, et commme $ABCD$ est un losange, $BK = AB = BC$ et les triangles ABK et KBC sont isocèles en B. Ainsi, $\widehat{CKB} = \widehat{BCK} = \alpha$, et $\widehat{KBC} = 180° - 2\alpha$. On sait que $\widehat{ABC} = \beta$, donc $\widehat{ABK} = \beta - \widehat{KBC} = \beta + 2\alpha - 180° = \alpha$ (puisque $\alpha + \beta = 180°$). Il suffit maintenant de calculer les angles de base du triangle isocèle ABK et on trouve

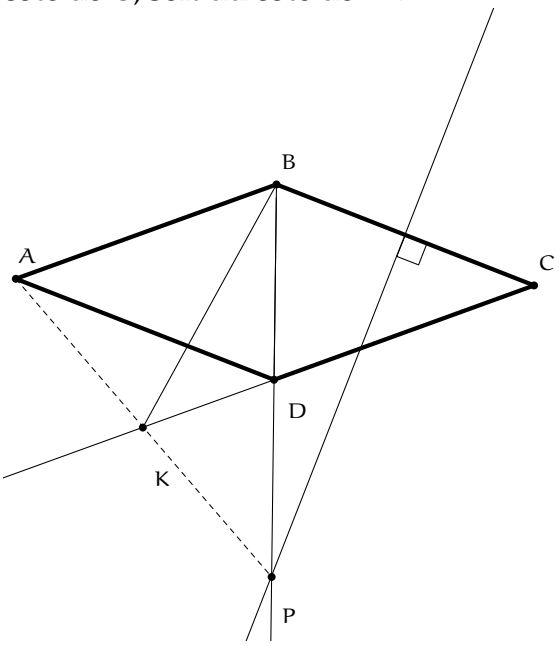
$$\widehat{BAK} = \frac{180° - \widehat{ABK}}{2} = \frac{\beta}{2}.$$

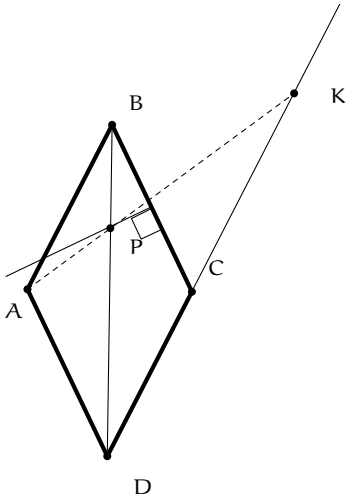
Calculons maintenant $\widehat{BAP}$. Le point P est l'intersection de la médiatrice de $[BC]$ et de la diagonale BD. Mais les diagonales d'un losange sont perpendiculaires et se coupent en leur milieu, donc BD est la médiatrice de $[AC]$. Le point P est donc le centre du cercle circonscrit

au triangle ABC, et PA = PB = PC. Les angles $\widehat{BAP}$, $\widehat{ABP}$, $\widehat{PBC}$ et $\widehat{PCB}$ sont égaux et valent tous $\frac{\beta}{2}$.

$$\widehat{BAP} = \frac{\beta}{2}.$$

ATTENTION : La preuve n'est pas terminée. Cette démonstration ne marche que dans le cas où les points sont dans la configuration de ma figure. Il faut également montrer que la démonstration marche dans les autres cas : lorsque K est à l'extérieur du segment [CD], soit du côté de C, soit du côté de D :





Ces démonstrations (semblables à la précédentes) sont laissées au lecteur.

Il est aussi possible de faire cet exercice de façon analytique. Il faut prendre le repère orthonormé $(O, \vec{i}, \vec{j})$, où O est le point d'intersection des diagonales du losange et $\vec{i}, \vec{j}$ sont des vecteurs unitaires colinéaires aux diagonales. Les coordonnées des quatre sommets sont alors $A : (a, 0)$, $B : (0, b)$, $C : (-a, 0)$ et $D : (0, -b)$. Les calculs sont un peu longs mais faisables.

Exercice 4

Les dénominateurs de deux fractions irréductibles sont 600 et 700. Quelle est la plus petite valeur possible du dénominateur de leur somme (lorsqu'on l'écrit comme fraction irréductible) ?

