STAGE OLYMPIQUE DE VALBONNE 2018

du 20 au 30 août 2018

Avant-propos

Le stage olympique de Valbonne 2018 a été organisé par l'association Animath.

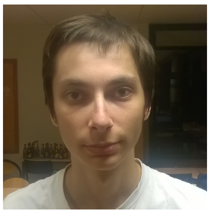
Son objet a été de rassembler 81 collégien-ne-s et lycéen-ne-s de quatrième à première,
de 12 à 17 ans, passioné-e-s de mathématiques
sélectionnés parmi les 781 candidats à la COUPE ANIMATH,
dont certains représenteront la France aux compétitions internationales :
Olympiades Internationales de Mathématiques (IMO),
Olympiades Balkaniques Junior de Mathématiques (JBMO),
Olympiades Européennes de Filles de Mathématiques (EGMO),
Romanian Masters of Mathematics (RMM),
Mediterranean Youth Mathematical Championship (MYMC).
Deux membres de l'équipe de France 2018 des Olympiades Internationales de Mathématiques
sont présents à ce stage,
l'un comme stagiaire, l'autre comme animateur,
et un certain nombre d'autres animateurs et stagiaires
ont déjà participé à l'une des compétitions ci-dessus.

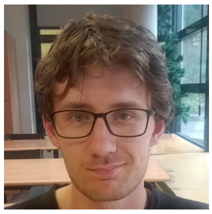
Nous tenons à remercier le Centre International de Valbonne pour son excellent accueil.

Les animatheurs


Martin Andler


Mathieu Barré


Félix Breton


Thomas Budzinski


Aline Cahuzac


Baptiste Collet


Guillaume Conchon--Kerjan


Raphael Ducatez


Pierre-Marie Esmenjaud


Héloise Gachet


Pierre Godfard


Cindy Hua


Vincent Jugé


Yakob Kahane


Savinien Kreczman


Ilyas Lebleu


Matthieu Lequesne

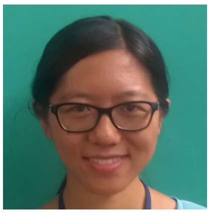

François Lo Jacomo


Frank Nguyen van Sang


Martin Rakovsky


Baptiste Serraille

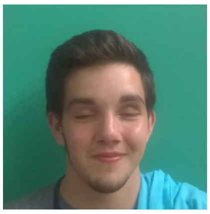

Victor Vermès


Lucie Wang

Les élèves


Solal Afota


Sacha Arroues-Paykin


Noé Artru


Elio Audusse


Emile Averous


Pierre Ayanides


Alexandre Barbu


Andrei Barbu


Stefan Barbu

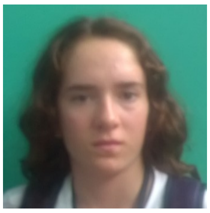

Léonard Berthellemy


Matthieu Bouyer


Elias Caiero


Justin Cahuzac


Alexandre Caillot

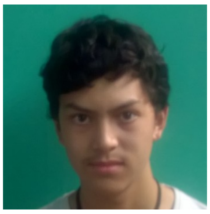

Nelly Cerf


Noémie Cerrina


Sylvain Chabredier


Clément Chapot


Michaël Chen


Victor Chen

Étienne Conchon--Kerjan

Daniel Cortild

Luc Dauge

Auguste de Lambilly

Gaspard Delabre

Yaël Dilliès

Emilhan Dürrüoglu

Katherine Ellison

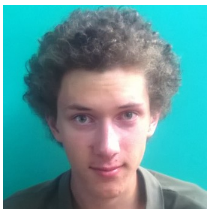
Benoît Fanton

Leonardo Finocchiaro

Isidore Fontaine

Théodore Fougereux

Aurélien Fourré



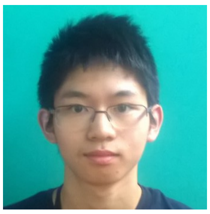
Sylvain Gay

Théo Goix

Rémi Guenet

Pierre Gueugneau

Adam Hamimed



Lucien Hua

Vladimir Ivanov


Gabriel Jimenez Calles


Léonie Kittel


Mithil Krishnan


Evelyne Le Bezvoët


Aymeric Legros


Joseph Lenormand


Charles Liu


Anna Luchinkova


Marie Maignant

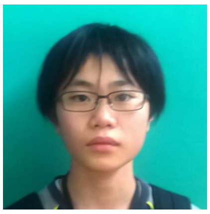

Suzanne Mairesse


Julien Michot


Gaëtan Narozniak


Roméo Nazaret


Quentin Nguyen


Ten Nguyen


Caleb Ott


Adrien Patoz


Marie Peeters

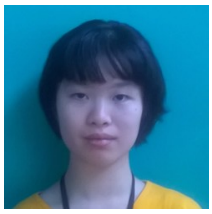

Jules Penot


Enora Petry


Xavier Pigé


Timothé Ringeard

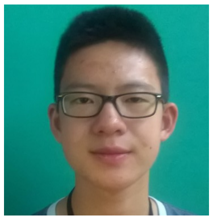

Timothée Rocquet


Claire Rong


Clément Rougeron


Domitille Saliou


Madison Shirazi

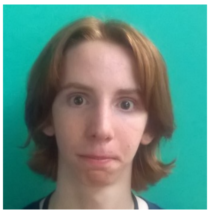

Dorian Song


Paul Stuckle


Adrià Tort


Jeanne Treyer


Gautier Vantalon


Louis Vassaux

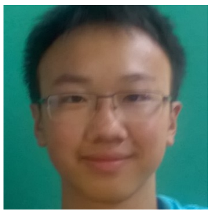

Baptiste Vibert

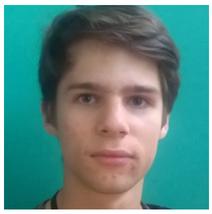

Pierrick Vincent


Matthieu Vogel


Lilou Wattez


Mathis Wetterwald


Jingjie Yang


Jean Zablocki


Emilie Zheng

Table des matières

I. Déroulement du stage

Pour la cinquième fois, le Centre International de Valbonne nous a accueillis du lundi 20 août vers 15 h au jeudi 30 août vers 11 h, avec un effectif final de 81 stagiaires et 23 animateurs.

Parmi les 781 candidats à la Coupe Animath (22% de plus que l'an passé), 564 ont franchi le cap des éliminatoires en ligne (41% de plus que l'an dernier) et ont donc composé le 6 juin dans leurs établissements scolaires respectifs. Sur la base des résultats de cette Coupe Animath, nous devions accueillir 80 stagiaires dont 40 de fin de première, 20 de seconde, 12 de troisième et 8 de quatrième ; compte tenu des désistements et de petits imprévus, nous en avions finalement 21 de seconde, mais bien 40 de première, 12 de troisième et 8 de quatrième. Ces élèves étaient âgés de 12 à 17 ans (âge moyen presque 16 ans). En prévision des EGMO, Olympiades Européennes pour Filles, nous avions, comme à l'accoutumée, favorisé les filles grâce à des bonifications, toutefois leur proportion était inférieure à l'an passé : 16 filles (20%), tout en restant plus élevée qu'aux stages précédents. Par ailleurs, en prévision des JBMO, Olympiades Balkaniques Junior, nous avions 12 jeunes nés en 2004 ou après (moins que l'an dernier).

Comme l'an passé, 23 élèves (29%) étaient scolarisés à Paris, dont 1 habitant dans l'Académie de Créteil et 5 dans l'Académie de Versailles. Cette dernière augmentait ses effectifs : 13 stagiaires y étaient scolarisés, contre 3 dans l'Académie de Créteil. Les Académies de Lille et Montpellier, représentées l'an passé par 7 élèves, étaient absentes cette année, mais trois « nouvelles » Académies apparaissaient : Limoges, Rouen et Strasbourg (un élève chacune). En tout 16 Académies étaient représentées : outre les six ci-dessus, Lyon (7 élèves), Grenoble (4), Toulouse (4), Bordeaux (3), Nantes (3), Nancy (2), Nice (2), Dijon (1), Orléans (1) et Rennes (1). Toutefois, deux élèves résidant dans les Académies de Strasbourg et Bordeaux étaient scolarisés en Allemagne et en Côte d'Ivoire. 11 autres élèves venaient de neuf pays sur quatre continents : Belgique (3), Allemagne, Émirats Arabes Unis, Espagne, États-Unis, Japon, Qatar, Royaume-Uni et Salvador. 23 animateurs, dont 15 de moins de 21 ans, se répartissent toutes les tâches du stage, avec quelques innovations. La plupart des animateurs étaient d'anciens stagiaires : deux membres de l'équipe de France aux Olympiades Internationales de Mathématiques 2018 étaient présents, l'un comme stagiaire et l'autre comme animateur.

Le stage était structuré comme ceux des années précédentes : deux périodes de quatre jours (21 - 24 août et 25 - 28 août), trois de cours / exercices, un test le matin du quatrième jour (9h à 12h, ou pour le groupe D : 9h à 13h) et une après-midi récréative, où plusieurs activités au choix étaient proposées aux élèves. Un programme de ce qu'il convenait d'enseigner notamment aux groupes A et B de stagiaires non expérimentés avait été fixé à l'avance, avec alternance des chapitres. Le mercredi 29 août, dernier jour du stage, était une journée d'« ouverture », consacrée à des cours à vocation culturelle, permettant de découvrir de nouveaux pans des mathématiques.

Le premier jour, lundi 20 août, nous avions préparé pour chaque élève et animateur, dans une enveloppe à son nom, non seulement son badge avec sa carte de chambre et sa carte de cantine, mais un livret d'accueil. Cinq animateurs étaient arrivés la veille après-midi, avaient récupéré les nouveaux T-shirts, bics, et autres colis à notre intention, préparé la muraille, le fléchage, etc... Presque tous les élèves sont arrivés lundi entre 13 h 30 et 16 h 40 (le bus du CIV de 52 places à 15 h 30). La répartition des stagiaires dans les différents groupes était presque achevée à leur arrivée, grâce à un formulaire en ligne que la grosse majorité d'entre eux avaient rempli à l'avance (bien qu'il ne leur ait été communiqué que moins d'une semaine à l'avance). Nous envisagions même un premier cours de 17 h à 18 h 30, mais certains stagiaires arrivaient d'un long voyage éprouvant, et il fallait quand même une brève présentation du stage à 17 h, quand tous les stagiaires (sauf trois) étaient finalement présents, avant de rendre définitive la répartition dans les groupes.

La présentation de la POFM, Préparation Olympique Française de Mathématiques et des compétitions auxquelles participeront environ un tiers des stagiaires, ainsi que la remise des coupes Animath, a eu lieu le premier soir, 20 août, suivie le lendemain d'une présentation d'autres activités d'Animath, notamment le Tournoi Français des Jeunes Mathématicien·ne·s, TFJM^2. Puis, mercredi, Thomas Budzinski a prouvé d'une manière originale la relation historiquement célèbre $1 + \frac{1}{4} + \frac{1}{9} + \cdots = \frac{\pi^2}{6}$. Les jeudi 23 et lundi 27 août, veilles de tests, les soirées étaient libres, et les tests étaient corrigés le soir même. Le 25 août, Vincent Jugé nous a montré comment être plus efficace grâce au hasard, entre autres pour les algorithmes de tri rapide, et le lendemain, Raphaël Ducatez a présenté les remarquables propriétés de la caractéristique d'Euler, en dimensions 2 et 3. Lors de la cérémonie de cloture, Martin Andler fera une conférence « De la science et des médailles », dans laquelle il évoquera notamment la personnalité des médaillés Fields et autres titulaires de grandes récompenses.

Nous avions droit cette année au bâtiment des classes préparatoires tant pour les cours, la muraille et la « salle orga » (nouveau nom de la salle des professeurs) que pour les conférences et séances plénières dans l'amphithéâtre où, le 29 août au soir, aura lieu la cérémonie de clôture du stage. Les derniers départs sont prévus pour 16 h, jeudi 30 août.

Comme l'an passé, l'horaire des repas était : petit déjeuner à 8 h, déjeuner entre 12 h et 13 h, dîner à 19 h. Les soirées commençaient à 20 h. Le bâtiment où nous étions logés (en chambres individuelles avec sanitaires à l'étage), Octogone, n'était pas le même que l'an dernier, mais lui aussi était un véritable labyrinthe, avec de nombreuses sorties, ce qui ne facilitait pas la surveillance. Quelques changements de chambres ont eu lieu juste avant ou pendant le stage.

Le budget du stage était similaire à celui du stage précédent, grâce aux financements de la DGESCO et de plusieurs sponsors publics et privés : CNRS, INRIA, Fondation Blaise Pascal, Polytechnique, Crédit Mutuel Enseignant, Casio, Texas Instruments, . . . Le polycopié imprimé est une nouvelle fois limité à une centaine de pages, alors que le polycopié complet sera mis en ligne très rapidement au format PDF.

Voici quelques liens utiles pour poursuivre le travail réalisé pendant ce stage :

— le site d'Animath : animath.fr ;

— le site de la POFM : maths-olympiques.fr et notamment

— les archives de problèmes (polycopiés etc. . .) : maths-olympiques.fr/?page_id=41 ;

— le site *Mathlinks* : mathlinks.ro ;

— le site *Art of Problem Solving* : artofproblemsolving.com.

		Groupe A	Groupe B
20 août	Soirée	PRÉSENTATION DU STAGE, DE LA POFM ET DES OLYMPIADES Présentation collective	
21 août	Matin	GÉOMÉTRIE Mathieu B.	GÉOMÉTRIE Martin R.
	Après-midi	ALGÈBRE Franck	ALGÈBRE Héloïse
	Soirée	PRÉSENTATION DU TFJM^2 Présentation collective	
22 août	Matin	GÉOMÉTRIE Pierre-Marie	GÉOMÉTRIE Héloïse, Lucie et Martin R.
	Après-midi	ALGÈBRE Pierre	ALGÈBRE Yakob
	Soirée	CONFÉRENCE : DES CERCLES, DES LAMPES ET $\pi^2/6$ Thomas	
23 août	Matin	ALGÈBRE Raphaël	GÉOMÉTRIE Lucie
	Après-midi	GÉOMÉTRIE Baptiste S., Franck et Mathieu B.	COMBINATOIRE Ilyas
	Soirée	ACTIVITÉS LIBRES	
24 août	Matin	SESSION D'ENTRAÎNEMENT SUR DES EXERCICES	
	Après-midi	ACTIVITÉS LIBRES	
	Soirée	CORRECTION DES EXERCICES	
25 août	Matin	COMBINATOIRE Raphaël	ARITHMÉTIQUE Pierre-Marie
	Après-midi	ARITHMÉTIQUE Baptiste C.	COMBINATOIRE Félix
	Soirée	CONFÉRENCE : ÊTRE PLUS EFFICACE GRÂCE AU HASARD Vincent	
26 août	Matin	COMBINATOIRE Savinien	ARITHMÉTIQUE Vincent
	Après-midi	COMBINATOIRE Pierre	ARITHMÉTIQUE Baptiste S.
	Soirée	CONFÉRENCE : ANGLES, COINS ET CARACTÉRISTIQUE D'EULER Raphaël	
27 août	Matin	ARITHMÉTIQUE Vincent	ARITHMÉTIQUE Aline, Cindy, Martin A. et Raphaël
	Après-midi	COMBINATOIRE Martin R. et Savinien	COMBINATOIRE Cindy
	Soirée	ACTIVITÉS LIBRES	
28 août	Matin	SESSION D'ENTRAÎNEMENT SUR DES EXERCICES	
	Après-midi	ACTIVITÉS LIBRES	
	Soirée	CORRECTION DES EXERCICES	
29 août	Matin	HOMOTHÉTIES Mathieu B.	SUITE DE THUE-MORSE Savinien
	Après-midi	DOUBLE-COMPTAGE Aline	NOMBRES COMPLEXES Cindy
	Soirée	SOIRÉE DE CLÔTURE	

		Groupe C	Groupe D
20 août	Soirée	Présentation du stage, de la POFM et des Olympiades Présentation collective	
21 août	Matin	Géométrie Thomas	Géométrie Baptiste S.
	Après-midi	Algèbre Ilyas	Arithmétique Baptiste C.
	Soirée	Présentation du $\mathbb{TFJM}^2$ Présentation collective	
22 août	Matin	Combinatoire Ilyas	Combinatoire Thomas
	Après-midi	Algèbre Franck	Géométrie Baptiste S. et Pierre-Marie
	Soirée	Conférence : Des cercles, des lampes et $\pi^2/6$ Thomas	
23 août	Matin	Algèbre Thomas	Géométrie Pierre-Marie
	Après-midi	Arithmétique Baptiste C.	Algèbre Lucie
	Soirée	Activités libres	
24 août	Matin	Session d'entraînement sur des exercices	
	Après-midi	Activités libres	
	Soirée	Correction des exercices	
25 août	Matin	Arithmétique Vincent	Arithmétique Yakob
	Après-midi	Géométrie Pierre-Marie	Combinatoire Pierre
	Soirée	Conférence : Être plus efficace grâce au hasard Vincent	
26 août	Matin	Géométrie Martin R.	Algèbre Félix
	Après-midi	Combinatoire Savinien	Algèbre Guillaume
	Soirée	Conférence : Angles, coins et caractéristique d'Euler Raphaël	
27 août	Matin	Algèbre Mathieu B.	Arithmétique Guillaume
	Après-midi	Géométrie Aline	IMO 2019 Félix
	Soirée	Activités libres	
28 août	Matin	Session d'entraînement sur des exercices	
	Après-midi	Activités libres	
	Soirée	Correction des exercices	
29 août	Matin	Groupes Raphaël	Groupes Martin A.
	Après-midi	Dénombrabilité Guillaume	Tests de primalité Vincent
	Soirée	Soirée de clôture	

II. Coupe Animath de printemps 2018

Le mercredi 6 juin 2018 avait lieu la coupe Animath de printemps. Parmi les 781 candidats, six candidats se sont distingués en particulier, puisqu'ils ont fini en première position pour leur catégorie d'âge. Les lauréats de la coupe Animath de printemps de 2018 sont donc :

— Émile AVEROUS et Marie PEETERS (parmi les élèves de première) ;

— Anna LUCHINKOVA (parmi les élèves de seconde) ;

— Elias CAIERO et Vladimir IVANOV (parmi les élèves de troisième) ;

— Alec LE HELLOCO (parmi les élèves de quatrième).

– Énoncés destinés aux élèves de collège –

Exercice 1
12 chaises sont numérotées de 1 à 12. Une sauterelle peut sauter de la chaise k à la chaise n si $k-n$ est l'un des quatre nombres $-8, -5, 5, 8$. On sait qu'elle a visité chaque chaise exactement une fois. Quelles sont les positions initiales possibles ?

Exercice 2

a) On pose $A = (1 + 1/2)/2$ et $B = (1 + 1/2 + 1/3)/3$. Montrer que $A > B$.

b) On pose $A = (1 + 1/2 + 1/3 + 1/4 + ... + 1/2017)/2017$ et
$B = (1 + 1/2 + 1/3 + 1/4 + ... + 1/2018)/2018$. Montrer que $A > B$.

Exercice 3
Soit n un entier naturel. On note $1 = d_1 < d_2 < d_3 < \cdots < d_k = n$ ses diviseurs. On remarque que $n = d_2^2 + d_3^3$. Déterminer toutes les valeurs possibles de n.

– Énoncés destinés à tous les élèves –

Exercice 4
Trouver tous les nombres réels a tels que $a + \frac{2}{3}$ et $\frac{1}{a} - \frac{3}{4}$ soient des entiers.

Exercice 5
Sur un demi-cercle de diamètre $[AD]$, on place deux points B et C tels que $AB = BC = 1$. On suppose que $AD = 3$. Calculer la longueur CD.

– Énoncés destinés aux élèves de lycée –

Exercice 6
Déterminer le plus petit entier N tel que l'on puisse trouver 125 entiers distincts $a_1, a_2, \ldots, a_{125}$ sur une ligne de sorte que :

(1) chacun de ces entiers soit strictement positif, et inférieur ou égal à N ;

(2) chacun des 123 entiers $a_2, \ldots, a_{124}$ soit strictement plus grand que la moyenne arithmétique de l'entier écrit à sa gauche et de l'entier écrit à sa droite.

N.B. La moyenne arithmétique de a et b est le nombre $\dfrac{a+b}{2}$.

Exercice 7
Soit $ABCD$ un trapèze avec (AB) et (CD) parallèles, tel que $AB + CD = AD$. Les diagonales (AC) et (BD) se coupent en un point E. La droite passant par E et parallèle à (AB) coupe (AD) en un point F. Montrer que $\widehat{BFC} = 90°$.

Exercice 8
Daphné et Loïs disposent de trois barres de longueur 1 mètre : une blanche, une bleue et une rouge. Daphné casse chacune des deux premières en trois morceaux, et Loïs casse la troisième en trois morceaux. Est-ce que Daphné peut faire en sorte qu'à la fin, quoi que fasse Loïs, elle soit sûre de pouvoir composer trois triangles (non aplatis) avec les neufs morceaux obtenus, de sorte que chaque triangle ait un côté de chaque couleur ?

– Solutions –

Solution de l'exercice 1
Dans le diagramme ci-dessous, on symbolise chaque chaise par son numéro, et on met un trait entre deux chaises si la sauterelle peut sauter de l'une à l'autre :

$$8 - 3 - 11 - 6 - 1 - 9 - 4 - 12 - 7 - 2 - 10 - 5.$$

Il est clair que les seules positions initiales possibles sont 5 et 8.

Solution de l'exercice 2

a) On peut le montrer par un calcul direct, ou bien comme dans b) ci-dessous.

b) On a

$$\begin{aligned} A - B &= (1 + 1/2 + 1/3 + 1/4 + ... + 1/2017)/2017 - \\ &\qquad (1 + 1/2 + 1/3 + 1/4 + ... + 1/2017)/2018 - 1/2018^2 \\ &= (1 + 1/2 + \ldots + 1/2017)(1/2017 - 1/2018) - 1/2018^2 \\ &> (1/2017 - 1/2018) - 1/2018^2 \\ &= 1/(2017 \times 2018^2) \\ &> 0 \end{aligned}$$

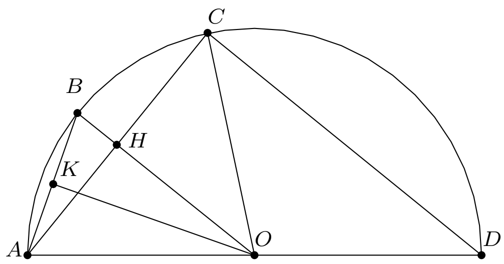
Donc $A > B$.

Solution de l'exercice 3
Si $d_2 \neq 2$, alors n est impair, donc d_3 est impair. Or, $d_2^2 + d_3^2$ est pair, ce qui contredit le fait que n est impair. Donc $d_2 = 2$ et n est pair.

Comme $d_3^3 = n - d_2^2$ est pair, on peut écrire $d_3 = 2m$. Alors m est un diviseur de n tel que $1 < m < d_3$, donc $m = 2$, ce qui implique $d_3 = 4$ et $n = 2^2 + 4^3 = 68$.

Solution de l'exercice 4
Notons m et n ces deux entiers. Comme $a = m - \frac{2}{3}$ et $\frac{1}{a} = n + \frac{3}{4}$, on a $3a = 3m - 2$ et $\frac{4}{a} = 4n + 3$ donc, en multipliant ces égalités, on obtient $12 = (3m-2)(4n+3)$. Comme $4n+3$ est impair et qu'il divise 12, il est égal à l'un des nombres suivants : $-3, -1, 1, 3$. Le cas $4n + 3 = -3$ est impossible. Si $4n + 3 = -1$ alors $n = -1$ et $3m - 2 = -12$, ce qui est impossible. Le cas $4n + 3 = 1$ est impossible. Reste le cas $4n + 3 = 3$ qui donne $n = 0$ et $3m - 2 = 4$ donc $m = 2$, puis $a = \frac{4}{3}$

Solution de l'exercice 5



Soit H l'intersection de $[AC]$ avec $[OB]$, où O est le centre du cercle. On a $CD = \sqrt{AD^2 - AC^2}$ avec $AC = 2AH$.

Soit K le milieu de $[AB]$. Le triangle AOB est isocèle en O. On note $\alpha = \widehat{HAB} = \widehat{BOK}$. On a $\cos\alpha = AH/AB = OK/OB$ donc $AH = \frac{2}{3}OK$. De plus, $OK = \sqrt{OA^2 - AK^2} = \sqrt{(3/2)^2 - (1/2)^2} = \sqrt{2}$, donc $AC = \frac{4}{3}\sqrt{2}$, et finalement $CD = \sqrt{9 - 32/9} = 7/3$.

Solution de l'exercice 6
Soit $d_i = a_{i+1} - a_i$. Soit m tel que a_m soit le maximum. On a alors $d_1 > d_2 > \cdots > d_{m-1} > 0 > d_m > \cdots > d_{124}$.

Supposons que $d_{m-1} = 1$ et $d_m = -1$. Alors $a_{m-1} = a_{m+1}$, ce qui contredit le fait que les 125 entiers sont tous distincts. On a donc, soit $d_{m-1} \geqslant 2$, soit $d_m \leqslant -2$. Quitte à renverser l'ordre des 125 nombres, on peut supposer que $d_{m-1} \geqslant 2$. On a alors $a_m = a_1 + (d_1 + \cdots + d_{m-1}) \geqslant 1 + \cdots + m$.

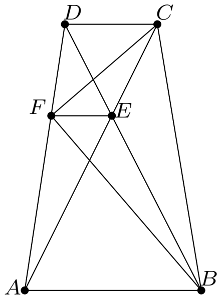
De même, $a_m = a_{125} - (d_m + \cdots + d_{124}) \geqslant 1 + (1 + 2 + \cdots + (125 - m))$.

L'un des nombres m ou $125 - m$ est $\geqslant 63$, donc $a_m \geqslant 1 + \cdots + 63 = 2016$.

Ce nombre peut être atteint en prenant $a_1 = 1$ et $d_i = 64 - i$ pour $i \leqslant 62$ et $d_i = 62 - i$ sinon. Vérifions que cette suite de nombres convient :

On a $1 = a_1 < a_2 < \cdots < a_{63} = 2016$ et $a_{63} > a_{64} > \cdots > a_{125} = 63$. De plus, s'il existe $i < j$ tels que $a_i = a_j$ alors $i < 63$ et $j > 63$ donc $0 = d_i + \cdots + d_{62} + d_{63} + \cdots + d_{j-1} = 2 + \cdots + (64 - i) - (1 + \cdots + (j - 63))$. Nécessairement, $64 - i > j - 63$, et donc en simplifiant il vient $(j - 63 + 1) + \cdots + (64 - i) = 1$, ce qui est impossible. Donc les 125 entiers sont bien distincts.

Solution de l'exercice 7



Comme $(FE) \parallel (CD)$, $\frac{AF}{FD} = \frac{AE}{EC}$. Comme $(AB) \parallel (CD)$, les triangles AEB et DEC sont semblables, donc $\frac{AE}{EC} = \frac{AB}{CD}$. On a donc $\frac{AF}{FD} = \frac{AB}{CD}$.

En ajoutant 1 aux deux membres, il vient $\frac{AF+FD}{FD} = \frac{AB+CD}{CD}$, donc $\frac{AD}{FD} = \frac{AD}{CD}$. On en déduit $FD = CD$, puis $AF = AB$. Autrement dit les triangles DFC et ABF sont isocèles en D et en A respectivement.

Comme la somme des angles d'un triangle vaut $180°$, on a $180° = \widehat{BAF} + 2\widehat{AFB}$ et $180° = \widehat{FDC} + 2\widehat{CFD}$. Il vient $\widehat{BFC} = 180° - \widehat{AFB} - \widehat{CFD} = 180° - (90° - \frac{1}{2}\widehat{BAF}) - (90° - \frac{1}{2}\widehat{FDC}) = \frac{1}{2}(\widehat{BAF} + \widehat{FDC}) = \frac{1}{2}(\widehat{BAD} + \widehat{ADC}) = 90°$.

Solution de l'exercice 8

Le cassage $(1/2, 1/4, 1/4)$, deux fois, permet à Daphné de s'en sortir : si $x \geqslant y \geqslant z$ sont les morceaux de Loïs, $(1/2, 1/2, x)$, $(1/4, 1/4, y)$ et $(1/4, 1/4, z)$ conviennent. En effet, si a et b sont des réels strictement positifs, alors (a, a, b) sont les côtés d'un triangle si et seulement si $b < 2a$.

Ici, on a bien $x < 1$. On a aussi $y < 1/2$ car si $y \geqslant 1/2$ alors $x \geqslant 1/2$, donc $z = 1 - x - y \leqslant 0$, ce qui est impossible.

III. Groupe A

Contenu de cette partie

1 Algèbre

1 Ensembles et calcul

Ce document a été rédigé à partir de ceux des années précédentes.

Introduction. L'objectif de ce cours est de consolider vos connaissances sur les techniques de factorisation, de développement et de développer l'aisance dans l'application de formules (pour établir des égalités ou des inégalités).

– Ensemble de nombres –

✌ **Explication** ✌ **(Approche intuitive : les nombres servent à compter)**

— Les entiers naturels sont les nombres positifs suivants :

$$0,\ 1,\ 2,\ 3, \text{etc}\ldots$$

On les utilise dans la vie de tous les jours pour compter :

1 carambar, 2 carambars, etc...

L'ensemble (c'est-à-dire le paquet) des entiers naturels est noté $\mathbb{N}$.

— Les entiers relatifs sont les nombres positifs ou négatifs suivants :

$$\ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \text{etc}\ldots$$

L'ensemble (c'est-à-dire le paquet) des entiers relatifs est noté $\mathbb{Z}$. Il contient l'ensemble des entiers naturels $\mathbb{N}$.

— Les rationnels sont les nombres qui peuvent s'écrire sous la forme d'un quotient de deux entiers relatifs :

$$\ldots,\ -\frac{5}{4}, -1, 0 = \frac{0}{1},\ \frac{2}{3},\ \text{etc}\ldots$$

L'ensemble (c'est-à-dire le paquet) des rationnels est noté $\mathbb{Q}$. Il contient l'ensemble des entiers relatifs $\mathbb{Z}$.

✌ **Explication** ✌ **(Approche en terme d'équation)** Pour résoudre l'équation $x + 1 = 0$ qui est à coefficients dans $\mathbb{N}$ (ensemble des entiers naturels), on a besoin d'aller chercher les solutions dans un ensemble plus grand, l'ensemble $\mathbb{Z}$ des entiers relatifs. De même, pour résoudre l'équation $2x - 1 = 0$ qui est à coefficients dans $\mathbb{Z}$, on ira chercher les solutions dans un ensemble plus grand, celui des rationnels $\mathbb{Q}$. Enfin, pour résoudre l'équation $x^2 = 2$ à coefficients rationnels, on a besoin d'aller chercher les solutions dans un ensemble encore plus grand, celui des nombres réels $\mathbb{R}$. Au final, on a la chaîne successive d'inclusions d'ensembles suivantes :

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Proposition 1.1.1.

— La somme, la différence, le produit de deux entiers naturels (resp. relatifs) est un entier naturel (resp. relatif).
— La somme, la différence, le produit de deux rationnels est un rationnel.

Démonstration. Montrons que la somme de deux rationnels est un rationnel.

Soit p_1/q_1 et p_2/q_2 deux rationnels avec p_1, p_2 des entiers relatifs et q_1, q_2 des entiers relatifs non nuls. Alors :

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1q_2 + p_2q_1}{q_1q_2} \in \mathbb{Q} \text{ car } (p_1q_2 + p_2q_1, q_1q_2) \in \mathbb{Z}^2.$$

□

– Développements et factorisations –

✌ **Explication** ✌ L'objectif de ce paragraphe est de vous rappeler certaines identités déjà bien connues, et d'en apprendre de nouvelles. Au-delà de cet apprentissage de formules, il est important de développer l'aisance dans la manipulation d'expressions littérales.

Propriétés algébriques

Proposition 1.1.2.
Soit a, b, c, d, k des réels.

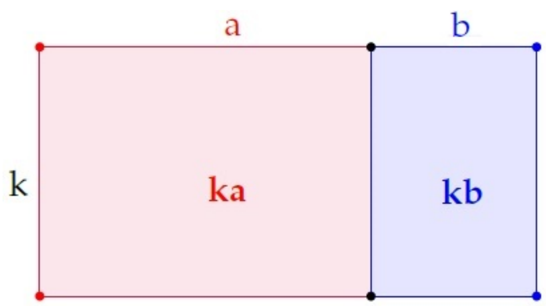
lecture gauche-droite : développement $\longrightarrow$

$k(a+b)$	$=$	$ka+kb$	*(Distributivité)*
$(a+b)(c+d)$	$=$	$ac+ad+bc+bd$	*(Identité du rectangle)*
$(a+b)^2$	$=$	$a^2+2ab+b^2$	*(Identité remarquable 1)*
$(a-b)^2$	$=$	$a^2-2ab+b^2$	*(Identité remarquable 2)*
$(a+b)(a-b)$	$=$	a^2-b^2	*(Identité remarquable 3)*

$\longleftarrow$ *lecture droite-gauche : factorisation*

Démonstration.

— *Distributivité* :



La notation $\mathscr{A}$ désigne une aire. Par interprétation géométrique de la figure ci-gauche, on a l'égalité suivante :

$$\underbrace{\mathscr{A}_{\text{grand rectangle}}}_{=k\times(a+b)} = \underbrace{\mathscr{A}_{\text{rectangle rouge}}}_{=k\times a} + \underbrace{\mathscr{A}_{\text{rectangle bleu}}}_{=k\times b}$$

— *Identité du rectangle* :
L'identité du rectangle s'obtient en appliquant successivement la propriété de distributivité. En effet,

$$\begin{aligned}(a+b)(c+d) &= (a+b)c+(a+b)d && \textit{(Distributivité)}\\ &= ac+bc+ad+bd && \textit{(Distributivité deux fois)}\end{aligned}$$

— *Identité remarquable 1* :
Sachant que $(a+b)^2 = (a+b)\times(a+b)$, l'identité remarquable 1 se déduit de l'identité du rectangle en choisissant $c = a$ et $d = b$.

— *Identités remarquables 2 et 3* :
De la même manière, les identités remarquables 2 et 3 se déduisent de l'identité du rectangle avec des valeurs de c et d judicieusement choisies. Faites-le !

L'identité du rectangle et les identités remarquables peuvent aussi se démontrer directement par interprétation géométrique (l'identité remarquable 1 a aussi été démontrée par interprétation géométrique en classe). □

✌ **Explication** ✌ De ces résultats élémentaires, trois idées importantes sont à retenir :

1) la première idée est d'avoir le réflexe de lire vos égalités de gauche à droite $\boxed{\text{ET}}$ de droite à gauche, et d'en dégager l'utilité pour chaque sens de lecture,

2) la seconde est que certaines formules peuvent s'obtenir par des interprétations géométriques simples,

3) la troisième est que certaines formules peuvent s'obtenir par déductions de formules déjà établies.

Exercice 1
Calculer sans calculatrice $1001^2 - 999^2$.

Solution de l'exercice 1
Il suffit d'appliquer l'identité remarquable 3 pour trouver :

$$1001^2 - 999^2 = (1001-999)(1001+999) = 2\times 2000 = 4000$$

Exercice 2 (avec des expressions littérales)
Soit a et b des réels positifs. Factoriser les expressions suivantes :

$$a^4 - b^4 \qquad\qquad a + b - 2\sqrt{ab}.$$

Solution de l'exercice 2

— $a^4 - b^4 = (a^2 - b^2)(a^2 + b^2) = (a - b)(a + b)(a^2 + b^2)$
— $a + b - 2\sqrt{ab} = (\sqrt{a} - \sqrt{b})^2$

Exercice 3
On dit qu'un entier naturel n est premier s'il admet pour seuls diviseurs 1 et lui-même.
Soit $k \in \mathbb{N}$. Montrer que $4k^4 + 1$ et $k^4 + 4$ ne sont jamais des nombres premiers.

Solution de l'exercice 3
Pour montrer que $4k^4+1$ n'est pas premier, il suffit d'en obtenir une factorisation non triviale. Calculons alors :

$$4k^4 + 1 = (2k^2 + 1)^2 - (2k)^2 = (2k^2 + 1 - 2k)(2k^2 + 1 + 2k)$$

De même, calculons :

$$k^4 + 4 = (k^2 + 2)^2 - (2k)^2 = (k^2 + 2 - 2k)(k^2 + 2 + 2k)$$

Identités remarquables avec du cube

Proposition 1.1.3.
Soit a et b des réels.

$$\begin{array}{rcl} (a+b)^3 & = & a^3 + 3a^2b + 3ab^2 + b^3 \\ (a-b)^3 & = & a^3 - 3a^2b + 3ab^2 - b^3 \\ a^3 - b^3 & = & (a-b)(a^2 + ab + b^2) \\ a^3 + b^3 & = & (a+b)(a^2 - ab + b^2) \end{array}$$

Démonstration. Il suffit de partir des expressions factorisées, puis développer. □

Exercice 4
Soit a et b deux réels. On pose $s = a + b$ et $p = ab$. Exprimer $a^3 + b^3$ en fonction de s et p uniquement.

Solution de l'exercice 4
Calculons :

$$a^3 + b^3 = (a + b)^3 - 3a^2b - 3ab^2 = (a + b)^3 - 3ab(a + b) = s^3 - 3sp.$$

Égalité de Bernoulli

✌ **Explication** ✌ On remarque les identités suivantes :

$$\begin{array}{rcl} a^1 - b^1 & = & (a-b) \times 1 \\ a^2 - b^2 & = & (a-b) \times (a+b) \\ a^3 - b^3 & = & (a-b) \times (a^2 + ab + b^2) \end{array}$$

On peut alors intuiter le résultat suivant :

Proposition 1.1.4.
Soit a, b des réels et n un entier naturel supérieur ou égal à 1. Alors :

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1})$$

Démonstration. Il suffit de développer la forme factorisée, puis des simplifications en cascade permettent d'aboutir au résultat voulu. □

Exercice 5
Soit x un réel et n un entier naturel supérieur ou égal à 1. Calculer :

$$1 + x + x^2 + \cdots + x^n$$

Solution de l'exercice 5
Une disjonction de cas est à effectuer suivant $x = 1$ et $x \neq 1$ et on trouve :

$$1 + x + x^2 + \cdots + x^n = \begin{cases} \dfrac{1 - x^{n+1}}{1 - x} & \text{si } x \neq 1 \\ n + 1 & \text{si } x = 1 \end{cases}$$

– Inégalités –

Manipulations de bases

Théorème 1.1.5.
Soit a, b, c, d, λ des réels.

- *Lien strict/large* : Si $a < b$, alors $a \leqslant b$. LA RÉCIPROQUE EST FAUSSE !
- *Somme* : Si $\begin{cases} a \leqslant b \\ c \leqslant d \end{cases}$, alors $a + c \leqslant b + d$.
- *Produit*
  - *par un réel positif* : si $a \leqslant b$ et $\boxed{\lambda \geqslant 0}$, alors : $\lambda a \leqslant \lambda b$.
  - *par un réel négatif* : si $a \leqslant b$ et $\boxed{\lambda \leqslant 0}$, alors : $\lambda a \geqslant \lambda b$.
  - *d'inégalités positives* : si $\begin{cases} \boxed{0} \leqslant a \leqslant b \\ \boxed{0} \leqslant c \leqslant d \end{cases}$, alors $0 \leqslant ac \leqslant bd$.
- *Carré et racine carrée* :

$$\begin{array}{rcl} 0 \leqslant a \leqslant b & \Longleftrightarrow & \sqrt{a} \leqslant \sqrt{b} \\ a^2 \leqslant b^2 & \Longleftrightarrow & |a| \leqslant |b| \end{array}$$

Inégalités triangulaires

Théorème 1.1.6.
Soit x et y deux réels. Alors on a les inégalités suivantes :

$$\begin{array}{rcll} |x+y| & \leqslant & |x|+|y| & \textit{(Inégalité triangulaire 1)} \\ \big||x|-|y|\big| & \leqslant & |x-y| & \textit{(Inégalité triangulaire 2)} \end{array}$$

Démonstration.

— *Inégalité triangulaire 1* : On compare les carrés et le résultat s'en suit sachant que $xy \leqslant |xy|$.

— *Inégalité triangulaire 2* : L'inégalité triangulaire 2 revient à montrer que

$$|x|-|y| \leqslant |x-y| \quad \text{et} \quad |y|-|x| \leqslant |x-y|$$

On a alors les inégalités suivantes :

$$|x| = |(x-y)+y| \underset{IT1}{\leqslant} |x-y|+|y|$$

□

Technique : un carré c'est positif !

✌ **Explication** ✌ Il est de notoriété publique qu'un carré est toujours positif :

$$5^2 = 25 \text{ est positif, } (-6)^2 = 36 \text{ est positif, etc...}$$

Plus généralement, il est bon de penser au théorème trivial suivant pour établir des inégalités :

Théorème 1.1.7.
Un carré est toujours positif, autrement dit :

$$\text{pour tout réel } x, \quad x^2 \geqslant 0$$

Exercice 6 (Inégalité arithmético-géométrique)
Soit a et b des réels positifs.

1) Montrer l'inégalité suivante, plus connue sous le nom d'inégalité arithmético-géométrique :

$$\frac{a+b}{2} \geqslant \sqrt{ab}$$

2) Soit a, b et c des réels positifs. Montrer que :

$$(a+b)(b+c)(c+a) \geqslant 8abc$$

Solution de l'exercice 6
Soit a et b des réels positifs.

1) On a les équivalences suivantes :

$$\frac{a+b}{2} \geqslant \sqrt{ab} \iff a+b \geqslant 2\sqrt{ab} \iff a+b-2\sqrt{ab} \geqslant 0 \iff (\sqrt{a}-\sqrt{b})^2 \geqslant 0$$

Un carré étant toujours positif, on peut en déduire que l'inégalité de départ est vraie.

2) On applique l'inégalité arithmético-géométrique à chaque facteur et on obtient :

$$\begin{array}{rcl} a+b & \geqslant & 2\sqrt{ab} \\ b+c & \geqslant & 2\sqrt{bc} \\ c+a & \geqslant & 2\sqrt{ca} \end{array}$$

Le produit de ces trois inégalités positives permet alors de conclure.

2 Calculs algébriques

– Énoncés –

Exercice 1
Trouver les solutions entières de $ab - a - b = 1$ pour $a > b > 0$.

Exercice 2
Sachant que a et b vérifient :
$$\frac{a}{1+b} + \frac{b}{1+a} = 1,$$
montrer que $a^3 + b^3 = a + b$.

Exercice 3
Montrer que, pour tous x,y, z réels :
$$|x| + |y| + |z| \leqslant |x + y - z| + |y + z - x| + |z + x - y|.$$

Exercice 4
Montrer que, pour tous a et b réels :
$$a^2 + b^2 + 2(a-1)(b-1) \geqslant 1.$$

Exercice 5
Trouver k tel que, pour tous a, b et c réels :
$$(a+b)(b+c)(c+a) = (a+b+c)(ab+bc+ca) + kabc.$$

Exercice 6
Trouver k tel que, pour tout n, la quantité suivante soit un carré :
$$4n^2 + kn + 9.$$

Exercice 7
Montrer que pour tout $x > 0$:
$$x + \frac{1}{x} \geqslant 2.$$

Exercice 8
Montrer que, pour tous a, b et c réels :
$$a^2 + b^2 + c^2 \geqslant ab + bc + ca.$$

Exercice 9
Montrer que $n^4 + n^2 + 1$ n'est pas un nombre premier pour $n > 1$.

Exercice 10
Soit a, b et c les longueurs des côtés d'un triangle. Montrer que :

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} < 2.$$

Exercice 11
Soit $a > b > 0$, montrer que :

$$4a^3(a-b) \geqslant a^4 - b^4.$$

– Solutions –

Solution de l'exercice 1
L'équation est équivalente à :

$$(a-1)(b-1) = 2.$$

Or $a > b > 0$, donc $b = 1$ et $a = 2$.

Solution de l'exercice 2
On multiplie par $(1+a)(1+b)$:

$$a + a^2 + b + b^2 = 1 + a + b + ab,$$

ce qui se simplifie en :

$$a^2 - ab + b^2 = 1.$$

On multiplie par $a + b$ des deux côtés et obtient l'égalité voulue car :

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2).$$

Solution de l'exercice 3

$$\begin{aligned} 2|x| &= |(x+y-z) + (x-y+z)| \leqslant |x+y-z| + |x-y+z| \\ 2|y| &= |(y+z-x) + (y-z+x)| \leqslant |y+z-x| + |y-z+x| \\ 2|z| &= |(z-y+x) + (z+y-x)| \leqslant |z-y+x| + |z+y-x| \end{aligned}$$

On obtient l'inégalité voulue en sommant ces trois inégalités.

Solution de l'exercice 4
Il s'agit de développer ceci :

$$(a+b-1)^2 \geqslant 0.$$

Solution de l'exercice 5
$k = -1$ convient.

Solution de l'exercice 6
$k = 12$ convient.

Solution de l'exercice 7
L'inégalité est équivalente à $x^2 + 1 \geqslant 2x$, soit $(x-1)^2 \geqslant 0$.

Solution de l'exercice 8
On prouve l'inégalité quand on double les termes $(a-b)^2 + (b-c)^2 + (c-a)^2 \geqslant 0$.

Solution de l'exercice 9
$n^4 + n^2 + 1 = (n^2 - n + 1)(n^2 + n + 1)$.

Solution de l'exercice 10
Comme $b + c > a$, $c + a > b$ et $a + b > c$:

$$\frac{a}{2(b+c)} < \frac{a}{a+b+c}.$$

En sommant cette manipulation il vient :

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} < 2\frac{a+b+c}{a+b+c} = 2.$$

Solution de l'exercice 11
On factorise la droite $(a-b)(a^3 + a^2b + ab^2 + b^3)$ Comme $a - b > 0$, l'inégalité se gentillise en :

$$4a^3 \geqslant a^3 + a^2b + ab^2 + b^3.$$

Or chaque terme du membre de droite est inférieur à a^3, ce qui conclut. ☺

3 Inégalités classiques

– Rappels, manipulations algébriques –

On commence par quelques rappels sur les manipulations algébriques des inégalités.

Les manipulations de base

Quelques exemples :

— Si $a \leqslant b$ et $c \leqslant d$ alors $a + c \leqslant b + d$

— Si $a \leqslant b$ et $u > 0$ alors $ua \leqslant ub$

— Si $a \leqslant b$ et f est une fonction croissante sur $\mathbb{R}$ alors $f(a) \leqslant f(b)$. Exemple $a^3 \leqslant b^3$. Attention $f(x) = x^2$ n'est pas une fonction croissante sur $\mathbb{R}$.

Proposition 1.3.1.
Si f et g sont deux fonctions croissantes sur $\mathbb{R}$. Alors

— $(f+g)(x) = f(x) + g(x)$ est une fonction croissante sur $\mathbb{R}$.

— $f \circ g(x) = f(g(x))$ est une fonction croissante sur $\mathbb{R}$.

Démonstration. Soit $a \leqslant b$, alors $f(a) \leqslant f(b)$ et $g(a) \leqslant g(b)$ car f et g sont croissantes donc $f(a) + g(a) \leq f(b) + g(b)$.

Soit $a \leqslant b$ alors $g(a) \leqslant g(b)$ car g est croissante. Donc $f(g(a)) \leqslant f(g(b))$ car f est une fonction croissante. □

Exemple 1.3.2.
La fonction $h(x) = (2x+1)^5 + x^3$ est une fonction croissante.

Le carré

Souvent, le meilleur moyen de montrer qu'un réel est positif est de montrer qu'il est égale carré (ou e somme de carrés).

$$\forall x, x^2 \geqslant 0.$$

A partir de ln en déduit que les polynmes de degré 2 de la forme $P(x) = x^2 + c$ sont positif sur $\mathbb{R}$, c'est-ire que $\forall x \in \mathbb{R}$, $P(x) \geqslant 0$) si $c \geqslant 0$.

On rappelle que les polynmes sont les fonctions qui peuvent s'écrire comme $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Avec $a_n \neq 0$, on dit que l'entier n est le degré de P.

Proposition 1.3.3.
Un polynme de degré 2 non constant

$$P(x) = ax^2 + bx + c$$

est positif sur $\mathbb{R}$ si $a > 0$ et $b^2 - 4ac \leqslant 0$.

Démonstration. Supposons $a > 0$. Alors

$$ax^2 + bx + c \geqslant 0 \Leftrightarrow a(x^2 + \frac{b}{a}x + \frac{c}{a}) \geqslant 0 \Leftrightarrow (x^2 + \frac{b}{a}x + \frac{c}{a}) \geqslant 0.$$

On va noter $b' = \frac{b}{a}$ et $c' = \frac{c}{a}$ et on va chercher si $x^2 + b'x + c' \geqslant 0$. L'astuce est de se débarrasser du b' avec l'identité remarquable $(x + \frac{b'}{2})^2$.

$$\begin{aligned}
&x^2 + b'x + c' \geqslant 0 \\
\Leftrightarrow &x^2 + 2\frac{b'}{2}x + (\frac{b'}{2})^2 - (\frac{b'}{2})^2 + c' \geqslant 0 \\
\Leftrightarrow &(x + \frac{b'}{2})^2 - \frac{(b')^2}{4} + c' \geqslant 0
\end{aligned}$$

Et on trouve bien que si $-\frac{(b')^2}{4} + c' = -\frac{b^2}{4a^2} + \frac{c}{a} = \frac{-b^2+4ac}{4a^2}$ est positif alors P est positif sur tout $\mathbb{R}$.

Inversement si $\frac{-b^2+4ac}{4a^2} < 0$ alors $P(-\frac{b}{2}) = 0^2 + \frac{-b^2+4ac}{4a^2} = \frac{-b^2+4ac}{4a^2}$ est strictement négatif. □

Exemple 1.3.4.
Soit $Q(x) = x^2 - 6x + 10$. Montrons que $Q(x) \geqslant 0$ pour tout $x \in \mathbb{R}$.

$$Q(x) = x^2 - 6x + 9 - 9 + 10 = (x-3)^2 + 1 \geqslant 0.$$

Exercice 1
Trouve le minimum de $((x-3)^2 + 2)^5$.

Exercice 2
Montrer que $x^2 + xy + y^2 \geqslant 0$.

Exercice 3
Montrer que $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} + \frac{x}{z} + \frac{z}{y} + \frac{y}{x} \geqslant 6$.

Les inégalités de moyennes

D'une mani un peu étrange, rtir d'un ensemble de nombres $a_1, a_2, \cdots, a_n$, on peut définir plusieurs moyennes différentes.

Définition 1.3.5.
Soient $a_1, a_2, \cdots, a_n$ des réels. On appelle la moyenne arithmétique

$$m = \frac{a_1 + a_2 + \cdots + a_n}{n}.$$

Exemple 1.3.6.
Avec $a_1 = 2$, $a_2 = 6$ et $a_3 = 7$, $m = \frac{2+6+7}{3} = 5$.

Définition 1.3.7.
Soient $a_1, a_2, \cdots, a_n$ des réels strictement positifs. On appelle la moyenne géométrique

$$g = \sqrt[n]{a_1 a_2 \cdots a_n}.$$

Exemple 1.3.8.
Avec $a_1 = 2$, $a_2 = 6$ et $a_3 = 7$, $g = \sqrt[3]{2 \times 6 \times 7} = \sqrt[3]{84} \approx 4,38$.

Définition 1.3.9.
Soient $a_1, a_2, \cdots, a_n$ des réels strictement positifs. On appelle la moyenne harmonique

$$h = \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}}.$$

Exemple 1.3.10.
Avec $a_1 = 2$, $a_2 = 6$ et $a_3 = 7$, $h = \frac{3}{\frac{1}{2} + \frac{1}{6} + \frac{1}{7}} \approx 3,37$.

Définition 1.3.11.
Soient $a_1, a_2, \cdots, a_n$ des réels. On appelle la moyenne quadratique

$$q = \sqrt{\frac{a_1^2 + a_2^2 + \cdots + a_n^2}{n}}$$

Exemple 1.3.12.
Avec $a_1 = 2$, $a_2 = 6$ et $a_3 = 7$, $q = \sqrt{\frac{2^2+6^2+7^2}{3}} \approx 5,45$.

Dans les exemples précédents et l'ensemble $2, 6, 7$, on remarque que $h \leqslant g \leqslant m \leqslant q$. Il se trouve que ce n'est pas un hasard et que l'on a un théor qui affirme que quelque soit les nombres $a_1, \cdots, a_n$ que l'on choisit les différentes moyennes seront toujours dans le m ordre.

Théorème 1.3.13 (S)**.**
ient $a_1, a_2, \cdots, a_n$ des réels strictement positifs, alors

$$\min \leqslant h \leqslant g \leqslant m \leqslant q \leqslant \max$$

où $\min$ est le plus petit des a_i et $\max$ est le plus grand des a_i.

Ce théor est beaucoup trop compliqué pour e démontré ici en toute généralité. Cependant, on va ici faire la preuve pour lorsque l'on a que deux nombres a et b.

Démonstration. On va supposer $a \leqslant b$.

— Montrons que $a \leqslant \frac{2}{\frac{1}{a}+\frac{1}{b}}$.

$$a \leqslant b \Rightarrow \frac{1}{a} \geqslant \frac{1}{b} \Rightarrow \frac{2}{a} \geqslant \frac{1}{b} + \frac{1}{a} \Rightarrow \frac{a}{2} \leqslant \frac{1}{\frac{1}{b}+\frac{1}{a}} \Rightarrow a \leqslant \frac{2}{\frac{1}{b}+\frac{1}{a}}$$

— Montrons que $\sqrt{ab} \leqslant \frac{a+b}{2}$

$$\sqrt{ab} \leqslant \frac{a+b}{2} \Leftrightarrow 2\sqrt{ab} \leqslant a+b \Leftrightarrow 0 \leqslant a - 2\sqrt{ab} + b \Leftrightarrow (\sqrt{a}-\sqrt{b})^2 \geqslant 0$$

et c'est bien toujours vérifier car c'est un carré

— Montrons que $\frac{2}{\frac{1}{a}+\frac{1}{b}} \leqslant \sqrt{ab}$

$$\frac{2}{\frac{1}{a}+\frac{1}{b}} \leqslant \sqrt{a \times b} \Leftrightarrow \frac{\frac{1}{a}+\frac{1}{b}}{2} \geqslant \sqrt{\frac{1}{a} \times \frac{1}{b}}$$

On reconnaît alors l'inégalité précédente avec $u = \frac{1}{a}$ et $v = \frac{1}{b}$.

— Montrons que $\frac{a+b}{2} \leqslant \sqrt{\frac{a^2+b^2}{2}}$

$$\frac{a+b}{2} \leqslant \sqrt{\frac{a^2+b^2}{2}} \Leftrightarrow \frac{a^2+2ab+b^2}{4} \leqslant \frac{a^2+b^2}{2} \Leftrightarrow 0 \leqslant \frac{a^2-2ab+b^2}{4} \Leftrightarrow 0 \leqslant \frac{(a-b)^2}{4}$$

— Montrons que $\sqrt{\frac{a^2+b^2}{2}} \leqslant b$

$$a \leqslant b \Rightarrow a^2 \leqslant b^2 \Rightarrow a^2+b^2 \leqslant 2b^2 \Rightarrow \frac{a^2+b^2}{2} \leqslant b^2 \Rightarrow \sqrt{\frac{a^2+b^2}{2}} \leqslant b$$

□

Exercices d'application

Exercice 4
CalculerL les moyennes h, g, m et q des réels 1, 10 et 100.

Exercice 5
Soit a, b des réels positifs tel que le produit $ab = 5$. Quelle est la valeur possible minimale $a + b$?

Exercice 6
Soit a, b des réels positifs tel que le produit $ab = 5$. Quelle est la valeur possible minimal de $\frac{1}{a} + \frac{1}{b}$?

– Inégalité de réarrangement –

L'inégalité de réarrangement est la suivante. Quels que soient les réels $x_1, \ldots, x_n, y_1, \ldots, y_n$ et la permutation σ de l'ensemble $\{1, \ldots, n\}$ (c'est-ire une fonction telle que tout entier k compris entre 1 et n s'écrit sous la forme $k = \sigma(\ell)$ avec $1 \leqslant k \leqslant n$), on a :

$$x_1y_n + \cdots + y_1x_n \leqslant x_1y_{\sigma(1)} + \ldots + x_ny_{\sigma(n)} \leqslant x_1y_1 + \ldots + x_ny_n$$

Exercice 7
$\frac{b}{ca} + \frac{c}{ab} + \frac{a}{bc} \geqslant a + b + c.$

Exercice 8
Soit f une fonction injective de $\mathbb{N}$ dans $\mathbb{N}$. Montrer que $\sum_{k \leqslant n} \frac{f(k)}{k} \geqslant n$.

Exercice 9
Soit a, b, c trois réels strictement positifs. Montrer que

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} \geqslant \frac{3}{2}$$

– Solutions –

2 Arithmétique

1 Vocabulaire de base et congruences

Ce cours est directement issu de la partie du cours d'arithmétique pour débutants, disponible sur le site de la POFM, qui traite des congruences.

2 Nombres premiers et lemme de Gauss

L'arithmétique est une partie des mathématiques dont l'objet principal est l'étude des nombres entiers et des quatre opérations usuelles sur ces nombres entiers, que l'on voit à l'école primaire : l'addition, la soustraction, la multiplication et la division.

Dans la suite, on considérera principalement trois ensembles d'entiers :

— l'ensemble des entiers relatifs $(\ldots, -2, -1, 0, 1, 2, \ldots)$, que l'on note $\mathbb{Z}$;

— l'ensemble des entiers naturels $(0, 1, 2, \ldots)$, c'est-à-dire des entiers relatifs supérieurs ou égaux à 0, que l'on note $\mathbb{N}$;

— l'ensemble des entiers naturels non nuls $(1, 2, 3, \ldots)$, que l'on note $\mathbb{N}^*$.

Les notes ci-dessous concernent les cours donnés le matin du 26 août au groupe B et le matin du 27 août au groupe A. La seule différence entre ces deux cours concerne la partie « Nombres premiers et crible d'Ératosthène », qui n'a été traitée qu'avec le groupe A, et la partie « Équations diophantiennes linéaires », qui n'a été traitée qu'avec le groupe B.

– La relation de divisibilité –

Une notion de première importance en arithmétique, et qui sera au cœur de ce cours, et la relation de divisibilité.

Définition 2.2.1.
Soit a et b deux entiers relatifs. On dit que b *divise* a [1] s'il existe un entier relatif q tel que $a = b \times q$. On notera usuellement « $b \mid a$ » le fait que b divise a.

Exercice 1
Montrer que 2 divise 32, puis que 20 divise 320.

Exercice 2
Montrer que tout entier divise 0, mais que 0 ne divise aucun entier non nul.

Venons-en tout de suite à deux résultats cruciaux sur la relation de divisibilité. Le premier résultat stipule que tout multiple non nul d'un entier k est au moins aussi grand que k, et le second résultat signifie que la relation de divisibilité est *transitive*.

Théorème 2.2.2.
Soit a et b deux entiers relatifs. Si b divise a, alors soit $a = 0$, soit $|a| \geqslant |b|$.

1. ou que *b est un facteur de a* ; que *b est un diviseur de a* ; que *a est un multiple de b* ; que *a est divisible par b*.

Exercice 3
Démontrer le Théorème 2.2.2.

Exercice 4
Montrer que 3 ne divise pas 31.

Théorème 2.2.3.
Soit a, b et c trois entiers relatifs. Si a divise b et si b divise c également, alors a divise c.

Démonstration. Si $a \mid b$ et $b \mid c$, soit q_a et q_b deux entiers tels que $b = a \times q_a$ et $c = b \times q_b$. Alors $q_a \times q_b$ est un entier tel que $c = b \times q_b = a \times (q_a \times q_b)$, ce qui montre bien que $a \mid c$. □

Exercice 5
Trouver les diviseurs positifs de 20.

Exercice 6
Soit n un entier naturel non nul, et soit s le nombre de diviseurs positifs de n. Montrer que s est impair si et seulement s'il existe un entier k tel que $n = k^2$ (on dit que n est un *carré parfait*).

– La division euclidienne –

La division euclidienne est la division des entiers telles que vue à l'école primaire, et que l'on redéfinit ci-dessous.

Théorème 2.2.4.
Soit a un entier relatif et b un entier naturel non nul. Il existe un unique paire d'entiers relatifs (q, r) telle que $0 \leqslant r < b$ et telle que $a = b \times q + r$.

Définition 2.2.5.
Soit a un entier relatif et b un entier naturel non nul. Le résultat de la *division euclidienne* de a par b est la paire d'entiers relatifs (q, r) tels que $0 \leqslant r \leqslant b - 1$ et $a = b \times q + r$. Les entiers q et r sont respectivement appelés *quotient* et *reste* de la division euclidienne de a par b.

Exercice 7
Calculer le quotient et le reste de la division euclidienne de 37 par 5.

Exercice 8
Calculer le quotient et le reste de la division euclidienne de 123456789 par 37.

– Les congruences –

Avec la relation de divisbilité et la division euclidienne vient la notion, fort simple mais fort utile en pratique, de congruence.

Définition 2.2.6.
Soit a et a' deux entiers relatifs, et b un entier naturel non nul. On dit que *a est congru à a' modulo b*, ce que l'on note $a \equiv a' \pmod{b}$, si b divise $a - a'$.

Exercice 9
Que dire des entiers n tels que $n \equiv 0 \pmod{2}$? tels que $n \equiv 1 \pmod{2}$? tels que $n \equiv 2018 \pmod{2}$?

Exercice 10
Soit a et b deux entiers, soit d un entier naturel non nul, et soit a' et b' les deux restes de la division euclidienne de a et b par d. Montrer que $a \equiv b \pmod{d}$ si et seulement si $a' = b'$.

Les relations de congruences ont ceci de remarquable qu'elles permettent, dès lors que l'on considère des opérations d'addition, de soustraction et de multiplication, de se comporter comme la relation d'égalité.

Théorème 2.2.7.
Soit a, b et c trois entiers, et d un entier naturel non nul. Si $b \equiv c \pmod{d}$, alors $a + b \equiv a + c \pmod{d}$, $a - b \equiv a - c \pmod{d}$ et $a \times b \equiv a \times c \pmod{d}$.

Exercice 11
Démontrer le Théorème 2.2.7.

Remarque 2.2.8.
Attention ! Dans le cas général, dès lors que l'on utilise des opérations de division, les relations de congruences et d'égalité ne se comportent pas du tout de la même manière, y compris si la division tombe juste, c'est-à-dire si elle donne un reste nul !

Exercice 12
Montrer qu'il existe quatre entiers a, b, c et d, avec $d \geqslant 1$, tels que $b \equiv c \pmod{d}$ et tels que a divise à la fois b et c, mais tels que $b/a \not\equiv c/a \pmod{d}$.

Exercice 13
Démontrer qu'un nombre est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

En outre, l'utilisation de congruences peut être extrêmement utile lorsque l'on veut montrer qu'une certaine équation n'admet pas de solutions entières.

Exercice 14
Soit n un entier. Montrer que $n^2 + 1$ n'est divisible ni par 3, ni par 4.

– Algorithme d'Euclide –

Outre la notion de congruences, la division euclidienne est également à la base du célèbre algorithme d'Euclide, qui permet de calculer le plus grand diviseur commun (aussi

Algorithme 1 : Algorithme d'Euclide

Argument(s) : a et b ▷ On veut calculer $a \wedge b$

si $a \geqslant b$ **alors** on pose $u_0 = a$ et $v_0 = b$
sinon on pose $u_0 = b$ et $v_0 = a$
on pose également $i = 0$
tant que $v_i \neq 0$ **:**
    soit q_i et r_i le quotient et le reste de la division euclidienne de u_i par v_i
    on pose $u_{i+1} = v_i$ et $v_{i+1} = r_i$
    on augmente i de 1
renvoyer u_i

noté PGCD) de deux entiers naturels a et b. Ce plus grand diviseur commun sera couramment noté $\text{PGCD}(a, b)$, ou encore $a \wedge b$.

L'algorithme d'Euclide est décrit ci-dessus. Cependant, avant d'utiliser un tel algorithme, il est évidemment indispensable de montrer qu'il est correct. Dans cette perspective, on va d'abord démontrer un résultat intermédiaire qui s'avérera fort utile. C'est le *lemme d'Euclide*.

Lemme 2.2.9 (Lemme d'Euclide)**.**
Soit a et b deux entiers naturel non nuls. Soit également q et r le quotient et le reste de la division euclidienne de a par b. Alors les diviseurs communs à a et à b sont exactement les diviseurs communs à b et à r.

Munis de ce résultat, on peut alors prouver que l'algorithme d'Euclide est bien correct.

Théorème 2.2.10.
Le résultat de l'algorithme d'Euclide est égal à $a \wedge b$, et les diviseurs communs à a et à b sont exactement les diviseurs de $a \wedge b$.

Exercice 15
Démontrer le lemme d'Euclide puis le Théorème 2.2.10.

Exercice 16
Calculer le plus grand diviseur commun à 15 et à 70.

– Nombres premiers et crible d'Ératosthène – Groupe A uniquement –

Certains entiers en particulier jouent un rôle de première importance : il s'agit des entiers dont le PGCD vaut 1.

Définition 2.2.11.
Soit a et b deux entiers. On dit que a et b sont *premiers entre eux* si $a \wedge b = 1$.

Par exemple, 2 et 3 sont premiers entre eux, alors que 4 et 6 ne le sont pas, puisqu'ils sont tous les deux pairs.

Exercice 17
Parmi les paires d'entiers (a, b) telles que $1 \leqslant a \leqslant b \leqslant 5$, combien y en a-t-il pour lesquelles a et b soient premiers entre eux ?

Par ailleurs, il existe également d'autres nombres, bien plus connus du grand public, ayant des propriétés de divisibilité remarquables : ce sont les nombres premiers.

Définition 2.2.12.
On dit qu'un entier n est *premier* si n a exactement 2 diviseurs positifs, que sont 1 et n. Sinon, on dit que n est *composé*.

Remarque 2.2.13.
L'entier 1 n'est donc pas premier !

De la définition des nombres premiers découle rapidement les résultats cruciaux que voici.

Théorème 2.2.14.
Soit n un entier et p un nombre premier. Soit p divise n, soit p est premier avec n, ces deux cas étant mutuellement incompatibles.

Démonstration. Tout d'abord, si p divise n, alors p est un diviseur commun à p et à n, donc $p \wedge n \neq 1$, ce qui montre que p et n ne sont pas premiers entre eux. Supposons maintenant que p ne divise pas n, et posons $d = p \wedge n$. Puisque d divise p, on sait que $d = 1$ ou que $d = p$. Puisque d divise n, c'est que $d \neq p$, et donc que $d = 1$. □

Théorème 2.2.15.
Soit n un entier tel que $n \geqslant 2$, et soit p le plus petit diviseur de n tel que $p \geqslant 2$. Alors l'entier p est un nombre premier.

Démonstration. Puisque $p \geqslant 2$, on sait déjà que 1 et p sont deux diviseurs distincts de p. Soit maintenant d un diviseur de p. D'après le Théorème 2.2.3, et puisque p divise n, on sait que d divise n également. Par minimalité de p, on en déduit que $d = 1$ ou $d = p$, ce qui signifie que p est premier. □

Il est donc très important de pouvoir détecter si un entier n est premier ou non. Y parvenir efficacement est une question difficile, qui sera l'objet du cours sur les « tests de primalité » donné au groupe D. En revanche, il existe déjà une méthode ancienne et relativement efficace quand n est petit : il s'agit du crible d'Ératosthène, qui permet d'identifier l'ensemble des nombres premiers inférieurs ou égaux à n.

Comme pour l'algorithme d'Euclide, il convient de montrer que le crible d'Ératosthène nous renvoie bien la liste des nombres premiers $p \leqslant n$.

Théorème 2.2.16.
La liste des entiers que renvoie le crible d'Ératosthène est bien la liste des nombres premiers $p \leqslant n$.

Algorithme 2 : Crible d'Ératosthène

Argument(s) : n ▷ On veut identifier les nombres premiers $p \leqslant n$
on écrit tous les entiers de 2 à n
au fur et à mesure, on va soit les rayer, soit les entourer d'un cercle
tant que l'on a un entier $p \leqslant \sqrt{n}$ ni rayé, ni entouré **:**
    on choisit le plus petit tel entier p et on l'entoure
    on raye tous les multiples de p compris entre p^2 et n et qui n'étaient pas déjà rayés
renvoyer la liste des entiers que l'on n'a pas rayés (même ceux qui ne sont pas entourés)

Démonstration. Notre preuve va procéder par récurrence sur n. Tout d'abord, si $n = 1$, le résultat est évident. On suppose donc que $n \geqslant 2$ et que, si l'on fait fonctionner le crible d'Ératosthène en lui donnant $n-1$ comme argument, il nous renvoie bien la liste des nombres premiers $p \leqslant n - 1$. Regardons alors comment il se comporte quand on lui donne n comme argument.

Déjà, il est clair que les entiers $k \leqslant n-1$ que l'on va rayer sont les mêmes, que l'argument de l'algorithme soit $n - 1$ ou n. Il reste donc à montrer que l'on va rayer si n est composé, mais pas si n est premier.

Si n est premier, on ne va clairement jamais le rayer. On traite donc le cas où n est composé. Soit alors p son plus petit diviseur tel que $p \geqslant 2$. Le Théorème 2.2.15 montre que p est premier. De plus, puisque $n = p \times (n/p)$ et que $p < n$, on sait que n/p est un diviseur de n supérieur ou égal à 2, donc que $n/p \geqslant p$. Cela montre que $p \leqslant \sqrt{n}$.

Puisque p est premier, on ne va jamais le rayer, donc on va finir par l'entourer. Ce faisant, et puisque $n \geqslant p^2$, on va nécessairement rayer n. Ceci conclut la preuve du théorème. □

Exercice 18
Lister tous les nombres premiers p tels que $2 \leqslant p \leqslant 100$.

– Théorèmes de Bézout et de Gauss –

Maintenant que tous les outils ci-dessus ont été définis, nous allons démontrer deux théorèmes très importants en arithmétique, et qu'il faut donc absolument connaître. Le premier théorème est dû à Étienne Bézout.

Théorème 2.2.17 (Théorème de Bézout)**.**
Deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers n et m tels que

$$a \times m + b \times n = 1.$$

On dit alors que l'égalité $a \times m + b \times n = 1$ ci-dessus est une *relation de Bézout*.
Démonstration. Soit X l'ensemble $\{a \times m + b \times n \ : \ m, n \in \mathbb{Z}\}$, et soit x le plus petit entier naturel non nul appartenant à l'ensemble X. Pour plus de commodité, et pour tout élément t de X, on notera par la suite m_t et n_t deux entiers relatifs tels que $t = a \times m_t + b \times n_t$.

Posons ensuite $d = a \wedge b$. On va montrer successivement que $d \leqslant x$ et que $x \leqslant d$. Cela signifiera que $x = d$, ce qui conclura la preuve du théorème.

Tout d'abord, soit a' et b' deux entiers tels que $a = d \times a'$ et $b = d \times b'$. Mais alors

$$x = a \times m_x + b \times n_x = d \times (a' \times m_x + b' \times n_x)$$

est divisible par d, ce qui montre que $d \leqslant x$.

Réciproquement, soit $u_0, v_0, \ldots, u_k, v_k$ les entiers construits lors de l'exécution de l'algorithme d'Euclide. On va prouver par récurrence sur i que chacun des entiers u_i et v_i appartient à X. L'initialisation, pour $i = 0$, est évidente puisque u_0 et v_0 sont égaux à a et b.

Passons maintenant à l'hérédité, et supposons que l'on dispose d'un entier $i \leqslant k - 1$ tels que u_i et v_i soient tous deux des éléments de X. Soit q_i et r_i le quotient et le reste de la division euclidienne de u_i par v_i. Alors $u_{i+1} = v_i$ appartient évidemment à X, et

$$v_{i+1} = r_i = u_i - q_i \times v_i = a \times (m_{u_i} - q_i \times m_{v_i}) + b \times (n_{u_i} - q_i \times n_{v_i})$$

appartient à X également.

Ceci prouve l'hérédité de notre récurrence. En particulier, cela montre que l'entier u_k, qui est égal à d d'après le Théorème 2.2.10, appartient bien à X. On en déduit que $x \leqslant d$, ce qui conclut comme prévu la preuve. □

Exercice 19
Soit n un entier naturel. Montrer que la fraction

$$\frac{21n + 4}{14n + 3}$$

est irréductible.

Exercice 20
Trouver les entiers naturels n tels que la fraction

$$\frac{21n + 4}{14n + 1}$$

soit irréductible.

Le second théorème est dû à Carl Friedrich Gauss.

Théorème 2.2.18 (Théorème de Gauss)**.**
Soit a, b et c trois entiers naturels tels que a divise $b \times c$. Si a et b sont premiers entre eux, alors a divise c.

Démonstration. Puisque $a \wedge b = 1$, le théorème de Bézout indique qu'il existe deux entiers m et n tels que $a \times m + b \times n = 1$. Soit ensuite k un entier tel que $b \times c = a \times k$. Il apparaît alors que

$$c = c \times (a \times m + b \times n) = a \times c \times m + b \times c \times n = a \times c \times m + a \times k \times n$$

est bien un multiple de a. □

Exercice 21
Soit p un nombre premier et soit a et b deux entiers tels que le produit $a \times b$ soit divisible par p. Montrer que p divise soit a, soit b (soit les deux).

Exercice 22
Soit m et n deux entiers tels que n divise $m(n + 1)$. Montrer que n divise m.

– Équations diophantiennes linéaires – Groupe B uniquement –

Les théorèmes de Bézout et de Gauss s'avèrent en fait très utiles dès l'instant où l'on souhaite résoudre des équations dont les inconnues sont des nombres entiers : on dit qu'il s'agit là d'équations *diophantiennes*. Regardons maintenant de plus près certaines de ces équations diophantiennes, que sont les équations diophantiennes linéaires.

Définition 2.2.19.
Une *équation diophantienne linéaire* est une équation de la forme

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = a_0,$$

où les entiers $a_0, a_1, \ldots, a_k$ sont donnés, et où l'on cherche les valeurs entières que peuvent prendre les inconnues $x_1, x_2, \ldots, x_k$.

Le mieux n'est sans doute pas d'essayer de développer une théorie générale sur la résolution de ces équations, mais de les pratiquer directement, dans le cas où elles ont deux variables.

Exercice 23
Résoudre les trois équations diophantiennes linéaires suivantes :

$$2x + 3y = 5,\ 2x + 5y = 10 \text{ et } 3x + 9y = 2018.$$

– Solutions des exercices –

Solution de l'exercice 1
Il suffit de remarquer que $32 = 2 \times 16$ et que $320 = 20 \times 16$.

Solution de l'exercice 2
Pour tout entier $n \in \mathbb{Z}$, l'égalité $0 = n \times 0$ montre bien que n divise 0. En revanche, si 0 divise n, alors il existe un entier $q \in \mathbb{Z}$ tel que $n = 0 \times q = 0$, ce qui signifie que n est nul.

Solution de l'exercice 3
Soit q un entier tel que $a = b \times q$. Si $a \neq 0$, alors $q \neq 0$, donc $|q| \geqslant 1$, de sorte que

$$|a| = |b \times q| = |b| \times |q| \geqslant |b|.$$

Solution de l'exercice 4
Procédons par l'absurde, et supposons qu'il existe un entier q tel que $31 = 3 \times q$. Alors $3 \times 10 = 30 < 31 = 3 \times q < 33 = 3 \times 11$, donc $10 < q < 11$, ce qui est impossible. Notre supposition était donc bien absurde, ce qui montre effectivement que 3 ne divise pas 31.

Solution de l'exercice 5
Soit d un diviseur positif éventuel de 20. D'après le Théorème 2.2.2, on sait que $0 \leqslant d \leqslant 20$. En vertu des égalités

$$20 = 1 \times 20 = 2 \times 10 = 4 \times 5 = 5 \times 4 = 10 \times 2 = 20 \times 1,$$

on sait déjà que 1, 2, 4, 5, 10 et 20 sont des diviseurs positifs de 20.

D'autre part, on sait que $d \neq 0$, pusique 0 ne divise aucun entier non nul. Par ailleurs, puisque $3 \times 6 = 18 < 20 < 21 = 3 \times 7$, $7 \times 2 = 14 < 20 < 21 = 7 \times 3$ et $8 \times 2 = 16 < 20 < 24 = 8 \times 3$, on sait que 3, 7 et 8 ne sont pas des diviseurs de 20.

Par ailleurs, 3 divise $6 = 3 \times 2$ et $9 = 3 \times 3$, donc puisque 3 ne divise pas 20, le Théorème 2.2.3 montre que 6 et 9 ne divisent pas 20 non plus. Enfin, pour tout entier k tel que $11 \leqslant k \leqslant 19$, on sait que $k < 20 < k \times 2$, donc que k ne divise pas 20.

En conclusion, les diviseurs positifs de 20 sont 1, 2, 4, 5, 10 et 20.

Solution de l'exercice 6

Soit $d_1 < d_2 < \ldots < d_s$ les diviseurs positifs de n. D'après le Théorème 2.2.2, on sait que $1 \leqslant d_1$ et que $d_s \leqslant n$. Or, pour tout diviseur d de n, on sait que n/d est aussi un diviseur de n, puisque $n = d \times (n/d)$.

Par conséquent, la fonction $x \mapsto n/x$ est une fonction injective de l'ensemble $\mathcal{D}_n = \{d_1, d_2, \ldots, d_s\}$ dans lui-même. Puisque $\mathcal{D}_n$ est fini, c'est une bijection, et elle est décroissante, de sorte que $d_\ell \times d_{s+1-\ell} = n$ pour tout $\ell \leqslant s$.

En particulier, si $n = k^2$, alors il existe un entier ℓ tel que $k = d_\ell$, et l'on en déduit que $d_\ell \times d_{s+1-\ell} = n = k^2 = d_\ell^2$, ce qui signifie que $s + 1 - \ell = \ell$, donc que $s = 2\ell - 1$ est impair. Réciproquement, si s est impair, en posant $\ell = (s+1)/2$, on a bien $n = d_\ell^2$, donc n est un carré parfait.

Solution de l'exercice 7

Il suffit de constater que $37 = 5 \times 7 + 2$ pour conclure que le quotient et le reste recherchés sont respectivement les entiers $q = 7$ et $r = 2$.

Solution de l'exercice 8

On ne va évidemment pas pouvoir parachuter la solution de cet exercice comme on l'a fait précédemment. On pose donc sagement la division de l'entier $a = 123456789$ par l'entier $b = 37$, comme suit :

$$
\begin{array}{ccccccccc|ccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 3 & 7 & & & & & \\
\cline{10-16}
 & 1 & 2 & 4 & & & & & & 3 & 3 & 3 & 6 & 6 & 6 & 9 \\
 & & 1 & 3 & 5 & & & & & & & & & & & \\
 & & & 2 & 4 & 6 & & & & & & & & & & \\
 & & & & 2 & 4 & 7 & & & & & & & & & \\
 & & & & & 2 & 5 & 8 & & & & & & & & \\
 & & & & & & 3 & 6 & 9 & & & & & & & \\
 & & & & & & & 3 & 6 & & & & & & &
\end{array}
$$

On en conclut que le quotient et le reste recherchés sont respectivement les entiers $q = 3336669$ et $r = 36$.

Solution de l'exercice 9

Les entiers n tels que $n \equiv 0 \pmod 2$, ou bien tels que $n \equiv 2018 \pmod 2$, sont les entiers pairs, alors que les entiers n tels que $n \equiv 1 \pmod 2$ sont les entiers impairs.

Solution de l'exercice 10

Soit q_a et q_b les quotients respectifs de a et b quand on les divise par d. Si $a' = b'$, alors

$$a - b = (q_a \times d + a') - (q_b \times d + b') = (q_a - q_b) \times d$$

est bien divisible par d, ce qui signifie que $a \equiv b \pmod{d}$.

Réciproquement, si $a \equiv b \pmod{d}$, alors d divise $a - b$, donc il existe un entier k tel que $a - b = d \times k$. On remarque alors que

$$a' - b' = (a - q_a \times d) - (b - q_b \times d) = (a - b) + (q_b - q_a) \times d = (k + q_b - q_a) \times d$$

est divisible par d. Or, a' et b' sont tous les deux compris entre 0 et $d - 1$. Cela montre que $1 - d \leqslant -b' \leqslant a' - b' \leqslant a' \leqslant d - 1$, donc que $|b' - a'| \leqslant d - 1 < d$. Par conséquent, le Théorème 2.2.2 montre que $b' - a' = 0$, ce qui conclut l'exercice.

Solution de l'exercice 11

Puisque $b \equiv c \pmod{d}$, soit k un entier tel que $b - c = k \times d$. Alors

$$(a + b) - (a + c) = k \times d,\ (a - b) - (a - c) = (-k) \times d \text{ et } (a \times b) - (a \times c) = (k \times a) \times d,$$

ce qui montre bien le Théorème 2.2.7.

Solution de l'exercice 12

Il suffit, par exemple, de choisir les entiers $a = 2$, $b = 4$, $c = 0$ et $d = 4$.

Solution de l'exercice 13

Soit $n = \sum_{k=0}^{d} 10^k \times n_k$ un entier, et soit $S = \sum_{k=0}^{d} n_k$ la somme de ses chiffres. Puisque $10 \equiv 1 \pmod{9}$, une récurrence immédiate montre, pour tout $k \geqslant 0$, que $10^k \equiv 1^k \equiv 1 \pmod{9}$. On en déduit que $n \equiv \sum_{k=0}^{d} 10^k n_k \equiv \sum_{k=0}^{d} n_k \equiv S \pmod{9}$. Cela signifie que 9 divise $n - S$, et donc, en particulier, que n est divisible par 9 si et seulement si S est divisible par 9.

Solution de l'exercice 14

On va traiter séparément les cas de la divisibilité par 3 et par 4, en procédant à chaque fois à une disjonction de cas.

Tout d'abord, si $n \equiv 0 \pmod{3}$, alors $n^2 + 1 \equiv 0^2 + 1 \equiv 1 \not\equiv 0 \pmod{3}$; si $n \equiv 1 \pmod{3}$, alors $n^2 + 1 \equiv 1^2 + 1 \equiv 2 \not\equiv 0 \pmod{3}$; et, si $n \equiv 2 \pmod{3}$, alors $n^2 + 1 \equiv 2^2 + 1 \equiv 5 \not\equiv 0 \pmod{3}$. On a ainsi montré que 3 ne divisait jamais $n^2 + 1$.

De même, selon que $n \equiv 0, 1, 2 \text{ ou } 3 \pmod{4}$, on vérifie que $n^2 + 1 \equiv 1, 2, 1 \text{ ou } 2 \pmod{4}$, ce qui montre bien que 4 ne divisie pas $n^2 + 1$ non plus.

Solution de l'exercice 15

Commençons par montrer le lemme d'Euclide. Soit d un diviseur commun à a et b, et soiet δ un diviseur commun à b et r. On note a_d et b_d les entiers tels que $a = d \times a_d$ et $b = d \times b_d$, et on note b_δ et r_δ les entiers tels que $b = \delta \times b_\delta$ et $r = \delta \times r_\delta$.

Alors $r = a - q \times b = d \times (a_d - q \times b_d)$ est bien divisible par d, et $a = r + q \times b = \delta \times (r_\delta + q \times b_\delta)$ est bien divisible par δ. Cela signifie que tout diviseur commun à a et à b divise également b et r, et réciproquement. Le lemme d'Euclide est donc démontré.

Soit alors $u_0, v_0, \ldots, u_k, v_k$ les entiers construits par l'algorithme d'Euclide. Une récurrence immédiate sur i montre alors que, pour tout entier i compris entre 0 et k, les diviseurs communs à u_i et v_i sont exactement les diviseurs communs à a et b. Puisque $v_k = 0$, ces diviseurs sont donc également les diviseurs de u_k.

En particulier, le plus grand diviseur commun à a et à b est également le plus grand diviseur de u_k, c'est-à-dire u_k lui-même, ce qui conclut la preuve du Théorème 2.2.10.

Solution de l'exercice 16

Il suffit d'appliquer l'algorithme d'Euclide : on vérifie aisément que $70 = 15 \times 4 + 10$, puis que $15 = 10 \times 1 + 5$, et enfin que $10 = 5 \times 2 + 0$. Cela montre que $70 \wedge 15 = 5$, ce qui n'était de toute façon pas très surprenant.

Solution de l'exercice 17
Il suffit de lister les diviseurs positifs de chaque entier compris entre 1 et 5 : chaque entier $n \in \{1, 2, 3, 5\}$ n'est divisible que par 1 et par lui-même, alors que 4 est divisible par 1, 2 et 4. Par conséquent, si $1 \leqslant a \leqslant b \leqslant 5$, l'entier $a \wedge b$ est différent de 1 si et seulement si $a = b \geqslant 2$ ou si $(a, b) = (2, 4)$.

Or, il existe $5+4+3+2+1 = 15$ paires (a, b) telles que $1 \leqslant a \leqslant b \leqslant 5$. Sur ces 15 paires, on vient d'en dénombrer 5 telles que $a \wedge b \neq 1$. Il y en a donc 10 telles que a et b soient premiers entre eux.

Solution de l'exercice 18
En appliquant directement le crible d'Ératosthène, on constate que les nombres premiers $p \leqslant 100$ sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 87 et 97.

Solution de l'exercice 19
Il s'agit en fait de montrer que les entiers $21n+4$ et $14n+3$ sont premiers entre eux. Mais c'est là une conséquence directe du théorème de Bézout et de l'égalité

$$3 \times (14n + 3) - 2 \times (21n + 4) = (3 \times 14 - 3 \times 21) \times n + (3 \times 3 - 2 \times 4) = 1.$$

Solution de l'exercice 20
Cette fois-ci, la méthode utilisée à l'exercice précédent ne marche pas exactement comme prévu. En effet, on ne peut pas obtenir beaucoup mieux que l'égalité

$$2 \times (21n + 4) - 3 \times (14n + 1) = (2 \times 21 - 3 \times 14) \times n + (2 \times 4 - 3 \times 1) = 5.$$

Soit alors d l'entier $(21n+4) \wedge (14n+1)$: on vient en fait de montrer que d divise nécessairement 5. Cela signifie que d vaut soit 1, soit 5.

Notons maintenant r le reste de la division euclidienne de n par 5. On vérifie aisément, en considérant une à une les 5 valeurs possibles de r, que $14r + 1 \equiv 0 \pmod 5$ si et seulement si $r = 1$. Puisque $14n + 1 \equiv 14r + 1 \pmod 5$, cela signifie que $14n + 1$ est divisible par 5 si et seulement si $n \equiv 1 \pmod 5$. Mais alors, dans ce cas, on a également $21n + 4 \equiv 21 + 4 \equiv 0 \pmod 5$, de sorte que $d = 5$.

En conclusion, on a $d = 5$ si $n \equiv 1 \pmod 5$, et $d = 1$ sinon. En particulier, les entiers n recherchés sont exactement les entiers n tels que $n \not\equiv 1 \pmod 5$.

Solution de l'exercice 21
Supposons que p ne divise pas a. Puisque les diviseurs de p sont 1 et p lui-même, cela signifie que $p \wedge a = 1$, c'est-à-dire que p et a sont premiers entre eux. Le théorème de Gauss indique alors que p divise b.

Solution de l'exercice 22
La relation de Bézout $(n + 1) - n = 1$ montre que n et $n + 1$ sont premiers entre eux. Par conséquent, le théorème de Gauss montre que n divise m.

Solution de l'exercice 23
Nous allons résoudre une par une chacune des trois équations diophantiennes de l'énoncé.

Tout d'abord, si $2x + 3y = 5$, alors $y \equiv 2x + 3y \equiv 5 \equiv 1 \pmod 2$ et $-x \equiv 2x + 3y \equiv 5 \equiv -1 \pmod 3$, donc $x \equiv 1 \pmod 3$. On peut alors poser $x = 3k + 1$ et $y = 2\ell + 1$, et notre équation devient :

$$2(3k + 1) + 3(2\ell + 1) = 5,$$

c'est-à-dire $6(k + \ell) = 0$. Les solutions (x, y) sont donc obtenues lorsque $\ell = -k$: il s'agit des éléments de l'ensemble $\mathcal{S}_1 = \{(3k + 1, -2k + 1) : k \in \mathbb{Z}\}$.

De même, si $2x + 5y = 10$, le même raisonnement indique qu'il existe des entiers k et ℓ tels que $x = 5k$ et $y = 2\ell$. Notre équation devient alors $10(k + \ell) = 1$, et les solutions (x, y) sont donc les éléments de l'ensemble $\mathcal{S}_2 = \{(5k, 2 - 2k) : k \in \mathbb{Z}\}$.

Enfin, si $3x + 9y = 2018$, en passant modulo 3, on remarque que $0 \equiv 2 \pmod 3$, ce qui est évidemment impossible. Il n'y a donc aucune solution (x, y) telle que x et y soient tous deux entiers.

3 Combinatoire

1 Raisonnements et principe des tiroirs

Ce cours est directement issu du cours de stratégies de base disponible sur le site de la POFM.

2 Récurrence

Ce cours a pour but d'introduire la récurrence simple et de proposer suffisamment d'exercices pour que les élèves puissent se familiariser avec cette notion. Il s'inspire entre autres du cours donné par Clara Ding à Valbonne en 2015.

– La récurrence –

La récurrence est une méthode de raisonnement mathématique qui permet notamment de prouver des propriétés du type « $\forall n \in \mathbb{N}$, la propriété $P(n)$ est vraie » où $P(n)$ est une propriété qui dépend d'un paramètre naturel n. Elle est un outil fort utile, principalement en arithmétique et en combinatoire. Elle peut être la principale idée de résolution d'un exercice, mais aussi intervenir dans la démonstration d'un simple résultat intermédiaire.

– Principe –

Le principe du raisonnement par récurrence est fort simple. Il consiste à montrer d'abord que la propriété est vraie pour 0, le premier nombre naturel, puis à supposer que la propriété est vraie pour un naturel j quelconque et, fort de cette information, à montrer qu'elle est également vraie pour le naturel $j+1$. Ainsi, puisque la propriété est vraie pour le naturel 0, elle est vraie pour $0+1=1$; comme elle est vraie pour 1, elle est vraie pour $1+1=2$, puis pour $2+1=3$ et ainsi de suite. Intuitivement, on peut comparer le raisonnement par récurrence à la montée d'une échelle : si on peut monter sur le premier barreau d'une échelle, et si d'un barreau on peut monter sur le suivant, alors on peut monter n'importe quelle échelle.

Plus rigoureusement, un raisonnement par récurrence se rédige en trois étapes :

1. **Initialisation** : Montrer que $P(0)$ est vraie.
2. **Hérédité** : Poser j un naturel quelconque. Supposer que $P(j)$ est vraie et montrer que $P(j+1)$ est vraie.
3. **Conclusion** : Conclure par récurrence que $P(n)$ est vraie pour tout $n \in \mathbb{N}$. (Cette étape est une étape importante dans la rédaction de la solution, même si on n'y fait aucun raisonnement)

Remarque 3.2.1.
Dans beaucoup de cas, la propriéte cherchée n'est pas à montrer pour tout $n \in \mathbb{N}$ mais bien pour tout n entier supérieur à N, où N est un entier fixé par le contexte ou l'énoncé. Le raisonnement par récurrence est toujours efficace, mais il doit s'adapter : on initialise en montrant $P(N)$ plutôt que $P(0)$, et dans l'hérédité j n'est plus un naturel quelconque mais un naturel supérieur à N.

Remarque 3.2.2.
La lettre utilisée pendant l'hérédité est muette, on peut utiliser n'importe quel symbole. Ici, on utilisera j par souci de clarté, mais on préfère généralement la lettre n.

– Premiers exemples –

Telle que décrite ci-dessus, la méthode peut paraître abstraite, voire obscure. Familiarisons-nous donc avec elle en résolvant quelques exercices.

Le premier est un grand classique, et une formule très importante à connaître.

Exemple 3.2.3.
Pour tout naturel n, soit $P(n)$ la propriété

$$0+1+\ldots+n=\frac{n(n+1)}{2}$$

Montrer que $P(n)$ est vraie pour tout n.

Solution :

— Initialisation : On a bien $0=\frac{0\cdot 1}{2}$, donc $P(0)$ est vraie.

— Hérédité : Supposons que $P(j)$ soit vraie, i.e. que $0+1+\ldots+j=\frac{j(j+1)}{2}$. On a alors

$$\begin{aligned} 0+1+\ldots+j+(j+1) &= (0+1+\ldots+j)+(j+1) \\ &= \frac{j(j+1)}{2}+(j+1) \\ &= \frac{j(j+1)+2(j+1)}{2} \\ &= \frac{(j+2)(j+1)}{2} \end{aligned}$$

où l'hypothèse de récurrence est utilisée entre les deux premières lignes, et donc $P(j+1)$ est également vérifiée.

— Conclusion : Par récurrence, $P(n)$ est dès lors vraie pour tout naturel n.

A présent, passons à un problème plus proche de ce que l'on peut trouver en Olympiades :

Exemple 3.2.4.
On trace n cercles distincts dans un plan, deux quelconques de ces cercles n'étant pas tangents. Montrer qu'on peut colorier chaque région ainsi délimitée du plan en bleu ou en rouge de telle sorte que deux régions séparées par un arc soient de couleurs différentes.

Solution :
On procède par récurrence sur la propriété $P(n)$: « Étant donnés n cercles distincts non tangents deux à deux, on peut colorier les régions ainsi déterminées en deux couleurs sans que deux régions adjacentes n'aient la même couleur », avec n un naturel supérieur ou égal à 1.

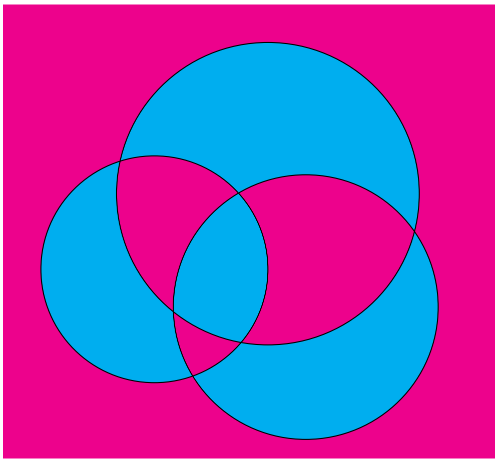


FIGURE 1 – Exemple de coloriage possible pour $n = 3$

— **Initialisation** : $P(1)$ est clairement vraie : Si on a 1 cercle dans le plan, il suffit de colorier son intérieur en rouge et son extérieur en bleu.

— **Hérédité** : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$: Soient $j+1$ cercles non tangents deux à deux. On peut les numéroter $1, \ldots, j+1$. Oublions momentanément le cercle numéroté $j+1$. Les j cercles restants ne sont pas tangents deux à deux, on peut donc colorier les régions délimitées en deux couleurs sans donner la même couleur à deux régions adjacentes, vu l'hypothèse de récurrence. A présent, rajoutons le cercle numéro $j+1$ et changeons la couleur de toutes les régions se trouvant à l'intérieur.

  Montrons qu'un tel coloriage respecte l'énoncé : Si deux régions sont adjacentes de part et d'autre du cercle $j+1$, elles sont bien de couleurs différentes, car seule une des deux a changé de couleur. Si elles étaient adjacentes de part et d'autre d'un autre cercle, elles étaient de couleurs différentes et ont soit changé toutes les deux, soit sont restées identiques. Elles sont donc toujours de couleurs différentes.

— **Conclusion** : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 1, et on a démontré ce qu'il fallait.

– Erreurs à éviter –

Deux embûches principales guettent l'élève distrait :

— **Oublier l'initialisation.** Bien qu'elle soit souvent facile, l'initialisation reste importante. L'oublier peut conduire au genre de raisonnement suivant :

  Montrons que $3^n + 1$ est multiple de 3 pour tout n naturel non nul. On a

$$\begin{aligned} 3^{j+1} + 1 &= 3 \cdot 3^j + 1 \\ &= 2 \cdot 3^j + (3^j + 1) \end{aligned}$$

  et comme les deux termes de droite sont multiples de 3, le premier de manière évidente et le deuxième par hypothèse de récurrence, $3^{j+1} + 1$ l'est également, donc on a fini la récurrence et $3^n + 1$ est multiple de $3 \quad \forall n \in \mathbb{N}$ avec $n \geqslant 1$.