Solution de l'exercice 4

Réponse : 168. On appelle a et b les numérateurs respectifs de ces deux fractions, de sorte que la somme recherchée s'écrive $\frac{a}{600} + \frac{b}{700}$.

Montrons, d'abord, que la valeur 168 est bien atteinte. En effet, en posant $a = 1$ et $b = 3$, on trouve :

$$\frac{1}{600} + \frac{3}{700} = \frac{7 \times 1}{7 \times 600} + \frac{6 \times 3}{6 \times 700} = \frac{7 + 18}{4200} = \frac{25}{4200} = \frac{1}{168};$$

les fractions $\frac{1}{600}$ et $\frac{3}{700}$ sont bien irréductibles, et la fraction $\frac{1}{168}$ aussi.

Montrons maintenant que le dénominateur ne peut pas être inférieur à 168. La somme qui nous intéresse s'écrit :

$$\frac{a}{600} + \frac{b}{700} = \frac{7a}{7 \times 600} + \frac{6b}{6 \times 700} = \frac{7a + 6b}{4200}.$$

Comme la fraction $\frac{a}{600}$ est irréductible, a est premier avec 600 (c'est-à-dire qu'il n'existe aucun nombre qui divise à la fois a et 600). Puisque $600 = 2^3 \times 3 \times 5^2$, on sait donc que a n'est divisible ni par 2, ni par 3, ni par 5. De même, b est premier avec 700 et $700 = 2^2 \times 5^2 \times 7$, donc b n'est divisible ni par 2, ni par 5, ni par 7.

On en déduit que le produit $7a$ est divisible par 7, mais pas par 2 ni par 3 ni par 5. De même $6b$ est divisible par 2 et 3, mais pas par 7. Or quel que soit p, la somme d'un nombre divisible par p et d'un nombre non divisible par p n'est jamais divisible par p. On en déduit que la somme $7a + 6b$ n'est divisible ni par 2, ni par 3, ni par 7.

On a $4200 = 2^3 \times 3 \times 5^2 \times 7$. D'après ce qui précède, on ne peut jamais simplifier la fraction $\frac{7a+6b}{4200}$ par 2, 3 ou 7. Donc le dénominateur de la fraction réduite sera encore divisible par $2^3 \times 3 \times 7$, c'est-à-dire par 168. Il sera en particulier supérieur ou égal à 168, CQFD.

Exercice 5

Soient m, n des entiers strictement positifs. Un pion appelé (m, n)-condylure se déplace sur un tableau comportant une infinité de lignes (une infinité vers la gauche ainsi que vers la droite) et de colonnes (une infinité vers le haut ainsi que vers le bas). À chaque coup, le condylure se déplace de m cases dans une direction (horizontale ou verticale) et de n cases dans la direction perpendiculaire. Le cheval du jeu d'échecs est donc un (2, 1)-condylure.

Pour quelles valeurs de m et de n peut-on colorier les cases de ce tableau en bleu et en rouge de sorte qu'à chaque coup, la case sur laquelle se trouve le condylure change de couleur ?

Solution de l'exercice 5

La difficulté de cet exercice consistait à bien comprendre que le tableau n'était pas colorié au départ.

C'est possible pour toute valeur de m et n.

a) On commence par étudier l'exemple du $(2, 1)$-condylure, qui n'est autre que le cavalier du jeu d'échecs. Ce dernier, en se déplaçant sur un échiquier bleu-rouge (voir Figure 1), change de couleur à chaque fois qu'il se déplace. La raison est que deux carrés de l'échiquier ont la même couleur si et seulement si on arrive de l'une à l'autre en faisant

– ou bien un nombre pair de pas horizontaux et un nombre pair de pas verticaux ;
– ou bien un nombre impair de pas dans chaque direction (horizontale et verticale).

Comme le $(2, 1)$-condylure se déplace d'un nombre impair de pas dans une direction et d'un nombre pair dans l'autre direction, il change forcément de couleur.

Considérons le cas général d'un (m, n)-condylure tel que m et n ont des parités différentes. On colorie le plan comme un échiquier infini (Figure 1). Le même argument que dans le cas du $(2, 1)$-condylure montre que le (m, n)-condylure change de couleur à chaque mouvement.

b) Prenons maintenant le cas d'un (m, n)-condylure ou m et n sont impairs. On sait qu'à chaque mouvement on se déplace d'un nombre impair de pas dans une direction donnée, disons verticalement. Cela nous donne l'idée de colorier comme dans la Figure 1. On constate facilement que deux carrés ont la même couleur si et seulement si ils sont sur la même ligne ou leurs lignes différent d'un nombre pair de pas.

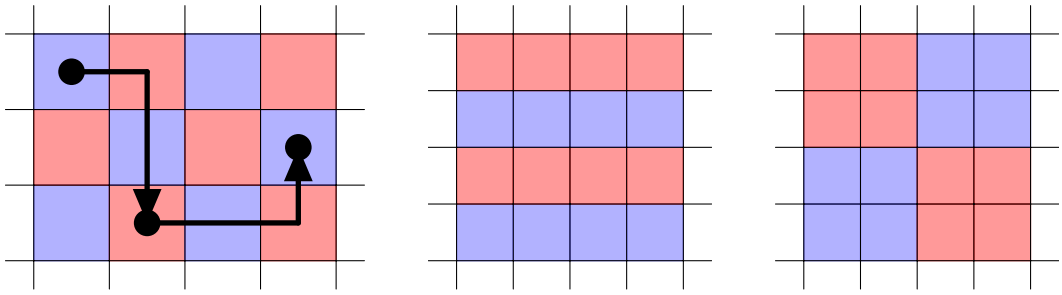


FIGURE 1 – Cas a : m et n de parités différentes. Cas b : m et n impairs. Cas c : $\text{pgcd}(m,n) \neq 1$.

c) Le cas ou m et n sont pairs se résout en se ramenant aux cas précédemment traités. En effet, posons $d = \text{pgcd}(m,n)$. Alors, on peut écrire $n = n'd$ et $m = m'd$ où n' et m' sont deux entiers premiers entre eux. En particulier, n' et m' ne peuvent pas être tous deux pairs. Alors, on colorie le plan en carrés de taille $d \times d$ correspondant au (n', m')-condylure. Voir la Figure 1 pour une illustration du cas où $d = 2$ et les entiers n' et m' ont des parités différentes.

Exercice 6

Le code secret du coffre-fort d'Animath est composé de 7 chiffres tous différents. Le coffre-fort s'ouvre lorsqu'on compose une suite de 7 chiffres si les deux conditions suivantes sont respectées : - les 7 chiffres sont tous différents, - au moins l'un des 7 chiffres est à la bonne place.
a) Est-il possible d'ouvrir le coffre en au plus 6 essais ?
b) Quel est le nombre minimal d'essais pour pouvoir ouvrir le coffre, quel que soit le code secret ?

Solution de l'exercice 6

a) Puisque le code secret comporte 7 chiffres différents, au moins 4 d'entre eux sont parmi $0, 1, 2, 3, 4, 5, 6$. La première idée qui vient est alors d'essayer le code 0123456, puis de faire tourner ces chiffres en essayant si besoin les codes 1234560,2345601,3456012,4560123,5601234 et 6012345. Comme chacun des 7 chiffres aura été utilisé à chacune des 7 positions possibles, n'importe lequel des 4 bons chiffres finira par être à la place requise, assurant ainsi l'ouverture du coffre.

Cela montre qu'en choisissant bien ses essais, on peut ouvrir le coffre en au plus 7 tentatives.

Evidemment, cela ne répond pas exactement à la question posée, puisqu'on voudrait y arriver en au plus 6 essais. Cela étant, rien ne prouve que la méthode ci-dessus est la meilleure possible, et justement une petite modification de celle-ci va nous permettre d'atteindre notre objectif : En effet, 4 bons chiffres parmi les 7, c'est plus qu'il n'en faut. Et si au lieu de faire tourner 7 chiffres sur les 7 places, on ne faisait qu'en tourner 6 sur 6 places ? Par exemple, on peut utiliser les codes

$$0123456, 1234506, 2345016, 3450126, 4501236, 5012346$$

Parmi les 6 chiffres $0, 1, 2, 3, 4, 5$, que l'on teste dans chacune des 6 premières positions, au moins 3 sont dans le code secret. Donc au moins 2 sont dans le code secret et dans les six premières positions. Ainsi, avec ces 6 essais, on ouvrira le coffre à coup sûr.

b) Peut-on encore améliorer notre méthode ou en trouver une autre plus efficace ? On va prouver que non et, du coup, prouver que le minimum cherché est 6.