— **Faire involontairement des suppositions sur j dans l'hérédité.** Lors de l'hérédité, il faut prendre garde à ne pas utiliser involontairement une propriété que tous les naturels n'ont pas, en pensant notamment aux « petits » nombres. Voici un exemple de raisonnement engendré par cette erreur :

Montrons que tous les chevaux sont de la même couleur, par récurrence sur le nombre n de chevaux avec la propriété : $P(n)$: « Dans un groupe de n chevaux quelconques, tous les chevaux sont de la même couleur ».

Initialisation : Si on a un groupe d'un seul cheval, il est évident que tous les chevaux du groupe sont de la même couleur.

Hérédité : Supposons que $P(j)$ est vraie et montrons $P(j+1)$: soit un groupe de $j+1$ chevaux. Les j premiers chevaux sont tous de la même couleur par hypothèse de récurrence, de même que les j derniers, et les deux couleurs communes sont identiques puisque les groupes ont des chevaux en commun. Dès lors, tous les chevaux sont de la même couleur.

L'erreur du raisonnement est d'affirmer que les groupes ont des chevaux en commun : cela n'est pas vrai quand $j = 1$, donc savoir que $P(1)$ est vraie ne permet pas d'affirmer que $P(2)$ l'est, et la récurrence s'effondre.

– Exercices –

Exercice 1
Montrer que pour tout entier $n \geqslant 1$, on a les deux égalités

$$\begin{aligned} 1^2 + 2^2 + \ldots + n^2 &= \frac{n(n+1)(2n+1)}{6} \\ 1^3 + 2^3 + \ldots + n^3 &= (1 + 2 + \ldots + n)^2 \end{aligned}$$

Exercice 2
Montrer que pour tout entier $n \geqslant 1$, on a les deux égalités

$$\begin{aligned} \sum_{k=1}^{n} \frac{1}{k(k+1)} &= \frac{n}{n+1} \\ \sum_{k=1}^{n} k \cdot k! &= (n+1)! - 1 \end{aligned}$$

Exercice 3
Soit $n \geqslant 1$ un naturel et $a > 0$. Montrer les inégalités suivantes :

$$\begin{aligned} 2^{n-1} &\leqslant n! \\ n! &\leqslant n^n \\ (n+3)^2 &\leqslant 2^{n+3} \\ 1 + n \cdot a &\leqslant (1+a)^n \end{aligned}$$

Exercice 4
La suite de Fibonnaci est définie par $F_0 = 0$, $F_1 = 1$ et pour tout $n \in \mathbb{N}$ avec $n \geqslant 2$: $F_n = F_{n-1} + F_{n-2}$. Montrer que pour tout $n \in \mathbb{N}$ on a

$$\sum_{k=0}^{n} F_k^2 = F_n \cdot F_{n+1}$$

Exercice 5
Montrer que pour tout entier $n \geqslant 1$, on a

$$\sum_{k=1}^{n} \frac{1}{k^2} \leqslant 2$$

Exercice 6
Trouver une formule permettant de calculer la somme des angles d'un polygone convexe à n côtés ($n \geqslant 3$).

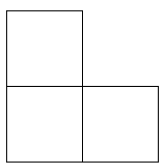
Exercice 7
Soit $n \geqslant 3$. Monter qu'il existe $x_1, \ldots, x_n$ des entiers positifs deux à deux distincts tels que

$$\frac{1}{x_1} + \ldots + \frac{1}{x_n} = 1$$

Exercice 8
Dans un certain pays, deux villes sont toujours reliées soit par une ligne aérienne, soit par un canal navigable. Montrer qu'un des deux moyens de transport permet de voyager de n'importe quelle ville à n'importe quelle autre.

Exercice 9
Les gentils animatheux organisent un tournoi de jeu de hex (il n'y a donc pas de parties nulles). Chacun joue contre tous les autres participants. A la fin du tournoi, chacun écrit la liste des joueurs qu'il a battus et des joueurs que ceux-ci ont battus. Montrer qu'un des joueurs a sur sa liste tous les autres participants.

Exercice 10
Soit n un naturel non nul. On considère un damier de côté 2^n dont on a supprimé une case quelconque. Montrer qu'on peut le recouvrir sans trou ni superposition par des pièces en L comme celle ci-dessous (rotations et symétries sont autorisées).



Exercice 11
Dans le plan, on donne un polygone régulier à $n \geqslant 3$ côtés. Ses sommets sont coloriés en rouge, bleu ou vert de manière à ce que deux sommets consécutifs ne soient jamais de la même couleur et qu'il y ait au moins un sommet de chaque couleur. Montrer qu'on peut tracer des diagonales du polygone qui ne s'intersectent que sur ses sommets de manière à le découper en triangles ayant chacun trois sommets de couleur différente.

– Solutions –

Solution de l'exercice 1
Pour le premier exercice, on procède par récurrence avec la propriété

$$P(n) : 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

— Initialisation : $P(1)$ est vraie : les deux membres valent 1.
— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. On a

$$\begin{aligned}
1^2 + \ldots + j^2 + (j+1)^2 &= (1^2 + \ldots + j^2) + (j+1)^2 \\
&= \frac{j(j+1)(2j+1)}{6} + (j+1)^2 \\
&= \frac{j(j+1)(2j+1) + 6(j+1)^2}{6} \\
&= \frac{(j+1)(j(2j+1) + 6(j+1))}{6} \\
&= \frac{(j+1)(2j^2 + 7j + 6)}{6} \\
&= \frac{(j+1)(j+2)(2j+3)}{6}
\end{aligned}$$

et $P(j+1)$ est donc vraie.
— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 1, et l'énoncé est démontré.

Pour le second, on fait de même avec la propriété $P(n) : 1^3+2^3+\ldots+n^3 = (1+2+\ldots+n)^2$ et en utilisant le premier exemple :
— Initialisation : $P(1)$ est vraie : les deux membres valent 1.
— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. On a

$$\begin{aligned}
1^3 + \ldots + j^3 + (j+1)^3 &= (1^3 + \ldots + j^3) + (j+1)^3 \\
&= \left(\frac{j(j+1)}{2}\right)^2 + (j+1)^3 \\
&= \frac{j^2(j+1)^2 + 4(j+1)^3}{4} \\
&= \frac{(j+1)^2(j^2 + 4(j+1))}{4} \\
&= \frac{(j+1)^2(j+2)^2}{4} \\
&= (1 + \ldots + (j+1))^2
\end{aligned}$$

et $P(j+1)$ est donc vraie.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 1, et l'énoncé est démontré.

Solution de l'exercice 2
Pour le premier exercice, on procède par récurrence avec la propriété

$$P(n) : \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$$

— Initialisation : $P(1)$ est vraie : les deux membres valent $\frac{1}{2}$.
— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. On a

$$\begin{aligned}
\sum_{k=1}^{j+1} \frac{1}{k(k+1)} &= \sum_{k=1}^{j} \frac{1}{k(k+1)} + \frac{1}{(j+1)(j+2)} \\
&= \frac{j}{(j+1)} + \frac{1}{(j+1)(j+2)} \\
&= \frac{j(j+2)+1}{(j+1)(j+2)} \\
&= \frac{(j+1)^2}{(j+1)(j+2)} \\
&= \frac{(j+1)}{(j+2)}
\end{aligned}$$

et $P(j+1)$ est donc vraie.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 1, et l'énoncé est démontré.

Pour le second, on fait de même avec la propriété $P(n) : \sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$

— Initialisation : $P(1)$ est vraie : les deux membres valent 1.
— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. On a

$$\begin{aligned}
\sum_{k=1}^{j+1} k \cdot k! &= \sum_{k=1}^{j} k \cdot k! + (j+1)(j+1)! \\
&= (j+1)! - 1 + (j+1)(j+1)! \\
&= (j+2)(j+1)! - 1 \\
&= (j+2)! - 1
\end{aligned}$$

et $P(j+1)$ est donc vraie.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 1, et l'énoncé est démontré.

Solution de l'exercice 3
Chacune des inégalités de l'énoncé est une propriété dépendant de n, qui peut être démontrée par récurrence sur n :

— Initialisation : On vérifie aisément que chaque inégalité est vraie pour $n = 1 : 1 \leqslant 1$, $1 \leqslant 1$, $16 \leqslant 16$, et $1 + a \leqslant 1 + a$.

— Hérédité : Pour chaque inégalité/propriété, supposons que $P(j)$ soit vraie et montrons $P(j + 1)$. On a

  — $2^{j-1} \leqslant j! \implies 2 \cdot 2^{j-1} \leqslant (j + 1)j!$ puisque $2 \leqslant j + 1$, donc $P(j) \implies P(j + 1)$.

  — $j! \leqslant j^j \implies (j + 1)j! \leqslant (j + 1)j^j$ or $(j + 1)j^j \leqslant (j + 1)^{j+1}$.

  — Montrons par récurrence sur $n \geqslant 1$ que $2 \cdot (n + 3) + 1 \leqslant 2^{n+3}$. Cette propriété est vraie quand $n = 1$, et si on a $2\cdot(j+3)+1 \leqslant 2^{j+3}$, alors $2\cdot(j+3)+1+2 \leqslant 2^{j+3}+2^{j+3}$ et donc $2 \cdot ((j + 1) + 3) + 1 \leqslant 2^{(j+1)+3}$.
  On a alors $(j + 3 + 1)^2 = (j + 3)^2 + 2 \cdot (j + 3) + 1 \leqslant 2^{j+3} + 2^{j+3} = 2^{(j+1)+3}$.

  — On a $1 + (j + 1)a = 1 + ja + a \leqslant (1 + ja)(1 + a) \leqslant (1 + a)^j(1 + a) = (1 + a)^{j+1}$.

— Conclusion : Dans chacun des cas, $P(n)$ est donc vraie pour tout n supérieur ou égal à 1, ce qui démontre l'énoncé.

Solution de l'exercice 4

L'égalité de l'énoncé est une propriété dépendant de n, montrons-la par récurrence sur n :

— Initialisation : $P(0)$ est vraie : on a $0 = 0$.

— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j + 1)$. On a les égalités suivantes :

$$\begin{aligned}\sum_{k=0}^{j+1} F_k^2 &= \sum_{k=0}^{j} F_k^2 + F_{j+1}^2 \\ &= F_j \cdot F_{j+1} + F_{j+1}^2 \\ &= (F_j + F_{j+1}) \cdot F_{j+1} \\ &= F_{j+2} \cdot F_{j+1}\end{aligned}$$

et $P(j + 1)$ est donc bien vraie.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n naturel, ce qu'il fallait montrer.

Solution de l'exercice 5

On considère la propriété $P(n) : \sum_{k=1}^{n} \frac{1}{k^2} \leqslant 2 - \frac{1}{n}$ et on la montre par récurrence sur $n \geqslant 1$, ce qui suffit :

— Initialisation : $P(1)$ est vraie : on a bien $1 \leqslant 1$.

— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j + 1)$. On a

$$\begin{aligned}\sum_{k=1}^{j+1} \frac{1}{k^2} &= \sum_{k=1}^{j} \frac{1}{k^2} + \frac{1}{(j+1)^2} \\ &\leqslant 2 - \frac{1}{j} + \frac{1}{(j+1)^2}\end{aligned}$$

A-t-on $2 - \frac{1}{j} + \frac{1}{(j+1)^2} \leqslant 2 - \frac{1}{j+1}$? Cette inégalité est équivalente à $\frac{1}{(j+1)^2} \leqslant \frac{1}{j} - \frac{1}{j+1} = \frac{1}{j(j+1)}$, ce qui est vrai. Dès lors, $P(j + 1)$ est vraie si $P(j)$ l'est.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 1, et l'énoncé est démontré.

Solution de l'exercice 6

Montrons par récurrence sur $n \geqslant 3$ la propriété $P(n)$: « La somme des angles d'un n-gone est $(n-2) \cdot 180°$ » :

— Initialisation : $P(3)$ est vraie : la somme des angles d'un triangle est bien $180°$.

— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. Considérons trois sommets consécutifs d'un polygone à $j+1$ côtés et traçons la diagonale qui relie les deux sommets extrêmes. On a séparé le polygone de départ en un triangle et un polygone à j côtés, et la somme des angles du polygone de départ vaut donc $180° + (j-2) \cdot 180° = ((j+1)-2) \cdot 180°$.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 3, et l'énoncé est démontré.

Solution de l'exercice 7

Montrons par récurrence sur $n \geqslant 3$ la propriété $P(n)$: « Il existe $x_1, \ldots, x_n$ des entiers positifs distincts tels que $\frac{1}{x_1} + \ldots + \frac{1}{x_n} = 1$ ».

— Initialisation : $P(3)$ est bien vraie, car avec $x_1 = 2$, $x_2 = 3$ et $x_3 = 6$ on a $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.

— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. Soient $x_1, \ldots, x_j$ des entiers positifs distincts tels que $\frac{1}{x_1} + \ldots + \frac{1}{x_j} = 1$ (de tels entiers existent bien, puisqu'on a supposé que $P(j)$ était vraie). L'ordre des x_i n'a pas d'importance, on peut donc supposer qu'ils sont triés par ordre croissant. Remarquons que

$$\frac{1}{x_j} = \frac{1}{x_j(x_j+1)} + \frac{1}{x_j+1}$$

Posons alors $x'_j = x_j + 1$ et $x_{j+1} = x_j(x_j+1)$. Ces deux entiers sont distincts et plus grands que x_j, donc que $x_1, \ldots, x_{j-1}$. Au final, $x_1, \ldots, x_{j-1}, x'_j, x_{j+1}$ sont $n+1$ entiers positifs distincts dont la somme des inverses est 1 : $P(j+1)$ est vraie.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 3, et l'énoncé est démontré.

Solution de l'exercice 8

Montrons par récurrence sur $n \geqslant 2$ la propriété $P(n)$: « Dans un pays de n villes, si deux villes sont reliées soit par avion soit par bateau, il existe un moyen de transport par lequel on peut aller de n'importe quelle ville à n'importe quelle autre ».

— Initialisation : $P(2)$ est vraie : Si le pays compte deux villes et qu'elles sont reliés par un moyen de transport, ce moyen de transport permet de passer de n'importe quelle ville à n'importe quelle autre.

— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. Soit un pays de $j+1$ villes. Choisissons-en une et écartons-la. Il nous reste un pays de j villes. Par hypothèse de récurrence, il existe un moyen de transport (on peut supposer vu la symétrie que c'est l'avion) qui permet de faire n'importe quel trajet entre ces j villes. Dès lors, si la ville supplémentaire est reliée par avion à une des j premières, l'avion permet de faire tout trajet entre les $j+1$ villes. Dans le cas contraire, la ville supplémentaire est reliée par bateau à toutes les autres, donc le bateau permet de faire tout trajet entre les $j+1$ villes (en passant par la dernière).

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 2, et l'énoncé est donc prouvé.

Solution de l'exercice 9
Montrons par récurrence sur $n \geqslant 2$ la propriété $P(n)$: « Dans un tournoi à n joueurs se passant comme dans l'énoncé, quelqu'un a sur sa liste le nom de tous les autres ».

— Initialisation : $P(2)$ est vraie : S'il n'y a que deux joueurs, l'un d'eux a battu l'autre et a le nom de l'autre joueur sur sa liste.

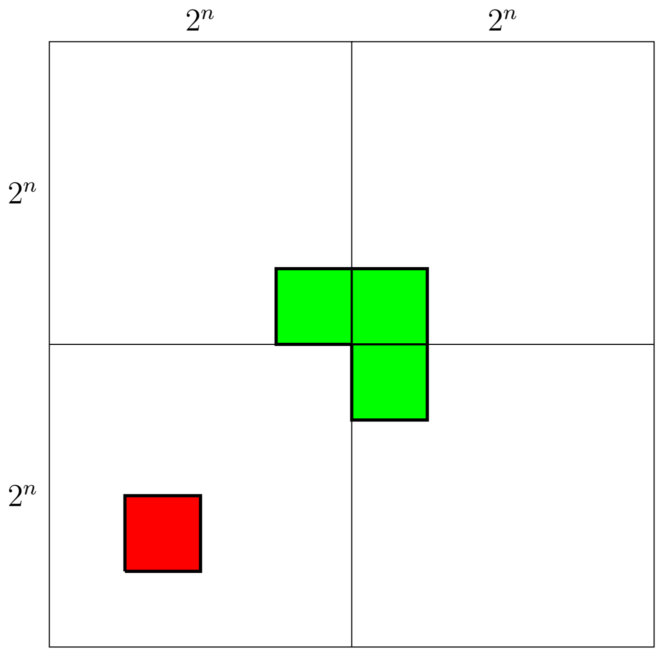
— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. Considérons un tournoi à $j+1$ joueurs. Choisissons un joueur X et ignorons-le momentanément. On peut considérer que les j autres joueurs ont joué un tournoi à eux seuls. Vu l'hypothèse de récurrence, il y a un joueur A qui a sur sa liste les noms de tous les autres joueurs. Soit S l'ensemble contenant A et les joueurs que A a battus. Reprenons maintenant X en compte. Si X a battu tous les joueurs de S, alors il a tous les joueurs sur sa liste (puisque tout le monde sauf X était sur la liste de A, tout le monde a été battu par un joueur de S). Sinon, il existe un joueur de S qui a battu X, donc A a battu un joueur qui a battu X : X est sur la liste de A, donc A a tout le monde sur sa liste.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 2, et l'énoncé est donc prouvé.

Solution de l'exercice 10
Montrons par récurrence sur $n \geqslant 1$ la propriété $P(n)$: « Un damier de côté 2^n peut être recouvert sans trou ni superposition par les pièces en L ».

— Initialisation : $P(1)$ est vraie : un damier de côté 2 auquel il manque une case est simplement de la forme d'une de nos pièces.

— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. Considérons un damier de côté 2^{j+1} auquel il manque une case. Coupons ce damier en quatre damiers de côté 2^j, et plaçons une pièce en L à cheval sur les trois petits damiers auxquels il ne manque pas déjà une case (voir figure ci-dessus). On a séparé notre damier en quatre damiers de côté 2^j auxquels il manque chacun une case, et qui sont donc pavables par des pièces en L par hypothèse de récurrence.



Dans cette figure, la case en rouge est celle manquante, les cases en vert sont celles de la pièce en L ajoutée.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n non nul : tout damier est recouvrable comme demandé.

Solution de l'exercice 11

Montrons par récurrence sur $n \geqslant 3$ la propriété $P(n)$: « Si les sommets d'un n-gone sont coloriés en bleu, rouge et vert de telle sorte que deux sommets consécutifs soient de couleurs différentes et que chaque couleur soit représentée, alors on peut le découper par des diagonales en triangles tricolores ».

— Initialisation : $P(3)$ est vraie : si les sommets d'un triangle sont coloriés de trois couleurs différentes et que chaque couleur est représentée, alors ce triangle est tricolore et ne pas tracer de diagonale conduit au découpage souhaité.

— Hérédité : Supposons que $P(j)$ soit vraie et montrons $P(j+1)$. Considérons un $(j+1)$-gone colorié en accord avec l'énoncé. Montrons par l'absurde qu'il possède trois sommets consécutifs de couleurs différentes : on peut numéroter les sommets dans le sens horlogique et supposer spdg que le premier sommet est bleu et le deuxième rouge. Dans ce cas, le troisième sommet ne peut être vert vu l'hypothèse d'absurde, ni rouge car deux sommets consécutifs sont de couleur différentes. Il est donc bleu. De même, le quatrième sommet est rouge, le cinquième bleu,... et aucun sommet n'est vert, ce qui est une contradiction puisque cette couleur doit être utilisée au moins une fois.

  Dès lors, considérons trois sommets consécutifs de couleurs différentes. Si le sommet du milieu est le seul de sa couleur, en le reliant à chacun des autres sommets, on obtient des triangles tricolores (puisque les deux autres sommets de chaque triangle sont consécutifs sur le polygone, donc de couleurs différentes). Si le sommet du milieu n'est pas le seul de sa couleur, en l'ignorant, on obtient un j-gone colorié en accord avec l'énoncé (il y a un sommet de chaque couleur puisque le sommet ignoré n'était pas le seul de sa couleur, et deux sommets consécutifs sont de couleurs différentes, puisque ceux de part et d'autre du sommet ignoré l'étaient). Par hypothèse de récurrence, on peut le découper en triangles tricolores. En rajoutant la diagonale liant les deux sommets de part et d'autre du sommet ignoré, on obtient un découpage correct du (j+1)-gone de départ.

— Conclusion : Par récurrence, $P(n)$ est donc vraie pour tout n supérieur ou égal à 3, et l'énoncé est donc prouvé.

3 Invariants

– Principe des tiroirs –

Exercice 1
Combien d'élèves faut-il dans une école pour être sûr qu'il existe trois élèves ayant la même date d'anniversaire.

Exercice 2
Montrer que parmis $n + 1$ entiers quelconques $a_0, \ldots, a_n$, il existe i et j tels que $n|a_i - a_j$.

Exercice 3
On dispose 6 points dans le plan. On trace tous les segments possibles entre ces points. On colorie chaque segment en bleu ou rouge. Montrer qu'il existe un triangle dont tous les segments sont de même couleur.

Exercice 4
Montrer que parmis les élèves du stage, il en existe 2 qui connaissent le même nombre de personnes.

Exercice 5
Une salle est faite de 7 rangées de 10 places. Une classe de 50 élève a cours dans la salle le matin et l'après-midi. Montrer qu'il existe 2 élèves qui ont été sur la même rangée le matin et l'après-midi.

Exercice 6
Soit 21 nombres entre 1 et 40. Montrer qu'il en existe 2 premiers entre eux.

Exercice 7
On choisit 10 nombres entre 1 et 100. Montrer que l'on peut choisir deux ensembles disjoints de ces nombres tels que la somme soit la même.

Exercice 8
On dispose n points dans le plan de tel sorte que parmi tout triplet de points, deux d'entre eux sont distant de moins de 1. Montrer qu'il existe un disque de rayon 1 contenant au moins $\lfloor \frac{n}{2} \rfloor$.

– Invariants et monovariants –

Exercice 9
On dispose de piles de jetons. L'on peut séparer une pile pour former deux piles ou fusionner deux pile pour en former une. Peut-on, en débutant avec une pile de 2014 jetons, obtenir 2015 piles de 1 jeton.

Exercice 10
On dispose 16 ampoules dans un carré de 4 par 4. On dispose d'un interrupteur par ligne et d'un interrupteur par colonne. Chque interrupteur inverse l'état (allumé ou éteint) de toutes les ampoule de sa ligne ou colonne. Au départ, seule l'ampoule en haut à gauche est allumée. Peut-on allumer toutes les ampoules ? Et si le carré était de 3 par 3 ?

Exercice 11
Un dragon a 100 têtes. Un chevalier tente de tuer le dragon. Pour cela, il doit lui couper toutes ses têtes. Le chevalier peut lui couper 13, 17 ou 6 exactement d'un coup. Si il reste 5 têtes ou moins, le dragon est invincible. Mais dans chacun de ces cas, s'il reste une tête au dragon, 7, 11 et 9 têtes repoussent respectivement. Le chevalier peut-il tuer le dragon ?

Exercice 12
On écrit les nombres de 1 à 2017 au tableau. À chaque étape, on efface deux nombres au tableau et on écrit leur différence. Peut-on finir avec seul 2 écrit au tableau ?

Exercice 13
Sur une île vivent des caméléons : 25 rouges, 12 verts et 8 bleus. Quand deux caméléons d'une même couleur se rencontrent, ils se font peur et prennent chacun une des deux autres couleur mais pas la même. Quand deux caméléons de couleurs différentes se rencontrent, ils se font peur et prennent tout deux la troisième couleur. Après un an, tous les caméléons sont de la même couleur. Cette couleur peut-elle être le bleu ?

– Correction des exercices –

Solution de l'exercice 1
Il y a 366 dates d'anniversaires possibles. Si il y a $2 \times 366 = 732$ ou moins élèves, l'on n'est pas certain d'avoir trois élèves avec la même date d'anniversaire. Si il y a 733 élèves ou plus, alors au moins 3 élèves ont la même date d'anniversaire d'après le principe des tiroirs.

Solution de l'exercice 2
Il y a n résidus modulo n et les a_i sont au nombre de $n+1$. Donc, d'après le principe des tiroirs, il existe i et j tels que $a_i \equiv a_j \mod n$, soit $n | a_i - a_j$.

Solution de l'exercice 3
Soit p un des points. Il y 5 segments partant de p. Par le principe des tiroirs, au moins 3 d'entre eux ont la même couleur, disons rouge. Alors, soit a_1,a_2 et a_3 trois points reliés à p par des segments rouges. Si un des 3 segments reliant a_1,a_2 et a_3 entre eux est rouge, disons $[a_1 a_2]$, alors le triangle pa_1a_2 est rouge. Si ce n'est pas le cas, le triangle $a_1a_2a_3$ est bleu. Donc dans tous les cas, il existe un triangle monochrome.

Solution de l'exercice 4
Il y a 81 élèves au stage. Chaque élève peut connaitre entre 0 et 80 autres élèves. Supposons

par l'absurde qu'il n'existe pas deux élèves connaissant le même nombre d'élèves. Alors, il existe exactement un élève connaissant 0 autres élèves, un élèves connaissant 1 autre élève,..., et un élève connaissant 80 autres élèves. Mais alors, l'élève qui connait les 80 autres connait celui qui n'en connait aucun, ce qui n'est pas possible. Donc il existe deux élèves qui connaissent le même nombre d'élèves.

Solution de l'exercice 5
Le matin, une certaine rangée contenait au moins 8 élèves par le principe des tiroirs ($7 \times 7 = 49 < 50$). Et donc, parmis ces élèves, deux d'entre eux étaient aussi sur la même rangée l'après-midi par le principe des tiroirs.

Solution de l'exercice 6
On considère les 20 tiroirs $\{1, 2\}, \{3, 4\}, \ldots, \{39, 40\}$. Comme 21 nombres ont été choisis, deux d'entre eux sont dans le même tiroir. Ces deux nombres consécutifs sont alors premiers entre eux. En effet, si $d|n$ et $d|n + 1$, alors $d|(n + 1) - (n)$, soit $d|1$.

Solution de l'exercice 7
Les sommes possibles sont entre 1 et $100+99+\cdots+91 = 955$. Or, il y a $2^{10} = 1024$ façons de faire des sommes avec nos 10 nombres. Donc, par le principe des tiroirs, deux ensembles donnent la même somme. En leur retirant leur intersection, on obtient deux ensembles disjoints de même somme.

Solution de l'exercice 8
Si tous les points sont deux à deux distant de moins de 1, alors en choisissant un point p quelconque, tous les points sont dans le disque de centre p et de rayon 1. Sinon, il existe deux points p_1 et p_2 distant de strictement plus que 1. Tout autre point est dans le disque de centre p_1 et de rayon 1 ou dans le disque de centre p_2 et de rayon 1 d'après l'hypothèse de l'énoncé. Il y a $n-2$ tel points. Donc, d'après le principe des tiroirs, un de ces deux disques en contient au moins $\lfloor \frac{n-2}{2} \rfloor$ de ces points. En comptant le centre du disque, cela fait au moins $\lfloor \frac{n-2}{2} \rfloor + 1 = \lfloor \frac{n}{2} \rfloor$ points à l'intérieur.

Solution de l'exercice 9
La réponse est non. Le nombre de jetons ne change jamais : l'on ne peut donc pas passer d'une configuration avec 2014 jetons à une configuration avec 2015 jetons.

Solution de l'exercice 10
Dans les deux cas, la réponse est non. Pour le carré de 4 par 4 : la parité du nombre d'ampoules allumées est invariante, l'on ne peut donc pas passer de la configuration initiale avec un nombre impair d'ampoules allumées à une configuration avec 16 ampoules allumées. Pour le carré de 3 par 3 : la parité du nombre de coins allumés est invariante, le même argument conclut alors.

Solution de l'exercice 11
Dans les trois cas, le nombre de têtes change de 6 ou 3. Donc à chaque étape, la cingruence modulo 3 du nombre de têtes est inchangée. Or 100 est congru à 1 modulo 3 et 0 n'est pas congru à 1 modulo 3, donc le dragon est invincible.

Solution de l'exercice 12
La réponse est non. Comme $a + b \equiv a - b \equiv b - a \mod 2$. La parité de la somme des nombres écrits au tableau est invariante. Or, la somme vaut initialement $2017 \times \frac{2018}{2} = 2017 \times 1009$. La somme reste donc toujour impaire : il n'est pas possible de terminer avec seulement 2 au tableau.

Solution de l'exercice 13
On note R et V les nombres de caméléons rouges et verts. On remarque que $R - V \mod 3$ est un invariant du problème. Or sa valeur initiale est $1 \mod 3$. Il ne peut donc pas être nul. Ainsi, il reste toujours un caméléon rouge ou un caméléon vert.

4 Principe de l'extremum

– Les principes de l'extremum –

Les deux principes de l'extremum sont les suivants :

Théorème 3.4.1.
Dans un ensemble fini de nombres réels, il y a un plus petit et un plus grand.

Théorème 3.4.2.
Dans un ensemble de nombres naturels, il y a un plus petit.

Ces deux résultats permettent de nombreux raisonnements par l'absurde, dans des problèmes d'arithmétique ou de combinatoire principalement. Pour les utiliser, on peut considérer le plus petit/grand objet d'un ensemble et aboutir au fait qu'il n'est pas le plus petit/grand, ce qui est une contradicition. Par exemple, on peut démontrer que $\sqrt{2}$ est irrationnel en considérant un nombre rationnel dont le carré est 2 et dont le dénominateur est minimal, puis en construisant une autre fraction dont le dénominateur est plus petit, ce qui est une contradiction. Dans les faits, supposer qu'une quantité est extrémale permet souvent de « gagner une hypothèse ».

– Exercices –

Exercice 1
Lors d'un bal, aucun garçon n'a dansé avec toutes les filles mais chaque fille a dansé avec au moins un garçon. Montrer que l'on peut trouver deux garçons g et g' et deux filles f et f' tels que g a dansé avec f mais pas f' et g' a dansé avec f' mais pas f.

Exercice 2
On considère tous les points du plan à coordonnées entières. A chaque point, on associe un entier strictement positif tel que chaque nombre est la moyenne arithmétique de ses quatre voisins. Montrer que tous les nombres sont égaux.

Exercice 3
On considère un ensemble de points du plan, tel que chaque point est le milieu de deux autres points de l'ensemble. Montrer qu'il y a un nombre infini de points.

Exercice 4
$2n + 1$ nombres sont tels que la somme de $n + 1$ d'entre eux est toujours plus grande que la

somme des n autres, quels que soient les $n+1$ nombres choisis. Monter que tous les nombres sont positifs.

Exercice 5
Lo Jac le sorcier possède une infinité de rubis et de saphirs. Il reçoit des lutins et veut donner à chacun un nombre naturel de rubis et de saphirs. Il sait que les lutins sont très jaloux : si un lutin voit qu'un autre a plus ou autant de rubis et plus ou autant de saphirs que lui, ils se battront. Montrer que Lo Jac peut contenter tous les lutins si et seulement si ceux-ci sont en nombre fini.

Exercice 6
Les nombres réels $x_1, \ldots, x_{2011}$ satisfont

$$x_1 + x_2 = 2x'_1, x_2 + x_3 = 2x'_2, \ldots, x_{2011} + x_1 = 2x'_{2011}$$

où $x'_1, \ldots, x'_{2011}$ est une permutation de $x_1, \ldots, x_{2011}$. Montrer que $x_1 = x_2 = \ldots = x_{2011}$.

Exercice 7
$2n+1$ élèves sont placés à des distances deux à deux distinctes les uns des autres. A un instant, chacun tire sur l'élève le plus proche de lui avec un pistolet à eau. On suppose que les élèves savent viser et donc touchent leur cible.

- Montrer que deux élèves se tirent dessus.
- Montrer qu'un élève reste sec.

Exercice 8
On considère un ensemble de 100 entiers strictement positifs tels que leur somme est égale à leur produit. Montrer qu'au moins 93 des entiers sont égaux à 1. Bonus : Trouver un meilleur minorant que 93.

Exercice 9
On donne des points $A_1, \ldots, A_n$ et $B_1, \ldots, B_n$ du plan, trois quelconques étant non alignés. Montrer que l'on peut renuméroter les B_i de sorte que les segments $[A_iB_i]$ ne se croisent jamais.

Exercice 10
La Reine d'Angleterre veut partager la Chambre des Lords de façon originale : chaque Lord ayant au plus trois ennemis (l'inimité est réciproque), elle veut partager la Chambre en deux groupes, chaque Lord ayant au plus un ennemi dans son groupe. Est-ce possible ?

Exercice 11
Une *bande* de largeur w est l'ensemble des points se trouvant entre deux droites parallèles distantes de w. Soit S un ensemble de $n \geqslant 3$ points tel que trois points de S peuvent toujours être recouverts par une bande de largeur 1. Montrer que S peut être recouvert par une bande de largeur 2.

Exercice 12
Montrer que toute suite de n^2+1 réels admet soit une sous-suite croissante de longueur $n+1$, soit une sous-suite décroissante de longueur $n+1$.

– Solutions –

Solution de l'exercice 1

Considérons le garçon g qui a dansé avec le plus de filles, f' une fille avec laquelle il n'a pas dansé et g' un garçon avec lequel f' a dansé. Si on ne peut trouver les quatre personnes désirées par l'énoncé, alors pour toute fille f ayant dansé avec g, f doit également avoir dansé avec g'. Mais alors, g' a dansé avec au moins une fille de plus que g, ce qui contrdit la maximalité de g. Absurde.

Solution de l'exercice 2

Les valeurs étant des entiers positifs ou nuls, on peut considérer m, la plus petite de ces valeurs. On se place en un point ayant cette valeur. Notons a, b, c, d les valeurs de ses quatre voisins. Par hypothèse, on a $m = (a+b+c+d)/4$ et m est inférieur ou égal à chacune des quatre valeurs a, b, c, d puisqu'il est minimal. Si m est strictement inférieur à l'une des quatre valeurs (spdg a), on a

$$m = \frac{a+b+c+d}{4} > \frac{m+b+c+d}{4} \geqslant \frac{m+m+m+m}{4} = m$$

et donc $m > m$ ce qui est absurde. On a donc nécessairement $m = a = b = c = d$, et on peut appliquer le raisonnement qu'on vient de faire à chacun des quatre voisins. On peut procéder ainsi de proche en proche, par récurrence sur la distance de Manhattan au point de départ, et aboutir à la conclusion.

Solution de l'exercice 3

Supposons par l'absurde qu'il n'y en ait qu'un nombre fini. On peut se placer dans un repère orthonormé tel que deux points soient toujours d'abscisses différentes (puisque n points déterminent $n(n-1)/2$ directions et qu'il suffit de ne pas prendre une de celles-ci). Mais alors, le point d'abscisse maximale ne peut être le milieu de deux autres. C'est une contradiction. On aurait également pu utiliser deux points A et B tels que la distance AB soit la plus grande possible.

Solution de l'exercice 4

Notons ces nombres $a_1, \ldots, a_{2n+1}$ avec $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_{2n+1}$. On a alors

$$\begin{array}{rcl} a_1 + \ldots + a_{n+1} & \geqslant & a_{n+2} + \ldots + a_{2n+1} \\ a_1 & \geqslant & a_{n+2} + \ldots + a_{2n+1} - a_2 - \ldots - a_{n+1} \\ a_1 & \geqslant & (a_{n+2} - a_2) + \ldots + (a_{2n+1} - a_{n+1}) \end{array}$$

ce qui conclut puisque chaque parenthèse est positive.

Solution de l'exercice 5

Montrons que Lo Jac ne peut contenter un nombre infini de lutins : remarquons que si deux lutins ont le même nombre de pierres précieuses d'un type, ils vont forcément se battre. Considérons le lutin qui a le moins de saphirs et notons n le nombre de rubis qu'il possède. Aucun lutin ne peut posséder plus de n rubis, sinon le premier se battra avec lui. Dès lors, puisque tous les lutins possèdent un nombre entier compris entre 0 et n de rubis et que tous ce nombres sont distincts, il n'y a forcément qu'un nombre fini de lutins. D'autre part, Lo Jac peut contenter n lutins en donnant i rubis et $n-i$ saphirs au i-ième lutin.

Solution de l'exercice 6
Remarquons que si l'on choisit $n < 2011$ équations, le nombre de x_i impliqués au membre de gauche dans ces équations est $> n$. Soit M le maximum des x_i et n le nombre de x_i égaux à M. Supposons $n < 2011$. Si l'on choisit les n équations du type $x_k + x_{k+1} = M$, on peut déduire $x_k = x_{k+1} = 2M$ dans chaque équation, donc on déduit que le nombre de x_i égaux à M est strictement supérieur à n, contradiction. Donc $n = 2011$: tous les nombres sont égaux au maximum.

Solution de l'exercice 7

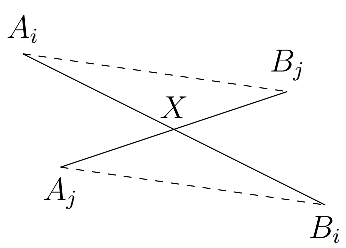
- L'ensemble des distances entre deux élèves est un ensemble fini de réels, il admet donc un plus petit élément : soient A et B deux élèves tels que la distance AB est minimale. Alors, A et B se tirent forcément dessus.
- On procède par récurrence sur n : l'initialisation à $n = 0$ ou $n = 1$ ne pose pas de problèmes. Ensuite, supposons que si $2n+1$ élèves se tirent dessus, l'un d'eux reste sec. Si $2n+3$ élèves se tirent dessus, soient A et B les deux élèves à distance minimale l'un de l'autre (qui se tirent donc dessus). Si un autre élève tire sur A ou B, il y a un élève qui est mouillé deux fois et donc un élève qui n'est pas mouillé, puisque le nombre de tirs est égal au nombre d'élèves. Sinon, A et B agissent indépendamment des $2n+1$ autres élèves et l'un de ces élèves reste donc sec par hypothèse de récurrece.

Solution de l'exercice 8
On peut supposer spdg que a_{100} est le plus grand des a_i. On a alors

$$\prod_{i=1}^{100} a_i = \sum_{i=1}^{100} a_i \leqslant 100a_{100}$$

En simplifiant par a_{100} on a que $\prod_{i=1}^{99} a_i \leqslant 100$. La conclusion vient du fait qu'aucun entier inférieur à 100 ne peut s'exprimer comme produit de plus de six naturels différents de 1, puisque $2^7 > 100$. On a alors au maximum a_{100} et six autres entiers qui peuvent être différents de 1, donc au moins 93 entiers sont égaux à 1. Pour le bonus, on se réfèrera à
http ://www.animath.fr/IMG/pdf/2016-10-test-ofm-corrige.pdf

Solution de l'exercice 9
Il n'existe qu'un nombre fini de renumérotations des B_i, considérons celle où la somme des longueurs des segments $[A_iB_i]$ est minimale. Supposons que les segments $[A_iB_i]$ et $[A_jB_j]$ se croisent en X. Alors, on a $|A_iB_j| + |A_jB_i| \leqslant |A_iX| + |XB_j| + |A_jX| + |XB_i|$ par inégalité triangulaire et donc $|A_iB_j| + |A_jB_i| \leqslant |A_iB_i| + |A_jB_j|$. En « décroisant » les deux segments, on obtient donc une configuration où la somme des longueurs est plus courte, ce qui est impossible.



Solution de l'exercice 10
Choisissons une répartition qui minimise le nombre de paires de Lords ennemis se trouvant dans le même groupe. Si un Lord était dans le même groupe que deux de ses ennemis, le nombre de telles paires diminuerait d'au moins 1 en le changeant de groupe, ce qui est impossible. Dès lors, la répartition choisie satisfait la condition imposée par la Reine.

Solution de l'exercice 11
Si l'on considère un triangle, la plus petite bande qui peut le contenir est perpendiculaire à la plus petite hauteur, et sa largeur est la longueur de la plus petite hauteur du triangle. Dès lors, considérons A et B les deux points les plus éloignés de S. Pour tout autre point C de S, le triangle ABC peut être recouvert par une bande de largeur 1, donc sa plus petite hauteur, celle associée au côté AB, a une longueur inférieure à 1. Dès lors, tous les points de S sont à distance 1 au plus de la droite AB. S peut donc être recouvert par la bande de largeur 2 « centrée » en la droite AB.

Solution de l'exercice 12
Supposons que ce ne soit pas le cas, et que toute sous-suite monotone soit de longueur inférieure à n. Notons $a_1, \ldots, a_{n^2+1}$ les éléments de la suite. A chaque élément a_i, on associe le couple (longueur de la plus grande suite croissante finissant en a_i, longueur de la plus grande suite décroissante finissant en a_i) qui est un couple d'entiers entre 1 et n. Il y a n^2 tels couples, donc on peut trouver a_i et a_j avec $i < j$ auxquels sont associés le même couple, par le principe des tiroirs. Si $a_i \leqslant a_j$, on peut rajouter a_j au bout de la suite croissante finissant en a_i et ainsi créer une sous-suite croissante de longueur plus grande que le maximum, une contradiction. Le cas $a_i \geqslant a_j$ se traite de la même façon.

5 Dénombrement et double comptage

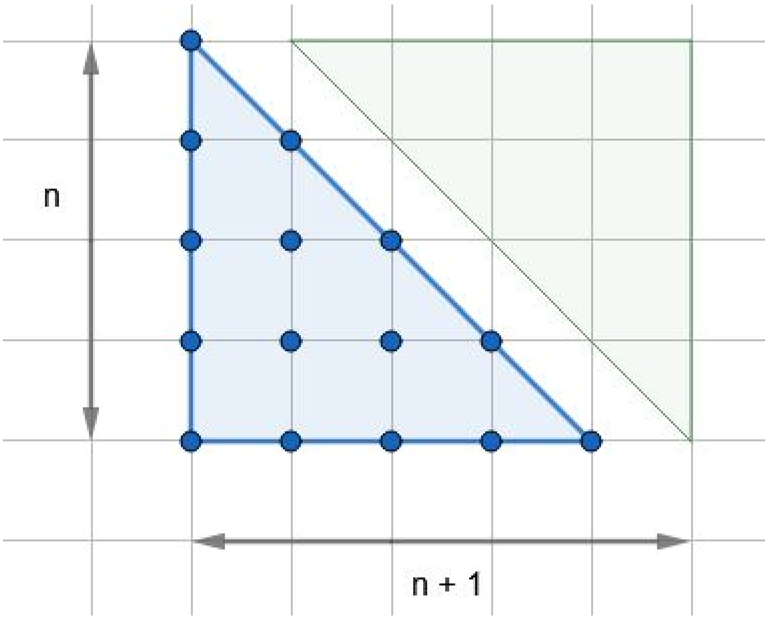
Comme son nom l'indique, le principe (combinatoire) de double comptage consiste à trouver différentes manières de compter les mêmes objets, ou de représenter les mêmes quantités : on peut ainsi établir des égalités, voire des inégalités, des formules de calcul,... On va surtout voir dans ce cours des façons d'appliquer ce principe à différents problèmes, pour retrouver quelques résultats classiques.

– Premiers exemples et formules utiles –

Pour clarifier cette présentation absconse, étudions quelques exemples :

Somme d'une suite arithmétique

Supposons que l'on veuille calculer la somme $1 + \ldots + n$ où $n \in \mathbb{N}$, c'est-à-dire en proposer une formule. Trouver cette formule, c'est la même chose que de trouver une formule pour compter les sommets du quadrillage dans un triangle de côté n, dessiné comme ci-dessous :



Or on remarque que si l'on duplique le triangle comme proposé, on couvre exactement tous les sommets contenus dans un rectangle de côtés n et $n+1$. Si on sait combien de points on a couvert, il suffit de diviser ce nombre par 2. Ainsi :

$$1 + \ldots + n = \frac{n(n+1)}{2}.$$

Exercice 1 (Un peu de graphes)
Un *graphe fini* est un ensemble fini de sommets reliés par des arêtes : on convient que deux sommets sont reliés par au plus une arête, mais une arête peut relier un sommet à lui-même. Le *degré* d'un sommet est le nombre d'arêtes dont il est une extrémité (une arête qui le relie à lui-même compte deux fois).

Les graphes sont très utilisés en combinatoire, et de nombreux résultats se montrent par récurrence ou double comptage (sur les arêtes, les faces, les sommets, ...), comme celui qui suit :

Montrer que nombre de sommets de degré impair est pair.

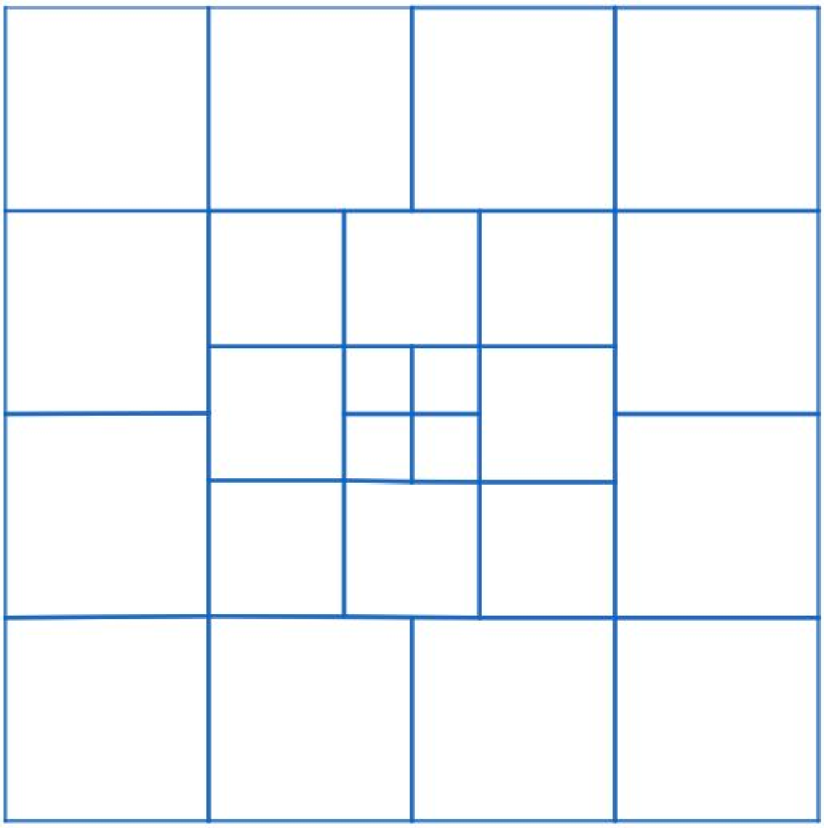
Solution de l'exercice 1
On compte plutôt le nombre de demi-arêtes qui sont sur un sommet de degré impair. On sait que :

— le nombre total de demi-arêtes est pair

— le nombre de demi-arêtes sur un sommet de degré pair est pair

Ainsi, le nombre total de demi-arêtes sur des sommets de degré impair est nécessairement pair : or pour qu'une somme d'entiers impairs soit paire, il faut sommer un nombre pair d'entiers. Le nombre de sommets de degré impair est donc pair.

Exercice 2 (Somme des cubes)
On construit de la façon illustrée ci-dessous une figure composée de n couronnes emboîtées, telle que $\forall k \in \{1, \ldots, n\}$, la k-ième couronne est composée de $4k$ carrés de côté k.
En déduire une formule de la somme : $S_n = 1^3 + \ldots + n^3$.



Solution de l'exercice 2
L'aire couverte par la k-ième couronne vaut $A_k = 4k \times k^2 = k^3$, donc $4 \times S_n$ est l'aire totale couverte par le carré de côté $n(n+1)$, d'où la formule :

$$1^3 + \ldots + n^3 = \frac{(n(n+1))^2}{4} = \left(\frac{n(n+1)}{2}\right)^2.$$

Remarque 3.5.1.
C'est le carré de la somme des n premiers entiers.

– Un peu de théorie –

On distingue quelques principes en combinatoire, qui peuvent être utiles en double comptage. Ces notions sont assez intuitives, mais il est utile de les connaître, ainsi que le vocabulaire associé, pour une rédaction claire notamment.

Définition 3.5.2.
Soit E un ensemble *fini*. Le *cardinal* de E, noté $\mid E \mid$ ou $\#E$ est le nombre de ses éléments.