Parmi les candidats qui ont abordé cette question, l'erreur commune a été de penser que si l'on trouvait 6 codes deux à deux sans un même chiffre à une même place (soit donc 6 codes qui éliminent chacun 7 possibilités de positionnement) et un code secret pour lequel le coffre ne s'ouvrirait pas, cela prouverait que le minimum cherché est 6. Hélàs, c'est faux. Par exemple, les 7 codes

0123456
1234067
2340178
3401289
4012395
5678901
6789512

ne testent jamais deux fois un même chiffre à une même position, et ne permettent pas d'ouvrir le coffre si la combinaison est 7895634. Pourtant, cela ne prouve pas que l'on ne peut pas ouvrir en 7 essais, puisqu'on peut même y arriver en 6 avec une meilleure "coordination" des choix...

On prouve maintenant notre affirmation initiale. Pour cela, supposons que l'on fasse les essais

$$\begin{array}{ccccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 \\ e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array}$$

Il s'agit de prouver qu'il existe un code

$$x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7$$

pour lequel les cinq essais ci-dessus ne conviennent pas. L'idée est de prendre successivement x_1 différent de a_1, b_1, c_1, d_1, e_1, puis x_2 différent de $x_1, a_2, b_2, c_2, d_2, e_2$, puis x_3 différent de $x_1, x_2, a_3, b_3, c_3, d_3, e_3$ etc.
Sauf que cela risque de coincer à partir de x_6, et qu'il va falloir être plus fin.

Dans le tableau 5×7, on note C_j l'ensemble des nombres qui apparaîssent dans la colonne j et $|C_j|$ le nombre d'éléments de C_j (i.e. le nombre de chiffres différents dans la colonne j). Ainsi, on a $|C_j| \leqslant 5$ pour tout j.

- Premier cas : si l'un des C_j ne contient pas plus de 4 nombres.

Sans perte de généralité, on peut supposer que $|C_7| \leqslant 4$. Il existe donc $x \in C_7$ qui apparaît au moins deux fois dans la colonne 7.

Si on avait $C_1 = C_2 = C_3 = C_4 = C_5 = C_6$, il n'y aurait pas plus de 5 nombres différents dans les 6 premières colonnes. En particulier, les nombres $a_1, a_2, a_3, a_4, a_5, a_6$ ne seraient pas tous distincts, en contradiction avec le fait que notre premier essai soit un code possible.
Ainsi, quitte à permuter des lignes ou des colonnes, on peut supposer que $a_6 \notin C_1$.

Si on avait $C_7 \subset C_j$ pour $j = 2, 3, 4, 5$, alors x apparaîtrait aussi au moins une fois dans chacune des colonnes C_2, C_3, C_4, C_5 et donc au moins 6 fois dans le tableau. Ce tableau ne contenant que 5 lignes, le principe des tiroirs assure que x apparaîtrait au moins deux fois dans une même ligne, ce qui nous redonnerait une contradiction comme ci-dessus.
Par conséquent, toujours sans perte de généralité, on peut supposer que C_7 n'est pas inclus dans C_2 et donc qu'il existe $\alpha \in C_7$ tel que $\alpha \notin C_2$.

On pose alors $x_1 = a_6$ et $x_2 = \alpha$.
Si on élimine $x_1, x_2, a_3, b_3, c_3, d_3, e_3$, il reste alors au moins 3 valeurs possibles pour x_3. Une d'elles étant choisie, il reste alors de même au moins 2 valeurs possibles pour x_4, puis à nouveau au moins une valeur possible pour x_5.
Puisque $x_1 \in C_6$, éliminer les valeurs x_1, x_2, x_3, x_4, x_5 et les au plus 4 autres valeurs qui apparaîssent dans C_6 laisse au moins une valeur disponible pour x_6.
De même, puisque $x_2 \in C_7$, éliminer les valeurs $x_1, x_2, x_3, x_4, x_5, x_6$ et les au plus 3 autres valeurs qui apparaîssent dans C_7 laisse au moins une valeur disponible pour x_7.

Ainsi, dans ce premier cas, il existe effectivement un code pour lequel nos essais ne permettent pas d'ouvrir le coffre.

- Deuxième cas : si $|C_j| = 5$ pour tout j.