Un problème de dénombrement, c'est toujours une recherche du cardinal d'un ensemble donné.

Définition 3.5.3.
Une *découpe* d'un ensemble E est un ensemble de parties de E deux à deux disjointes, et dont l'union vaut E. Autrement dit, découper E, c'est répartir tous ses éléments en « paquets ».

Ainsi, si on découpe l'ensemble que l'on souhaite dénombrer, et que l'on sait dénombrer chacune des parties de la découpe, la somme de leurs cardinaux est égale au cardinal de l'ensemble initial.

Découpe selon une application

Soit une fonction f d'un ensemble E vers un ensemble F (à chaque élément x de E, on associe un unique élément de F, appelé image de x par f et noté $f(x)$). Pour $y \in \mathbb{F}$, on note $f^{-1}(\{y\})$ l'image réciproque de $\{y\}$ par f, c'est-à-dire l'ensemble des éléments x de E tels que $f(x) = y$ (ensemble des antécédents de y). On peut alors découper E selon l'image de ses éléments :

$$\left\{ f^{-1}\{y\} \mid y \in F \right\}$$

est une découpe de E.

Lemme 3.5.4 (Lemme du berger)**.**
On veut compter les éléments d'un ensemble F fini (*les moutons d'un troupeau*). On suppose qu'il existe une fonction $f : E \to F$ et un entier $p \leqslant 1$, tel que $\forall\, y \in F$, $f^{-1}(y)$ compte exactement p éléments (*on compte le nombre de pattes, on sait qu'exactement 4 appartiennent au même mouton*). Alors :

$$\mid F \mid = \frac{\mid E \mid}{p}$$

(*le nombre de moutons est le quart du nombre de pattes*)

Définition 3.5.5.
Soit $f : E \to F$. On dit que :

— f est *injective* si deux éléments distincts de E ont toujours deux images distinctes par f. Autrement dit, tout élément de F a *au plus un antécédent* par f (il peut n'en avoir aucun).

— f est *surjective* si tous les éléments de F ont *au moins un antécédent* par f.

— f est *surjective* si elle est injective et bijective, c'est à dire que tout élément y de F a *exactement un antécédent* par f.

Proposition 3.5.6.
Soit E et F deux ensembles finis et $f : E \to F$.

— Si f est *injective*, alors $\mid E \mid \leqslant \mid F \mid$.

— Si f est *surjective*, alors $\mid E \mid \geqslant \mid F \mid$.
— Si f est *bijective*, alors $\mid E \mid = \mid F \mid$.

Ainsi, en double comptage, on s'intéresse aux bijections : si on connaît le cardinal d'un ensemble en bijection avec l'ensemble que l'on veut compter, on a résolu notre problème. Il s'agit donc de trouver une bijection qui convienne, et un ensemble « facile à compter ».

Définition 3.5.7.
Une *permutation* d'un ensemble fini E est une application σ bijective de E dans lui-même. Pour $n \in \mathbb{N}$, on note S_n l'ensemble des permutations de $\{1, \ldots, n\}$.

Définition 3.5.8.
Soit E et F deux ensembles. Le *produit cartésien* de E et F, noté $E \times F$, est l'ensemble des couples (x, y) où $x \in E$ et $y \in F$.

Proposition 3.5.9.
$\mid E \times F \mid = \mid E \mid \times \mid F \mid$.

Pour dénombrer un ensemble, on peut ainsi le voir comme produit cartésien d'autres ensembles que l'on connaît mieux, et en déduire son cardinal.
Exercice 3 (Permutations et points fixes)
Soit $n \in \mathbb{N}$. Pour $k \in \mathbb{N}$, on note P_k le nombre d'éléments de S_n qui ont exactement k point fixes.
Montrer que

$$\sum_{k=0}^{n} kP_k = n!$$

Solution de l'exercice 3
On établit d'abord que pour tout $m \in \mathbb{N}$, $\mid S_m \mid = m!$: on a m choix pour l'image de 1, $m-1$ pour l'image de 2, etc. Puis on compte l'ensemble E des paires $(\sigma, x) \in S_n \times \{1, \ldots, n\}$ telles que $\sigma(x) = x$.

— Pour $\sigma \in S_n$, soit k son nombre de points fixes et $x_1, \ldots, x_k$ ces points fixes. σ apparaît dans les paires $(\sigma, x_1), \ldots, (\sigma, x_k)$ dans E, soit exactement k fois. Donc en découpant E selon la première composante de ses éléments :

$$\mid E \mid = \sum_{k=0}^{n} kP_k$$

— Pour tout $x \in \{1, \ldots, n\}$, il y a $\mid S_{n-1} \mid$ éléments de S_n qui fixent x, donc x apparaît dans exactement $(n-1)!$ paires dans E. En découpant E selon la deuxième composante de ses éléments :

$$\mid E \mid = \sum_{i=1}^{n} (n-1)! = n \times (n-1)! = n!$$

D'où le résultat par double comptage.

– Autour du binôme –

Formule du binôme et calcul

Ce qu'on appelle le « binôme », c'est une expression de la forme $(a+b)^n$ où a, b sont deux nombres (il faudrait définir ce qu'est un nombre, disons ici que l'on prend des réels ou des complexes) et $n \in \mathbb{N}$. La célèbre *formule du binôme de Newton* donne un développement de cette expression, en regroupant les termes selon les exposants de a et b :

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

Cette formule fait apparaître les *coefficients binomiaux* : pour $k, n \in \mathbb{N}$ le coefficient $\binom{n}{k}$ se lit "k parmi n", et vaut le *nombre de sous-ensembles à k éléments dans un ensemble à n éléments*.

On a déjà deux façons de « représenter » $\binom{n}{k}$ (qu'il est facile de ramener l'une à l'autre en fait) : pour en donner une expression que l'on puisse calculer, on peut ainsi en chercher une représentation facile à manipuler.

Par exemple, on imagine que l'on a n boules numérotées (toutes distinctes), et on compte le nombre de façon dont on peut en piocher k :

— si $k > n$, ce n'est pas possible : $\binom{n}{k} = 0$

— sinon, alors on pioche les boules une à une : on a n choix pour la première, $(n-1)$ pour la deuxième, ..., $(n-k+1)$ pour la k-ième. On peut donc faire $n \times \ldots \times (n-k+1) = \frac{n!}{(n-k)!}$ choix différents de cette façon.

— Mais puisqu'on ne s'intéresse pas à l'ordre dans lequel on a pioché nos k boules, on a en fait compté plusieurs fois le même lot. Par exemple, pour avoir le lot $\{1, 2, \ldots, k\}$, on a k choix pour la première boule, puis $k-1$ pour la deuxième, et un seul pour la dernière : on a compté de cette façon $k!$ fois chacun des objets que l'on voulait compter (les lots de k boules). On applique donc le lemme du berger : on divise notre première valeur par $k!$:

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

Autres applications classiques

On retrouve ces coefficients un peu partout, à chaque fois en fait que l'on peut ramener la situation à compter les sous-ensembles de même effectif d'un premier ensemble fini. Quelques exemples :

— Loi binomiale en probabilités : on lance n fois ($n \in \mathbb{N}$) une pièce qui a une probabilité $p \in [0,1]$ de tomber sur "pile" et $1-p$ de tomber sur face : *quelle est la probabilité d'obtenir k pile ?* ($k \in \mathbb{N}$)

— La Cigale se déplace en faisant des pas vers le Nord ou l'Est uniquement : *combien de chemins peut-elle emprunter pour se rendre chez la Fourmi, n pas plus au Nord et k plus à l'est ?* ($n, k \in \mathbb{N}$)

— Soit $n, k \in \mathbb{N}$. *Combien existe-t-il de k-uplets d'entiers positifs $(a_1, \ldots, a_k)$ tels que $a_1 + \ldots + a_k = n$?* Même question avec des entiers strictement positifs.

Formules et propriétés pratiques

Exercice 4 (Élisons le maire...)
Montrer que, $\forall n, k \in \mathbb{N}*$, on a :

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

Indice : dans un village de $n \in \mathbb{N}$ habitants, le conseil comporte $k \leqslant n$ membres, dont un est maire et les autres conseillers. Combien de façons y a-t-il de constituer ce conseil ?

Solution de l'exercice 4
On peut constituer le conseil de trois manières :

— On élit les k membres du conseil parmi toute la population, puis on désigne le maire parmi eux : cela fait $\binom{n}{k}$ façons de constituer le conseil, puis pour un même conseil, k possibilités pour le maire.

— On élit d'abord le maire parmi toute la population : on a n candidats. Puis, on choisit les $k-1$ conseillers restants parmi la population restante, ce qui laisse $\binom{n-1}{k-1}$ possibilités.

— On élit d'abord les $k-1$ conseillers, pour lesquels on a $\binom{k-1}{n}$ possibilités, puis pour chacune, on a encore $n-(k-1) = n-k+1$ choix pour le maire.

On a bien compté trois fois les mêmes objets (les conseils possibles), d'où les égalités.

Exercice 5 (Formule de Pascal)
Montrer que, $\forall n, k \in \mathbb{N}$, on a :

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

Solution de l'exercice 5
On répartit les sous-ensembles de $\{1, \ldots, n, n+1\}$ en deux catégories disjointes :

— Ceux qui contiennent l'élément $n+1$: il y en a exactement autant que de sous-ensembles à $k-1$ éléments de $1, \ldots, n$, soit $\binom{n}{k+1}$

— Ceux qui ne contiennent pas l'élément $n+1$: il y en a $\binom{n}{k+1}$

D'où la formule de Pascal.

Remarque 3.5.10.
On en déduit une façon de calculer de proche en proche les coefficients du binôme, en représentant le « triangle de Pascal ». En complétant les lignes par des zéros (non représentés), on obtient exactement que chaque coefficient est la somme des deux immédiatement au-dessus de lui :

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Exercice 6 (Formule de Pascal étendue)
Soit $k, n, p \in \mathbb{N}$. Montrer que

$$\sum_{j=n}^{p} \binom{k}{j} = \binom{p+1}{k+1} - \binom{n}{k+1}.$$

(On somme sur une « diagonale montante » du triangle de Pascal)

Solution de l'exercice 6
On découpe l'ensemble des parties à $k+1$ éléments de $\{1, \ldots, p+1\}$ selon la valeur de leur maximum. Pour $j \leqslant p+1$, il y a autant de tels sous-ensembles ayant j pour maximum que de parties de $\{1, \ldots, j-1\}$ à $k-1$ éléments (tous les éléments restants sont strictement plus petits que le maximum).

Ainsi, la somme étudiée correspond en fait au nombre de parties à $k+1$ éléments de $\{1, \ldots, p+1\}$ dont le maximum est $n+1$, $n+2$, ... ou $p+1$. Cela comprend donc toutes les parties, sauf celles qui sont des parties de $\{1, \ldots, n\}$. D'où la formule.

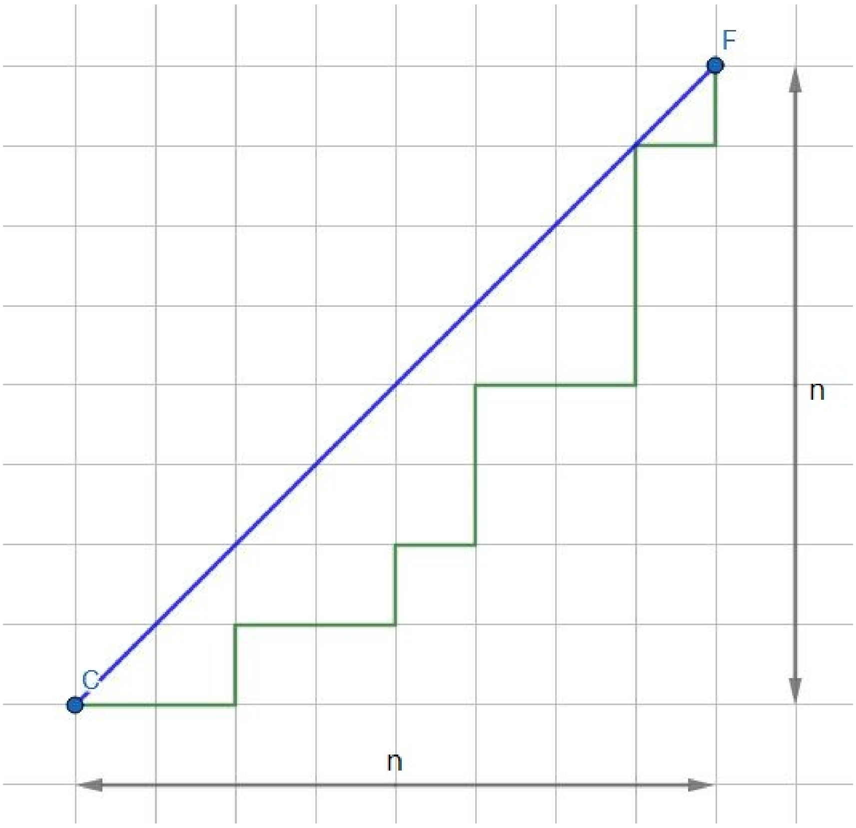
Remarque 3.5.11.
On s'est servi, pour découper notre ensemble, de la fonction $\max$ sur les parties d'un ensemble.

Remarque 3.5.12.
On aurait aussi pu aussi utiliser la formule de Pascal et un télescopage.

– Nombres de Catalan –

Ces nombres, un peu comme les coefficients binomiaux, apparaissent dans de nombreux problèmes combinatoires. Nous en présenterons quelques uns.

Exercice 7 (Le retour de la Cigale)
La Cigale se déplace toujours en faisant des pas exclusivement vers le Nord ou vers l'Est. La Fourmi habite n pas plus au Nord et n plus à l'Est, mais cette fois une rivière suit la ligne droite (diagonale) entre les deux amies, que la Cigale ne peut traverser : elle peut aller sur la rive, mais doit rester « au-dessus » ou « au-dessous » de la diagonale. De combien de chemins dispose-t-elle à présent ?



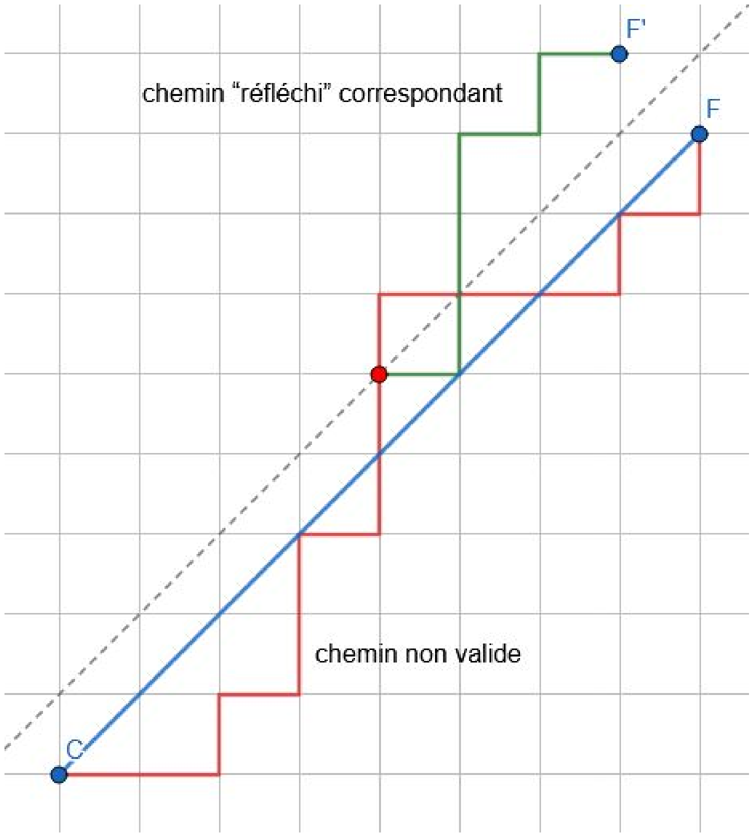
Un chemin empruntable entre C et F.

Solution de l'exercice 7
On a vu qu'il était facile, avec le mode de déplacement de la Cigale, de compter le nombre de chemins qu'elle pouvait emprunter entre deux points, sans tenir compte de la rivière.

Ainsi, il y a au total $\binom{n}{n+n} = \binom{n}{2n}$ chemins entre C et F si on oublie la rivière. On trace le plan de la situation dans un quadrillage. Comptons les chemins qui partent par exemple sous la diagonale, mais la dépassent à partir d'un moment.

Traçons la surdiagonale : tout chemin invalide passe nécessairement par un de ses sommets. Pour un chemin invalide, on appelle C son premier point sur la surdiagonale, et on considère le chemin qui coïncide avec celui-ci jusqu'à C, et avec son symétrique par rapport à la surdiagonale après C, comme indiqué sur la figure ci-dessous.

On retrouve le chemin initial en appliquant la même transformation au nouveau chemin : c'est une transformation involutive. Le nouveau chemin arrive en F', symétrique de F par rapport à la surdiagonale. Réciproquement, soit un chemin de C à F'. En lui appliquant la même transformation, on obtient un chemin invalide de C à F : la correspondance entre les chemins invalides de C à F et les chemins de C à F' est bijective.



On sait alors qu'il y a $\binom{(n+1)+(n+1)}{n-1} = \binom{2n}{n-1}$ chemins invalides à retirer aux $\binom{2n}{n}$ chemins au total. On obtient l'expression de $\mathcal{C}_n$, le n-ième nombre de Catalan.

$$\mathcal{C}_n = \binom{2n}{n} - \binom{2n}{n-1} = \frac{(2n)!}{(n!)^2} - \frac{(2n)!}{(n-1)!(n+1)!} = \frac{(2n)!}{(n!)^2} - \frac{n}{n+1} \times \frac{(2n)!}{(n!)^2} = \frac{1}{n+1}\binom{2n}{n}.$$

Autres exemples

On peut retrouver les nombres de Catalan à chaque fois que l'on peut représenter la situation par un dénombrement des « chemins dans le carré qui restent sous la diagonale » :

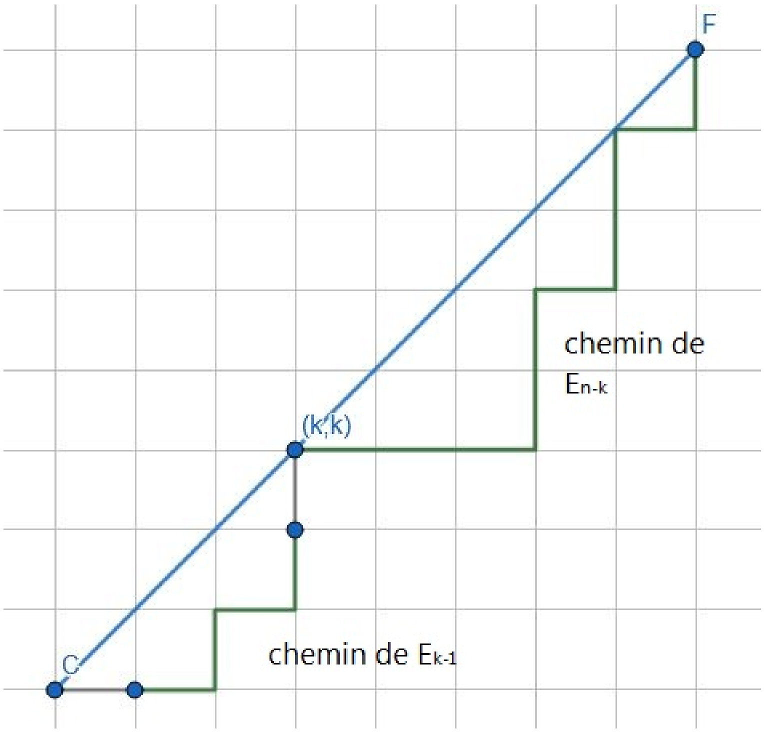
— Deux candidats A et B à une élection ont reçu n voix chacun ($n \in \mathbb{N}$), cependant, pendant tout le dépouillement, A est resté en tête, c'est-à-dire que la pile des voix pour B n'a jamais dépassé celle des voix pour A. *De combien de façons aurait-on pu ranger les bulletins pour que ceci se produise ?*

— Un parenthésage, constituée de parenthèses ouvrantes et fermantes, est valide s'il compte autant de parenthèses ouvrantes que fermantes, et si on ne ferme jamais de parenthèse non ouverte auparavant. *Combien de parenthésages valides de longueur $2n$ ($n \in \mathbb{N}$) existe-t-il ?*

Exercice 8 (Relation de récurrence vérifiée par les nombres de Catalan)
Montrer que, pour tout $n \in \mathbb{N}$:

$$\mathcal{C}_n = \sum_{k=0}^{n-1} \mathcal{C}_k \mathcal{C}_{n-k-1}.$$

<u>*Solution de l'exercice 8*</u>
On conserve, par exemple la représentation des « chemins dans le carré » de taille $n \times n$. On peut découper l'ensemble E_n les chemins qui restent sous la diagonale, selon l'abscisse k de leur premier point d'intersection avec la diagonale (hormis l'origine). Ce nombre est compris entre 1 et n, et pour $k \in \{1, \dots, n\}$, on appelle A_k l'ensemble des chemins de E_n qui rencontrent la diagonale pour la première fois à l'abscisse k.



On remarque alors qu'un chemin de A_k est exactement déterminé par le sous-chemin entre les positions $(1, 0)$ et $(k, k-1)$ et le sous-chemin entre les positions (k, k) et (n, n), qui correspondent respectivement à un chemin de E_{k-1} et un chemin de E_{n-k}. Réciproquement, on vérifie qu'avec un chemin de E_{k-1} et un chemin de E_{n-k}, on peut faire exactement un chemin de A_k.
Donc la correspondance est bijective : $\mid A_k \mid = \mid E_{k-1} \times E_{n-k} \mid = \mid E_{k-1} \mid \times \mid E_{n-k} \mid = \mathcal{C}_{k-1}\mathcal{C}_{n-k}$.
D'où la formule suivante :

$$\mathcal{C}_n = \sum_{k=1}^{n} \mathcal{C}_{k-1}\mathcal{C}_{n-k} = \sum_{k=0}^{n-1} \mathcal{C}_k \mathcal{C}_{n-k-1}.$$

Remarque 3.5.13.
De même que pour les coefficients binomiaux, cette relation permet de calculer effectivement les nombres de Catalan sans avoir à manipuler de factorielles par exemple.

– Exercices d'application –

Exercice 9 (JBMO 2018)
n nombres sont écrits sur un tableau, vérifiant les propriétés suivantes :

— tous les nombres ont 3 chiffres

— aucun ne contient de 0

— deux nombres différents n'ont jamais le même chiffre des centaines, ou le même chiffre des dizaines, ou le même chiffre des unités

— la somme des chiffres de chaque nombre vaut 9

Quelle est la valeur maximale possible pour n ?

Solution de l'exercice 9
On constate déjà que $n \leqslant 7$, car on ne peut pas utiliser les chiffres plus grands que 7 et on doit utiliser n chiffres des unités différents. La somme des $3n$ chiffres utilisés doit être égale à $9n$. Or la somme des chiffres des unités, par exemple, vaut au moins : $1 + \ldots + n = \frac{n(n+1)}{2}$. D'où l'inéquation vérifiée par n :

$$9n \geqslant \frac{3n(n+1)}{2}.$$

On a : $9 \times 7 = 63 < \frac{3 \times 7 \times 8}{2} = 84$ et $9 \times 6 = 54 < \frac{3 \times 6 \times 7}{2} = 63$, mais on constate que 5 vérifie l'inégalité, et que c'est même alors une égalité : $9 \times 5 = 45 = \frac{3 \times 5 \times 6}{2}$

Si c'est possible avec 5 nombres, on sait alors que seuls les chiffres 1, 2, 3, 4, 5 sont utilisés. On arrive par exemple aux 5 nombres suivants, ce qui permet de vérifier que 5 est bien le maximum (atteint) : 135, 252, 324, 441, 513.

4 Géométrie

1 Chasse aux angles

Le cours a repris en partie le cours de chasse aux angles donné au groupe B lors du stage olympique de Montpellier en 2016 (disponible ici). Les notions qui furent effectivement traitées sont :

— Angles alternes-internes, angles correspondants
— Somme des angles d'un triangle, d'un quadrilatère (avec preuve)
— Triangle isocèle
— Théorème de l'angle au centre (avec preuve)
— Théorème de l'angle inscrit (avec preuve, sans cas limite)
— Triangle rectangle, théorème de Thalès anglais (avec preuve)
— Cocyclicité, théorème de Fifi (preuve du sens direct)

– Exercices abordés –

Exercice 1
Soient Γ_1 et Γ_2 deux cercles s'intersectant en A et B. Une droite d passant par A coupe Γ_1 en P et Γ_2 en Q. De même, une droite d' passant par B recoupe Γ_1 en P' et Γ_2 en Q'. Montrer que les droites (PP') et (QQ') sont parallèles.

Exercice 2
Soient A, B, C et D quatre points cocycliques. On note respectivement A' et C' les projetés orthogonaux de A et C sur (BD), et B' et D' les projetés orthogonaux de B et D sur (AC). Montrer alors que A', B', C' et D' sont également cocycliques.

Exercice 3
Tynawedd met sur une table une pièce de 1 euro, de 2 euros, de 2 centimes et de 50 centimes, comme sur la figure ci-dessous.

Montrer qu'A, B, C et D sont cocycliques.

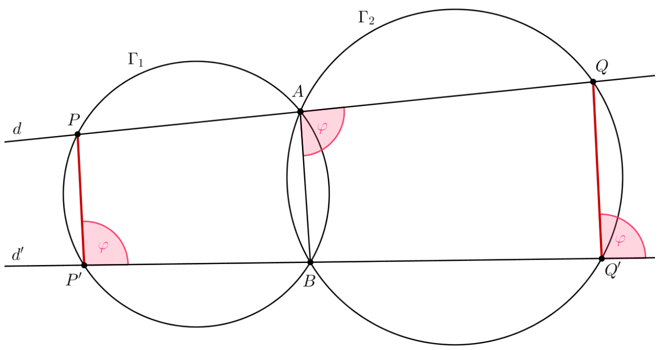
– Exercices bonus –

Exercice 4
Soit ABC un triangle et O le centre de son cercle circonscrit. Soient H_B et H_C les pieds des hauteurs issues de B et C. Prouver que $(H_BH_C) \perp (AO)$.

Exercice 5
Soit $ABCD$ un trapèze circonscriptible, avec $(AB) \mathbin{//} (CD)$ et $AB > CD$. Le cercle inscrit au triangle ABC est tangent aux côtés $[AB]$ et $[AC]$ en M et N respectivement. Montrer que le centre du cercle inscrit à $ABCD$ appartient à la droite (MN).

– Solutions des exercices –

Solution de l'exercice 1
La chasse aux angles classiques figure sur le dessin ci-dessous.



En rédigeant avec les angles orientés, on écrit

$$\begin{aligned}(P'B, P'P) &= (AB, AP) \text{ car } A, B, P' \text{ et } P \text{ sont cocycliques}\\ &= (AB, AQ) \text{ car } P, A \text{ et } Q \text{ sont alignés}\\ &= (Q'B, Q'Q) \text{ car } A, B, Q' \text{ et } Q \text{ sont cocycliques}\\ &= (P'B, Q'Q) \text{ car } P', B \text{ et } Q' \text{ sont alignés}\end{aligned}$$

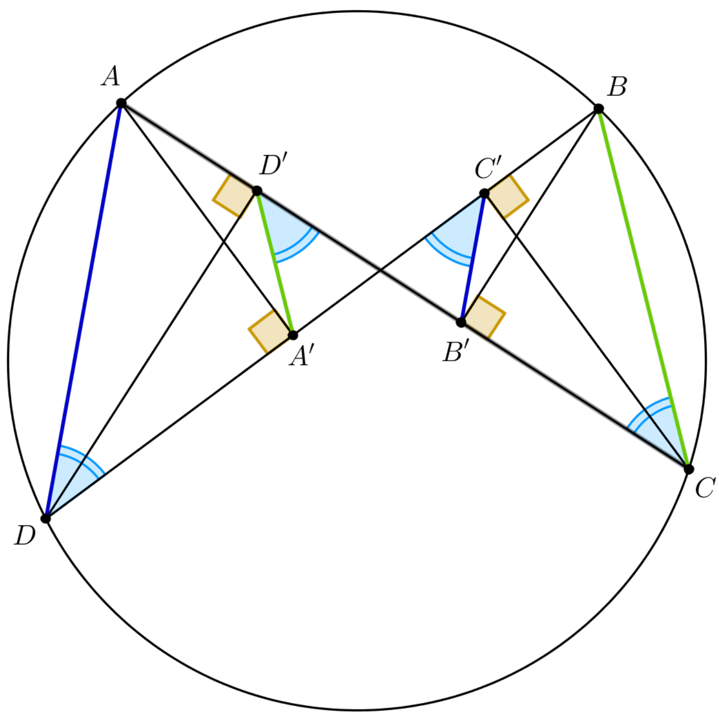
ce qui signifie bien que (PP') et (QQ') sont parallèles puisqu'on peut écrire

$$(P'P, Q'Q) = (P'P, P'B) + (P'B, Q'Q) = -(P'B, Q'Q) + (P'B, Q'Q) = 0$$

Solution de l'exercice 2
Puisque $\widehat{AD'D} = \widehat{AA'D} = 90$, le théorème de l'angle inscrit permet d'affirmer que A, D, A' et D' sont cocycliques. On obtient de la même façon que B, C, B' et C' sont cocycliques.

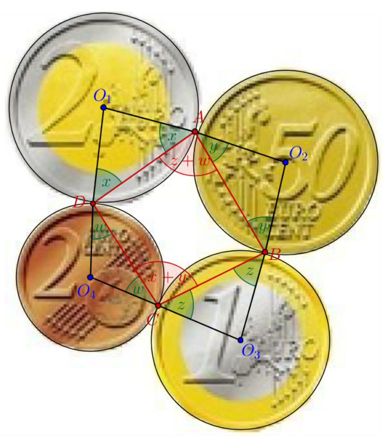
On en déduit alors que $(DA', DA) = (D'A', D'A)$ car A, D, A' et D' sont cocycliques et que $(CB, CB') = (C'B, C'B')$ car B, C, B' et C' sont cocycliques. Or, A, B, C et D étant cocycliques, nous savons que $(DB, DA) = (CB, CA)$ et l'alignement des points D, A' et B d'une part et de C, B' et A d'autre part fait que cette dernière égalité se réécrit $(DA', DA) = (CB, CB')$.

Finalement, on en conclut que $(D'A', D'A) = (C'B, C'B')$ soit $(D'A', D'B') = (C'A', C'B')$, ce qui démontre que A', B', C' et D' sont cocycliques.



Solution de l'exercice 3
Soient O_1, O_2, O_3 et O_4 les centres respectifs des pièces de 2 euros, 50 centimes, 1 euro et 2 centimes. La tangente commune aux pièces de 2 euros et de 50 centimes en A étant perpendiculaire à (O_1A) et à (O_2A), on en déduit que O_1, A et O_2 sont alignés. On prouve de même que $B \in (O_2O_3)$, $C \in (O_3O_4)$ et que $D \in (O_4O_1)$.

On remarque alors qu'on a alors énormément de triangles isocèles dans la figure, à savoir O_1AD, O_2AB, O_3BC et O_4CD, respectivement isocèles en O_1, O_2, O_3 et O_4. Il est donc naturel de poser $\widehat{O_1AD} = \widehat{O_1DA} = x$, $\widehat{O_2AB} = \widehat{O_2BA} = y$, $\widehat{O_3BC} = \widehat{O_3CB} = z$ et $\widehat{O_4CD} = \widehat{O_4DC} = w$, comme sur la figure ci-dessous.



La somme des angles du quadrilatère $O_1O_2O_3O_4$ donne

$$\widehat{O_4O_1O_2} + \widehat{O_1O_2O_3} + \widehat{O_2O_3O_4} + \widehat{O_3O_4O_1} = 360$$

soit

$$(180 - 2x) + (180 - 2y) + (180 - 2z) + (180 - 2w) = 360$$

ce qui se réécrit plus simplement $x + y + z + w = 180$.

On en conclut alors que

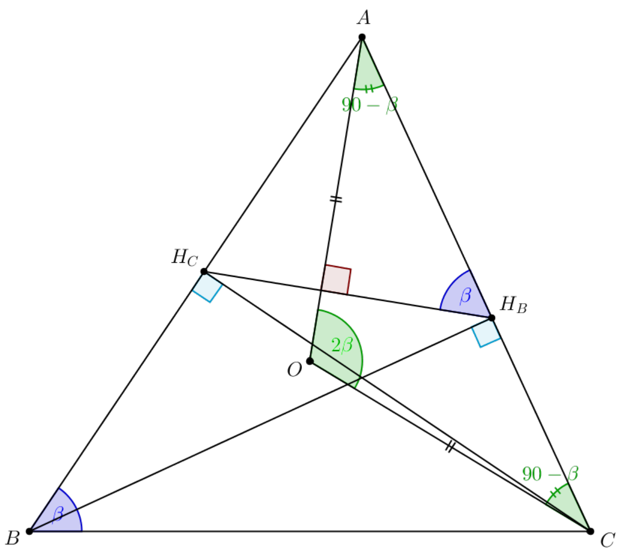
$$\widehat{DAB} + \widehat{BCD} = (180 - x - y) + (180 - z - w) = (z + w) + (x + y) = 180$$

ce qui permet d'affirmer que les points A, B, C et D sont cocycliques.

Solution de l'exercice 4

Les triangles BH_BC et BH_CC étant respectivement rectangles en H_B et H_C, le théorème de l'angle inscrit nous dit que B, C, H_B et H_C sont cocycliques, d'où on tire que $(BC, BH_C) = (H_BC, H_BH_C)$ soit $(BC, BA) = (H_BA, H_BH_C)$.

D'autre part, le théorème de l'angle au centre indique que $(OC, OA) = 2(BC, BA)$. Le triangle AOC étant isocèle en O, on en déduit que $(AO, AH_B) = (AO, AC) = 90 - (BC, BA)$.



La relation de Chasles donne finalement

$$(AO, H_BH_C) = (AO, H_BA) + (H_BA, H_BH_C) = 90 - (BC, BA) + (BC, BA) = 90$$

Solution de l'exercice 5

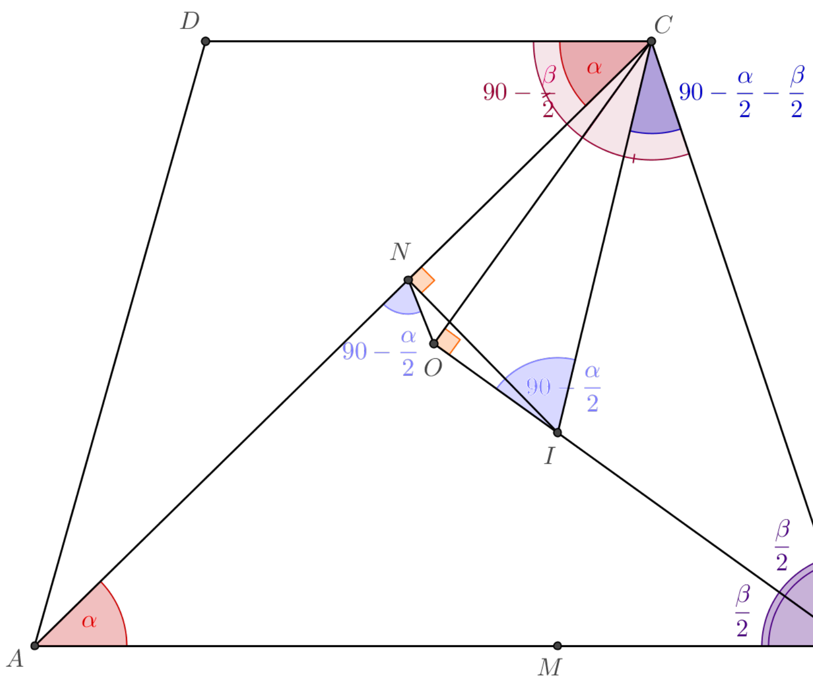
Le triangle AMN étant isocèle en A, $(NA, NM) = 90 - \frac{(AB,AC)}{2}$. Pour prouver que N, O et M sont alignés, il suffit donc de montrer que $(NA, NO) = 90 - \frac{(AB,AC)}{2}$.

$ABCD$ étant un trapèze, $(CD, CB) = 180 - (BC, BA)$. Puisque O est le centre du cercle inscrit à $ABCD$, on a $(CO, CB) = \frac{(CD,CB)}{2} = 90 - \frac{(BC,BA)}{2}$. De plus, I étant le centre du cercle inscrit à ABC, $(BC, BI) = \frac{(BC,BA)}{2}$. On en déduit alors que

$$\begin{aligned}
(OB, OC) &= (OB, BC) + (BC, OC) \text{ par la relation de Chasles} \\
&= -(BC, OB) - (OC, BC) \\
&= -(BC, BI) - (CO, CB) \text{ car } B, I \text{ et } O \text{ sont alignés} \\
&= -90 \text{ d'après les calculs faits précedemment} \\
&= 90 \text{ par définition modulo 180 des angles orientés}
\end{aligned}$$

Par ailleurs, par définition du point N, $(IN) \perp (AC)$. Ainsi, $(OB, OC) = (NI, NC)$, si bien que N, O, I et C sont cocycliques d'après le théorème de l'angle inscrit. On sait alors que $(NA, NO) = (IC, IO)$. Pour conclure, on calcule enfin

$$\begin{aligned}
(IC, IO) &= (IC, BC) + (BC, BI) \text{ d'après la relation de Chasles} \\
&= \frac{(CA, CB)}{2} + \frac{(BC, BA)}{2} \text{ par définition du point I} \\
&= \frac{(CA, BA)}{2} \text{ encore par Chasles} \\
&= 90 - \frac{(AB, AC)}{2}
\end{aligned}$$



2 Points remarquables

– Énoncés des exercices –

Exercice 1
Soient γ et γ' deux cercles tangents extérieurement en un point A. Soit t une tangente commune aux deux cercles, touchant γ (resp. γ') en T (resp. T'). On appelle M le milieu de $[TT']$.

Montrer que $MT = MA = MT'$.

Exercice 2
Soit $ABCD$ un quadrilatère cyclique dont les diagonales (AC) et (BD) sont perpendiculaires en X. Soit M le milieu de $[AB]$.

Montrer que $(MX) \perp (CD)$.

Exercice 3
Soit ABC un triangle inscrit dans un cercle Γ de centre O et d'orthocentre H. On note H_A le pied de la hauteur issue de A et M le milieu de $[BC]$. Montrer que

1. Le symétrique H' de H par rapport à M appartient à Γ.
2. Le symétrique H^* de H par rapport à (BC).
3. Montrer que $(H'H^*) \mathbin{/\!/} (BC)$

Exercice 4
Montrer que dans un triangle ABC d'orthocentre H inscrit dans un cercle de centre O, $\widehat{OAB} = \widehat{HAC}$.

Exercice 5
Soit $ABCD$ un quadrilatère quelconque. On note M (resp. N, O, P) le milieu de $[AB]$ (resp. $[BC], [CD], [DA]$). Montrer que $MNOP$ est un paralèllogramme.

Exercice 6
Soient γ et γ' deux cercles qui se coupent en A et B. On trace t la tangente commune à ces deux cercles , touchant γ (resp. γ') en T (resp. T') tel que TAT' contienne B. Soit B^* le symétrique de B par rapport à t.

Montrer que

1. A, T, T', B^* sont cocycliques.
2. Les cercles ATT' et BTT' ont même rayon
3. Quel exercice retrouve-t-on au cas limite où $A = B$?

– Solutions –

Solution de l'exercice 1
On introduit la tangente commune aux deux cercles en A, qui intersecte (TT') en un point M'. Alors par lemme de la tangente gloutonne pour le cercle γ, $M'T = M'A$, et de même pour le cercle γ', $M'A = M'T'$.

Mais alors $M'T = M'T'$, donc M' est le milieu de $[TT']$, et $M = M'$, donc on a bien $MT = MA = MT'$. Cela signifie que $\widehat{TAT'}$ est un angle droit.

Solution de l'exercice 2
Notons H l'intersection de (MX) et (CD).

Tout d'abord, notons que ABX est rectangle en X, donc $MA = MB = MX$. On en déduit que $\widehat{MAX} = \widehat{AXM} = \alpha$, et que $\widehat{DXH} = \widehat{MXB} = 90 - \alpha$.

Par angle inscrit, $\widehat{BAC} = \widehat{BDC} = \widehat{XDH}$. De là on déduit que le dernier angle du triangle XDH vaut $90°$, ce qui conclut.

Solution de l'exercice 3

1. Comme les segments $[HH']$ et $[BC]$ se coupent en leur milieu, leurs extrémités forment un parallélogramme, donc $BHCH'$ est un parallélogramme.

   En particulier, $\widehat{BHC} = \widehat{BH'C}$.

   Calculons $\widehat{BHC}$: remarquons que $\widehat{BAH} = \widehat{HCB} = \alpha$ par cocyclicité, et que $\widehat{CAH} = \widehat{HBC} = \beta$ par cocyclicité. Donc $\widehat{BHC} = 180 - \alpha - \beta = 180 - \widehat{BAC}$.

   Donc $\widehat{BH'C} = 180 - \widehat{BAC}$, et les pooints A, B, C et H' sont bien cocycliques.

2. De la même façon, on remarque que $\widehat{BHC} = \widehat{BH^*C}$ par symétrie axiale, donc $\widehat{BH^*C} = 180 - \widehat{BAC}$, donc les points A, B, C et H^* sont cocycliques.

3. (BC) est la droite des milieux dans $HH'H^*$, donc le théorème des milieux nous dit que $(BC) \mathbin{/\!/} (H'H^*)$

Solution de l'exercice 4
On sait que $OA = OC$ donc $\widehat{OAB} = \widehat{OBA} = \alpha$, et $\widehat{BOA} = 180 - 2\alpha$. Par angle au centre, $\widehat{BCA} = 90 - \alpha$, et en prolongeant la hauteur issue de A, on trouve que $\widehat{HAC} = 180 - (\widehat{BCA} + 90) = \alpha$, CQFD.

Solution de l'exercice 5
Dans le triangle ABC, on applique le théorème des milieux, qui dit que $MN = \frac{1}{2}AC$ et $(MN) \mathbin{/\!/} (AC)$. De la même façon, dans ABD on trouve que $OP = \frac{1}{2}AC$ et $(OP) \mathbin{/\!/} (AC)$.

On en déduit que $(MN) \mathbin{/\!/} (OP)$ et $MN = OP$. Or un quadrilatère respectant ces conditions est un parallélogramme, d'ou la conclusion.

Solution de l'exercice 6

1. On remarque que $\widehat{TB^*T'} = \widehat{TBT'}$ par symétrie. Remarquons que par théorème de l'angle tangent, on a $\widehat{BAT} = \widehat{BTT'} = \alpha$ et $\widehat{BAT'} = \widehat{BT'T} = \beta$, donc $\widehat{TBT'} = 180 - \alpha - \beta = 180 - \widehat{TAT'}$.

   Nous en déduisons que les angles $\widehat{TAT'}$ et $\widehat{TB^*T'}$ sont supplémentaires, donc que le quadrilatère $TAT'B^*$ est cyclique.

2. LEs cercles circonscrits à TBT' et TB^*T' sont symétriques par rapport à t, donc ils ont le même rayon. Or le cercle circonscit à Tb^*T' est aussi circonscrit à TAT' d'après 1., d'où le résultat.

3. Dans le cas où $A = B$, les deux cercles sont tangents extérieurement en A, et on retrouve l'exercice 1, avec son angle droit.

3 Angles tangents et triangles semblables

Le TD fut organisé en trois parties :

— Exercices autour de l'angle tangent (cas limite de l'angle inscrit)

— Mini-cours sur les triangles semblables (définition, propriétés métriques)

— Exercices utilisant des triangles semblables

— Exercices en groupes : les élèves étaient répartis en groupes de 3 ou 4 personnes et avaient un exercice à chercher en équipe. Les exercices étaient difficiles mais un animateur encadrait chaque groupe et donnait des indications pour aider les élèves à avancer. Une fois l'exercice résolu, chaque groupe a dû préparer une présentation orale et détailler les étapes de la preuve devant ses camarades qui n'avaient pas cherché le même exercice. Ce format a permis d'instaurer une grande écoute entre les élèves et de leur donner la satisfaction de résoudre un problème difficile ensemble, avec une aide minime distillée par les animateurs.

– Exercices sur l'angle tangent –

Exercice 1
Soit ABC un triangle. La bissectrice de $\widehat{BAC}$ recoupe $[BC]$ en D et le cercle circonscrit à ABC en S. Montrer que la droite (SB) est tangente au cercle circonscrit à ABD.

Exercice 2
Soient A, B, C et D quatre points sur un cercle Γ de telle sorte que les cordes $[AB]$ et $[CD]$ s'intersectent en un point E à l'intérieur de Γ et soit P un point arbitraire sur $[BE]$. La tangente t au cercle circonscrit de DEP en E coupe (BC) en F et (AC) en G. Démontrer que $\widehat{FGC} = \widehat{BDP}$.

– Exercices sur les triangles semblables –

Exercice 3
(puissance d'un point par rapport à un cercle) Soit $\mathcal{C}$ un cercle et P un point à l'extérieur de $\mathcal{C}$. Deux droites partant de P recoupent $\mathcal{C}$ en A, B et en C, D respectivement. Montrer que $PA.PB = PC.PD$. Que devient ce résultat si P est à l'intérieur du cercle ?

Exercice 4
Soit ABC un triangle rectangle en A et H le pied de la hauteur issue de A. Trouver des triangles semblables dans la figure et en déduire une démonstration du théorème de Pythagore.

– Exercices à chercher en groupe –

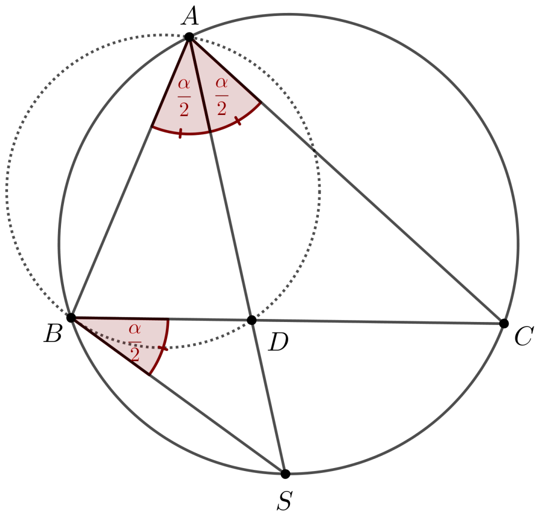
Exercice 5 (Adrià, Caleb, Clément)
Soient A, B, C, D et E cinq points dans cet ordre sur un cercle, vérifiant $AB = BC$ et $CD = DE$. On appelle respectivement P, Q et T l'intersection des droites (AD) et (BE), (AC) et (BD), (BD) et (CE). Montrer que le triangle PQT est isocèle.

Exercice 6 (Alexandre, Jeanne, Mithil, Nelly)
Soient ABC un triangle et D l'intersection de la bissectrice intérieure issue de A avec $[BC]$. La médiatrice de $[AD]$ recoupe la bissectrice issue de B en M et celle issue de C en N. Montrer que les points A, M, N et I sont sur un même cercle.

Exercice 7 (Étienne, Gaspard, Kate, Matthieu)
Soit $ABCD$ un quadrilatère cyclique et P un point sur le côté de $[AB]$. La diagonale (AC) coupe (DP) en Q. La droite parallèle à (CD) passant par P coupe (BC) en K et la droite parallèle à (DB) passant par Q coupe (CB) en L. Montrer que les cercles de BKP et CLQ sont tangents.