Comme $C_j \subset \{0, 1, 2, \cdots, 9\}$ pour tout j, les ensembles $C_1, C_2, \cdots, C_7$ ne sont pas tous disjoints. Sans perte de généralité, on peut donc supposer que $a_7 \in C_6$.

D'autre part, le chiffre b_7 n'apparaît pas plus d'une fois par ligne, et donc pas plus de 5 fois dans le tableau. Ainsi, au moins deux des colonnes ne contiennent pas b_7, et donc l'une d'elles n'est pas la colonne 6. Quitte à renuméroter les colonnes, on peut donc supposer que $b_7 \notin C_1$.

De même, a_7 n'apparaît pas dans au moins deux des colonnes mais appartient aux colonnes 6 et 7, donc a_6 n'apparaît pas dans une colonne qui n'est ni la colonne 1 ni la colonne 6 ni la colonne 7. Sans perte de généralité, on suppose donc que $a_7 \notin C_2$.

On pose alors $x_1 = b_7$ et $x_2 = a_7$.
Comme ci-dessus, on vérifie facilement qu'il reste au moins 3 valeurs pour x_3, puis au moins 2 valeurs pour x_4, et enfin au moins une valeur pour x_5.
Comme $x_2 \in C_6$, éliminer x_1, x_2, x_3, x_4, x_5 et au plus 4 autres valeurs qui sont dans C_6 laisse au moins une valeur disponible pour x_6.
Enfin, puisque x_1 et x_2 sont dans C_7, éliminer $x_1, x_2, x_3, x_4, x_5, x_6$ et au plus 3 autres valeurs qui sont dans C_7 laisse au moins une valeur disponible pour x_7.

Ainsi, dans ce deuxième cas également, il existe un code pour lequel nos essais ne permettent pas d'ouvrir le coffre, ce qui conclut.

XIII. Citations mémorables

- Arthur : « On dirait que le bâtiment a été conçu par Numérobis : on a utilisé des tuiles et des volets pour les murs... »
- Élève, pendant la soirée de présentation : « Je suis en 1ère... euh non, en 4ème... »
- Florent : « Qui est le maître du jeu ? »
  Guillaume : « Moi ! »
  Florent : « Qui a dit moi ? »
  Guillaume : « Moi ! »
- Marc, en parlant de géométrie projective : « Et pour les cercles, ça donne quoi ? »
  Pierre (prof pendant ce cours) : « Euh...ben... non, on ne regarde pas les cercles. »
- Louis : « Qui a fait arithmétique avancée l'année dernière ? »
  Quelques mains se lèvent.
  Louis : « Et qui avait compris ? »
  Gros blanc.
- Paul : « C'est qu'il a un cerveau fait pour faire des maths, pas pour réfléchir »
- Vincent M : « Je t'assure que 9 divise 9 ! »
- Vincent M, en jouant au mao : « J'aime violer les ratons laveurs ! »
- Colin : « La Grèce, c'est la Turquie, mais à l'envers. »
- Florent, pendant une partie de loup-garou : « La personne vampirisée se réveille et se fait sucer... le sang. »
- Vincent J : « $\hbar$ est un mec supérieur à 0... »
  Arthur : « Un mec ? »
  Vincent J : « Bon, d'accord, une fille ! »
- Antoine : « Vincent : 1, Vincent : 0 ! » après que Vincent M casse Vincent J (ou le contraire !)
- Clara : « C'est quoi, automates ? »
  Lucie : « C'est des graphes orientés, quelque chose comme ça. »
  Marc : « Et un gratin automate, c'est un gratin avec des tomates. »
- Louis : « Un élève joue aux cartes pendant mon cours. »
  Igor : « Faut jeter les cartes par la fenêtre. »
  Louis : « Non, l'élève. »
- Timothée, après que Vincent M ouvre l'écran de projection en disant « Sésame, ouvre-toi ! » : « Depuis quand il y a des hobbits mages ? »
- Paul : « Ah Que Coucou ! Bob ! »
- Myriam : « Mais en fait, ça veut dire quoi, que $\mathbb{Q}$ est dense dans $\mathbb{R}$? »
  Marc G : « Bah regarde ! » (Petite danse ridicule) « Là mon cul danse dans l'air. »
- « Eh, Robert ! »
- « Considérons deux objets mathématiques : les billes et les torches... »
- Romain F, pendant le cours sur les équations fonctionnelles : « Il faut vérifier que vos fonc-

tions fonctionnent. »