– Solutions des exercices –

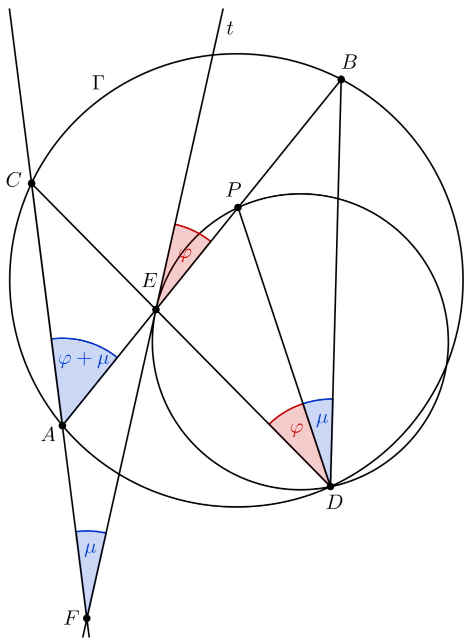
Solution de l'exercice 1
D'après le théorème de l'angle tangent, il suffit de montrer que $\widehat{BAD} = \widehat{SBD}$. Or, (AS) étant la bissectrice de $\widehat{BAC}$, on a : $\widehat{BAD} = \widehat{SAC} = \frac{\alpha}{2}$. Comme B, A, C et S sont cocycliques, le théorème de l'angle inscrit donne $\widehat{SBC} = \widehat{SAC}$ et on a bien $\widehat{SBD} = \widehat{BAD} = \frac{\alpha}{2}$.



Solution de l'exercice 2
A, B, C et D étant cocycliques, on a $(AB, AC) = (DB, DC)$. (EF) est tangente au cercle circonscrit de DEP, donc nous savons d'après le cas limite du théorème de l'angle inscrit que $(DP, DE) = (EP, EF)$. On écrit alors successivement

$$\begin{aligned}
\widehat{EFC} &= (FE, FC) \\
&= (AE, FC) + (FE, AE) \text{ d'après la relation de Chasles} \\
&= (AB, AC) - (EP, FE) \text{ car } E \in (AP) \text{ et } F \in (AC) \\
&= (DB, DC) - (DP, DE) \text{ d'après ce qui précède} \\
&= (DB, DE) + (DE, DP) \text{ car } D, E \text{ et } C \text{ sont alignés} \\
&= (DB, DP) \text{ d'après la relation de Chasles} \\
&= \widehat{BDP}
\end{aligned}$$

Solution de l'exercice 3
Réécrivons l'égalité à prouver sous la forme d'un ratio de longueur pour nous rapprocher



de la propriété métrique des triangles semblables : $PA.PB = PC.PD \Leftrightarrow \frac{PA}{PC} = \frac{PD}{PB}$. Cette écriture suggère de montrer que $PAC \sim PDB$, ce qui est une conséquence du théorème de Fifi. Le résultat reste vrai si P est à l'intérieur du cercle. C'est alors le théorème de l'angle inscrit qu'on utilise pour montrer que $PAC \sim PDB$.

Solution de l'exercice 4

En notant $\beta = \widehat{CBA}$, on a successivement $\widehat{BAH} = 90 - \beta$, $\widehat{HAC} = \beta$ et $\widehat{ACH} = 90 - \beta$. Ainsi, $ABC \sim HBA$ et $ABC \sim HAC$. Écrivons les propriétés métriques correspondantes :

$$\frac{AB}{HB} = \frac{BC}{BA} = \frac{AC}{HA}$$

et

$$\frac{AB}{HA} = \frac{BC}{AC} = \frac{AC}{HC}$$

Afin de démontrer le théorème de Pythagore, repérons les termes quadratiques dans ces deux égalités : ce sont $AB^2 = BC.HB$ et $AC^2 = BC.HC$. Par somme, $AB^2+AC^2 = BC.(HB+HC)$. Or $HB + HC = BC$ et on retrouve bien $AB^2 + AC^2 = BC^2$.

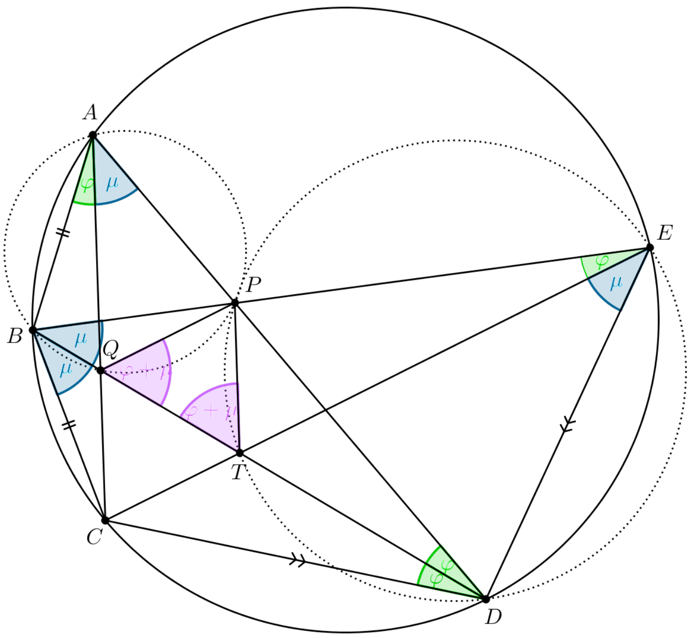
Solution de l'exercice 5

Les points A, B, C et D étant cocycliques, le théorème de l'angle inscrit nous permet d'écrire $(BC, BD) = (AC, AD)$. Puisque D est le milieu de l'arc $\widehat{CE}$, le théorème du pôle Sud affirme que $(BC, BD) = (BD, BE)$. Les deux résultats précédents, combinés à l'alignement des points B, P et E d'une part et B, Q, T et D d'autre part, donnent $(AQ, AP) = (BQ, BP)$, ce qui démontre que les points A, B, P et Q sont cocycliques. On prouve de la même façon que les points E, D, P et T sont cocycliques.

On a ainsi $(AB, AP) = (QT, QP)$ et $(EP, ED) = (TP, TQ)$. Mais $(AB, AP) = (EP, ED)$ car A, B, D et E sont cocycliques, d'où $(QT, QP) = (TP, TQ)$. Le triangle PQT est donc isocèle en P.

Solution de l'exercice 6

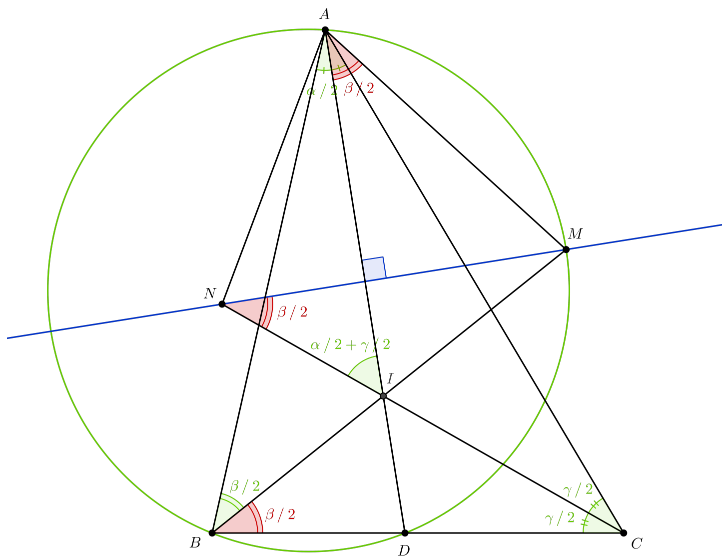
Le point M est défini comme l'intersection de la médiatrice de $[AD]$ avec la bissectrice de



$\widehat{ABD}$. D'après le théorème du pôle Sud, M, A, B et D sont donc cocycliques. On en déduit que $(BD, BM) = (AD, AM) = \frac{(BC,BA)}{2}$. Par ailleurs,

$$\begin{aligned}(NM, NI) &= (NM, IA) + (AI, AC) + (CA, CI) \text{ (relation de Chasles)} \\ &= 90 + \frac{(AB, AC)}{2} + \frac{(CA, CB)}{2} \text{ par définition de } I \\ &= \frac{(AB, CB)}{2} \text{ d'après la relation de Chasles}\end{aligned}$$

Dès lors, $(NM, NI) = (AM, AI)$, ce qui prouve que A, M, I et N sont cocycliques.



Solution de l'exercice 7

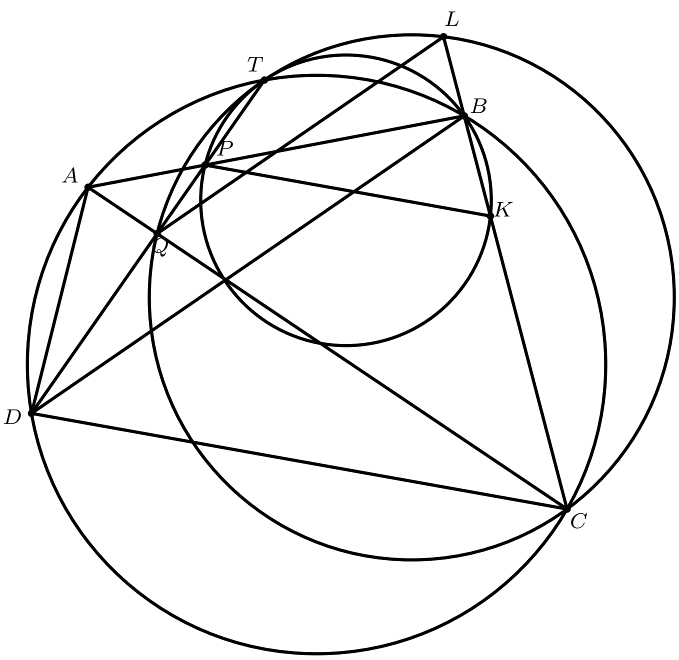
On note T l'intersection de (DP) et du cercle ABD, on va démontrer que les cercle BKP et CLQ sont tangents au point T. On va donc tout d'abord montrer qu'il est sur ces deux cercles.

On a $\widehat{BKP} = \widehat{BCD}$ par angles correspondants et que $(PK)//(DC)$. Par cocyclicité des points T, B, C et Q, on a $\widehat{BCD} = 180 - \widehat{DTB}$. Mais $\widehat{DTB} = \widehat{PTB}$, ce qui montre que $180 - \widehat{DTB} = 180 - \widehat{PTB}$. On a ainsi $\widehat{BKP} = 180 - \widehat{PTB}$, ce qui montre bien que les points P, T, B et K sont cocycliques.

On a $\widehat{QLC} = \widehat{DBC}$ car $(QL)//((DB)$ et par angles correspondants. On a ensuite $\widehat{DBC} = \widehat{DTC}$ par cocyclicité des points B, C, D et T. On a ensuite $\widehat{DTC} = \widehat{QTC}$. On trouve enfin que $\widehat{QLC} = \widehat{QTC}$ ce qui montre que les points T, L, Q et C sont cocycliques.

Cela permet d'oublier les points L et K de l'énoncé et de montrer que les cercles PTB et TQC sont tangents.

On veut démontrer que les cercles PTB et TQC sont tangents. On introduit (t) la tangente en T au cercle TPB, si on parvient à démontrer que le droite (t) est aussi tangente au cercle TQC on pourra en conclure que les cercles PTB et TQC sont tangents. L'angle entre (t) et l droite PT est l'angle $\widehat{TBC}$ par angle avec la tangente. On a de plus, $\widehat{TBP} = \widehat{TBA}$ et $\widehat{TBA}$ est l'angle entre la tangente au cercle TQC en T et la droite QT, ainsi l'angle entre la tangente au cercle TPB en T avec la droite TP est le même que l'angle entre la tangente au cercle TQC en T avec la droite TQ comme les points T, P et Q sont alignés il doit forcément s'agir de la même droite ce qui montre bien que les cercles TPB et TQC ont une tangente commune en T.



4 Homothéties

Le cours a repris la trame de la section « Homothéties » du merveilleux cours sur les transformations géométriques de Thomas Budzinski, sans trop s'attarder sur la notion de vecteur.

La preuve de la concourance des médianes et de l'alignement de O, G et H sur la droite d'Euler a été faite en exercice. Les exercices 5 (construction d'un carré inscrit dans un triangle) et 10 ont également été abordés.

5 Exercices d'entraînement

1 Entraînement de mi-parcours

– Énoncés –

Exercice 1
Soit ABC un triangle. On note respectivement H_A, H_B et H_C les pieds des hauteurs issues de A, B et C. Montrer que (AH_A) est la bissectrice de $\widehat{H_CH_AH_B}$.

Exercice 2
Soit $a, b > 0$. Montrer que

$$\left(1+\frac{a}{b}\right)^2+\left(1+\frac{b}{a}\right)^2 \geqslant 8$$

Exercice 3
Soit $ABCD$ un quadrilatère cyclique (c'est-à-dire que A, B, C et D sont cocycliques) et tangentiel (c'est-à-dire dont tous les côtés sont tangents à un même cercle inscrit dans le quadrilatère). On note respectivement E, F, G et H les points de tangence de son cercle inscrit avec les côtés $[AB]$, $[BC]$, $[CD]$ et $[DA]$. Prouver que $(EG) \perp (HF)$.

Exercice 4
Soit $x, y, z > 0$.

1. Montrer que

$$\frac{\frac{x}{y}+\frac{y}{z}+\frac{z}{x}}{3} \geqslant 1$$

2. Montrer que

$$\frac{x^2}{y^2}+\frac{y^2}{z^2}+\frac{z^2}{x^2} \geqslant \frac{(\frac{x}{y}+\frac{y}{z}+\frac{z}{x})^2}{3}$$

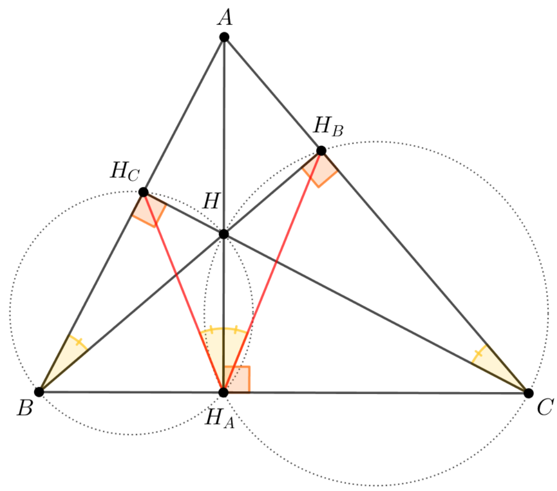
3. En déduire que

$$\frac{x^2}{y^2}+\frac{y^2}{z^2}+\frac{z^2}{x^2} \geqslant \frac{x}{y}+\frac{y}{z}+\frac{z}{x}$$

– Solutions –

Solution de l'exercice 1
Étant donné que la figure comporte de nombreux triangles rectangles, plusieurs quadruplets de points cocycliques apparaissent. En effet, $\widehat{BH_CH}+\widehat{BH_AH} = 90+90 = 180$ donc le théorème de Fifi permet d'affirmer que B, H_C, H et H_A sont cocycliques. De même, C, H_B, H et H_A sont cocycliques.

Par le théorème de l'angle inscrit, $\widehat{H_CBH} = \widehat{H_CH_AH}$ d'une part et $\widehat{HH_AH_B} = \widehat{HCH_B}$ d'autre part. Par ailleurs, B, H_B, H_C et C sont également cocycliques si bien que $\widehat{H_CBH} =$



$\widehat{HCH_B}$. En combinant les trois égalités précédentes, on obtient $\widehat{H_CH_AH} = \widehat{HH_AH_B}$, ce qui montre bien que (H_AA) est la bissectrice de $\widehat{H_CH_AH_B}$.

Solution de l'exercice 2
Première solution : avec l'inégalité des moyennes arithmétique et quadratique on a

$$\sqrt{\frac{(1+\frac{a}{b})^2+(1+\frac{b}{a})^2}{2}} \geqslant \frac{(1+\frac{a}{b})+(1+\frac{b}{a})}{2} = \frac{2+\frac{a}{b}+\frac{b}{a}}{2}$$

De plus en notant $u = \frac{a}{b}$ on a que $\frac{a}{b}+\frac{b}{a} = u + \frac{1}{u} \geq 2$. Donc

$$\sqrt{\frac{(1+\frac{a}{b})^2+(1+\frac{b}{a})^2}{2}} \geqslant 2$$

et alors

$$\frac{(1+\frac{a}{b})^2+(1+\frac{b}{a})^2}{2} \geqslant 4$$

Seconde solution : En développant

$$(1+\frac{a}{b})^2+(1+\frac{b}{a})^2 = 1+2\frac{a}{b}+\frac{a^2}{b^2}+1+2\frac{b}{a}+\frac{b^2}{a^2} = 2+2(\frac{a}{b}+\frac{b}{a})+(\frac{a^2}{b^2}+\frac{b^2}{a^2})$$

Deux possibilités s'offrent alors à nous :

1. Avec $u = \frac{a}{b}$, on a $\frac{a}{b}+\frac{b}{a} = u+\frac{1}{u} \geq 2$. Avec $v = \frac{a^2}{b^2}$, on a également $\frac{a^2}{b^2}+\frac{b^2}{a^2} = u+\frac{1}{u} \geq 2$, d'où l'on déduit

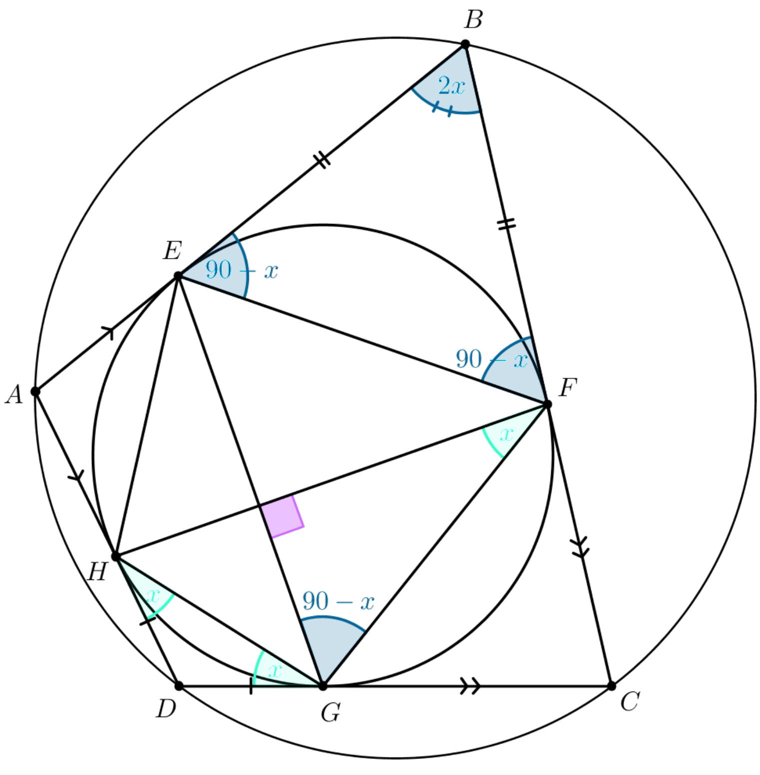
$$(1+\frac{a}{b})^2+(1+\frac{b}{a})^2 \geqslant 2+2\times 2+2 \geqslant 8$$

2. Sinon, on fait ainsi :

$$\begin{aligned}
&2+2(\frac{a}{b}+\frac{b}{a})+(\frac{a^2}{b^2}+\frac{b^2}{a^2})-8\geqslant 0\\
&\Leftrightarrow 2(\frac{a}{b}+\frac{b}{a}-2)+(\frac{a^2}{b^2}+\frac{b^2}{a^2}-2)\geqslant 0\\
&\Leftrightarrow 2(\frac{a^2-2ab+b^2}{ab})+(\frac{a^4-2a^2b^2+b^4}{a^2b^2})\geqslant 0\\
&\Leftrightarrow 2\frac{(a-b)^2}{ab}+\frac{(a^2-b^2)^2}{a^2b^2}\geqslant 0
\end{aligned}$$

Solution de l'exercice 3

$$\begin{aligned}
(GE,HF) &= (GE,GF)+(FG,FH) \text{ d'après la relation de Chasles}\\
&= (FE,FB)+(GD,GH) \text{ (cas limite du théorème de l'angle inscrit)}\\
&= \frac{(BE,BF)}{2}+\frac{(DA,DC)}{2} \text{ car } BE=BF \text{ et } DG=DH\\
&= 90 \text{ car } A, B, C \text{ et } D \text{ sont cocycliques, soit } (BA,BC)+(DA,DC)=180
\end{aligned}$$



Solution de l'exercice 4

1. Par l'inégalité arithmétique et géométrique,

$$\frac{\frac{x}{y}+\frac{y}{z}+\frac{z}{x}}{3}\geqslant\sqrt[3]{\frac{x}{y}\cdot\frac{y}{z}\cdot\frac{z}{x}}=\sqrt[3]{1}=1$$

2. Par l'inégalité arithmétique et quadratique

$$\sqrt{\frac{\frac{x^2}{y^2}+\frac{y^2}{z^2}+\frac{z^2}{x^2}}{3}} \geqslant \frac{\frac{x}{y}+\frac{y}{z}+\frac{z}{x}}{3}$$

Donc

$$\frac{\frac{x^2}{y^2}+\frac{y^2}{z^2}+\frac{z^2}{x^2}}{3} \geqslant \frac{(\frac{x}{y}+\frac{y}{z}+\frac{z}{x})^2}{9}$$

Conclusion :

$$\frac{x^2}{y^2}+\frac{y^2}{z^2}+\frac{z^2}{x^2} \geqslant \frac{(\frac{x}{y}+\frac{y}{z}+\frac{z}{x})^2}{3}$$

3. Il suffit de regrouper les deux résultats des questions précédentes.

$$\begin{aligned}\frac{x^2}{y^2}+\frac{y^2}{z^2}+\frac{z^2}{x^2} &\geqslant \frac{(\frac{x}{y}+\frac{y}{z}+\frac{z}{x})^2}{3}\\ &\geqslant (\frac{x}{y}+\frac{y}{z}+\frac{z}{x})\frac{(\frac{x}{y}+\frac{y}{z}+\frac{z}{x})}{3}\\ &\geqslant (\frac{x}{y}+\frac{y}{z}+\frac{z}{x})\end{aligned}$$

2 Entraînement final

– Énoncés –

Exercice 1
Montrer que $n-1$ divise $2n^n+3n-5$.

Exercice 2
Soit un damier 10×10. On met un jeton sur la case en bas à gauche. On peut bouger le jeton d'une case à une autre si les deux cases sont côte à côte, c'est-à-dire partagent un même côté. Peut-on atteindre la case en haut à droite en passant par toutes les cases du damier une et une seule fois ?

Exercice 3
On pose $u_1 = 5$ et pour tout $n \geqslant 1$, on a la relation $u_{n+1} = u_n + (2n+5)$.

1. Montrer que, pour $n \geqslant 1$: $u_n = n^2 + 4n$.
2. En déduire que $\frac{5^2+7^2+\ldots+(2n+3)^2}{n} \geqslant (n+4)^2$

Exercice 4
On dispose d'une pile de 100 pièces. De là, il est possible d'effectuer deux types d'opérations :

1. enlever une pièce d'un tas d'au moins 3 pièces et diviser le tas restant en deux tas (non vides) de tailles quelconque, ou bien

2. supprimer un tas d'une seule pièce.

Est-il possible, après une succession de telles opérations, d'arriver à la situation où l'on n'a plus aucune pièce ?

– Solutions –

Solution de l'exercice 1
Travaillons modulo $n-1$: puisque $n \equiv 1 \pmod{n-1}$, on peut substituer les occurrences de l'entier n en mettant des 1 à la place (sauf pour le n de l'exposant, bien sûr). On trouve alors directement

$$2 \times n^n + 3n - 5 \equiv 2 \times 1^n + 3 \times 1 - 5 \equiv 0 \pmod{n-1},$$

ce qui conclut.

Solution de l'exercice 2
On colorie le damier avec des cases noires et des cases blanches comme un damier ordinaire. La case en bas à gauche est noire. Puisque la case en haut à droite est sur la même diagonale que la case en bas à gauche, celle ci est également noire.

Lorsque l'on bouge le jeton, on alterne cases blanches et noires. La $1^{\text{ère}}$ case visitée étant la case en bas à gauche, elle est noire. Puis la $2^{\text{ème}}$ est blanche, la $3^{\text{ème}}$ est blanche, etc. Ainsi, la $k^{\text{ème}}$ case visitée est blanche si k est pair, et noire si k est impair.

La $100^{\text{ème}}$ case visitée est donc blanche, et il ne peut donc pas s'agir de la case en haut à droite, puisque celle-ci est noire.

Solution de l'exercice 3

1. On procère par récurrence. Soit H_n la propriété Â« $u_n = n^2 + 4n$ Â».
   Initialisation : Puisque $u_1 = 5 = 1^2 + 4 \times 1$, la propriété H_1 est bien vraie.
   Hérédité : Montrons que H_n implique H_{n+1}. Si H_n est vrai, alors $u_n = n^2 + 4n$, donc

   $$u_{n+1} = u_n + 2n + 5 = n^2 + 4n + 2n + 5 = (n^2 + 2n + 1) + (4n + 4) = (n+1)^2 + 4(n+1).$$

   Cela signifie que H_{n+1} est vraie.
   Conclusion : La propriété H_n est vraie pour tout $n \geqslant 0$.
2. Puisque l'on voit une moyenne arithmétique de carrés, on va utiliser l'inégalité entre moyennes arithmétique et géométrique :

   $$\sqrt{\frac{5^2 + 7^2 + ... + (2n+3)^2}{n}} \geqslant \frac{5 + 7 + \cdots + (2n+3)}{n}.$$

   Or, la question précédente indique que $u_n = 5 + 7 + \ldots + (2n+3) = n^2 + 4n$. On en déduit que

   $$\sqrt{\frac{5^2 + 7^2 + ... + (2n+3)^2}{n}} \geqslant \frac{n^2 + 4n}{n} = n + 4,$$

   c'est-à-dire que

   $$\frac{5^2 + 7^2 + ... + (2n+3)^2}{n} \geqslant (n+4)^2.$$

Solution de l'exercice 4

Soit p le nombre de pièces et t le nombre de tas à un moment donné. Au début, $p = 100$ et $t = 1$. En regardant les deux actions possibles, vérifions que $p + t$ est impair :

1. soit p diminue de 1 et t augmente de 1, de sorte que $p + t$ ne change pas ;
2. soit p et t diminuent tous deux de 1, de sorte que $p + t$ diminue de 2.

La somme $p + t$ reste donc toujours impaire : avoir 0 pièce et 0 tas est donc impossible.

IV. Groupe B

Contenu de cette partie

1 Algèbre

1 Ensembles, calcul et inégalités

– Nombres rationnels et réels –

Proposition 1.1.1.
i) La somme de deux nombres rationnels est elle aussi rationnelle.
ii) Le produit de deux nombres rationnels est aussi un nombre rationnel.
iii) Le produit d'un nombre rationnel non nul et d'un nombre irrationnel est un nombre irrationnel.
iv) La somme d'un nombre rationnel et d'un nombre irrationnel est un nombre irrationnel.

Démonstration. Soit $a = \frac{p_1}{q_1}$ et $b = \frac{p_2}{q_2}$, $p_1, p_2, q_1, q_2 \in \mathbb{Z}$. Soit $x \in \mathbb{R} \backslash \mathbb{Q}$
i) $a + b = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2} \in \mathbb{Q}$

ii) $a \times b = \frac{p_1 p_2}{q_1 q_2} \in \mathbb{Q}$

iii) Par l'absurde, on suppose que le produit est rationnel : $a \times x = \frac{p}{q}$ avec $p, q \in \mathbb{Z}$.
Alors $x = \frac{p}{qa} = \frac{pq_1}{qp_1} \in \mathbb{Q}$, ce qui contredit l'irrationalité de x. Donc le produit est irrationnel.

iv) Par l'absurde, on suppose que la somme est rationnelle : $a + x = \frac{p}{q}$ avec $p, q \in \mathbb{Z}$.
Alors, $x = \frac{p}{q} - a = \frac{pq_1 - p_1 q}{qq_1} \in \mathbb{Q}$, ce qui contredit l'irrationalité de x. Donc la somme est irrationnelle. □

Remarque 1.1.2.
Attention : on ne peut rien obtenir pour la somme et le produit de deux nombres irrationnels !
Par exemple : $\sqrt{2} + (-\sqrt{2} + 1) = 1 \in \mathbb{Q}$ alors que $\sqrt{2}$ et $(-\sqrt{2} + 1)$ sont irrationnels.
$\sqrt{2} \times \sqrt{2} = 2 \in \mathbb{Q}$

Exercice 1
Montrer que $\sqrt{2}$ est un nombre irrationnel.

– Coefficient binomiaux –

Définition 1.1.3.
Le coefficient binomial « k parmi n », noté $\binom{n}{k}$ est le nombre de façons de choisir simultanément k éléments dans un ensemble de n éléments différents (l'ordre n'a pas d'importance).

Notation.
Soit $n \in \mathbb{N}$. On note $n! = \prod_{k=1}^{n} k$ et on lit « factorielle n ».

Proposition 1.1.4.
Pour $k \in [\![0;n]\!]$, on a $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Pour $k > n$, $\binom{n}{k} = 0$

Démonstration. Tout d'abord, le nombre de manière d'ordonner n éléments est $n!$. En effet, on a n choix pour le premier élément, puis $n-1$ pour le deuxième etc jusqu'au dernier élément pour lequel on a une seule possibilité.

Comptons maintenant le nombre de k-uplets d'un ensemble à n éléments distincts (l'ordre importe). On a n possibilités pour le premier élément, $n-1$ pour le deuxième élément etc jusqu'au k-ième élément pour lequel on a $n-k+1$ possibilités. Au total, le nombre de k-uplets est égal à $n(n-1)...(n-k+1) = \frac{n!}{(n-k)!}$.

Maintenant, on peut trouver une autre façon de compter les k-uplets : on choisit les k éléments (on a $\binom{n}{k}$ possibilités) puis on leur impose un ordre (on a $k!$ possibilités).

Ainsi $k! \times \binom{n}{k} = \frac{n!}{(n-k)!}$ donc $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ □

Proposition 1.1.5.
Soit $n \in \mathbb{N}$ et $k \in [\![0;n]\!]$. Alors on a $\binom{n}{k} = \binom{n}{n-k}$.

Démonstration. Immédiat avec la formule.

On peut aussi voir une preuve combinatoire : choisir k éléments parmi n revient à choisir les $n-k$ éléments qu'on ne veut pas. □

Proposition 1.1.6 (Formule de Pascal)**.**
Soit $n \in \mathbb{N}$ et $k \in [\![0;n]\!]$ avec $(k;n) \neq (0;0)$.

Alors on a : $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

Démonstration. On peut utiliser la formule explicite du coefficient binomial ce qui nous donne finalement :

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\ &= \frac{(n-k)(n-1)! + k(n-1)!}{(k)!(n-k)!} \\ &= \frac{n!}{k!(n-k)!} = \binom{n}{k}\end{aligned}$$

On peut aussi montrer cette formule de manière combinatoire : on compte le nombre de sous-ensembles à k éléments de $\{1, 2, ..., n\}$. On trie selon l'appartenance de n au sous-ensemble sélectionné : il y a $\binom{n-1}{k}$ sous-ensembles ne contenant pas n et $\binom{n-1}{k-1}$ sous-ensembles contenant n.

D'où la formule de Pascal. □

Remarque 1.1.7.
On peut alors construire le triangle de Pascal : la case de la ligne n et de la colonne k contient le coefficient binomial $\binom{n-1}{k-1}$.

$$\begin{array}{cccccccc}
1 \\
1 & 1 \\
1 & 2 & 1 \\
1 & 3 & 3 & 1 \\
1 & 4 & 6 & 4 & 1 \\
1 & 5 & 10 & 10 & 5 & 1 \\
1 & 6 & 15 & 20 & 15 & 6 & 1 \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1
\end{array}$$

– Factorisations –

Proposition 1.1.8.
Identités remarquables :

$(a+b)^2 = a^2 + 2ab + b^2$

$(a-b)^2 = a^2 - 2ab + b^2$

$(a-b)(a+b) = a^2 - b^2$

Démonstration. Développer par double distributivité. □

Exemple 1.1.9.
Une petite factorisation pour commencer !

$x^2-1+(2x+2)(x+3) = (x-1)(x+1)+2(x+1)(x+3) = (x+1)(x-1+2x+6) = (x+1)(3x+5)$

Proposition 1.1.10.
Formule du binôme de Newton : Soit $a, b \in \mathbb{R}$ et $n \in \mathbb{N}^*$

$(a+b)^n = \sum\limits_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Démonstration. On utilise pour cela la formule la formule de Pascal : $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$

Montrons cette formule par récurrence sur n :

Initialisation : pour $n = 0$, $(a+b)^0 = 1 = \binom{0}{0} a^0 b^0$

Hérédité : Soit $n \in \mathbb{N}$ tel que la formule du binôme est vérifiée. Montrons qu'elle est alors aussi vérifiée au rang $n+1$.

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)\times(a+b)^n \\
&= (a+b)\times\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k}+\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k+1} \\
&= \sum_{k=1}^{n+1}\binom{n}{k-1}a^kb^{n-k+1}+\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k+1} \\
&= \binom{n}{0}a^0b^{n+1}+\binom{n}{n}a^{n+1}b^0+\sum_{k=1}^{n}\left(\binom{n}{k-1}+\binom{n}{k}\right)a^kb^{n-k+1} \\
&= b^{n+1}+a^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}a^kb^{n-k} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^kb^{n+1-k}
\end{aligned}$$

Ainsi la formule est vérifiée au rang n+1.
D'après le principe de récurrence, la formule du binôme est vérifiée pour tout $n \in \mathbb{N}$.

□

Proposition 1.1.11.

Pour tout $n \in \mathbb{N}$, $a^n - b^n = (a-b)\sum\limits_{k=0}^{n-1} b^k a^{n-1-k}$

Démonstration. Développer et remarquer que la somme est télescopique. □

Remarque 1.1.12.

On en déduit notamment que pour tout n impair, $a^n + b^n = \sum\limits_{k=0}^{n-1}(-1)^k b^k a^{n-1-k}$.

Un cas particulier utile pour b = 1 : $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + ... + x + 1)$

Exercice 2 (Somme d'une suite géométrique)
Soit $x \in \mathbb{R}$, $n \in \mathbb{N}$. Selon la valeur de x, déterminer la valeur de $\sum_{k=0}^{n} x^k$.

Proposition 1.1.13.
Soient a_1, a_2, ..., $a_n \in \mathbb{R}$. Alors $\left(\sum_{k=1}^{n} a_k\right)^2 = \sum_{k=1}^{n} a_k^2 + 2 \sum_{1 \leq i < j \leq n} a_i a_j$

– Manipulation d'inégalités –

Lemme 1.1.14.
Pour tout a, b, c et $d \in \mathbb{R}$: $a \leqslant c$ et $b \leqslant d \Rightarrow a + b \leqslant c + d$

Lemme 1.1.15.
Pour tout $a, b \in \mathbb{R}$, $k \in \mathbb{R}_+^*$: $a \leqslant b \Leftrightarrow ka \leqslant kb$

Lemme 1.1.16.
Pour tout $a, b \in \mathbb{R}$, $k \in \mathbb{R}_-^*$: $a \leqslant b \Leftrightarrow ka \geqslant kb$

Lemme 1.1.17.
Soit $f : A \to \mathbb{R}$ une fonction croissante sur un intervalle $B \subseteq A$.
Alors pour tout $a, b \in B$: $a \leq b \Rightarrow f(a) \leq f(b)$.
Si de plus f est strictement croissante on a : $a \leq b \Leftrightarrow f(a) \leq f(b)$.

Lemme 1.1.18.
Soit $f : A \to \mathbb{R}$ une fonction décroissante sur un intervalle $B \subseteq A$.
Alors pour tout $a, b \in B$: $a \leq b \Rightarrow f(a) \geq f(b)$.
Si de plus f est strictement décroissante on a : $a \leq b \Leftrightarrow f(a) \geq f(b)$.

Remarque 1.1.19.
Une somme de termes positifs est donc toujours positive. De plus, la somme est nulle si et seulement si tous les termes sont nuls.

– Un carré est toujours positif –

Proposition 1.1.20.
Pour tout $x \in \mathbb{R}$, $x^2 \geqslant 0$ avec égalité si et seulement si $x = 0$

Exemple 1.1.21.
Ainsi on a directement que pour tout $a, b \in \mathbb{R}$: $a^2 + b^2 \geqslant 2ab$ avec égalité si et seulement si $a = b$.

Exercice 3
Montrer que pour tout $x, y > 0$: $\frac{x}{x^4+y^2} + \frac{y}{x^2+y^4} \leqslant \frac{1}{xy}$

– Résolution des équations de degré 2 –

On cherche une méthode de résolution des équations de type $ax^2+bx+c = 0$ avec $a, b, c \in \mathbb{R}$, $a \neq 0$. Les solutions d'une telle équation sont appelées racines du polynôme $aX^2 + bX + c$.

$$\begin{aligned} ax^2 + bx + c &= a(x^2 + \frac{b}{a}x + \frac{c}{a}) \\ &= a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) \\ &= a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right) \end{aligned}$$

Notation.
On note $\Delta = b^2 - 4ac$ et on appelle Δ le discriminant du polynôme $aX^2 + bX + c$.

Alors $ax^2 + bx + c = 0 \Leftrightarrow \left(x + \frac{b}{2a}\right)^2 = \frac{\Delta}{4a^2}$

On distingue alors trois cas :
Cas 1 : Si $\Delta < 0$ alors l'équation $ax^2 + bx + c = 0$ n'admet pas de solutions réelles.
Cas 2 : Si $\Delta = 0$ alors l'équation admet une seule racine réelle dite racine double qui est $x_0 = \frac{-b}{2a}$.
Cas 3 : Si $\Delta > 0$ alors l'équation admet deux racines réelles distinctes qui sont $x_1 = \frac{-b+\sqrt{\Delta}}{2a}$ et $x_2 = \frac{-b-\sqrt{\Delta}}{2a}$.

Exemple 1.1.22.
Factoriser $P(X) = X^2 - X - 1$ dans $\mathbb{R}$.
On calcule le discriminant de ce polynôme : $\Delta = (-1)^2 - 4 \times (-1) = 1 + 4 = 5 > 0$.
Les racines de P sont donc les suivantes : $x_1 = \frac{1+\sqrt{5}}{2}$ et $x_2 = \frac{1-\sqrt{5}}{2}$.
On peut alors écrire $P = (X - x_1)(X - x_2) = (X - \frac{1-\sqrt{5}}{2})(X - \frac{1+\sqrt{5}}{2})$

Exercice 4
Factoriser le polynôme $P(X) = 2X^3 + 3X^2 - 3X - 2$ dans $\mathbb{R}$.

Exercice 5
Quelles sont les solutions réelles de l'équation $x^4 - x^2 - 2 = 0$?

– Inégalité de Cauchy-Schwarz –

Théorème 1.1.23.
Soient $a_1, a_2, ..., a_n \in \mathbb{R}$ et $b_1, b_2, ..., b_n \in \mathbb{R}$. Alors on a l'inégalité de Cauchy-Schwarz :

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right) \times \left(\sum_{i=1}^{n} b_i^2\right)$$

Cette inégalité est une égalité si et seulement si les vecteurs $(a_1, a_2, ..., a_n)$ et $(b_1, b_2, ..., b_n)$ sont colinéaires.

Démonstration. On pose P le polynôme suivant : $P(X) = \left(\sum\limits_{i=1}^{n} a_i^2\right) X^2 + 2\left(\sum\limits_{i=1}^{n} a_i b_i\right) X + \left(\sum\limits_{i=1}^{n} b_i^2\right)$.

Si $\sum\limits_{i=1}^{n} a_i^2 = 0$, alors pour tout i, $a_i = 0$ donc $\sum\limits_{i=1}^{n} a_i b_i = 0$, l'inégalité est alors vérifiée et c'est un des cas d'égalité.

On suppose alors qu'il existe un i tel que $a_i \neq 0$ de sorte que $\sum\limits_{i=1}^{n} a_i^2 \neq 0$.

On calcule le discriminant de P : $\Delta = 4\left(\sum\limits_{i=1}^{n} a_i b_i\right)^2 - 4\left(\sum\limits_{i=1}^{n} a_i^2\right) \times \left(\sum\limits_{i=1}^{n} b_i^2\right)$

Ainsi, l'inégalité de Cauchy-Schwarz est vérifiée si et seulement si $\Delta \leq 0$ ie P est du signe de $\left(\sum\limits_{i=1}^{n} a_i^2\right)$ c'est-à dire positif.

Or on remarque que $P(X) = \sum\limits_{i=1}^{n} a_i^2 X^2 + 2a_i b_i X + b_i^2 = \sum\limits_{i=1}^{n} (a_i X + b_i)^2 \geq 0$.

Donc l'inégalité de Cauchy-Schwarz est bien vérifiée.

On a égalité si et seulement si les a_i sont tous nuls (voir ci-dessus) ou $\Delta = 0$ ie il existe $\lambda \in \mathbb{R}$ tel que $P(\lambda) = \sum\limits_{i=1}^{n} (a_i \lambda + b_i)^2 = 0$ ce qui est équivalent à :
pour tout $i \in [\![1; n]\!]$, $a_i \lambda + b_i = 0 \Leftrightarrow b_i = -\lambda a_i$ □

Exercice 6
Soient $a, b, c, d \in \mathbb{R}$ tels que $a + 3b + 5c + 7d = 14$. Trouver la valeur minimale possible de $a^2 + b^2 + c^2 + d^2$.

Exercice 7
Montrer que pour tout $x_1, ..., x_n > 0$ on a : $(x_1 + x_2 + ... + x_n)\left(\frac{1}{x_1} + \frac{1}{x_2} + ... + \frac{1}{x_n}\right) \geq n^2$.

– Inégalité entre la moyenne arithmétique et la moyenne géométrique –

Théorème 1.1.24 (IAG)**.**
Soient $x_1, x_2, ..., x_n \geq 0$. Alors on a :

$$\frac{x_1 + x_2 + ... + x_n}{n} \geq \sqrt[n]{x_1 x_2 ... x_n}$$

avec égalité si et seulement si $x_1 = x_2 = ... = x_n$.

Démonstration. Soit $m_a = \frac{x_1+x_2+\ldots+x_n}{n}$

On va modifier les termes x_i de façon à ce que le membre de gauche reste inchangé et le membre de droite soit strictement plus grand.

Tout d'abord, on constate que si les x_i sont tous égaux, alors les deux membres sont égaux donc l'inégalité est bien vérifiée.

Sinon, il existe i, j tels que $x_i < m_a < x_j$.

On pose alors $\widetilde{x_i} = m_a$ et $\widetilde{x_j} = x_i + x_j - m_a$. Ainsi $\frac{x_1+\widetilde{x_i}+\widetilde{x_j}+\ldots+x_n}{n} = \frac{x_1+m_a+x_i+x_j-m_a+\ldots+x_n}{n} = \frac{x_1+x_i+x_j+\ldots+x_n}{n} = m_a$.

De plus, $\widetilde{x_i}\widetilde{x_j} = m_a(x_i+x_j-m_a) = m_a x_i + m_a x_j - {m_a}^2 + x_i x_j - x_i x_j = x_i x_j + (m_a - x_i)(x_j - m_a)$.

Donc $\widetilde{x_i}\widetilde{x_j} > x_i x_j$.

Ainsi cette opération fait augmenter la moyenne géométrique et remplace un des termes par la moyenne arithmétique qui reste inchangée. Cet algorithme finit donc et lorsqu'il s'arrête, tous les x_k sont égaux, l'inégalité est alors vérifiée lors de l'arrêt avec l'égalité des deux termes et elle est stricte avant l'arrêt. □

Exercice 8

Soient $a, b, c \in \mathbb{R}_+^*$. Prouver que :

$$\frac{abc(a+b+c+\sqrt{a^2+b^2+c^2})}{(a^2+b^2+c^2)(ab+bc+ac)} \leq \frac{3+\sqrt{3}}{9}$$

Exercice 9 (Inégalité de Nesbitt)

Soient $a, b, c > 0$. Montrer que $\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{b+a} \geq \frac{3}{2}$.

Exercice 10 (IMO 2001)
Soient $a, b, c > 0$. Montrer que $\frac{a}{\sqrt{a^2+8bc}} + \frac{b}{\sqrt{b^2+8ac}} + \frac{c}{\sqrt{c^2+8ab}} \geq 1$

– Solutions des exercices –

Solution de l'exercice 1
Par l'absurde, on suppose que $\sqrt{2} = \frac{p}{q}$ avec $p \wedge q = 1$.
Alors $2q^2 = p^2$ d'où p^2 est pair donc p est pair. On pose donc $p = 2p'$.
Alors $2q^2 = 4p'^2$ donc $q^2 = 2p'^2$ donc q est pair ce qui contredit l'hypothèse $p \wedge q = 1$.
Donc $\sqrt{2}$ est irrationnel.

Solution de l'exercice 2
Pour $x = 1$, $\sum\limits_{k=0}^{n} x^k = \sum\limits_{k=0}^{n} 1 = n + 1$

Pour $x \neq 1$, utiliser la Remarque 8 : $\sum\limits_{k=0}^{n} x^k = \frac{x^{n+1}-1}{x-1}$

Solution de l'exercice 3
$\frac{x}{x^4+y^2} + \frac{y}{x^2+y^4} \leqslant \frac{x}{2\sqrt{x^4y^2}} + \frac{y}{2\sqrt{x^2y^4}} \leqslant \frac{x}{2x^2y} + \frac{y}{2xy^2} = \frac{1}{xy}$

Solution de l'exercice 4
Ici pour se ramener au cas qu'on connaît bien (polynôme de degré 2), on essaie de trouver une "racine évidente". On calcule alors rapidement $P(1)$, $P(-1)$ pour voir si le polynôme P s'annule en ± 1 (mais on essaie rarement plus de valeurs à la main...)

Dans ce cas, on remarque que $P(1) = 0$, on peut alors réécrire P : $P(X) = (X-1)Q(X)$ avec $Q(X) = 2X^2 + 5X + 2$.
On calcule alors le discriminant : $\Delta = 5^2 - 4 \times 2 \times 2 = 25 - 16 = 9 > 0$.
Les racines de Q sont alors $x_1 = \frac{-5+3}{4} = \frac{-1}{2}$ et $x_2 = \frac{-5-3}{4} = -2$.
On peut donc écrire $P = 2(X-1)(X+2)\left(X + \frac{1}{2}\right)$.

Solution de l'exercice 5
On fait un changement de variable $y = x^2$ pour se ramener à un polynôme de degré 2.
On cherche alors les solutions de l'équation $y^2 - y - 2 = 0$.
$\Delta = (-1)^2 - 4 \times (-2) = 1 + 8 = 9 > 0$
D'où $y_1 = \frac{1-3}{2} = -1$ et $y_2 = \frac{1+3}{2} = 2$
Toutefois, il ne faut pas oublier de se ramener à la variable initiale x.
Comme $y_1 < 0$, il n'existe pas de $x \in \mathbb{R}$ tel que $x^2 = y_1$. On cherche alors les $x \in \mathbb{R}$ tels que $x^2 = y_2 = 2$ ce qui nous donne deux solutions réelles $x_1 = \sqrt{2}$ et $x_2 = -\sqrt{2}$.
Ces deux solutions vérifient l'équation initiale.

Solution de l'exercice 6
D'après l'inégalité de Cauchy-Schwarz, on a :

$$(a + 3b + 5c + 7d)^2 \leq (a^2 + b^2 + c^2 + d^2) \times (1^2 + 3^2 + 5^2 + 7^2)$$

d'où : $(a^2 + b^2 + c^2 + d^2) \geq \frac{14^2}{1^2+3^2+5^2+7^2} = \frac{7}{3}$
On a égalité si $b = 3a$, $c = 5a$ et $d = 7a$ ie si $a = \frac{1}{6}$, $b = \frac{1}{2}$, $c = \frac{5}{6}$ et $d = \frac{7}{6}$.
Ainsi la valeur minimale de l'expression $(a^2 + b^2 + c^2 + d^2)$ est $\frac{7}{3}$.

Solution de l'exercice 7

D'après l'inégalité de Cauchy-Schwarz,

$$(x_1+x_2+\ldots+x_n)\left(\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}\right)\geq\left(\sum_{i=1}^{n}\sqrt{x_i}\times\frac{1}{\sqrt{x_i}}\right)^2=n^2$$

Solution de l'exercice 8

D'après l'inégalité de Cauchy-Schwarz, $a+b+c\leq\sqrt{3}\sqrt{a^2+b^2+c^2}$. D'après l'IAG, $ab+bc+ca\geq 3\sqrt[3]{a^2b^2c^2}=3(abc)^{\frac{2}{3}}$ et $\sqrt{a^2+b^2+c^2}\geq\sqrt{3}(abc)^{\frac{1}{3}}$. Ainsi :

$$\begin{aligned}\frac{abc((a+b+c+\sqrt{a^2+b^2+c^2})}{(a^2+b^2+c^2)(ab+bc+ac)} &\leq \frac{abc(1+\sqrt{3})\sqrt{a^2+b^2+c^2})}{3(a^2+b^2+c^2)(abc)^{\frac{2}{3}}}\\ &= \frac{abc^{\frac{1}{3}}(1+\sqrt{3})}{3\sqrt{a^2+b^2+c^2}}\\ &\leq \frac{1+\sqrt{3}}{3}\times\frac{abc^{\frac{1}{3}}}{\sqrt{3}abc^{\frac{1}{3}}}\\ &= \frac{3+\sqrt{3}}{9}\end{aligned}$$

Solution de l'exercice 9

D'après l'inégalité de CS :

$\left(\frac{a}{b+c}+\frac{b}{a+c}+\frac{c}{b+a}\right)\times(a(b+c)+b(a+c)+c(a+b))\geq(a+b+c)^2$.

Il suffit alors de montrer que $(a+b+c)^2\geq\frac{3}{2}(a(b+c)+b(a+c)+c(a+b))$

$\Leftrightarrow a^2+b^2+c^2+2(ab+bc+ca)\geq 3(ab+bc+ca)$

$\Leftrightarrow a^2+b^2+c^2\geq ab+bc+ca$.

Or d'après l'IAG : $a^2+b^2+c^2=\left(\frac{a^2+b^2}{2}+\frac{c^2+b^2}{2}+\frac{a^2+c^2}{2}\right)\geq ab+cb+ac$.

D'où l'inégalité de Nesbitt.

Solution de l'exercice 10

On pose $A=\frac{a}{\sqrt{a^2+8bc}}+\frac{b}{\sqrt{b^2+8ac}}+\frac{c}{\sqrt{c^2+8ab}}$

$B=a\sqrt{a^2+8bc}+b\sqrt{b^2+8ac}+c\sqrt{c^2+8ab}$

D'après l'inégalité de Cauchy-Schwarz, $A\times B\geq(a+b+c)^2$.

Il suffit donc de montrer que $(a+b+c)^2\geq B$.

D'après CS, $B^2\leq(a+b+c)\times(a(a^2+8bc)+b(b^2+8ac)+c(c^2+8ab))$.

Il suffit donc de montrer que $(a+b+c)^3\geq(a(a^2+8bc)+b(b^2+8ac)+c(c^2+8ab))$

$\Leftrightarrow a^3+b^3+c^3+3(a^2b+a^2c+b^2c+b^2a+c^2a+c^2b)+6abc\geq a^3+8abc+b^3+8abc+c^3+8abc$

$\Leftrightarrow 3(a^2b+a^2c+b^2c+b^2a+c^2a+c^2b)\geq 18abc$

Or d'après l'IAG, $a^2b+a^2c+b^2c+b^2a+c^2a+c^2b\geq 6\sqrt[6]{a^6b^6c^6}=6abc$.

Donc l'inégalité est bien vérifiée.

2 Fonctions et équations fonctionnelles

Une équation fonctionnelle est un équation dont l'inconnue est une fonction. Pour la résoudre, il faut trouver toutes les images des éléments de l'ensemble de départ. Nous allons illustrer cela grâce à un exemple :

Exercice 1

Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$f(x+y) = f(x) - f(y).$$

Solution de l'exercice 1
On va faie une substitution. Cela consiste à remarquer que si l'équation fonctionnelle est vraie pour tout x, elle l'est aussi pour $x = 0$. On substitue alors 0 à x et 0 à y. On obtient alors

$$f(0+0) = f(0) + f(0)$$

d'où $f(0) = 0$. En subsituant seulement 0 à x dans notre équation de départ, on obtient

$$f(y) = -f(y)$$

d'où f(y) = 0. On a déterminé la seule fonction qui peut être solution de notre équation fonctionnelle, il faut vérifier qu'elle est bien une solution valide : on remplace dans l'équation de départ f par la fonction à vérifier : $0 = 0 + 0$ donc la seule solution de cette équation fonctionnelle est $f(x) = x$.

Exercice 2
Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$f(x - f(y)) = 1 - x - y.$$

Solution de l'exercice 2
En substituant 0 à y on obtient

$$f(x - f(0)) = 1 - x - f(0)$$

.En posant $y = x - f(0)$, l'équation devient :

$$f(z) = 1 - z - 2f(0)$$

Les solutions de l'équation sont donc de la forme f(z) = $-z + a$ avec $a = 1 - 2f(0)$. On cherche donc les fonctions de la forme $f(x) = -x + a$ qui soient solutions de l'équation fonctionnelle. En l'insérant dans l'équation fonctionnelle de départ, on a alors :

$$f(x - (-y + a)) = 1 - x - y$$

$$-(x - (-y + a)) + a) = 1 - x - y$$

d'où $a = -\frac{1}{2}$. L'unique solution de l'équation fonctionnelle est donc $f(x) = -x + \frac{1}{2}$

Exercice 3
Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$f(x^2 - y^2) = (x - y)(f(x) + f(y)).$$

Solution de l'exercice 3
En posant $x = 0, y = 0$, On a $f(0) = 0$, Pour $y = -x$,il vient $f(0) = 2x(f(x) + f(-x))$ d'où f(x) = 0 pour tout $x \neq 0$. En substituant $-y$ à y, l'équation devient

$$f(x^2 - (-y)^2) = (x + y)(f(x) + f(-y))$$

$$f(x^2 - y^2) = (x + y)(f(x) - f(y))$$

Combinons cettte équations avec l'équation fonctionnelle initiale :

$$(x - y)(f(x) + f(y)) = (x + y)(f(x) - f(y))$$

$$xf(y) = yf(x)$$

et en prenant $y = 1$, on obtient $f(x) = xf(1)$, On cherche donc les solutions de la fomre $f(x) = ax$:

$$a(x^2 - y^2) = (x - y)(ax + ay)$$

donc $f(x) = ax$ est solution pour tout a.

Exercice 4
Déterminer les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que :

$$f(f(x)) = x + 1.$$

Solution de l'exercice 4
L'astuce est la suivante : calculer $f(f(f(x)))$ de deux manières distinctes.

Déjà, il est clair que

$$f(f(f(x))) = f(x + 1).$$

En effet, il suffit juste d'appliquer f de chaque côté de l'équation initiale.

D'autre part, on peut écrire, pour $y = f(x)$,

$$f(f(y)) = f(y) + 1 \implies f(f(f(x))) = f(x) + 1$$

Cette astuce n'est pas facile à visualiser mais est très utile et doit être maîtrisée. D'après les deux résultats suivants, on obtient :

$$f(x + 1) = f(x) + 1.$$

Par une récurrence immédiate, si on pose $f(0) = c$, on obtient $f(x) = x + c$. Mais de nouveau, il ne faut pas crier victoire ! En effet, si l'on remplace cela dans l'équation initiale, on obtient

$$x + 2c = x + 1 \implies f(0) = c = \frac{1}{2}.$$

Ceci est impossible, puisque f est à valeurs dans $\mathbb{N}$, donc il n'y a pas de solutions.

On dit d'une fonction $f : A \to B$ qu'elle est surjective si pour tous les éléments b dans B, il existe a dans A tel que $f(a) = b$. Autrement dit, on exige ici que tous les éléments de l'ensemble d'arrivée soient l'image d'un élément de l'ensemble de départ. Par exemple, la fonction

$$f : \mathbb{R} \to \mathbb{R}$$
$$f : x \to x^2 + 1$$

n'est pas surjective car il n'existe pas de réel x tel que $f(x) = -1$.

On dit qu'une fonction $f : A \to B$ est injective si pour toute paire a_1 et a_2 dans A si $a_1 \neq a_2$ alors $f(a_1) \neq f(a_2)$

On dit qu'une fonction est bijective si elle est injective et surjective.

Exercice 5
Pour chacune des équations fonctionnelles suivantes, dire si les solutions seront surjectives, injectives ou bijectives :

1. $f((f(x) - 1) = x + 1$
2. $f(2x + f(3y)) = f(x) + y^5$
3. $f(f(x) - f(y))) = xf(x - y)$
4. $f(f(x) + f(y)) - f(f(x) - f(y)) = 2x + 3y$

Solution de l'exercice 5

1. La première fonction est bijective, en effet soit b appartenant à $\mathbb{R}$ en prenant $x = b - 1$ on a $f(f(b-1) - 1) = b$, donc b a un antécédent donc f est surjective. Prenons a et b tel que que $f(a) = f(b)$, on a donc $a + 1 = f(f(a) - 1) = f(f(b) - 1) = b + 1$ donc $a = b$ donc f est injective.
2. Soient a et b tel que $f(a) = f(b)$ En prenant $y = a/3, x = 0$ on a
$$f(0) + (a/3)^5 = f(0 + f(a)) = f(0 + f(b)) = f(0) + (b/3)^5$$
d'où a=b donc f est injective.Soit b un réel, en prenant $x = 0$, $y = \sqrt[5]{b - f(0)}$, on a $f(f(3y)) = f(0) + y^5 - f(0) = y^5 = b$ donc b a un antécédent, f est donc surjective
3. On remarque que la fonction $f(x) = 0$ est solution, cette fonction n'est ni surjective ni injective.
4. Soient a et b tels que $f(a) = f(b)$ en remplacant x par a et y par 0, on a
$$2a = f(f(a) + f(0)) - f(f(a) - f(0)) = f(f(b) + f(0)) - f(f(b) - f(0) = 2b$$
donc $a = b$ donc f est injective. Soit b un réel en prenant $x = y = \dfrac{b - f(0)}{5}$, on obtient
$$f(2f(x)) - f(0) = 5\frac{b - f(0)}{5}$$
donc $f(2f(x)) = b$.

   b a un antécédent, ce qui prouve que f est surjective. f est donc bijective

Exercice 6
Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que :

$$f(f(x+1)+y-1) = f(x)+y.$$

Solution de l'exercice 6
$x = 0 donne f(f(1)+y-1) = f(0)+y$, soit b un réel, en prenant $y = b - f(0)$, on obtient $f(f(0)+y-1) = b$ donc f est surjective. Soit t un antécédent de 1,

$$f(1+y-1) = f(t)+y$$

donc f est de la forme $f(y) = y+c$. En injectant cette fonction dans l'équation de départ, on trouve $c = 0$ donc les solutions sont $f(x) = x$.

Exercice 7
Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que :

$$f(f(f(x))) + f(f(y)) = f(y) + x.$$

Solution de l'exercice 7
On remarque tout d'abord qu'en prenant $y = 0$, on obtient :

$$f(f(f(x))) = x - f(0) - f(f(0))$$

donc f est surjective. Soient a et b tel que $f(a) = f(b)$, en remplaçant x par a, on a

$$f(y) + a = f(f(f(a))) + f(f(y)) = f(f(f(b))) + f(f(y)) = f(y) + b$$

donc $a = b$ donc f est injective. f est surjective donc on peut remplacer $f(y)$ par t qui peut prendre n'importe quelle valeur dans $\mathbb{R}$. En posant $x = 0$, on a alors :

$$f(f(f(0))) + f(t) = t$$

donc f est de la forme $f(x) = x - a$, en injectant dans l'équation initiale, on trouve que la seule solution est $f(x) = x$

Exercice 8
Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que :

$$f(f(x)f(y)) = f(x)y.$$

Solution de l'exercice 8
On vérifie que $f(x) = 0$ est solution de l'équation fonctionnelle. On suppose maintenant qu'il existe un réel a tel que $f(a) \neq 0$. Soit b un réel, en posant $x = 0$ et $y = \frac{b}{f(a)}$, on a alors :

$$f(f(a)f(\frac{b}{f(a)}) = b$$

donc f est surjective. on peut donc remplacer $f(x)$ par t, soit k l'antécédent de 1, on a alors $f(t) = tk$, il suffit alors de tester toutes les fonctions de la forme $f(x) = kx$, et il en découle que la seule solution est $f(x) = x$.

– Équation de Cauchy –

Cette partie n'a pas été abordée en cours, et j'invite toute personne intéressée à se référer au cours proposé au groupe C à ce sujet, en page 175.

2 Arithmétique

1 Théorèmes de Bézout et de Gauss

On pourra se reporter directement au cours d'arithmétique donné au groupe A, et dont les notes figurent en page 38.

2 Propriétés de la suite de Fibonacci

– Exercices –

Exercice 1
Montrer que, si $x + \frac{1}{x} \in \mathbb{Z}$, alors $x^n + \frac{1}{x^n} \in \mathbb{Z}$ pour tout entier $n \in \mathbb{N}$.

Définition 2.2.1.
On définit la suite de Fibonacci de la manière suivante : $F_0 = 0$, $F_1 = 1$ et ensuite $F_n = F_{n-1} + F_{n-2}$ pour tout $n \geqslant 2$.

Exercice 2
Calculer les premières valeurs de la suite.

Exercice 3
Trouver tout les quadruplets d'entiers $(a, b, c, d) \in \mathbb{N}_{\geqslant 2}$ tel que $F_a + F_b = F_c + F_d$.

Exercice 4
Démontrer que $F_n^2 = F_{n-1}F_{n+1} - (-1)^n$.

Exercice 5
Montrer que : $F_{2n+1} = F_{n+1}^2 + F_n^2$.

Exercice 6
Soit u_n la suite définie par $u_1 = 4$, $u_2 = 9$ et ensuite $u_n = 3u_{n-1} - u_{n-2} - 2 \cdot (-1)^n$. Trouver u_n.

Exercice 7
Montrer que :

$$\sum_{i=0}^{n} F_k^2 = F_n F_{n+1}$$

Exercice 8
Trouver la limite de la suite suivante :

$$u_n = \sum_{i=1}^{n} \frac{1}{F_i F_{i+2}}.$$

Exercice 9
Montrer que :

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

Exercice 10
Montrer l'inégalité suivante :

$$\sum_{i=0}^{n} \frac{F_i}{2^i} < 2$$

Exercice 11
Montrer que il n'existe pas deux entiers consécutifs pairs dans la suite de Fibonacci.

Exercice 12
Montrer que $F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$.

Exercice 13
En déduire que $\text{PGCD}(F_m, F_n) = F_{\text{PGCD}(m,n)}$.

Exercice 14
Démontrer qu'il existe une infinité d'entiers k tel que $F_k + 5$ soit divisible par 2017.

Exercice 15
Démontrer la formule de Binet :

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{\sqrt{5}+1}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Remarque 2.2.2.
Le moyen d'obtenir cette formule est une théorie plus large sur les suite définies par k premier termes et chaque terme est ensuite déterminé par combinaison linéaire des k termes précédents. Ces suites sont appelés suites récurrentes linéaires.

– Solutions –

Solution n°1 de l'exercice 1
Nous allons procéder par récurrence forte sur n.

Initialisation : On remarque que $x^0 + \frac{1}{x^0} = 2 \in \mathbb{Z}$, et l'on sait que $x + \frac{1}{x} \in \mathbb{Z}$.

Hérédité : On suppose que P_k est vraie jusqu'au rang $n-1$. P_n est-elle aussi vraie ?

$$\begin{aligned}\left(x+\frac{1}{x}\right)^n &= \sum_{i=0}^{n}\binom{n}{i}x^{n-i}\frac{1}{x^i} = x^n+\frac{1}{x^n}+\sum_{i=0}^{n}\binom{n}{i}x^{n-2i}\\ &= x^n+\frac{1}{x^n}+\underbrace{\sum_{i=0}^{\left\lfloor\frac{n-1}{2}\right\rfloor}\binom{n}{i}\left(x^{n-2i}+\frac{1}{x^{n-2i}}\right)}_{\text{Entier d'après HR (forte!!)}}+\underbrace{\binom{n}{n/2}\cdot 1}_{\text{si } n \text{ est pair}}\end{aligned}$$

et $\left(x+\frac{1}{x}\right)^n \in \mathbb{Z}$. Donc $x^n+\frac{1}{x^n}$ est bien un entier (comme soustraction de deux entiers).

Conclusion : P_0 et P_1 sont vraies (P_0 est implicitement utilisée) et P_n est héréditaire, donc P_n est vraie pour tout n entier.

Solution n°2 de l'exercice 1

On va démontrer P_n : « $x+\frac{1}{x} \in \mathbb{Z}$ » par récurrence forte ; une double initialisation sera nécessaire.

Initialisation : Pour $n = 0$, on a $x^0+\frac{1}{x^0} = 2 \in \mathbb{Z}$, donc P_0 est vraie ; pour $n = 1$, on a $x+\frac{1}{x} \in \mathbb{Z}$ d'après l'énoncé, donc P_1 est vraie également.

Hérédité : On suppose P_n et P_{n-1} vraies. P_{n+1} est-elle aussi vraie ?

On a $\left(x^n+\frac{1}{x^n}\right)\left(x+\frac{1}{x}\right) = x^{n+1}+\frac{1}{x^{n+1}}+x^{n-1}+\frac{1}{x^{n-1}}$. Par conséquent, $x^{n+1}+\frac{1}{x^{n+1}} = \left(x^n+\frac{1}{x^n}\right)\left(x+\frac{1}{x}\right)-x^{n-1}-\frac{1}{x^{n-1}}$ est entier d'après P_1, P_{n-1} et P_n. Donc P_{n+1} est vraie également.

Ainsi, la propriété P_n est héréditaire.

Conclusion : Puisque P_0 et P_1 sont vraies et que P_n est héréditaire d'ordre 2 (c'est pourquoi il faut P_0 et P_1), la propriété P_n est vraie pour tout n entier.

Solution de l'exercice 2

Les premières valeurs de la suite de Fibonacci sont : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, ...

Solution de l'exercice 3

On peut supposer sans perte de généralité que $a \geqslant b, c, d \geqslant 2$ ainsi que $c \geqslant d$, alors soit $a = c$ ce qui donne $b = d$.

Soit $a \geqslant c+2$, alors $F_b+F_a > F_a = F_{a-1}+F_{a-2} > F_c+F_d$.

Il reste le cas où $c = a-1$, alors si $d \geqslant a-2$ on a $F_a+F_b > F_a = F_{a-1}+F_{a-2} = F_c+F_{a-2} \geqslant F_c+F_d$ ce qui est une contradiction avec la relation que l'on veut. Donc $d = a-1$, alors $F_b = -F_a+2F_{a-1} = F_{a-1}-F_{a-2} = F_{a-3}$.

On obtient donc les solutions suivantes : (a, b, a, b), (a, b, b, a), $(a, a-3, a-1, a-1)$, $(a-3, a, a-1, a-1)$, $(a-1, a-1, a, a-3)$ et $(a-1, a-1, a-3, a)$.

Solution de l'exercice 4

On va démontrer la propriété P_n par récurrence.

Initialisation : $n = 1$, $F_1^2 = 1 = 0\cdot 1+1 = F_0F_2-(-1)^1$.

Hérédité : On suppose que la propriété est vraie au rang n. Est-elle vraie au rang $n+1$? Ici, oui, car

$$F_nF_{n+2} = F_{n^2} + F_nF_{n+1} = F_{n-1}F_{n+1} - (-1)^n + F_nF_{n+1} = F_{n+1}^2 + (-1)^{n+1},$$

ce qui conclut l'hérédité.

Conclusion : P_0 est vraie et P_n est héréditaire donc P_n est vraie pour tout n.

Solution de l'exercice 5
Cet exercice est un cas particulier de l'exercice 12 avec $n = m + 1$.

Solution de l'exercice 6
En calculant les premiers termes de la suite on trouve $4, 9, 25, 64, \ldots$ On reconnait les carrés des premiers termes de la suite de Fibonacci. On va démontrer que $u_n = F_{n+2}^2$. Cette relation est bonne pour les premiers termes.

$3F_{n-1}^2 - F_{n-2}^2 - 2(-1)^n = 2(F_{n-1}^2 + (-1)^{n+1}) + F_{n-1}^2 - F_{n-2}^2 = 2F_nF_{n-2} + F_{n-1}^2 - F_{n-2}^2$ où le dernière ligne est issue de l'exercice 4. $2F_nF_{n-2} + F_{n-1}^2 - F_{n-2}^2 = -F_n^2 + 2F_nF_{n-2} - F_{n-2}^2 + F_{n-1}^2 + F_n^2 = -(F_n - F_{n-2})^2 + F_{n-1}^2 + F_n^2 = F_n^2$ donc F_{n+2} vérifie bien la bonne récurrence, ce qui conclut.

Solution de l'exercice 7
On va démontrer la propriété P_n par récurrence.

Initialisation : Pour $n = 0$, on a $\sum_{i=0}^{0} F_i^2 = 0 = 0 \cdot 1$.

Hérédité : On suppose P_k vraie jusqu'à n. P_{n+1} est-elle aussi vraie ? Oui, car

$$\sum_{i=0}^{n+1} F_i^2 = \sum_{i=0}^{n} F_i^2 + F_{n+1}^2 = F_nF_{n+1} + F_{n+1}^2 = F_{n+1}F_{n+2}.$$

Conclusion : P_0 est vraie et P_n est héréditaire, donc P_n est vraie pour tout n.

Solution de l'exercice 8
On trouve que $\dfrac{1}{F_kF_{k+2}} = \dfrac{1}{F_kF_{k+1}} - \dfrac{1}{F_{k+1}F_{k+2}}$. Donc

$$u_n = \sum_{i=0}^{n} \frac{1}{F_iF_{i+2}} = \sum_{i=0}^{n} \left(\frac{1}{F_iF_{i+1}} - \frac{1}{F_{i+1}F_{i+2}} \right) = 1 - \frac{1}{F_{n+1}F_{n+2}}$$

par somme télescopique.

Or F_k tend vers l'infini donc la limite de u_n est 1.

Solution de l'exercice 9
On change un peu l'énoncé pour avoir :

$$F_n = \sum_{k=p}^{2p} \binom{p}{k} F_{n-k}.$$

On va démontrer la propriété par récurrence sur p.

Initialisation : Pour $p = 0$, $F_n = \binom{0}{0} F_n$, donc le rang $p = 0$ est vrai.

Hérédité : On suppose la propriété vraie au rang n et on veut la démontrer au rang $n+1$. On a

$$\begin{aligned} F_n &= \sum_{k=p}^{2p} \binom{p}{k} F_{n-k} = \sum_{k=p}^{2p} \binom{p}{k} (F_{n-k-1} + F_{n-k-2}) \\ &= \sum_{k=p+1}^{2p+2} \left(\binom{p}{k-1} + \binom{p}{k} \right) F_{n-k} = \sum_{k=p+1}^{2p+2} \binom{p+1}{k} F_{n-k}. \end{aligned}$$

Ceci conclut l'hérédité.

Conclusion : La propriété est vraie pour $p=0$ et elle est héréditaire donc la propriété est vraie pour tout entier p.

Solution de l'exercice 10

Si l'on note $S_n = \sum_{i=0}^{n} \frac{F_i}{2^i}$, alors on a :

$$\begin{aligned} S_n &= F_0 + \frac{F_1}{2} + \frac{F_2}{4} + \frac{F_3}{8} + \ldots + \frac{F_n}{2^n} \\ \frac{S_n}{2} &= 0 + \frac{F_0}{2} + \frac{F_1}{4} + \frac{F_2}{8} + \ldots + \frac{F_{n-1}}{2^n} + \frac{F_n}{2^{n+1}} \\ \frac{S_n}{4} &= 0 + 0 + \frac{F_0}{4} + \frac{F_1}{8} + \ldots + \frac{F_{n-2}}{2^n} + \frac{F_{n-1}}{2^{n-1}} + \frac{F_n}{2^{n+2}}. \end{aligned}$$

On en déduit que

$$\frac{S_n}{4} = S_n - \frac{S_n}{2} - \frac{S_n}{4} = \frac{F_1}{2} - \frac{F_n}{2^{n+1}} - \frac{F_{n-1}}{2^{n-1}} - \frac{F_n}{2^{n+2}} < \frac{F_1}{2} = \frac{1}{2},$$

ce qui signifie que $S_n < 2$.

Solution de l'exercice 11

On regarde la suite modulo 2, si il y a deux nombres consécutifs pairs pour la première fois, alors ils valent 0, mais alors le nombre précédent était aussi 0 (grâce à la définition de la suite de Fibonacci), ce qui invalide le fait que l'on ai pris la première paire de tel nombres. Il suffit maintenant de vérifier que la première paire n'est pas composée de deux nombres pairs, mais il s'agit de 0 et 1, cela conclut.

Solution de l'exercice 12

On va faire une récurrence d'ordre 2 sur n pour démontrer la propriété P_n.

Initialisation : Pour $n=1$, $F_{m+1} = F_m \cdot 0 + F_{m+1} \cdot 1 = F_m F_0 + F_{m+1} F_1$. Donc P_1 est juste. De même, pour $n=2$, $F_{m+2} = F_m \cdot 1 + F_{m+1} \cdot 1 = F_m F_1 + F_{m+1} F_2$, donc P_2 est également vraie.

Hérédité :Supposons que P_{n-2} et P_{n-1} soient vraies ; P_n est-elle également vraie ? Oui, car

$$\begin{aligned} F_{m+n} &= F_{m+n-1} + F_{m+n-2} = F_m F_{n-2} + F_{m+1} F_{n-1} + F_m F_{n-3} + F_{m+1} F_{n-2} \\ &= F_m (F_{n-2} + F_{n-3}) + F_{m+1} (F_{n-1} + F_{n-2}) = F_m F_{n-1} + F_{m+1} F_{F_n}, \end{aligned}$$

ce qui conclut l'hérédité.

Conclusion : P_1 et P_2 sont vraie et P_n est héréditaire d'ordre 2, donc P_n est vraie pour tout n.

Solution de l'exercice 13
On va appliquer l'algorithme d'Euclide aux dénominateurs.

$$\mathrm{PGCD}(F_{m+n}, F_n) = \mathrm{PGCD}(F_m F_{n-1} + F_{m+1} F_n, F_n) = \mathrm{PGCD}(F_m F_{n-1}, F_n) = \mathrm{PGCD}(F_m, F_n)$$

car F_{n-1} et F_n sont premiers entre eux. On peut donc appliquer l'algorithme du PGCD au indices, ce qui conclut.

Solution de l'exercice 14
On remarque tout d'abord que la suite F_n est péridique modulo 2017. En effet, le nombre de valeurs prises modulo 2017 est fini, donc on retombe sur deux valeurs consécutives déjà vu à un moment et alors on cycle, en prenant la suite dans l'autre sens la suite est périodique. On peut maintenant regarder la suite de Fibonacci dans l'autre sens. On a $F_{-1} = -1$, $F_{-2} = 1$, $F_{-3} = -2$, $F_{-4} = 3$, $F_{-5} = -5$, donc à un moment la suite de Fibonacci vaut -5 modulo 2017. Un tel entier k existe donc bien.

Solution de l'exercice 15
On va démontrer que la formule

$$\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

est bonne pour les deux premiers termes puis qu'elle vérifie bien la relation de récurrence de la suite de Fibonacci.

Initialisation : Pour $n = 0$,

$$F_0 = 0 = \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{5}} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^0 - \left(\frac{1-\sqrt{5}}{2}\right)^0\right)$$

et, pour $n = 1$,

$$F_1 = 1 = \frac{2\sqrt{5}}{2\sqrt{5}} = \frac{1-1+2\sqrt{5}}{2\sqrt{5}} = \frac{1+\sqrt{5}}{2\sqrt{5}} - \frac{1-\sqrt{5}}{2\sqrt{5}} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right).$$

L'initialisation est donc complète.

Hérédité : On remarque que $\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$ sont les racines de $x^2 - x - 1 = 0$. Donc $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}$ et $\frac{-1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n = \frac{-1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-1} + \frac{-1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}$. En sommant les deux dernières équations ont a clairement que la formule vérifie la relation de récurrence de la suite de Fibonacci.

Conclusion : La propriété est vraie au rang $n = 0$ et $n = 1$ et est héréditaire d'ordre 2, ce qui montre bien la formule de Binet.

3 Nombres premiers et congruences

Ce cours est directement issu de la partie du cours d'arithmétique pour débutants, disponible sur le site de la POFM, qui traite des congruences.

3 Combinatoire

1 Récurrence

Nous avons commencé par la présentation d'un nouveau principe de démonstration : le raisonnement par récurrence, dont voici la rédaction type.

On va montrer par récurrence sur n que la propriété : « [PROPRIÉTÉ À PROUVER] » est vraie pour tout entier $n \geqslant 0$.

1. *Initialisation* : Montrons que la propriété est vraie au rang 0. [DÉMONSTRATION] Ceci conclut l'initialisation.
2. *Hérédité* : Supposons la propriété vraie au rang k et montrons qu'elle est alors vraie au rang $k+1$. [DÉMONSTRATION] La propriété est donc héréditaire.
3. *Conclusion* : La propriété est vraie pour tout $n \geqslant 0$.

Il arrive parfois qu'on ait besoin de la propriété du rang k et $k-1$ pour prouver que la propriété est vraie au rang $k+1$, dans l'hérédité. Il faut alors légèrement modifier le raisonnement, en démontrant que la propriété est vraie au rang a et $a+1$ dans l'initialisation, puis en supposant la propriété vraie aux rangs $k-1$ et k dans l'hérédité.

De la même façon, on peut avoir besoin de la propriété au rang $\frac{k}{2}$ par exemple, ou encore de la propriété du rang a à k pour prouver qu'elle est vraie au rang $k+1$. Dans ce cas, l'initialisation ne change pas, mais il faut préciser qu'on suppose la propriété vraie pour tous les rangs inférieurs à k et supérieurs à a dans l'hérédité. Ce type de récurrence est une récurrence forte.

Nous avons ensuite démontré par récurrence l'existence et l'unicité de la division euclidienne :

On va montrer par récurrence sur n que la propriété $\mathcal{P}_n$: « pour tous $a \in \mathbb{Z}$ et tout $n \in \mathbb{N}$ tels que $a \neq 0$, il existe un unique couple d'entiers $q \in \mathbb{Z}$ et $r \in \{0, 1, \ldots, |a|-1\}$ tels que $n = aq + r$ » est vraie pour tout entier $n \geqslant 0$.

1. *Initialisation* : Montrons que la propriété $\mathcal{P}_0$ est vraie.

   Si $0 = aq + r$ et $\|a| \geqslant 1$, alors $aq = -r$, donc $1 > |r| = |-r| = |aq| \geqslant |q|$, ce qui montre que $q = 0$ puis que $r = n - aq = 0$. Réciproquement, le couple $(q, r) = (0, 0)$ convient manifestement, ce qui conclut l'initialisation.
2. *Hérédité* : Supposons la propriété $\mathcal{P}_i$ vraie pour tout entier i compris entre 0 et k, et montrons que $\mathcal{P}_{k+1}$ est vraie.

   On sait que le couple (q, r) est l'unique couple qui respecte $k = aq + r$ par hypothèse de récurrence. Alors, en posant $q' = q + 1$ si $a > 0$ et $q' = q - 1$ si $a < 0$, on remarque que $k + 1 = aq + (r + 1)$ si $r < |a| - 1$, et que $k + 1 = aq' + 0$ sinon. On dispose donc bien d'un couple (q', r') tel que $k + 1 = aq' + r'$.

   D'autre part, étant donné (q', r') et le signe de a, on peut retrouver le couple (q, r) dont on était parti. Puisque ce couple est unique, le couple (q', r') l'est aussi.

   La propriété est donc héréditaire.
3. *Conclusion* : La propriété $\mathcal{P}_n$ est donc vraie pour tout $n \geqslant 0$.

Le théorème est démontré pour $n \geqslant 0$, reste à la montrer pour les entiers négatifs : on sait que $n = aq + r$, donc $-n = a(-q) - r$.

Si $r = 0$, c'est bon, car $(q' = -q, r' = 0)$. Sinon, $-|q| < -r < 0$, donc $0 < r' = |q| - r < |q|$ et on peut écrire $-n = a(q \pm 1) + |q| - r$ en fonction du signe de q, et (q', r') marche. Comme le couple (q, r) était unique, le nouveau l'est aussi, ce qui conclut.

Enfin, nous avons démontré que pour tout nombre naturel $b \geqslant 2$, on pouvait écrire le nombre $n \geqslant 0$ de façon unique sous la forme

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b^1 + a_0 b^0$$

avec $0 \leqslant a_i < b$. C'est sa représentation en base b, aussi notée $\overline{a_k a_{k-1} \ldots a_1 a_0}_{(b)}$.

Par exemple, le nombre binaire (en base 2) $\overline{101010}_{(2)}$ s'écrit aussi $1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 \cdot 1 = 32 + 8 + 2 = 42$ en base 10.

– Exercices –

Exercice 1
Montrer que la somme des entiers de 1 à n est égale à $\frac{n(n+1)}{2}$

Exercice 2
Montrer qu'un graphe à n sommets dans lequel il existe un unique chemin pour aller d'un sommet à l'autre (un arbre), alors le nombre d'arêtes est de $n - 1$.

Exercice 3
Trouver les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que $f(n) + f(f(n)) = 2n$

Exercice 4
Montrer que si $N = \underbrace{111\ldots1}_{n}$ est premier, alors n est aussi premier.

Exercice 5
Peut-on trouver 2018 nombres naturels distincts tous plus petits que 150000, tels que trois ne forment jamais une suite arithmétique (c'est à dire qu'on ait jamais trois nombres a, b, c tels que $a + c = 2b$) ?

Exercice 6
Soit $f : \mathbb{N}^* \to \mathbb{N}^*$ une fonction qui respecte les conditions suivantes :

1. $f(1) = 1$
2. $f(2n) = f(n)$
3. $f(2n+1) = f(n) + 1$

Quelle est la plus grande valeur de $f(n)$ pour $1 \leqslant n \leqslant 2018$?

– Solutions –

Solution de l'exercice 1
On va montrer par récurrence sur n que la propriété $\mathcal{P}_n$: « $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ » est vraie pour tout entier $n \geqslant 1$.

1. *Initialisation* : Montrons que $\mathcal{P}_1$ est vraie.
   On peut vérifier directement que $1 = \frac{1\times 2}{2}$. Ceci conclut l'initialisation.
2. *Hérédité* : Supposons la propriété vraie au rang k et montrons qu'elle est alors vraie au rang $k+1$.
   Si $\mathcal{P}_k$ est vraie, alors $\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$. La propriété est donc héréditaire.
3. *Conclusion* : La propriété est vraie pour tout $n \geqslant 1$.

Solution de l'exercice 2
Soit $\mathcal{G}_n$ un graphe à n sommets respectant la condition de l'énoncé. On va montrer par récurrence sur n que la propriété $\mathcal{P}_n$: « La graphe $\mathcal{G}_n$ a $n-1$ arêtes » est vraie pour tout entier $n \geqslant 1$.

1. *Initialisation* : Montrons que $\mathcal{P}_1$ est vraie.
   Le graphe à un sommet respecte les conditions de l'énoncé et possède $1-1=0$ arête. Ceci conclut l'initialisation.
2. *Hérédité* : Supposons la propriété vraie au rang k et montrons qu'elle est alors vraie au rang $k+1$.
   On prend notre graphe $\mathcal{G}_{k+1}$. On va commencer par prouver qu'il existe un sommet de degré 1 : supposons que tous le sommets aient un degré supérieur ou égal à 2. Alors partons d'un sommet au hasard X_0. On peut aller vers un sommet X_1, puisque son degré est plus grand que 2, puis sur un sommet X_3, et ainsi de suite. On peut ainsi continuer jusqu'à ce qu'on retombe sur un sommet X_i qu'on avait déjà visité (car il n'y a qu'un nombre fini de sommet). Mais alors il existe un cycle formé des points $X_i, X_{i+1}, \ldots$, et pour aller de X_i à X_{i+1}, on peut emprunter l'arête directe ou le cycle, ce qui contredit l'énoncé.
   Il existe donc au moins un sommet avec une seule arête ou zéro. S'il en a 0, comme notre graphe comporte au moins deux sommets, il n'existe pas de moyen de passer du premier au second, donc cette situation n'est pas possible. Par conséquent, il existe un sommet A de degré 1.
   On retire ce sommet et son arête pour obtenir le graphe $\mathcal{G}_k$ à k sommets. Par hypothèse de récurrence il possède $k-1$ arêtes, donc $\mathcal{G}_{k+1}$ en possède bien k.
   Ceci montre que la propriété est héréditaire.
3. *Conclusion* : La propriété est vraie pour tout $n \geqslant 1$.

Solution de l'exercice 3
Remarquons que si $f(n) = f(n')$ alors $f(n)+f(f(n)) = f(n')+f(f(n'))$ donc $2n = 2n'$ et $n = n'$ donc la fonction est injective. En cherchant les premières valeurs de $f(n)$, on a l'intuition que f est l'identité, donc on va essayer de montrer cela par récurrence.

On va montrer par récurrence forte sur n que la propriété $\mathcal{P}_n$: « $f(n) = n$ » est vraie pour tout entier $n \geqslant 0$.

1. *Initialisation* : Montrons que $\mathcal{P}_0$ est vraie.

   Comme f associe à chaque entier naturel un entier naturel, on sait que $f(n) \geqslant 0$ pour tout $n \geqslant 0$. Or, on sait que $f(0) + f(f(0)) = 0$. Cela n'est donc possible que si $f(0) = 0$, ce qui conclut l'initialisation.

2. *Hérédité* : Supposons la propriété vraie aux rangs $0, 1, \ldots, k$ et montrons qu'elle est alors vraie au rang $k+1$.

   Par hypothèse de récurrence forte, on sait que $f(i) = i$ pour tout $i \leqslant k$. Puisque f est injective, on en déduit que $f(k+1) \geqslant k+1$, puis que $f(f(k+1)) \geqslant k+1$. Comme $f(k+1) + f(f(k+1)) = 2k+2$, cela montre que $f(k+1) = k+1$. La propriété est donc héréditaire.

3. *Conclusion* : La propriété est vraie pour tout $n \geqslant 0$.

Il ne reste plus qu'à vérifier que $f : n \to n$ est bien une solution de notre équation, ce qui est le cas.

Solution de l'exercice 4

On va démontrer l'exercice par l'absurde : supposons que N soit premier et que n ne soit pas premier. Alors $N = \sum_{k=0}^{n-1} 10^k = \frac{10^n-1}{10-1}$.

Si n n'est pas premier, il s'écrit nécessairement sous la forme pq avec $p \geqslant q > 1$, donc on peut factoriser N :

$$N = \frac{10^{pq}-1}{9} = \frac{10^{pq}-1}{9} = \frac{(10^p-1)\left(\sum_{k=0}^{q-1} 10^p k\right)}{9}$$
$$= \frac{(10-1)\left(\sum_{k=0}^{p-1} 10^k\right)\left(\sum_{k=0}^{q-1} 10^p k\right)}{9}$$
$$= \left(\underbrace{\sum_{k=0}^{p-1} 10^k}_{>1}\right)\left(\underbrace{\sum_{k=0}^{q-1} 10^p k}_{>1}\right).$$

L'entier N est donc le produit de deux facteurs plus grands que 1, et c'est un nombre composé, ce qui est contradictoire. Donc l'énoncé est vrai.

Solution de l'exercice 5

Oui on peut ! Et on va exhiber 2018 tels nombres. On écrit le nombre i en binaire, $i = \overline{a_k \ldots a_0}_{(2)}$, et on pose $t_i = \overline{a_k\ ldotsa_0}_{(3)}$.
Alors supposons qu'il existe trois indices k, l, m tels que $t_k + t_m = 2t_l$.

À droite, l'écriture ternaire de $2t_l$ est constituée uniquement de 2 et de 0. À gauche, on sait qu'il existe une position u pour laquelle le chiffre de t_k est différent du chiffre de t_m (sinon les deux nombres seraient identiques), donc leur somme fait 1, et comme il ne peut pas y avoir de retenu (car $1+1<3$), l'un des chiffres de la somme de gauche est 1. Mais ceci est contradictoire, car l'écriture d'un nombre en base 3 est unique. Donc trois de nos nombres ne forment jamais une suite arithmétique.

Reste à vérifier qu'ils sont tous plus petits que notre borne : $2018 = \overline{11110001010}_{(2)}$ donc $t_{2018} = \overline{11110001010}_{(3)} = 3^10 + 3^9 + 3^8 + 3^7 + 3^3 + 3^1 < 2 \cdot 3^10 = 6561 \cdot 18 < 150000$, donc c'est bon, nous avons notre exemple.

Solution de l'exercice 6

Comme beaucoup de 2 apparaissent dans la définition de f, on a l'idée de regarder les nombres en base 2. Quand on multiplie un nombre par 2, on lui ajoute un 0, et quand on lui ajoute 1, on augmente le chiffre des unités de 1. Calculons les premières valeurs de f : $f(\overline{1}_{(2)}) = 1$, $f(\overline{10}_{(2)}) = 1$, $f(\overline{11}_{(2)}) = 2$, $f(\overline{100}_{(2)}) = 1$, $f(\overline{101}_{(2)}) = 2$, $f(\overline{110}_{(2)}) = 2$, $f(\overline{111}_{(2)}) = 3\ldots$ On a l'intuition que $f(n)$ vaut le nombre de 1 dans la représentation en binaire de n.

On va montrer par récurrence forte sur n que la propriété $\mathcal{P}_n$: « $f(n)$ est le nombre de 1 dans la représentation en binaire de n » est vraie pour tout entier $n \geqslant 1$.

1. *Initialisation* : Montrons que $\mathcal{P}_1$ est vraie.

   On peut vérifier directement que $f(1) = f(\overline{1}_{(2)}) = 1$. Ceci conclut l'initialisation.

2. *Hérédité* : Supposons $\mathcal{P}_1, \ldots, \mathcal{P}_k$, et montrons qu'alors $\mathcal{P}_{k+1}$ est vraie aussi. On va distinguer deux cas :

   — Si $k+1$ est pair, il s'écrit sous la forme 2ℓ, avec $1 \leqslant \ell \leqslant k$. La représentation binaire de ℓ comporte $f(\ell)$ chiffres 1 par hypothèse de récurrence, et celle de 2ℓ a aussi $f(\ell)$ chiffres 1 d'après le début de notre raisonnement. Or, $f(2\ell) = f(\ell)$, donc dans ce cas, notre propriété est toujours vraie.

   — Sinon, $k+1$ est impair et s'écrit sous la forme $2\ell+1$ avec $1 \leqslant \ell \leqslant k$. La représentation binaire de ℓ comporte $f(\ell)$ uns, et celle de $2\ell+1$ en comporte $f(\ell)+1$. Or, $f(2\ell+1) = f(\ell) + 1$ donc notre propriété est aussi vraie dans ce cas.

   La propriété est donc héréditaire.

3. *Conclusion* : La propriété est vraie pour tout $n \geqslant 1$.

Réciproquement, on peut vérifier que notre fonction marche bien.

Reste maintenant à trouver quel est le nombre de notre intervalle qui a le plus de 1 dans sa représentation binaire. $2018 = \overline{11110001010}_{(2)}$, donc un chiffre plus petit que 2018 ne peut pas avoir plus de 11 chiffres 1 dans sa représentation binaire. Mais 10 chiffres 1 sont possibles, par exemple pour $1023 = 2^{10} - 1$. Le maximum de $f(n)$ est donc 10.

2 Dénombrement

Ce cours est directement issu du cours de dénombrement disponible sur le site de la POFM.

3 Raisonnements et principe des tiroirs

Ce cours est directement issu du cours de stratégies de base disponible sur le site de la POFM.

4 Invariants et principe de l'extremum

Ce cours est essentiellement tiré du cours analogue proposé lors du stage olympique d'été organisé à Montpellier en 2013 et de son polycopié. Des références concernant les invariants et le principe de l'extremum sont respectivement en pages 45 et 50.

5 Suite de Thue-Morse et théorème de Van der Waerden

Ce cours a pour but d'être une introduction à la combinatoire des mots et la théorie de Ramsey, en présentant un problème proche des fondements de chacune.

– Qu'est-ce qu'un mot ? –

Définition 3.5.1.
Un *alphabet* est un ensemble, dont les éléments sont appelés *lettres*. Un *mot* sur un alphabet A est une suite (finie ou infinie) de lettres de A. La *longueur* d'un mot est le nombre de lettres qu'il contient.

Exemples :

— Les mots français sont des mots sur un alphabet de 42 lettres (si les lettres accentuées comptent chacune pour une lettre différente).

— Un mot binaire est un mot sur un alphabet à deux lettres, qui sont généralement notées 0 et 1.

— Une séquence d'ADN peut être vue comme un mot sur un alphabet à 4 lettres, ces 4 lettres étant les 4 bases azotées (généralement notées A,T,C et G).

— La plupart des textes écrits sur Internet utilisent l'alphabet unicode, qui compte 137734 lettres.

— Sur tout alphabet, il existe un unique mot de longueur 0, qui est appelé le mot vide.

Dans ce cours, on s'intéressera à certaines formes de régularité des mots, en se posant deux fois une question de la forme « tout mot suffisamment long contient-il telle structure ? ». Pour aborder la première question, définissons une forme de structure d'un mot.

Définition 3.5.2.
Un mot *carré* est un mot non vide composé de deux parties égales consécutives. Par exemple, le mot $papa$ est un carré, de même que le mot ternaire 01210121. Un mot est *sans facteur carré*, ou *sans carré*, si aucun des sous-mots obtenus en tronquant le mot de départ au début et/ou à la fin n'est un mot carré. Par exemple, le mot $carre$ n'est pas sans carré, car on peut le tronquer pour obtenir rr. Le mot $triangle$, lui, est sans carré.

Dès lors, une question naturelle est « tout mot suffisamment long est-il avec carré ? », i.e. existe-t-il N tel que tout mot de longueur $\geqslant N$ est avec carré ? Bien entendu, la réponse à une telle question dépend de la taille de l'alphabet dans lequel on se place. Avec un alphabet infini, il existe des mots sans carré arbitrairement longs : il suffit de prendre une seule fois chaque lettre dont on dispose.

A l'inverse, avec l'alphabet de deux lettres $\{0, 1\}$, tout mot de longueur 4 contient un carré. Pour le montrer, il suffit de procéder par exhaustion des cas. On peut suposer spdg que la première lettre du mot est 0. Pour éviter les carrés, les lettres suivantes doivent être 1, puis 0, et on est bloqué à ce point : pour la quatrième lettre, un 0 donnerait le carré 00, et un 1 donnerait le carré 0101. Le mot sans carré le plus long sur un alphabet à deux lettres est donc de longueur 3 (par exemple, le mot 010 en est un).

On peut se demander, entre ces deux extrêmes, quel est le nombre minimum de lettres dans l'alphabet pour que des mots sans carré existent, et quel est le k minimal pour que des mots à deux lettres sans puissance k-ième existent (remarquons qu'il est a priori possible qu'un de ces nombres ne soit pas défini). Les réponses à ces deux questions vont être données par la suite de Thue-Morse.

– Trois définitions de la suite de Thue-Morse –

Dans la suite du cours, les lettres des mots seront indexées à partir de 0. Un mot infini peut être vu comme une fonction qui à chaque naturel n associe la n-ième lettre du mot. La suite de Thue-Morse peut être définie de trois manières, dont on va montrer qu'elles sont équivalentes.

Définition 3.5.3.
La *suite de Thue-Morse* (ou *mot de Thue-Morse*, ou *séquence de Thue-Morse*) est le mot sur l'alphabet $\{0, 1\}$ dont la j-ième lettre, notée T_j, est le nombre de chiffres 1 dans la décomposition binaire de j, modulo 2.

Par exemple, $T_{42} = 1$ car 42 s'écrit 101010 en binaire, 101010 a trois chiffres 1, et $3 \equiv 1 (\bmod 2)$. La suite de Thue-Morse commence par $0110100110010110100101 10 \ldots$
On peut remarquer plusieurs choses à partir de cette définition :

— On a $T_n = T_{2n}$ pour tout naturel n. En effet, la décomposition binaire de $2n$ s'obtient en rajoutant un 0 à droite de celle de n. Passer de n à $2n$ ne change donc pas le nombre de 1 dans la décomposition, d'où la conclusion.

— On a $T_{2n+1} \neq T_n$ par un raisonnement similaire : la décomposition binaire de $2n+1$ s'obtient en rajoutant un 1 à droite de celle de n, donc la parité du nombre de 1 dans la décomposition change.

— Les deux observations ci-dessus sont suffisantes pour déterminer une unique suite, une fois que T_0 est donné et qu'on sait que l'alphabet n'a que deux symboles. Ceci conduit à la deuxième définition de la suite :

Définition 3.5.4.
La *suite de Thue-Morse* est le mot sur l'alphabet $\{0, 1\}$ défini par les relations suivantes :

$$T_0 = 0, \qquad T_{2n} = T_n \quad \forall n \in \mathbb{N}, \qquad T_{2n+1} \neq T_n \quad \forall n \in \mathbb{N}$$

— Si les 2^n premiers termes de la suite sont connus, les 2^n termes suivants peuvent eux aussi être déduits. En effet, si $x < 2^n$, alors la décomposition binaire de $x + 2^n$ s'obtient en remplissant éventuellement à gauche par des zéros et en rajoutant un unique chiffre 1 dans la décomposition de x. Les 2^n termes cherchés s'obtiennent donc en prenant les 2^n termes connus et en remplaçant chaque lettre par l'autre. A nouveau, cette propriété est assez forte pour être une définition, une fois le premier terme connu.

Définition 3.5.5.
La *suite de Thue-Morse* est le mot sur l'alphabet $\{0, 1\}$ défini par $T_0 = 0$ et, si les 2^n premiers termes de la suite sont connus, par $T_{x+2^n} \neq T_x \quad \forall x < 2^n$.

– Propriété d'absence de recouvrement et construction d'un mot infini sans carré –

Définition 3.5.6.
Un mot est *sans recouvrement* si il ne peut pas être tronqué en un mot de la forme $aXaXa$, où a est une lettre et X est un mot, éventuellement vide.

Nous allons montrer que le mot de Thue-Morse est sans recouvrement en suivant la preuve d'Allouche et Shallit, ce qui sera suffisant pour répondre aux deux questions de la fin de la première section.

Théorème 3.5.7 (Thue, 1906)**.**
Le mot de Thue-Morse est sans recouvrement.

Démonstration. Tout d'abord, si la suite de Thue-Morse contient un recouvrement, alors elle peut s'écrire comme $UaXaXaV$, où a est une lettre, U et X sont des mots finis et V un mot infini. Notons k la longueur de U et m la longueur de aX. m est un entier $\geqslant 1$, donc il existe un m minimum sur tous les recouvrements de la suite. Par définition d'un recouvrement, de k et de m, on a $T_{k+j} = T_{k+j+m} \quad \forall j$ tel que $0 \leqslant j \leqslant m$. On procède alors par disjonction de cas sur k et m.

— Cas 1 : m et k sont pairs.
On peut alors écrire $k = 2k'$ et $m = 2m'$. On a $T_{2k'+j} = T_{2k'+j+2m'} \quad \forall j$ tel que $0 \leqslant j \leqslant m$, et en particulier $T_{2k'+2j'} = T_{2k'+2j'+2m'} \quad \forall j'$ tel que $0 \leqslant j' \leqslant m'$. Puisqu'on sait vu la deuxième définition que $T_{2n} = T_n$, on a $T_{k'+j'} = T_{k'+j'+m'} \quad \forall j'$ tel que $0 \leqslant j' \leqslant m'$, ce qui est la condition pour avoir un autre recouvrement, dont la longueur serait $m' < m$, ce qui contredit la minimalité de m, absurde.

— Cas 2 : m est pair, k est impair.
De la même façon, on a $k = 2k' + 1$ et $T_{2k'+1+2j'} = T_{2k'+1+2j'+2m'} \quad \forall j'$ tel que $0 \leqslant j' \leqslant m'$. Puisque $T_{2n+1} = 1 - T_n$, on atteint la même contradiction que dans le cas précédent.

Avant de passer aux trois derniers cas, définissons la suite $b_n = (T_n + T_{n-1}) \pmod 2$, indexée à partir de 1. Pour tout naturel n, on a $b_{4n+2} = 0$ car les développements binaires de $4n+1$ et $4n+2$ ont le même nombre de chiffres 1. On a aussi $b_{2n+1} = 1$ car le développement binaire de $2n+1$ a un chiffre 1 de plus que celui de $2n$. Enfin, si la suite admet un recouvrement avec les notations ci-dessus, on a $b_{k+j} = b_{k+j+m} \quad \forall j$ tel que $1 \leqslant j \leqslant m$.

— Cas 3 : m impair et plus grand que 5.
  Vu $m \geqslant 5$, il existe j tel que $1 \leqslant j \leqslant m$ et $k+j \equiv 2 (\bmod 4)$. Dès lors, on a $b_{k+j} = 0$. Par le recouvrement, on a aussi $b_{k+j+m} = 0$, mais $k+j+m$ est impair, donc $b_{k+j+m} = 1$. Absurde.
— Cas 4 : $m = 3$.
  j prend alors les valeurs $1, 2$ et $3 (\bmod 4)$, donc $k+j$ prend toutes les valeurs sauf une mod 4. Si $k+j$ prend la valeur 2 mod 4 à un moment, on atteint la contradiction ci-dessus. Sinon, il prend à un moment la valeur 3. On a alors $b_{k+j} = 1$ et par le recouvrement on a $b_{k+j+3} = 1$, or $k+j+3 \equiv 2 (\bmod 4)$, et donc $b_{k+j+3} = 0$, absurde.
— Cas 5 : $m = 1$.
  On a alors trois termes consécutifs de la suite égaux, ce qui est absurde vu que $\forall n \in \mathbb{N}, T_{2n+1} \neq T_n = T_{2n}$.

Au final, tous les cas aboutissent à une absurdité. Il n'existe donc pas de longueur de recouvrement minimale dans la suite de Thue-Morse, et celle-ci est par conséquent sans recouvrement. □

Corollaire 3.5.8.
La suite de Thue-Morse est sans cube et non périodique.

Ainsi, nous avons répondu à notre seconde question : « Quel est le k minimal pour que des mots à deux lettres sans puissance k-ième existent ? ». Nous avons montré que $k = 3$. La réponse à la première, « Quel est le nombre minimum de lettres dans l'alphabet pour que des mots sans carré existent », découle également du résultat, et la réponse sera à nouveau 3.

Théorème 3.5.9 (Thue, 1906)**.**
Il existe un mot infini et sans carré sur un alphabet de trois lettres.

Démonstration. Considérons le mot dont la n-ième lettre, c_n, est le nombre de lettres 1 entre le n-ième 0 de la suite de Thue-Morse et le $n+1$-ième. Il s'agit d'un mot sur $\{0, 1, 2\}$: $c_n \geqslant 0$ de manière évidente et $c_n < 3$ car sinon la suite de Thue-Morse contiendrait un sous-mot 111. Montrons qu'il est sans carré, par l'absurde. S'il avait un carré de la forme $p_1 p_2 \dots p_n p_1 p_2 \dots p_n$, alors par définition de ce mot, la suite de Thue-Morse contiendrait à un moment le sous-mot

$$01^{p_1}01^{p_2}0 \dots 01^{p_n}01^{p_1} \dots 1^{p_n}0$$

où 1^{p_1} signifie que la lettre 1 est répétée p_1 fois. C'est une contradiction, puisqu'un tel sous-mot constitue un recouvrement. □

– Le problème de Prouhet-Tarry-Escott –

Le problème pose la question de savoir s'il existe deux ensembles disjoints A et B tels que

$$\forall n \in \{0, 1, \ldots, k\}, \quad \sum_{j\in A} j^n = \sum_{j\in B} j^n$$

A nouveau, la suite de Thue-Morse est un outil bien utile pour résoudre le problème, qu'on pourra même généraliser.

Définissons $X_k = \{x \in \{0, \ldots, 2^{k+1} - 1\} : T_x = 0\}$ et $Y_k = \{x \in \{0, \ldots, 2^{k+1} - 1\} : T_x = 1\}$. Remarquons que X_0 et Y_0 contiennent le même nombre d'éléments. Dès lors,

Théorème 3.5.10 (Prouhet, 1851)**.**
Pour tout polynôme P de degré inférieur ou égal à k,

$$\sum_{j\in X_k} P(j) = \sum_{j\in Y_k} P(j)$$

ce qui est une généralisation du problème posé.

Démonstration. La démonstration se fait par récurrence sur k. L'initialisation à $k = 0$ ne pose pas de problème. A présent, supposons que la propriété soit vérifiée pour un certain k et montrons qu'elle l'est pour $k+1$. Soit Q un polynôme quelconque de degré $k+1$ au plus, et soit $R(x) = Q(x + 2^{k+1}) - Q(x)$. En développant la définition de R, on peut voir que les termes de degré $k+1$ se simplifient, R est donc un polynôme de degré au plus k et on a

$$\sum_{j\in X_k} R(j) = \sum_{j\in Y_k} R(j)$$

par hypothèse de récurrence. De là, il vient

$$\begin{aligned}
\sum_{j\in X_k} (Q(j+2^{k+1}) - Q(j)) &= \sum_{j\in Y_k} (Q(j+2^{k+1}) - Q(j)) \\
\sum_{j\in X_k} Q(j+2^{k+1}) - \sum_{j\in X_k} Q(j) &= \sum_{j\in Y_k} Q(j+2^{k+1}) - \sum_{j\in Y_k} Q(j) \\
\sum_{j\in X_k} Q(j+2^{k+1}) + \sum_{j\in Y_k} Q(j) &= \sum_{j\in Y_k} Q(j+2^{k+1}) + \sum_{j\in X_k} Q(j)
\end{aligned}$$

Or, puisque $j < 2^{k+1}$ et vu la troisième définition, on a $T_{j+2^{k+1}} = 1 - T_j$, et dès lors

$$\{j + 2^{k+1} : j \in X_k\} = Y_{k+1} \setminus Y_k$$

et de même pour Y_k. En réécrivant les sommes, on a donc

$$\begin{aligned}
\sum_{j\in Y_{k+1}\setminus Y_k} Q(j) + \sum_{j\in Y_k} Q(j) &= \sum_{j\in X_{k+1}\setminus X_k} Q(j) + \sum_{j\in X_k} Q(j) \\
\sum_{j\in Y_{k+1}} Q(j) &= \sum_{j\in X_{k+1}} Q(j)
\end{aligned}$$

ce qui conclut, puisque Q était un polynôme quelconque de degré au plus $k+1$. $\square$

– Une dernière application –

Considérons la suite suivante :

$$\frac{1}{2}, \frac{\frac{1}{2}}{\frac{3}{4}}, \frac{\left(\frac{\frac{1}{2}}{\frac{3}{4}}\right)}{\left(\frac{\frac{5}{6}}{\frac{7}{8}}\right)}, \ldots$$

Nous allons « montrer » que cette suite converge et déterminer sa limite. Tout d'abord, remarquons que l'on peut réécrire chaque terme de la suite comme une fraction simple, avec un seul numérateur et dénominateur. Il nous faut déterminer quels nombres apparaîtront au numérateur dans cette fraction. On peut constater que 1 apparaît toujours au numérateur et 2 toujours au dénominateur, et que si l'on sait à quelle place les nombres de 1 à 2^k apparaissent, alors on peut déduire où les nombres de $2^k + 1$ à 2^{k+1} se trouvent. En effet, dans la fraction simplifiée, $2^k + x$ se trouve de l'autre côté de la barre de fraction par rapport à x, puisqu'il est sous une barre de fraction supplémentaire dans la fraction de départ, toutes choses étant identiques par ailleurs. Ceci fait penser à la troisième définition de la suite de Thue-Morse, et il s'agit effectivement de celle-ci, bien que décalée d'une unité. Le k-ième terme de la séquence (en commençant l'indexation à 0) est donc

$$\prod_{n=0}^{2^{k+1}-1} (n+1)^{(-1)^{T_n}}$$

On peut également considérer que les éléments atomiques de la fraction sont non pas des entiers mais bien des rationnels (les plus petits quotients). On peut remarquer que $\frac{2n+1}{2n+2}$ est au numérateur ssi $2n+1$ l'est, donc ssi $T_{2n} = 0$ c'est à dire ssi $T_n = 0$. En faisant donc ce changement, on obtient que le k-ième terme de la séquence est

$$\prod_{n=0}^{2^k-1} {\frac{2n+1}{2n+2}}^{(-1)^{T_n}}$$

On peut montrer que ce produit converge effectivement vers un nombre strictement positif lorsque k tend vers l'infini, en passant au logarithme et en utilisant le test de Dirichlet, mais cela sort du cadre de ce cours. Supposons que la limite soit D, i.e.

$$D = \prod_{n=0}^{\infty} {\frac{2n+1}{2n+2}}^{(-1)^{T_n}}$$

Définissons

$$E = \prod_{n=1}^{\infty} {\frac{2n}{2n+1}}^{(-1)^{T_n}}$$

qui converge selon le même raisonnement.

En multipliant, on obtient

$$DE = \frac{1}{2} \prod_{n=1}^{\infty} {\frac{n}{n+1}}^{(-1)^{T_n}}$$

On peut séparer le produit selon la parité de n :

$$DE = \frac{1}{2}\prod_{n=0}^{\infty} \frac{2n+1}{2n+2}^{(-1)^{T_{2n+1}}} \cdot \prod_{n=1}^{\infty} \frac{2n}{2n+1}^{(-1)^{T_{2n}}}$$

et puisque $T_{2n} = T_n$ et $T_{2n+1} = 1 - T_n$, on a en fait que $DE = \frac{1}{2}D^{-1}E$, c'est à dire $D = \frac{\sqrt{2}}{2}$ puisqu'il est positif. Remarquons que l'on a aucune information sur la valeur de E, c'est un simple outil de calcul.

– Le théorème de Van der Waerden –

En 1927, Van der Waerden a démontré le théorème suivant :

Théorème 3.5.11 (Van der Waerden, 1927).
$\forall k, r \in \mathbb{N}_{\geqslant 2}, \exists W(k,r)$ tel que si les entiers de 1 à $W(k,r)$ sont coloriés en r couleurs, il existe une progression arithmétique unicolore de longueur k.

La longueur d'une progression arithmétique désigne le nombre d'entiers qu'elle contient (deux entiers forment donc toujours une progression arithmétique de longueur 2). La suite sera consacrée à la démonstration de ce théorème, qui ne nécessite pas d'outils très complexes malgré les apparences.

– Un premier cas : $k = 3$, $r = 2$ –

Une simple exhaustion des cas permet de conclure que $W(3,2) = 9$. Nous présentons une autre méthode qui donne une borne nettement moins bonne, mais se généralise plus facilement.

On montre que $W(3,2) \leqslant 325$. Le choix de 325 peut paraître arbitraire mais va s'éclairer d'ici peu. Supposons qu'on ait colorié les nombres de 1 à 325 sans progression arithmétique monochrome de longueur 3. On divise les nombres de 1 à 325 en 65 blocs de 5 entiers consécutifs. Puisqu'il n'y a que 32 façons de colorier un bloc de cinq en deux couleurs, on peut trouver deux blocs coloriés identiquement parmi les 33 premiers. Notons-les A_1 et $A_1 + d_1$. Puisque ces blocs sont parmi les 33 premiers, le bloc $A_1 + 2d_1$ est l'un des 65 considérés. Au sein des trois premiers éléments de chaque bloc, il y en a deux de la même couleur (spdg rouge), qu'on peut noter A_0 et $A_0 + d_0$. Puisque ces deux nombres font partie des trois premiers d'un bloc de cinq, on a que $A_0 + 2d_0$ appartient au même bloc. Il est bleu, sinon on a une progression arithmétique. Dès lors, vu l'hypothèse que A_1 et $A_1 + d_1$ sont coloriés de manière identique, A_0 et $A_0 + d_0 + d_1$ sont rouges et $A_0 + 2d_0$ et $A_0 + 2d_0 + d_1$ sont bleus. Mais les deux affirmations précédentes impliquent simultanément que $A_0 + 2d_0 + 2d_1$ est bleu et rouge, contradiction.

Au final, le nombre 325 vient du fait qu'il faut des blocs de 5 pour s'assurer que les 3 premiers entiers contiennent une progression arithmétique de longueur 2 qui peut se prolonger à l'intérieur du bloc, puis qu'il faut 65 blocs pour que les 33 premiers contiennt deux blocs identiques, une « progression de longueur 2 » qui peut se prolonger dans les 65 blocs considérés.

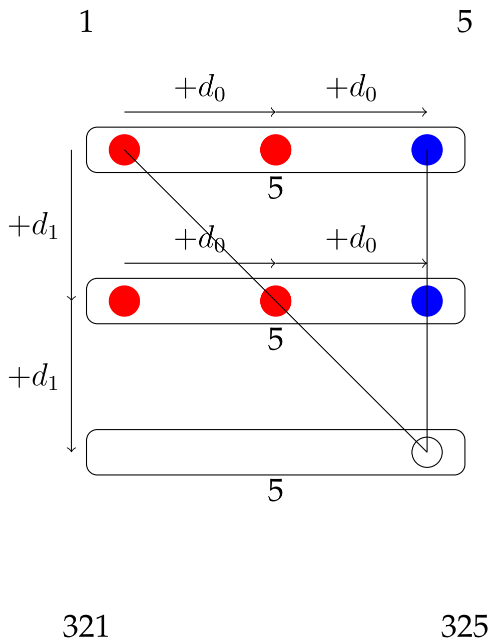


FIGURE 1 – Une représentation plus visuelle du raisonnement ci-dessus

– Une première généralisation : $k = 3$, $r = 3$ –

Ici, on peut réutiliser une partie du raisonnement précedent. Il faut cependant prendre des blocs de 7 entiers puis prendre $2 \cdot 3^7 + 1$ blocs, ce qui garantit que deux blocs identiques se trouvent dans la première moitié et peuvent donc être « prolongés » par un troisième dans la limite des blocs cosidérés. Cependant, le raisonnement ne permet plus de conclure puisqu'en reprenant les mêmes notations, l'entier $A_0 + 2d_0 + 2d_1$ peut maintenant être colorié dans la troisième couleur (spdg vert). La solution consiste à considérer les $N_1 = 7 \cdot (2 \cdot 3^7 + 1)$ entiers déjà coloriés comme un seul gros bloc (qu'on appelera un 2-bloc). Il y a 3^{N_1} manières de colorier un 2-bloc, donc si l'on prend $2 \cdot 3^{N_1} + 1$ 2-blocs consécutifs, il y en a deux coloriés identiquement dans la première moitié, qu'on peut appeler A_2 et $A_2 + d_2$, de telle sorte que $A_2 + 2d_2$ fasse partie des 2-blocs considérés. Mais alors, A_0 et $A_0 + d_0 + d_1 + d_2$ sont rouges, $A_0 + 2d_0$ et $A_0 + 2d_0 + d_1 + d_2$ sont bleus et $A_0 + 2d_0 + 2d_1$ et $A_0 + 2d_0 + 2d_1 + d_2$ sont verts, donc $A_0 + 2d_0 + 2d_1 + 2d_2$ ne peut être ni rouge, ni bleu, ni vert. C'est une contradiction. On a donc montré que $W(3, 3) \leqslant N_1 \cdot (2 \cdot 3^{N_1} + 1)$. Pour information, ce nombre vaut un peu plus de $4,222 \cdot 10^{14616}$, tandis qu'on peut montrer par exhaustion que la vraie valeur est $W(3, 3) = 27$.

– $k = 3$, r quelconque –

Dans cette section, tentons de généraliser la méthode des deux sections précédentes à un nombre de couleurs quelconque. On définit les n-blocs par récurrence sur n :

— Un 0-bloc est un entier.

— Un 1-bloc est un bloc de $2r + 1$ entiers consécutifs.

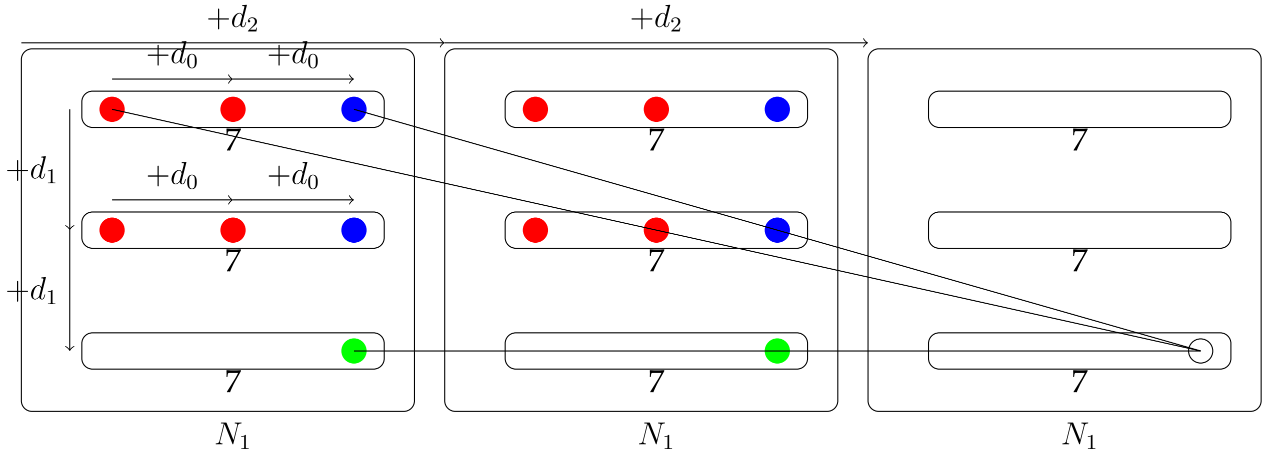


FIGURE 2 – Il peut être utile de se représenter les 2-blocs empilés les uns sur les autres comme des « tranches » d'un cube, la direction d_2 devenant donc la verticale.

— Si les blocs sont définis jusqu'aux $n-1$-blocs, et si la taille de ceux-ci est N_{n-1}, un n-bloc est un bloc de $2 \cdot r^{N_{n-1}} + 1$ $n-1$-blocs consécutifs, et la taille d'un tel bloc est notée N_n.

On va montrer que $W(3,r) \leqslant N_r$. On considère donc les choses à l'intérieur d'un seul r-bloc. Supposons qu'il soit colorié en r couleurs sans progression arithmétique de longueur 3. D'abord, on va construire des progessions de longueur 2 potentiellement prolongeables dans les limites de notre r-bloc, et ce par récurrence descendante sur l'indice du bloc :

— Parmi les $r^{N_{r-1}}+1$ premiers $r-1$-blocs, on peut en trouver deux coloriés de manière identique. Appelons-les A_{r-1} et $A_{r-1}+d_{r-1}$. On vérifie que $A_{r-1}+2d_{r-1}$ est dans le r-bloc auquel on se restreint.

— Si A_n est défini, avec $n \geqslant 1$, on peut trouver au sein de la première moitié de A_n deux $n-1$-blocs coloriés de manière identique, qu'on appelle A_{n-1} et $A_{n-1}+d_{n-1}$. On vérifie que $A_{n-1}+2d_{n-1}$ appartient bien à A_n.

On « remonte » alors les niveaux pour interdire de plus en plus de couleurs à certains entiers spécifiques :

— A_0 et A_0+d_0 sont de la même couleur (spdg la couleur 0), donc A_0+2d_0 ne peut être de cette couleur, on peut supposer qu'il est de la couleur 1.

— Si la couleur de $A_0+2\sum_{j=0}^{n} d_j$ est connue, alors on sait que $\forall i \leqslant n+1$, $A_0+2\sum_{j=0}^{i-1} d_j$ et $A_0+\sum_{j=i}^{n+1} d_j + 2\sum_{j=0}^{i-1} d_j$ sont de la couleur i. Dès lors, $A_0+2\sum_{j=i}^{n+1} d_j + 2\sum_{j=0}^{i-1} d_j$ ne peut être de la couleur i. On a en fait que $A_0+2\sum_{j=0}^{n+1} d_j$ ne peut être de la couleur i pour aucun i entre 0 et $n+1$, il est donc spdg de la couleur $n+2$.
En particulier on a donc que $A_0+2\sum_{j=0}^{(r-2)+1} d_j$ ne peut être de la couleur i pour aucun i entre 0 et $r-1$, c'est à dire qu'il ne peut être d'aucune des r couleurs utilisées. C'est une contradiction.

– $k=4, r=2$ –

Pour généraliser à $k > 3$, on peut se rappeler de la remarque à la fin du cas $k = 3, r = 2$: le but était de trouver une progression de longueur 2 (c'est-à-dire 2 blocs identiques) qu'on peut prolonger dans la limite du bloc dans lequel on se trouve, et ce à tous les niveaux de blocs. Pour $k = 4$, il va nous falloir trouver des progression de longueur 3 de blocs identiques et prolongeables dans la limite qu'on se donne. Heureusement, on vient de montrer qu'on sait trouver des progressions arithmétiques monocolores de longueur 3 quel que soit le nombre de couleurs. Pour le cas $k = 4, r = 2$, les choses se passent donc ainsi :

On groupe les entiers par blocs de $2 \cdot 325$. Ainsi, on peut trouver une progression de longueur 3 dans la première moitié de chaque bloc, et puisqu'elle est dans la première moitié, on peut potentiellement la prolonger en une progression de longueur 4 au sein du bloc (remarquons qu'on peut améliorer le facteur 2 en un facteur $3/2$, par exemple). Ensuite, il y a 2^{650} manières de colorier chaque bloc. Chaque manière de colorier le bloc peut être vue comme une « couleur », et puisque $W(3, 2^{650})$ existe, on peut trouver une progression arithmétique de 3 blocs de la même « couleur », i.e. coloriés de manière identique. Montrons alors que $W(4, 2) \leqslant 650 \cdot 2 \cdot W(3, 2^{650})$.

Parmi les $W(3, 2^{650})$ premiers blocs, on peut trouver une progression de longueur 3 de blocs coloriés de manière identique. Appelons ces blocs A_1, $A_1 + d_1$ et $A_1 + 2d_1$. Puisque ces trois blocs ont été choisis parmi la première moitié des blocs considérés, $A_1 + 3d_1$ fait partie des blocs considérés. Au sein de A_1, on peut trouver une progression de longueur 3 d'entiers coloriés de la même couleur. On appelle ces entiers A_0, $A_0 + d_0$ et $A_0 + 2d_0$, et on suppose qu'ils sont rouges. De même, $A_0 + 3d_0$ appartient lui aussi à A_1, et si il n'est pas bleu on a fini. Mais alors, A_0, $A_0 + d_0 + d_1$ et $A_0 + 2d_0 + 2d_1$ sont tous trois rouges et $A_0 + 3d_0$, $A_0 + 3d_0 + d_1$ et $A_0 + 3d_0 + 2d_1$ sont tous trois bleus. Puisque $A_0 + 3d_0 + 3d_1$ est soit rouge soit bleu, il prolonge une de ces deux progressions en une progression monocolore de longueur 4, ce qui conclut.

– Le cas général –

Notons $\Lambda(r, k)$ la proposition « $\exists W(k, r)$ tel que si les nombres de 1 à $W(k, r)$ sont coloriés en r couleurs, il existe une progression arithmétique unicolore de longueur k » et Λ_k la proposition « $\Lambda(r, k)$ est vraie pour tout $r \geqslant 2$ ». On va montrer que Λ_k est vraie pour tout $k \geqslant 3$ par récurrence sur k. On a déjà montré Λ_3, qui sera notre cas de base. A présent, supposons Λ_k et montrons Λ_{k+1} :

À nouveau, on définit des n-blocs par récurrence sur n :

— Un 0-bloc est un entier.

— Si les $n-1$-blocs sont définis et ont pour taille N_{n-1}, un n-bloc est un bloc de $(2 \cdot W(k, r^{N_{n-1}}))$ $n-1$-blocs consécutifs.

On va montrer que $W(k+1, r) \leqslant N_r$. On considère donc les choses à l'intérieur d'un seul r-bloc. Supposons qu'il soit colorié en r couleurs sans progression arithmétique de longueur $k+1$. On commence par construire des progressions monocolores de longueur k prolongeables dans le bloc d'intérêt à chaque niveau de bloc, par récurrence descendante sur le niveau des blocs.

— Le r-bloc qu'on considère est composé de $(2 \cdot W(k, r^{N_{r-1}}))$ $r-1$-blocs consécutifs. Ces $r-1$-blocs peuvent être coloriés de $r^{N_{r-1}}$ façons différentes, qui peuvent être vues comme autant de couleurs. Vu le nombre de blocs en présence, on peut trouver dans la première moitié une progression arithmétique de longueur k de blocs de « couleur » identique. Appelons ces blocs $A_{r-1}, A_{r-1} + d_{r-1}, \ldots A_{r-1} + (k-1)d_{r-1}$. Puisque tous ces blocs sont dans la première moitié du r-bloc considéré, $A_{r-1} + kd_{r-1}$ lui appartient également.

— Supposons que A_n soit défini pour un $n \geqslant 1$. Il est composé de $(2 \cdot W(k, r^{N_{n-1}}))$ $n-1$-blocs consécutifs. En suivant le même raisonnement que ci-dessus, on peut trouver des blocs $A_{n-1}, A_{n-1} + d_{n-1}, \ldots A_{n-1} + (k-1)d_{n-1}$ en progression arihmétique et coloriés de la même façon, de telle sorte que $A_{n-1} + kd_{n-1}$ appartienne à A_n.

Comme pour le cas $k = 3$, on « remonte » alors les niveaux de blocs pour aboutir à une contradiction.

— $A_0, A_0 + d_0, \ldots, A_0 + (k-1)d_0$ sont de la même couleur (spdg la couleur 0), donc $A_0 + kd_0$ ne peut être de cette couleur, on peut supposer qu'il est de la couleur 1.

— Si la couleur de $A_0 + k\sum_{j=0}^{n} d_j$ est connue, alors on sait que $\forall i \leqslant n+1, \forall m \leqslant k-1$, les $A_0 + m\sum_{j=i}^{n+1} d_j + k\sum_{j=0}^{i-1} d_j$ sont de la couleur i. Dès lors, $A_0 + k\sum_{j=i}^{n+1} d_j + k\sum_{j=0}^{i-1} d_j$ ne peut être de la couleur i. On a en fait que $A_0 + k\sum_{j=0}^{n+1} d_j$ ne peut être de la couleur i pour aucun i entre 0 et $n+1$, il est donc spdg de la couleur $n+2$.
En particulier on a donc que $A_0 + k\sum_{j=0}^{(r-2)+1} d_j$ ne peut être de la couleur i pour aucun i entre 0 et $r-1$, c'est à dire qu'il ne peut être d'aucune des r couleurs utilisées. C'est une contradiction.

– Conclusion –

Nous avons donc prouvé le théorème de Van der Waerden en donnant une (très mauvaise) borne supérieure pour $W(k,r)$. Il peut être intéressant d'étudier la croissance de la borne prévue, mais ce ne sera pas fait ici. Il est également intéressant de noter que Timothy Gowers a montré en 2001 que

$$W(k,r) \leqslant 2^{2^{r^{2^{2^{k+9}}}}}$$

ce qui est une borne bien plus raisonnable (!) que celle obtenue par la méthode présentée ici. Enfin, Ronald Graham offre 1000$ à toute personne qui montrera que $W(k,2) \leqslant 2^{k^2}$. Le problème de trouver des bornes « raisonnables », et à fortiori de trouver les vraies valeurs de $W(k,r)$, est donc bien ouvert.

– Sources –

Ce cours se base sur les deux articles suivants :

[1] Westra, D.B. *A proof of Van der Waerden's theorem*. Automne 2017 : mat.univie.ac.at/~westra/van_der_waerden_thm.pdf
[2] Williamson, Christopher. *An Overview of the Thue-Morse Sequence*. 4 juin 2012 : sites.math.washington.edu/~morrow/336_12/papers/christopher.pdf

ainsi que sur les articles Wikipédia « Combinatoire des mots », « Suite de Prouhet-Thue-Morse », « Théorème de Van der Waerden », « Nombres de Van der Waerden » et leurs conteparties anglaises.

4 Géométrie

1 Chasse aux angles et points remarquables

Ce cours a pour but une introduction aux problèmes de géométrie d'olympiades. On pourra retrouver les différents théorèmes présentés pendant le cours, à savoir le théorème de l'angle inscrit, de l'angle au centre et l'étude des triangles semblables et quelques exercices dans le cours épique de Cécile Gachet du stage de Montpellier 2014 à la page 244. D'autres exercices abordés en cours figurent dans le premier cours donné au groupe B du stage Valbonne 2017 à la page 138. On a également traité les exercices suivants :

– Exercices utilisant une chasse aux angles –

Exercice 1
Soit $ABCD$ un parallélogramme, Γ le cercle circonscrit au triangle ABD. Soit S la seconde intersection de (AC) avec Γ. Montrer que (DB) est tangente au cercle circonscrit au triangle CSB.

Exercice 2
Soit k_1 et k_2 deux cercles se coupant en A et B. La tangente à k_2 en A recoupe k_1 en C. La tangente à k_1 en B recoupe k_2 en D. Montrer que (AD) et (BC) sont parallèles.

Exercice 3
Soit ABC un triangle, E le pied de la hauteur issue de B et F le projeté orthogonal de C sur la tangente au cercle (ABC) en B. Montrer que (EF) et (AB) sont parallèles.

– Exercices utilisant des triangles semblables –

Exercice 4
Dans un parallélogramme $ABCD$, on prend un point M sur la diagonale (AC). De M on trace (ME) perpendiculaire à (AB) et (MF) perpendiculaire à (AD). Démontrer que $\frac{ME}{MF} = \frac{AD}{AB}$.

Exercice 5
Soit $ABCD$ un parallélogramme avec $AB > AD$ et P et A sur la diagonale (AC) tels que $AP = CQ$ et P est plus proche de A que de C. Soit E l'intersection de (BP) avec (AD) et F l'intersection de (BQ) et (CD). Montrer que (EF) et (AC) sont parallèles.

– Théorème du Pôle Sud –

Théorème 4.1.1.
Soit ABC un triangle. Montrer que la médiatrice de $[BC]$ et la bissectrice de $\widehat{BAC}$ se coupent sur le cercle circonscrit du triangle ABC. Ce point est appelé pôle Sud de A.

Démonstration. On va plutôt montrer que le point d'intersection de la médiatrice de $[BC]$ avec le cercle circonscrit à ABC est sur la bissectrice de $\widehat{BAC}$. Soit S l'intersection de la médiatrice de $[BC]$ avec le cercle circonscrit à ABC. Par définition de la médiatrice, $SB = SC$. Donc $\widehat{SBC} = \widehat{SCB}$. Le théorème de l'angle inscrit donne alors, étant donné que S est sur le cercle circonscrit à ABC : $\widehat{SAB} = \widehat{SCB} = \widehat{SBC} = \widehat{SAC}$ donc S est sur la bissectrice de $\widehat{BAC}$, ce qui conclut. □

– Solutions –

Solution de l'exercice 1

Par théorème de l'angle inscrit, vu que les points A, D, S, B sont cocycliques, $\widehat{DBS} = \widehat{DAS}$. Comme (AB) et (CD) sont parallèles, $\widehat{DAS} = \widehat{SCB}$ donc $\widehat{DBS} = \widehat{BCS}$ et on conclut par la réciproque de l'angle tangent.

Solution de l'exercice 2

Par angles tangents, $\widehat{ACB} = \widehat{ABD}$ car (BD) est tangente à k_1 en B. Toujours par angle tangent, $\widehat{CAD} = \widehat{CAB} + \widehat{BAD} = \widehat{ADB} + \widehat{BAD} = 180 - \widehat{ABD}$ donc les droites (AD) et (CB) sont parallèles.

Solution de l'exercice 3

Comme $\widehat{CFB} = 90 = 180 - 90 = 180 - \widehat{CEB}$, les points C, E, B, F sont cocycliques. A partir de là et par angles tangents, on a $\widehat{CAB} = \widehat{CBF} = \widehat{CEF}$ donc par angles correspondants les droites (EF) et (AB) sont parallèles.

Solution de l'exercice 4

Comme $\widehat{AEM} = 90 = 180 - 90 = 180 - \widehat{AFM}$, les points A, E, M, F sont cocycliques. On a alors, en utilisant les parallélismes de (AB) et (CD), $\widehat{MFE} = \widehat{MAE} = \widehat{ACD}$ et par ailleurs $\widehat{MEF} = \widehat{MAF} = \widehat{CAD}$. Donc les triangles MEF et DAC sont semblables. On déduit $\frac{ME}{MF} = \frac{AD}{CD} = \widehat{AD}AB$.

Solution de l'exercice 5

Par Thalès pour les segments $[AE]$ et $[BC]$ avec $EB)$ et (AC) se coupant en P, on a $\frac{EP}{PB} = \frac{AP}{PC}$. Par Thalès pour les segments $[CF]$ et $[AB]$ avec (AC) et (BF) se coupant en Q, on a $\frac{FQ}{BQ} = \frac{CQ}{AQ}$. Or $CQ = AP$ et donc aussi $CP = AQ$ donc $\frac{EP}{PB} = \frac{AP}{PC} = \frac{CQ}{AQ} = \frac{FQ}{BQ}$ et on conclut par la réciproque du théorème de Thalès.

2 Exercices divers

– Chasse aux angles –

Exercice 1

Soit $ABCD$ un trapèze non rectangle, tel que (AB) parallèle à (CD). Soit P un point sur $[BC]$. La parallèle à (AP) passant par C coupe $[AD]$ en Q, la parallèle à (DP) passant par B coupe $[AD]$ en R. Montrer que $Q = R$.

Exercice 2 (Premier théorème de Miquel)
Soient Γ_1 et Γ_2 deux cercles de centres respectifs O_1 et O_2, s'intersectant en deux points X et Y. Soit A un point de Γ_1 distinct de X et Y, on note B l'intersection de (AY) et Γ_2. Montrer que les triangles XO_1O_2 et XAB sont semblables.

Exercice 3
Soient Γ et Γ' deux cercles tangents en T, Γ' étant à l'intérieur de Γ. Soit B un point de Γ' autre que T, on note M et N les points d'intersection de la tangente à Γ' en B avec Γ. Montrer que : $\widehat{BTM} = \widehat{BTN}$.

Exercice 4
Soit ABC un triangle, Γ son cercle circonscrit. La tangente à Γ en A coupe (BC) en D. La bissectrice de $\widehat{CDA}$ coupe (AB) en E et (AC) en F. Montrer que : $AE = AF$.

Exercice 5
Soit Γ un cercle de centre O, A et B deux points de Γ tels que : $AB > AO$. La bissectrice de $\widehat{OAB}$ recoupe le cercle Γ en un point C. Soit D le deuxième point d'intersection du cercle circonscrit à OCB avec (AB). Montrer que le triangle ADO est isocèle en A.

– Autour de l'orthocentre –

Exercice 6
Soit ABC un triangle, A', B' et C' les pieds des hauteurs issues respectivement de A, B et C et H l'orthocentre du triangle ABC.

1. Montrer que les quadrilatères $ABA'B'$, $BCB'C'$, $CAC'A'$, $AB'HC'$, $BA'HC'$ et $CB'HA'$ sont cycliques.
2. Montrer que les triangles ABC, $AB'C'$, $A'BC'$, $A'B'C$ sont semblables.

Exercice 7
Soit ABC un triangle et B', C' les pieds des hauteurs issues de B et C respectivement. Soient X et Y les points d'intersections de $(B'C')$ avec le cercle circonscrit au triangle ABC. Montrer que : $AX = AY$.

Exercice 8
Soit ABC un triangle, B' et C' les pieds des hauteurs issues de B et C respectivement et O le centre du cercle circonscrit au triangle ABC. Montrer que (AO) et $(B'C')$ sont perpendiculaires.

Exercice 9
Soit ABC un triangle, O le centre de son cercle circonscrit et H son orthocentre. Montrer que : $\widehat{BAO} = \widehat{CAH}$.

Exercice 10
Soit ABC un triangle, A', B' et C' les pieds des hauteurs issues respectivement de A, B et C. Montrer que le centre du cercle inscrit au triangle $A'B'C'$ est l'orthocentre du triangle ABC.

Exercice 11
Soit ABC un triangle, H son orthocentre, O le centre de son cercle circonscrit, M_A, M_B, M_C les milieux respectifs des côtés $[BC], [AC]$ et $[AB]$ et A', B', C' les pieds des hauteurs issues respectivement de A, B, C.

1. Montrer que les symétriques de H par rapport à A', B', C' appartiennent au cercle circonscrit au triangle ABC.
2. Montrer que les symétriques de H par rapport à M_A, M_B, M_C appartiennent au cercle circonscrit du triangle ABC.

Bonus :

3. Montrer que l'intersection de (OA) et du cercle circonscrit au triangle ABC est le symétrique de H par rapport à M_A.
4. En déduire que : $AH = 2OM_A$.

– Autour du pôle Sud –

On se propose dans cette partie d'explorer les propriétés classiques du pôle Sud. Le cadre est le suivant : soit ABC un triangle, Γ son cercle circonscrit et S le pôle Sud de A.

Exercice 12 (Pôle Sud)
Montrer que la bissectrice intérieure de $\widehat{BAC}$ et la médiatrice de $[BC]$ s'intersectent sur le cercle Γ.

On appelle ce point d'intersection S *pôle Sud* de A.

Exercice 13 (Pôle Nord)
Montrer que la bissectrice extérieure de $\widehat{BAC}$ et la médiatrice de $[BC]$ s'intersectent sur le cercle Γ.

On appelle ce point d'intersection N *pôle Nord* de A.

Exercice 14
Montrer que la tangente en S à Γ est parallèle à (BC).

Exercice 15 (Cercle antarctique)

1. Montrer que les points B, C, I, I_A sont cocycliques, où I est le centre du cercle inscrit à ABC et I_A le centre du cercle exinscrit relatif à A.
2. Montrer que S est le centre du cercle passant par B, C, I, I_A.

   On appelle ce cercle *cercle antarctique* relatif à A.

Exercice 16 (Cercle arctique)

1. Montrer que les points B, C, I_B, I_C sont cocycliques.
2. Montrer que N est le centre du cercle passant par B, C, I_B, I_C.

Exercice 17
Soit D le point d'intersection de (AI) et (BC). Montrer que : $SA \cdot SD = SI^2$.

– Pour les plus rapides –

Exercice 18
Soit ABC un triangle, le point D appartient à $[AC]$ et vérifie $BD = CD$. Un droite parallèle à (BD) coupe $[BC]$ en E et coupe (AB) en F. Le point d'intersection des droites (AE) et (BD) est G. Montrer que : $\widehat{BCG} = \widehat{BCF}$.

Exercice 19 (Problème 1, EGMO 2017)
Soit $ABCD$ un quadrilatère convexe tel que $\widehat{DAB} = \widehat{BCD} = 90$ et $\widehat{ABC} > \widehat{CDA}$. Soient Q et R des points de $[BC]$ et $[CD]$ respectivement, tels que (QR) coupe les droites (AB) et (AD) en P et S respectivement et tels que $PQ = RS$. Soit M le milieu de $[BD]$ et N celui de $[QR]$. Montrer que A, N, M, C sont cocycliques.

Exercice 20 (Problème 2, BxMO 2011)
Soit ABC un triangle et I le centre de son cercle inscrit. Les bissectrices $(AI), (BI), (CI)$ coupent $[BC], [CA], [AB]$ en D, E, F respectivement. La médiatrice du segment $[AD]$ coupe les droites (BI) et (CI) en M et N. Montrer que A, I, M, N sont cocycliques.

Exercice 21 (Problème 3, JBMO 2010)
Soit ABC un triangle non isocèle. Les bissectrices des angles $\widehat{BAC}$ et $\widehat{ABC}$ coupent $[BC]$ et $[AC]$ respectivement en L et K. La médiatrice de $[BK]$ coupe (AL) en M. La parallèle à (MK) passant par L coupe (BK) en N. Montrer que : $LN = NA$.

Exercice 22 (Problème 3, JBMO 2017)
Soit ABC un triangle non isocèle, Γ son cercle circonscrit et O le centre de Γ. Soit M le milieu de $[BC]$ et D le point de Γ tel que (AD) et (BC) sont perpendiculaires. Soit T le point tel que $BDCT$ est un parallélogramme et Q un point du même côté de (BC) que A tel que $\widehat{BQM} = \widehat{BCA}$ et $\widehat{CQM} = \widehat{CBA}$. La droite (AO) coupe Γ en $E \neq A$. Le cercle circonscrit au triangle ETQ coupe Γ en $X \neq E$. Montrer que A, M, X sont alignés.

– Solutions des exercices –

Solution de l'exercice 1
On introduit le point d'intersection S entre les droites (AD) et (BC).
D'après le théorème de Thalès dans le triangle SQC, on a :

$$\frac{SA}{SQ} = \frac{SP}{SC} \Leftrightarrow SA \times SC = SP \times SQ.$$

Puis, d'après le théorème de Thalès dans le triangle SPD, on a :

$$\frac{SB}{SP} = \frac{SR}{SD} \Leftrightarrow SB \times SD = SR \times SP.$$

Ainsi, $\frac{SQ}{SR} = \frac{SA \times SC}{SB \times SD}$. D'après le théorème de Thalès dans le triangle SDC, on a donc :

$$\frac{SA}{SD} = \frac{SB}{SC} \Leftrightarrow \frac{SA \times SC}{SD \times SB} = 1.$$

On en conclut que $SR = SQ$, donc que $Q = R$.

Solution de l'exercice 2
Procédons par chasse aux angles, afin de montrer que les triangles XO_1O_2 et XAB ont les mêmes angles. En posant : $\alpha = \widehat{XAY}$, on trouve : $\widehat{XO_1Y} = 2\alpha$ grâce au théorème de l'angle au centre. Or, la figure (excepté les points A et B) étant symétrique par rapport à l'axe (O_1O_2), on en déduit que : $\widehat{XO_1O_2} = \alpha = \widehat{XAY}$. De même, on montre que : $\widehat{XO_2O_1} = \widehat{XBA}$, ce qui conclut.

Remarque 4.2.1.
On remarque au passage que, pour deux cercles de centres O_1 et O_2 s'intersectant en deux points X et Y, les droites (O_1O_2) et (XY) sont perpendiculaires.

Solution de l'exercice 3
Soit P le point d'intersection des tangentes à Γ' en B et en T, supposons sans perte de généralité que les points P, M, B, N sont alignés dans cet ordre. En appliquant le cas limite de l'angle inscrit dans Γ et Γ', on a :

$$\widehat{BTM} = \widehat{BTP} - \widehat{MTP} = \widehat{PBT} - \widehat{MNT} = \widehat{BTN}.$$

Solution de l'exercice 4

Soient α, β, γ les angles du triangle ABC (notation générique). On suppose sans perte de généralité que D, B, C sont alignés dans cet ordre ($\beta > \gamma$), quitte à intervertir B et C.
Par le cas limite de l'angle inscrit : $\widehat{BAD} = \gamma$, d'où : $\widehat{CDA} = \widehat{ABC} - \widehat{BAD} = \beta - \gamma$. Il vient alors :

$$\widehat{AEF} = \widehat{EAD} + \widehat{ADE} = \gamma + \frac{\beta - \gamma}{2} = \frac{\beta + \gamma}{2} = 90° - \frac{\alpha}{2}.$$

Ainsi, le triangle AEF a pour angles : $\widehat{EAF} = \alpha$ et : $\widehat{AEF} = \widehat{AFE} = 90° - \frac{\alpha}{2}$, d'où : $AE = AF$.

Solution de l'exercice 5

On cherche à calculer les angles du triangle ADO à partir d'un ou plusieurs angles de référence. Pour cela, notons α l'angle $\widehat{DAO}$. Comme dans l'exercice précédent, il suffit pour conclure d'avoir : $\widehat{ADO} = 90° - \frac{\alpha}{2}$.
Par cocyclicité des points B, C, D, O, on a : $\widehat{ADO} = \widehat{BCO}$. Le point O étant le centre du cercle circonscrit à ABC : $\widehat{ACO} = \widehat{CAO} = \frac{\alpha}{2}$, et par l'angle au centre : $\widehat{BCA} = \frac{1}{2}\widehat{BOA} = 90° - \alpha$. Finalement :

$$\widehat{ADO} = \widehat{BCO} = \widehat{ACO} + \widehat{BCA} = 90° - \frac{\alpha}{2}.$$

Solution de l'exercice 6

1. On a $\widehat{B'BC} = 90 = \widehat{C'CB}$ donc les points C', B', C et B sont cocycliques par la réciproque du théorème de l'angle inscrit. De même $A'B'AB$ et $A'C'AC$ sont cycliques.

   De même, $\widehat{HB'} = \widehat{BB'A} = 90 = 180 - 90 = 180 - \widehat{CC'A} = 180 - \widehat{HC'A}$ donc $AB'HC'$ est cyclique par la réciproque du théorème de l'angle inscrit. De même, $BA'HC'$ et $CA'HB'$ sont cycliques.
2. D'après ce qui a été établi précédemment, $B'C'BC$ est un quadrilatère cyclique. Donc $\widehat{C'B'A} = 180 - \widehat{C'B'C}$ car A, B', C sont alignés, et donc par le théorème de l'angle inscrit $\widehat{C'B'A} = 180 - \widehat{C'B'C} = \widehat{C'BC} = \widehat{ABC}$. Donc les triangles $AB'C'$ et ABC ont deux paires d'angles égaux, ils sont semblables. De la même façon, $A'BC'$ et $A'B'C$ sont semblables à ABC.

Solution de l'exercice 7

On va se servir du fait (établi dans les exercices précédents) que $AB'C'$ et ABC sont semblables. Donc $\widehat{B'C'A} = \widehat{BCA}$. Par le théorème de l'angle inscrit $\widehat{YXA} = \widehat{YBA}$. De plus $\widehat{ABY} = \widehat{C'BY} = 180 - \widehat{BC'Y} - \widehat{C'YB}$. Toujours par le théorème de l'angle inscrit, $\widehat{C'YB} = \widehat{XYB} = 180 - \widehat{XCB}$, et on a vu que $\widehat{BC'Y} = \widehat{B'C'A} = \widehat{ACB}$. D'où

$$\widehat{ABY} = 180 - \widehat{ACB} - (180 - \widehat{XCB}) = \widehat{XCB} - \widehat{ACB} = \widehat{XCA}$$

Le théorème de l'angle inscrit donne $\widehat{XCA} = \widehat{XYA}$. Mis bout-à-bout, on a donc

$$\widehat{AXY} = \widehat{ABY} = \widehat{ACX} = \widehat{AYX}$$

donc le triangle XAY est isocèle en A, ce que nous voulions.

Solution de l'exercice 8

On peut avoir ce résultat rapidement en utilisant le concept d'anti-parallèle, mais nous allons tout de même présenter une preuve élémentaire ici. On utilise les résultats établis aux exercices précédents. Soit D l'intersection de $(B'C')$ et de (AO). On a alors $\widehat{DAC'} = \widehat{OAB} = \widehat{HAC} = 90 - \widehat{ACB} = 90 - \widehat{BCB'} = 90 - (180 - \widehat{BC'B'}) = 90 - \widehat{AC'D}$ donc $\widehat{C'DA} = 90$ et (AO) et $(B'C')$ sont bien perpendiculaires.

Solution de l'exercice 9

Comme O est centre du cercle circonscrit à ABC, donc $AO = OB$ donc $\widehat{OAB} = \widehat{OBA}$. Comme la somme des angles d'un triangle fait 180, on a $\widehat{BOA} = 180 - \widehat{ABO} - \widehat{BAO} = 180 - 2\widehat{BAO}$. Le théorème de l'angle au centre nous donne $\widehat{BCA} = \frac{1}{2}\widehat{BOA} = 90 - \widehat{BAO}$. Si on introduit D le pied de la hauteur issue de A, on obtient, comme H est sur $[AD]$:

$$\widehat{HAC} = \widehat{DAC} = 90 - \widehat{DCA} = 90 - \widehat{BCA} = \widehat{BAO}$$

ce qui conclut.

Solution de l'exercice 10

Montrons que $\widehat{B'A'H} = \widehat{HA'C'}$. Pour cela on utlise notamment que les triangles $A'BC'$ et $A'B'C$ sont semblables à ABC, et donc que $\widehat{BA'C'} = \widehat{BAC} = \widehat{B'A'C}$. On a alors $\widehat{B'A'H} = 90 - \widehat{B'A'C} = 90 - \widehat{BAC} = 90 - \widehat{BA'C'} = \widehat{HA'C'}$ donc H est sur la bissectrice de $\widehat{B'A'C'}$. De même H est sur la bissectrice de $\widehat{A'B'C'}$ et de $\widehat{A'C'B'}$ ce qui fait de H le centre du cercle inscrit de $A'B'C'$, comme voulu.

Solution de l'exercice 11

1. Comme les points A, B', C', H sont cocycliques, on a $\widehat{CAB} = 180 - \widehat{B'HC'} = 180 - \widehat{BDC}$. De plus, la symétrie centrale par rapport à A' envoie H sur H_A le symétrique de H par rapport à BC. Donc $\widehat{BHC} = \widehat{BH_AC}$ avec H_A le symétrique de H par rapport à BC. Ainsi $\widehat{CAB} = 180 - \widehat{BH_AC}$ donc A, B, H_A, C sont cocycliques. De même H_B et H_C les symétriques de H par rapport à B' et C' sont sur le cercle circonscrit au triangle ABC.
2. Soit H_{M_A} le symétrique de H par rapport à M_A. Comme M_A est le milieu de $[BC]$, alors $BH_{M_A}CH$ est un parallélogramme donc $\widehat{BHC} = \widehat{BH_{M_A}C}$. De même que dans le 1) $\widehat{BHC} = 180 - \widehat{BAC}$ donc A, B, H_{M_A}, C sont cocycliques. De même H_{M_B} et H_{M_C} les symétriques de H par rapport à M_B et M_C sont sur le cercle circonscrit au triangle ABC.

Bonus :

3. Soit $\tilde{A}$ l'intersection entre (OA) et le cercle circonscrit à ABC. $O\tilde{A}$ est alors un diamètre du cercle donc $\widehat{AC\tilde{A}} = 90$ donc $(\tilde{A}C)$ est parallèle à $(B'H)$. De même,$\widehat{AB\tilde{A}} = 90$ donc $(\tilde{A}B)$ est parallèle à $(C'H)$.
   Donc $HB\tilde{A}C$ est un parallélogramme donc l'intersection entre BC et $H\tilde{A}$ est M_A milieu de $[BC]$ et milieu de $[H\tilde{A}]$. Donc $\tilde{A}$ est le symétrique de H par rapport à M_A.

4. Les droites OM_A et AH sont parallèles donc d'après le théorème de Thalès dans le triangle $AH\tilde{A}$, on a : $\frac{AH}{OM_A} = \frac{\tilde{A}H}{\tilde{A}M_A} = 2$ d'où $AH = 2OM_A$.

Solution de l'exercice 12
Soit S le point d'intersection de la médiatrice de $[BC]$ et Γ, on va montrer que S est sur la bissectrice de $\widehat{BAC}$. Le triangle BCS est isocèle en S, d'où : $\widehat{BCS} = \widehat{CBS}$. Par le théorème de l'angle inscrit : $\widehat{BCS} = \widehat{BAS}$, et : $\widehat{CBS} = \widehat{CAS}$. Ainsi : $\widehat{BAS} = \widehat{CAS}$, d'où (AS) bissectrice de $\widehat{BAC}$.

Solution de l'exercice 13
Définissons N comme le point d'intersection de la médiatrice de $[BC]$ et du cercle Γ, montrons que (AN) est la bissectrice extérieure de $\widehat{BAC}$. Soit O le centre de Γ. La médiatrice de $[BC]$ correspond à (OS), ce qui fait de N le point diamétralement opposé à S sur le cercle Γ. Par conséquent : $\widehat{SAN} = 90°$, ce qui termine car les bissectrices intérieure et extérieure forment un angle droit entre elles.

Solution de l'exercice 14
Soit D le point d'intersection de (AS) avec (BC). L'angle formé entre les droites (AS) et (BC) est : $\widehat{BDA} = \widehat{DAC} + \widehat{DCA} = \frac{\alpha}{2} + \gamma$. Celui formé entre la tangente en S et (AS) est, d'après le cas limite de l'angle inscrit : $\widehat{ACS} = \widehat{ACB} + \widehat{BCS} = \gamma + \frac{\alpha}{2}$. Finalement, par angles correspondants, la tangente en S et la droite (BC) sont parallèles.

Solution de l'exercice 15

1. Les bissectrices intérieure et extérieure de $\widehat{ABC}$ forment un angle droit entre elles, d'où : $\widehat{IBI_A} = 90°$. De même en C : $\widehat{ICI_A} = 90°$. Ainsi, les points B, C, I, I_A appartiennent au cercle de diamètre $[II_A]$.
2. Il suffit de montrer que S est le centre du cercle circonscrit à BIC, ce qu'on établit par chasse aux angles. Dans le triangle BIS : $\widehat{IBS} = \widehat{IBC} + \widehat{CBS} = \frac{\beta}{2} + \frac{\alpha}{2}$, et : $\widehat{BIS} = \widehat{ABI} + \widehat{BAI} = \frac{\beta}{2} + \frac{\alpha}{2}$. On a donc BIS isocèle en S et de même, CIS isocèle en S. Le point S est équidistant de B, I et C, il s'agit donc du centre du cercle antarctique.

Solution de l'exercice 16

1. Les bissectrices intérieure et extérieure d'un angle forment un angle droit entre elles, d'où : $\widehat{I_BBI_C} = \widehat{I_BCI_C} = 90°$. Ainsi, les points B, C, I_B, I_C appartiennent au cercle de diamètre $[I_BI_C]$.
2. Le point N est d'une part aligné avec I_B, I_C sur la bissectrice extérieure de $\widehat{BAC}$, d'autre part sur la médiatrice du segment $[BC]$. D'après la question précédente, le centre du cercle passant par B, C, I_B, I_C est le milieu de $[I_BI_C]$, il est ainsi d'une part sur (I_BI_C) et d'autre part sur la médiatrice de $[BC]$. Or, deux droites (ni confondues ni parallèles) ne se coupent qu'en un et un seul point. Finalement, N est le centre du cercle passant par B, C, I_B, I_C.

Solution de l'exercice 17
D'après l'exercice précédent (S centre du cercle antarctique), l'énoncé revient à montrer que : $SA \cdot SD = SB^2$. On a : $\widehat{SBD} = \widehat{SAC} = \widehat{SAB}$, d'où les triangles SAB et SBD semblables. Il vient : $\frac{SA}{SB} = \frac{SB}{SD}$, ce qui conclut.

Solution de l'exercice 18

Soit H l'intersection de (EF) et de $[AC]$. Montrons que les triangles FHC et CDG sont semblables.

Les triangles BDC et EHC sont semblables (par exemple d'après le théorème de Thalès) donc $EH = HC$. (GD) et (EH) sont parallèles donc le théorème de Thalès donne $\frac{GD}{EH} = \frac{AD}{AH}$. (BD) et (FH) sont parallèles donc le théorème de Thalès donne $\frac{AD}{AH} = \frac{BD}{FH}$. en combinant toutes ces égalités de rapports :

$$\frac{GD}{HC} = \frac{GD}{EH} = \frac{AD}{AH} = \frac{BD}{FH} = \frac{CD}{FH}$$

De plus $\widehat{GDC} = \widehat{FHC}$ donc les triangles GDC et FHC sont semblables. On conclut alors par une chasse aux angles

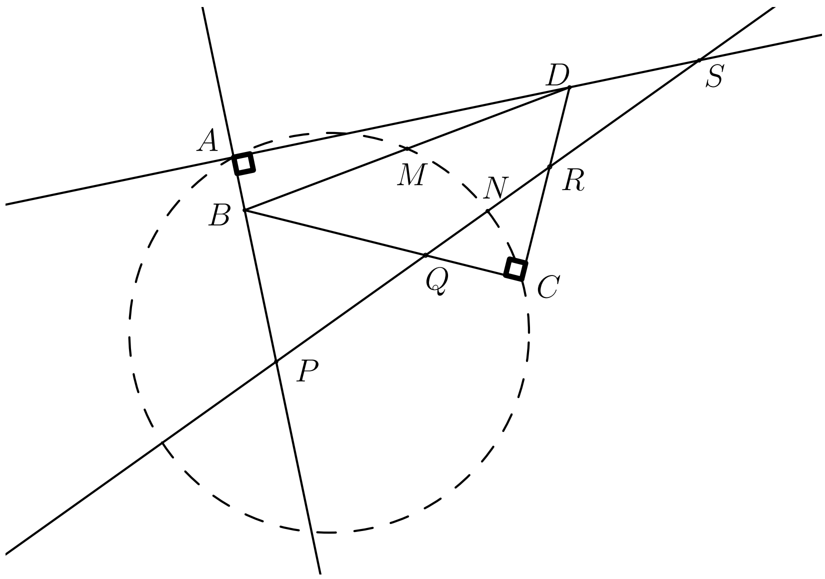
$$\widehat{BCF} = \widehat{ECF} = 180 - \widehat{CEF} - \widehat{EFH} = \widehat{HEC} - \widehat{HFC}$$

Les triangles GDC et CHF étant semblables, $\widehat{EFC} = \widehat{GCD}$. Donc

$$\widehat{BCF} = \widehat{HEC} - \widehat{HFC} = \widehat{HCB} - \widehat{GCD} = \widehat{GCB}$$

ce qui conclut.

Solution de l'exercice 19



On a : $\widehat{DRS} = \widehat{CRQ}$ (angles opposés) $= \widehat{RCN}$ car le triangle CQR est rectangle et N est le milieu de son hypoténuse donc le centre de son cercle circonscrit.De la même manière, on a $\widehat{BDC} = \widehat{DCM}$ car BCD est un triangle rectangle et M est le milieu de son hypoténuse.

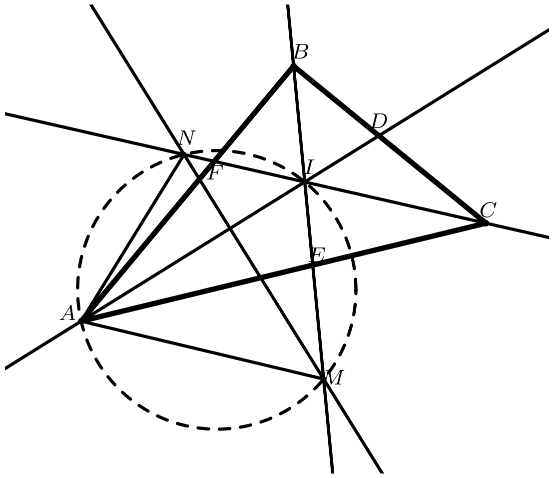
Ainsi, $\widehat{NCM} = \widehat{DCM} - \widehat{RCN}$.

Dans le triangle rectangle APS, comme N est le milieu de QR et $PQ = RS$, N est le milieu de l'hypoténuse donc le triangle ANS est isocèle donc $\widehat{PSA} = \widehat{SAN}$.

Dans le triangle rectangle BAD, M est le milieu de l'hypoténuse donc le triangle MAD est isocèle. Donc $\widehat{MAD} = \widehat{BDA}$. Comme les points A, D et S sont alignés, on a $\widehat{BDA} + \widehat{RDB} + (180 - \widehat{DRS} - \widehat{DSR}) = 180$ donc $\widehat{BDA} = \widehat{DRS} + \widehat{DSR} - \widehat{RDB}$.

Ainsi, $\widehat{NAM} = \widehat{NAD} - \widehat{MAD} = \widehat{MAD} + \widehat{CDB} - \widehat{DRS} - \widehat{MAD} = \widehat{CDB} - \widehat{DRS} = \widehat{DCM} - \widehat{RCN} = \widehat{NCM}$ car le triangle MDC est isocèle (donc $\widehat{CDB} = \widehat{MCD}$). Donc les points A, M, N et C sont cocycliques.

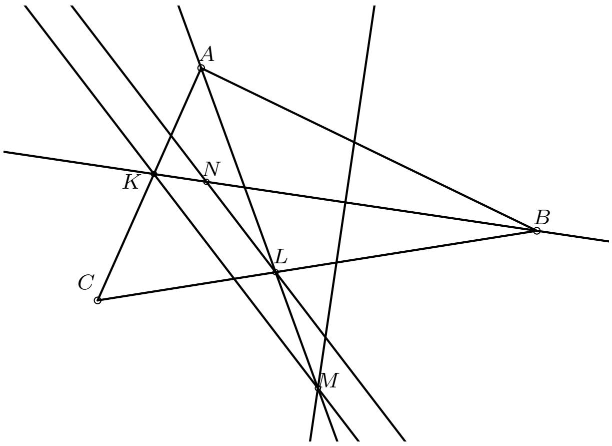
Solution de l'exercice 20



On constate que N est le pôle sud de ADC et M est le pôle sud de ABD. D'après les propriétés du pôle sud, les points A, D, C, N sont cocycliques et les points A, B, D, M sont cocycliques.

Ainsi $\widehat{AMB} = \widehat{ADB}$ et $\widehat{ANC} = \widehat{ADC}$. Donc $\widehat{AMI} + \widehat{ANI} = \widehat{ADB} + \widehat{ADC} = 180°$, de sorte que A, N, I, M sont cocycliques.

Solution de l'exercice 21



M est le pôle sud du triangle AKB. Donc d'après les propriétés su pôle sud, les points A, K, M, B sont cocycliques. Ainsi $\widehat{KMA} = \widehat{KBA}$ (angles inscrits). Comme BK est la bissectrice de $\widehat{ABC}$, alors $\widehat{KBA} = \widehat{KBC}$. De plus, comme LN est parallèle à MK, $\widehat{KMA} = \widehat{NLA}$.

Ainsi N, L, B, A sont cocycliques donc $\widehat{NAL} = \widehat{NBM} = \widehat{NLA}$, ce qui montre que $NL = NA$.

Solution de l'exercice 22

Cet exercice nécessite de maîtriser les résultats établis précédemment sur l'orthocentre. Soit

H l'orthocentre du triangle. Le symétrique de H par rapport à M est E, de telle sorte que $HCEB$ est un parallélogramme. $BD = BH$ et $\widehat{CBD} = \widehat{CBH}$ donc les parallélogrammes $CTBD$ et $HBEC$ sont symétriques par rapport à (OM). Comme H est symétrique de D par rapport à (BC), T est symétrique de E par rapport à (BC). Donc (ET) et (BC) sont perpendicualires. Soit X' l'intersection de Γ avec (AM). On a $\widehat{CX'M} = \widehat{CBA} = \widehat{CQM}$ et de même $\widehat{MX'B} = \widehat{MQB}$ donc X' est symétrique de Q par rapport à X', donc (QX') et (BC) sont parallèles. Donc $[QT]$ et $[EX']$ sont symétriques par rapport à (BC), donc $ETQX'$ est trapèze isocèle et X' appartient au cerlce Γ et au cercle circonscrit au triangle ETQ, donc $X = X'$ et X est sur (AM).

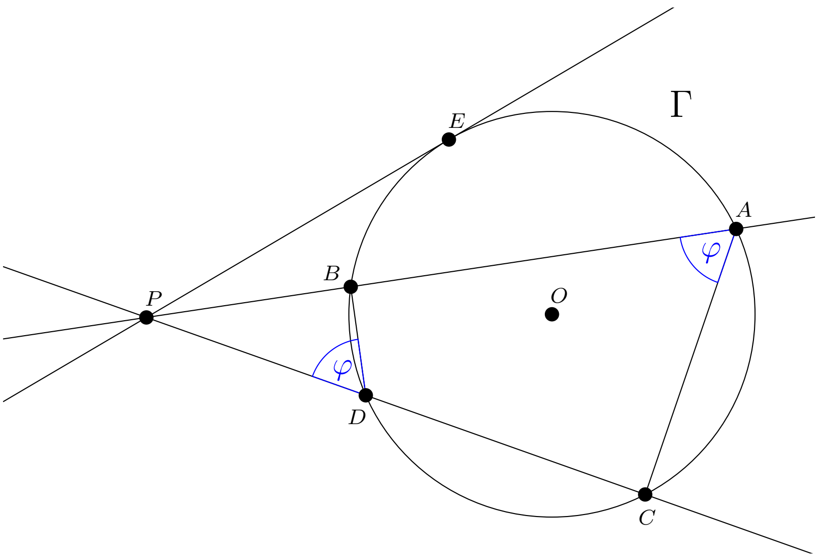
3 Puissance d'un point et axes radicaux

L'objet de ce cours est d'introduire deux notions fondamentales en géométrie du cercle : celle de puissance d'un point par rapport à un cercle, et à partir d'elle celle d'axe radical. Nous nous proposons d'en étudier les principales propriétés, et d'appliquer ces savoirs fraîchement acquis à travers des exercices brassant l'ensemble des acquis de la période.

En classe, seuls les exercices 4 et 9 n'ont pas été abordés, le dernier ayant été proposé à chercher aux élèves les plus rapides.

– Puissance d'un point –

Soient un cercle Γ de centre O et de rayon r et un point P. On considère trois droites passant par P et coupant le cercle Γ : la première le coupe en A et B, la deuxième en C et D, et la troisième est une tangente au cercle, qu'elle ne coupe donc qu'en un point, E.



Théorème 4.3.1 (Puissance d'un point par rapport à un cercle)**.**
On a alors : $PA \cdot PB = PC \cdot PD = PE^2 = PO^2 - r^2$.

Démonstration. Par chasse aux angles, on marque les angles φ et on constate que les triangles PAC et PDB sont semblables. Ainsi, $\frac{PA}{PC} = \frac{PD}{PB}$, d'où le résultat. Cet argument vaut aussi pour le cas de la tangente. Enfin, lorsqu'on considère la droite PO, on a toujours la même égalité pour $(PO - r)(PO + r)$, ce qui conclut. $\square$

Ainsi, la quantité $PA \cdot PB$ ne dépend pas de la droite passant par P avec laquelle on intersecte Γ. On appelle ce produit la *puissance* du point P par rapport au cercle Γ, notée $\mathcal{P}_\Gamma(P)$.

Remarque 4.3.2.
L'usage veut qu'on travaille avec des mesures algébriques, en accord avec le signe de l'expression $PO^2 - r^2$. Ainsi, la puissance de P par rapport à Γ est positive si P est à l'extérieur du cercle, nulle si P est dessus et négative si P est à l'intérieur.

Remarque 4.3.3.
Le théorème 4.3.1 admet une réciproque fort utile : soient deux droites (AB) et (CD) s'intersectant en P, si $PA \cdot PB = PC \cdot PD$ (en mesures algébriques) alors A,B,C,D sont cocyliques. La puissance d'un point par rapport à un cercle fournit donc une caractérisation pour la cocyclicité de 4 points.

Exercice 1
Dans un triangle ABC, la hauteur issue de C coupe le cercle de diamètre $[AB]$ en M et N. La hauteur issue de B coupe le cercle de diamètre $[AC]$ en P et Q. Montrer que les points M,N,P,Q sont cocyliques.

Exercice 2
Soit ABC un triangle, Γ son cercle circonscrit et S le pôle Sud de A. On note D le point d'intersection de (AS) avec (BC). Une droite passant par S recoupe (BC) en E et Γ en F. Montrer que $SA \cdot SD = SE \cdot SF$.

Exercice 3
Soit $ABCD$ un quadrilatère inscrit dans un cercle Γ. La parallèle à (BC) passant par D coupe (AC) en P, (AB) en Q et recoupe Γ en R. La parallèle à (AB) passant par D coupe (AC) en S, (BC) en T et recoupe Γ en U. Montrer que $\frac{PQ}{QR} = \frac{TU}{ST}$.

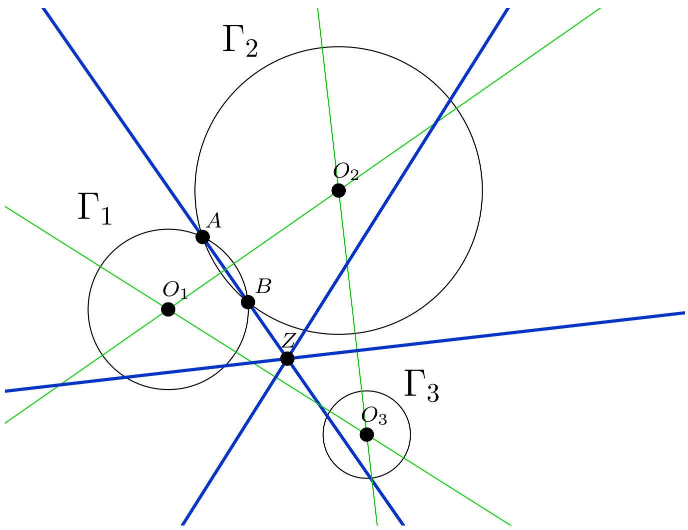
Exercice 4
Soit $ABCD$ un parallélogramme, H l'orthocentre du triangle ABC. La parallèle à (AB) passant par H coupe (BC) en P et (AD) en Q. La parallèle à (BC) passant par H coupe (AB) en R et (CD) en S. Montrer que P,Q,R,S sont cocycliques.

– Axes radicaux –

On considère deux cercles Γ_1, de centre O_1, et Γ_2, de centre O_2. Quel est alors le lieu des points ayant la même puissance par rapport à Γ_1 et Γ_2 ? À l'aide de l'expression $PO^2 - r^2$ et du théorème de Pythagore, on montre qu'il s'agit d'une droite perpendiculaire à O_1O_2, appelée *axe radical* des cercles Γ_1 et Γ_2.

Remarque 4.3.4.
Si les cercles Γ_1 et Γ_2 s'intersectent en deux points A et B, alors leur axe radical est la droite (AB), dont on a vu en TD qu'elle était perpendiculaire à la droite des centres. On a aussi le cas limite : si Γ_1 et Γ_2 sont tangents entre eux, alors leur axe radical et leur tangente commune.

Théorème 4.3.5 (Axes radicaux)**.**
Soient Γ_1, Γ_2 et Γ_3 trois cercles. Alors les trois axes radicaux obtenus deux à deux sont soit concourants, soit parallèles (éventuellement confondus). De plus, les axes radicaux sont parallèles si et seulement si les centres des trois cercles sont alignés.



En vert, les droites reliant les centres. En bleu, les trois axes radicaux concourants.

Démonstration. Supposons que les axes radicaux de Γ_1 avec Γ_2 et de Γ_2 avec Γ_3 ne sont pas parallèles. Soit alors P leur point d'intersection. On a $\mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_2}(P)$ et $\mathcal{P}_{\Gamma_2}(P) = \mathcal{P}_{\Gamma_3}(P)$, d'où $\mathcal{P}_{\Gamma_3}(P) = \mathcal{P}_{\Gamma_1}(P)$. Donc P est, par définition sur le troisième axe radical.

Supposons maintenant que les axes radicaux de Γ_1 avec Γ_2 et de Γ_2 avec Γ_3 sont parallèles. On a alors $(O_1O_2) /\!/ (O_2O_3)$ (deux droites perpendiculaires à une même droite sont parallèles entre elles), d'où les points O_1, O_2, O_3 alignés. Dès lors, l'axe radical de Γ_3 avec Γ_1 est aussi perpendiculaire à la droite des trois centres, donc parallèle aux deux autres. Réciproquement, l'alignement des centres O_1, O_2, O_3 implique que les axes radicaux sont parallèles entre eux, de direction perpendiculaire à la droite des centres. $\square$

Exercice 5
Soient deux cercles Γ_1 et Γ_2 s'intersectant en deux points A et B. On considère une tangente commune à ces deux cercles, tangente en P à Γ_1 et en Q à Γ_2. Montrer que (AB) coupe $[PQ]$ en son milieu.

Exercice 6
Soient deux cercles Γ_1 et Γ_2 tangents extérieurement en un point T. On considère une tangente commune à ces deux cercles, tangente en P à Γ_1 et en Q à Γ_2. Montrer que le triangle PQT est rectangle.

Exercice 7
Soit ABC un triangle, H son orthocentre. Soient M un point quelconque sur le segment $[AB]$ et N un point quelconque sur le segment $[AC]$. On note P et Q les points d'intersection des cercles de diamètres respectifs $[BN]$ et $[CM]$. Montrer que les points P, Q, H sont alignés.

Exercice 8 (cercle d'Euler)
Soit ABC un triangle. On note M_A, M_B, M_C les milieux respectifs des côtés $[BC], [CA], [AB]$, et H_A, H_B, H_C les pieds des hauteurs issues de A, B, C respectivement.

1. Montrer que les six points $M_A, M_B, M_C, H_A, H_B, H_C$ sont cocycliques.
2. Soient A', B', C' les milieux respectifs des segments $[AH], [BH], [CH]$, où H est l'orthocentre de ABC. Montrer que A', B', C' sont cocycliques avec les six points mentionnés ci-dessus.

Exercice 9
Soient quatre points cocycliques A, B, C, D. Quel est le lieu des points M tels que le cercle circonscrit à MAB et le cercle circonscrit à MCD soient tangents ?

– Solutions des exercices –

Solution de l'exercice 1
Soit H l'orthocentre de ABC, H_A le pied de la hauteur issue de A. Par orthogonalité, H_A appartient aux cercles de diamètre $[AB]$ et $[AC]$. La puissance de H_A par rapport à ces cercles fournit respectivement : $HM \cdot HN = HA \cdot HH_A$, et : $HP \cdot HQ = HA \cdot HH_A$, d'où : $HM \cdot HN = HP \cdot HQ$. Par la réciproque de la puissance d'un point, on en déduit M, N, P, Q cocycliques.

Solution de l'exercice 2
Par le théorème 4.3.1, l'exercice revient à montrer que les points A, D, E, F sont cocycliques. On peut pour cela procéder par chasse aux angles à partir des angles α, β, γ du triangle ABC. D'une part : $\widehat{AFE} = \widehat{ACS} = \widehat{ACB} + \widehat{BAS} = \gamma + \frac{\alpha}{2}$, d'autre part : $\widehat{ADB} = \widehat{ACD} + \widehat{DAC} = \gamma + \frac{\alpha}{2}$. Ainsi : $\widehat{AFE} + \widehat{ADE} = 180°$, ce qui conclut.

Solution de l'exercice 3
Pour calculer $\frac{PQ}{QR}$ (resp. $\frac{TU}{ST}$), on va passer par la longueur intermédiaire QA (resp. TC).

$$\begin{aligned}
\frac{PQ}{QR} &= \frac{PQ}{QA} \cdot \frac{QA}{QR} \\
&= \frac{BC}{BA} \cdot \frac{QD}{QB} \quad \text{(les triangles } ABC \text{ et } AQP \text{ sont semblables par Thalès, } QA \cdot QB = QD \cdot QR \text{ par pui} \\
&= \frac{BC}{BA} \cdot \frac{TB}{TD} \quad (QBTD \text{ est un parallélogramme}) \\
&= \frac{TC}{TS} \cdot \frac{TU}{TC} \quad \text{(les triangles } ABC \text{ et } STC \text{ sont semblables par Thalès, } TB \cdot TC = TD \cdot TU \text{ par puiss} \\
&= \frac{TU}{TS}.
\end{aligned}$$

Solution de l'exercice 4
Par la réciproque de la puissance d'un point, il suffit de montrer que : $HP \cdot HQ = HR \cdot HS$. Par chasse aux angles alternes-internes de la figure, il vient que les triangles ARH, AQH,

CPH, HSC sont semblables entre eux (et deux par deux isométriques). Fort de cela, on peut reprendre la stratégie de l'exercice précédent :

$$\begin{aligned}\frac{HQ}{HR} &= \frac{HQ}{HA} \cdot \frac{HA}{HR} \\ &= \frac{HS}{HC} \cdot \frac{HC}{HP} \quad \text{(les triangles } ABC \text{ et } AQP \text{ sont semblables par Thalès, } QA \cdot QB = QD \cdot QR \text{ par pu} \\ &= \frac{HS}{HP}.\end{aligned}$$

Solution de l'exercice 5
Soit M le point d'intersection de (AB) et (PQ). La puissance de M par rapport à Γ_1 est MP^2, celle par rapport à Γ_2 est MQ^2. M est sur l'axe radical (AB) de Γ_1 et Γ_2 (cas de deux cercles s'intersectant en deux points), d'où : $\mathcal{P}_{\Gamma_1}(M) = \mathcal{P}_{\Gamma_2}(M)$. Finalement : $MP = MQ$, M est bien le milieu de $[PQ]$.

Solution de l'exercice 6
Commençons par introduire la tangente commune Δ aux deux cercles en T. D'après l'exercice précédent (cas limite où l'axe radical correspond à Δ), elle coupe le segment $[PQ]$ en son milieu M. Par égalité de longueur des tangentes MP, MT et MQ, le point T est sur le cercle de diamètre $[PQ]$, d'où PQT rectangle en T.

Solution de l'exercice 7
Notons Γ_B le cercle de diamètre $[BN]$, Γ_C celui de diamètre $[CM]$. La droite (PQ) correspond à l'axe radical de Γ_B et Γ_C, il s'agit donc de montrer que H a même puissance par rapport aux deux cercles.
On remarque que les pieds H_B et H_C des hauteurs issues de B et de C vérifient : $H_B \in \Gamma_B$ et : $H_C \in \Gamma_C$. La puissance de H par rapport à Γ_B est alors $HB \cdot HH_B$, celle par rapport à Γ_C est $HC \cdot HH_C$. Par cocyclicité des points B, C, H_B, H_C, alors on a l'égalité : $HB \cdot HH_B = HC \cdot HH_C$, ce qui conclut.

Solution de l'exercice 8
Pour établir les cocyclicités, on va se servir de la réciproque de la puissance d'un point.

1. Puisque B, C, H_B, H_C sont cocycliques sur le cercle de diamètre $[BC]$, alors : $AH_B \cdot AC = AH_C \cdot AB$. En divisant par 2 de part et d'autre, on en déduit : $AH_B \cdot AM_B = AH_C \cdot AM_C$, d'où les points M_B, M_C, H_B, H_C cocycliques. Par le même raisonnement, il vient que M_A, M_C, H_A, H_C sont cocycliques, et de même pour M_A, M_B, H_A, H_B. Il reste à voir pourquoi les trois cercles ainsi formés sont en fait confondus. Si ce n'était pas le cas, par l'absurde, alors on aurait trois cercles $\Gamma_A, \Gamma_B, \Gamma_C$ distincts. Leurs axes radicaux deux à deux seraient : $(M_AH_A) = (BC), (M_BH_B) = (AC), (M_CH_C) = (AB)$. Or ces droites ne sont ni concourantes ni parallèles, ce qui met en défaut le théorème 4.3.5. Ainsi, l'hypothèse était absurde, d'où $M_A, M_B, M_C, H_A, H_B, H_C$ cocycliques sur un même cercle Γ, appelé *cercle d'Euler*.

2. Montrons que A' appartient au cercle d'Euler : on procèdera alors de même pour B' et C'. Par cocyclicté des points B, H, H_A, H_C, on a : $AH_C \cdot AB = AH \cdot AH_A$. En divisant par 2, il vient : $AH_C \cdot AM_C = AA' \cdot AH_A$. Par la réciproque de la puissance d'un point, les points A', H_A, H_C, M_C sont cocycliques, ce qui conclut.

Solution de l'exercice 9
Il s'agit de caractériser les points M qui vérifient la condition de l'énoncé. Soit Z le point d'intersection des droites AB et CD. L'avantage d'introduire ce point est que cela nous permet de connaître tous nos axes radicaux. En effet, pour tout point M, l'axe radical du cercle circonscrit à $ABCD$ et du cercle circonscrit à MAB est la droite AB, l'axe radical du cercle circonscrit à $ABCD$ et du cercle circonscrit à MCD est la droite CD, et l'axe radical du cercle circonscrit à MAB et du cercle circonscrit à MCD passe par M et est concourant aux deux autres axes radicaux (qui se coupent en Z) : c'est donc la droite ZM.

Ainsi, Z appartient aux trois axes radicaux, et donc la puissance de Z est la même par rapport aux trois cercles. Or les cercles circonscrits à MAB et à MCD sont tangents si et seulement si leur axe radical est leur tangente commune en M, autrement dit si et seulement si la droite ZM est leur tangente commune. C'est le cas si et seulement si la puissance de Z par rapport aux cercles circonscrits à MAB et à MCD vaut ZM^2, autrement dit si et seulement si $ZA \times ZB = ZC \times ZD = ZM^2$.

En bref, sachant que les points Z, A, B, C, D sont fixés, le point M satisfait la condition de l'énoncé si et seulement si $ZM = \sqrt{ZA \times ZB}$. Donc le lieu de nos points M est un cercle de centre Z et de rayon $\sqrt{ZA \times ZB}$.

4 Nombres complexes et géométrie

Ce cours a pour but de présenter les nombres complexes d'un point de vue géométrique. Il n'a pas pour ambition d'être complet ou rigoureux, mais de transmettre au lecteur une première intuition.

– Bric à brac des nombres complexes –

Considérons l'équation :

$$x^2 + 1 = 0$$

Il n'existe pas de solution dans $\mathbb{R}$, l'ensemble des nombres réels. On se propose de s'imaginer un « nombre » i tel que $i^2 = -1$. i est un nombre complexe et on définit alors :

Définition 4.4.1.
On définit l'ensemble des nombres complexes z, noté $\mathbb{C}$, comme l'ensemble des nombres de la forme $z = a + ib$, où $a, b \in \mathbb{R}$. Le réel a (resp. b) est nommé partie réelle (resp. partie imaginaire) de z, et est noté $Re(z)$ (resp. $Im(z)$). Si $b = 0$, z est un réel. Si $a = 0$, z appartient à l'ensemble des imaginaires purs, noté $i\mathbb{R}$.

On définit l'addition et la multiplication comme extention naturelle à celles sur l'ensemble des réels :

Définition 4.4.2.
Soit $z, z' \in \mathbb{C}$ tels que $z = a + ib$ et $z' = c + id$ où $a, b, c, d \in \mathbb{R}$. On définit :

$$z + z' = (a + c) + i(b + d)$$

$$z.z' = (ac - bd) + i(bc + ad)$$

Les nombres complexes sont donc essentiellement la donnée d'un couple $(a, b) \in \mathbb{R}^2$. Représentons les dans un plan :

Définition 4.4.3.
On définit un plan nommé plan complexe, muni d'un repère orthonormé direct $(O, \overrightarrow{i}, \overrightarrow{j})$. Tout point M de coordonnées (a,b) du plan est caractérisé par le nombre complexe $z = a + ib$, nommé affixe du point M.

Définition 4.4.4.
Considérons un vecteur $\overrightarrow{u} = a\overrightarrow{i} + b\overrightarrow{j}$. L'affixe du vecteur $\overrightarrow{u}$, noté $z_{\overrightarrow{u}}$, est le complexe $a + ib$.

Afin de ne pas alourdir le document, sauf mention contraire, on notera un nombre complexe $z = a + ib$ où a, b sont des réels.

Définition 4.4.5.
Le conjugué d'un nombre complexe $z = a + ib$, noté $\overline{z}$, est le nombre complexe $\overline{z} = a - ib$.

Proposition 4.4.6.
Soit M un point du plan complexe d'affixe $z \in \mathbb{C}$. Le symétrique de M par rapport à l'axe des abscisses a pour affixe $\overline{z}$.

Exercice 1
Soit M, M′ d'affixe respectives z, z'. Montrer que M et M′ sont symétriques par rapport à (Oy) si, et seulement si $z' = -\overline{z}$.

Solution de l'exercice 1
Posons $z = a + ib$ et $z' = a' + ib'$. M et M′ symétriques par rapport à (Oy) ssi $y' = y$ et $x' = -x$ ie. $z' = -x + iy = -\overline{z}$.

Proposition 4.4.7.
Pour tout $z, z' \in \mathbb{C}$, on a :

$$\overline{z + z'} = \overline{z} + \overline{z'}$$
$$\overline{zz'} = \overline{z}\,\overline{z'}$$

Proposition 4.4.8.
Pour tout $z \in \mathbb{C}$, on a :

$$z + \overline{z} = 2Re(z)$$
$$z - \overline{z} = 2iIm(z)$$

Définition 4.4.9.
Soit $z = a + ib$ un nombre complexe. On définit le module de z, noté $|z|$,comme le réel positif $\sqrt{a^2 + b^2}$.

Proposition 4.4.10.
Soit M un point du plan complexe d'affixe $z \in \mathbb{C}$. La distance du point M à l'origine est $|z|$.

Remarque 4.4.11.
Soit M et M' deux points du plan complexe d'affixe $z \in \mathbb{C}$ et $z' \in \mathbb{C}$. La distance MM' vaut $|z - z'|$.

Proposition 4.4.12.
Soit $z \in \mathbb{C}$. On a :

$$z\overline{z} = |z|^2$$

Proposition 4.4.13.
Soit $z, z' \in \mathbb{C}$. On a :

$$|zz'| = |z||z'|$$

Finalement, définissons l'argument d'un complexe :

Définition 4.4.14.
Soit $z = a + ib$ un nombre complexe non nul. Notons que $\frac{z}{|z|}$ se trouve sur le cercle unité, donc il existe $\theta \in \mathbb{R}$ tel que :

$$cos(\theta) = \frac{a}{|z|}$$

$$sin(\theta) = \frac{b}{|z|}$$

θ est alors un argument de z et est défini modulo 2π

Proposition 4.4.15.
Soit M un point du plan complexe d'affixe $z \in \mathbb{C}$. L'angle orienté entre l'axe des abscisses et la droite (OM) est $arg(z)$.

Proposition 4.4.16.
Soit z, z' deux nombres complexes non nuls. On a :

$$arg(zz') = arg(z) + arg(z')$$

Dans un premier temps, nous avons défini un point (et donc un nombre complexe) dans le plan comme les coordonnées (abcisse, ordonnée). Remarquons que la donnée de la distance à l'orgine et l'angle par rapport à l'axe des abscisses défini aussi uniquement ce point. Ces dernières définissent les coordonnées polaires. En raison des propriétés énoncées ci-dessus, on introduit le formalisme d'exponentielle complexe :

Définition 4.4.17.
Soit z un nombre complexe non nul de norme $|z|$ et d'argument θ.L'écriture exponentielle de z est $z = |z|e^{i\theta}$.

Remarque 4.4.18.
Remarquons que $i = e^{i\frac{\pi}{2}}$. On notera de manière similaire $j = e^{i\frac{2\pi}{3}}$.

– Premières propriétés géométriques –

Théorème 4.4.19 (Inégalité triangulaire).
Pour tout $z, z', z'' \in \mathbb{C}$,

$$|z - z''| \leqslant |z - z'| + |z' - z''|$$

Théorème 4.4.20 (Angle au centre et angle inscrit).
Soit $\alpha, \beta, \theta \in \mathbb{R}$. Notons A, B, M, O les points d'affixes $e^{i\alpha}, e^{i\beta}, e^{i\theta}$ et 0. On a $2(\overrightarrow{MB}, \overrightarrow{MA}) = (\overrightarrow{OB}, \overrightarrow{OA})[2\pi]$.

Démonstration. On a :

$$\frac{e^{i\alpha} - e^{i\theta}}{e^{i\beta} - e^{i\theta}} = \frac{e^{\frac{\alpha+\theta}{2}}(e^{i\frac{\alpha-\theta}{2}} - e^{-i\frac{\alpha-\theta}{2}})}{e^{\frac{\beta+\theta}{2}}(e^{i\frac{\beta-\theta}{2}} - e^{-i\frac{\beta-\theta}{2}})} = \frac{e^{\frac{\alpha+\theta}{2}} sin(\frac{\alpha-\theta}{2})}{e^{\frac{\beta+\theta}{2}} sin(\frac{\beta-\theta}{2})} = e^{i\frac{\alpha-\beta}{2}} \frac{sin\frac{\alpha-\theta}{2}}{sin\frac{\beta-\theta}{2}}$$

Par conséquent, un argument de $\frac{e^{i\alpha}-e^{i\theta}}{e^{i\beta}-e^{i\theta}}$ est $\frac{\alpha-\beta}{2}[\pi]$ (et non modulo 2π car on ne connait pas le signe de $\frac{sin\frac{\alpha-\theta}{2}}{sin\frac{\beta-\theta}{2}}$. Ainsi :

$$2(\overrightarrow{MB}, \overrightarrow{MA}) = \alpha - \beta[2\pi] = (\overrightarrow{OB}, \overrightarrow{OA})[2\pi]$$

□

Proposition 4.4.21.
Soit A, B, C trois points distincts d'affixes respectives a, b, c. Soit $z = \frac{c-a}{b-a}$. Alors $|z| = \frac{AC}{AB}$ et $arg(z) = (\overrightarrow{AB}, \overrightarrow{AC})[2\pi]$.

Exercice 2
Caractérisons un triangle équilatéral de sens direct. Soit A, B, C trois points d'affixes respectives a, b, c.
1) Montrer que : $z = \frac{c-a}{b-a} = e^{i\frac{\pi}{3}} = -j^2$ et $arg(\frac{c-a}{b-a}) = \frac{\pi}{3}$
2)Montrer que : $a + jb + j^2c = 0$.
3)Supposons maintenant seulement que ABC est équilatéral (direct ou indirect). Montrer que : $a^2 + b^2 + c^2 - ab - bc - ca = 0$ ie $(a-b)^2 + (b-c)^2 + (c-a)^2 = 0$.

Solution de l'exercice 2
1)ABC est équilatéral de sens direct si, et seulement si : $AB = AC$ et $(\overrightarrow{AB}, \overrightarrow{AC}) = \frac{\pi}{3}[2\pi]$.

2) D'après la question 1, ABC équilatéral direct si, et seulement si :

$$\begin{aligned} & c-a=-j^2(b-a) \\ \Leftrightarrow\quad & (1+j^2)a-j^2b-c=0 \\ \Leftrightarrow\quad & -ja-j^2b-c=0 \\ \Leftrightarrow\quad & a+jb+j^2c=0 \end{aligned}$$

On obtient de même que ABC est équilatéral de sens indirect si, et seulement si, $a+j^2b+jc=0$.
3) Ainsi, ABC est équilatéral si :

$$\begin{aligned} & (a+jb+j^2c=0)(a+j^2b+jc=0)=0 \\ \Leftrightarrow\quad & a^2+b^2+c^2+(j+j^2)(ab+bc+ca)=0 \\ \Leftrightarrow\quad & a^2+b^2+c^2-ab-bc-ca=0 \\ \Leftrightarrow\quad & \frac{1}{2}[(a-b)^2+(b-c)^2+(c-a)^2]=0 \end{aligned}$$

Exercice 3
Considérons ABC un triangle quelconque et B′, C′ tels que : $AC=AC'$, $(\overrightarrow{AC},\overrightarrow{AC'})=\frac{\pi}{2}[2\pi]$ et $AB=AB'$, $(\overrightarrow{AB},\overrightarrow{AB'})=-\frac{\pi}{2}[2\pi]$. Soit I le milieu de [BC] et I′ le milieu de [B′C′]. Montrer que $(AI)\perp(B'C')$, $2AI=B'C'$ et $(AI')\perp(BC)$, $2AI'=BC$.

Solution de l'exercice 3
Notons a, b, c, b′, c′ les affixes de A, B, C, B′, C′. z_I l'affixe de I, $z_{I'}$ l'affixe de I′.
Interprétons les données de la figure :

$$|\frac{c'-a}{c-a}|=1, arg(\frac{c'-a}{c-a})=(\overrightarrow{AC},\overrightarrow{AC'})=\frac{\pi}{2}$$

Autrement dit : $\frac{c'-a}{c-a}=i$. Ainsi : $c'=a+i(c-a)=(1-i)a=ic$.
De même :

$$|\frac{b'-a}{b-a}|=1, arg(\frac{b'-a}{b-a})=(\overrightarrow{AB},\overrightarrow{AB'})=-\frac{\pi}{2}[2\pi]$$

Ce qui équivaut à : $\frac{b'-a}{b-a}=-i$ soit encore $b'=a-i(b-a)=(1+i)a-ib$.
De plus : $z_I=\frac{1}{2}(b+c)$ et $z_{\overrightarrow{AI}}=z_I-a=\frac{1}{2}(b+c)-a=\frac{1}{2}(b+c-2a)$
Et : $z_{\overrightarrow{B'C'}}=c'-b'=(1-i)a+ic-(1+i)a+ib=i(b+c-2a)=2iz_{\overrightarrow{AI}}$
D'où : $\frac{z_{B'C'}}{z_{\overrightarrow{AI}}}=2i$ d'où le résultat.
Par réciprocité des rôles, on a encore $2AI'=BC$ et $(\overrightarrow{AI},\overrightarrow{B'C'})=\frac{\pi}{2}[2\pi]$.

Exercice 4
Théorème de Napoléon
Soit ABC un triangle de sens direct quelconque. Soit M, N, P trois points tels que BMC, CNA, APB soient équilatéraux de sens direct.
1) Montrer que ABC et MNP ont le même sens de gravité.

2) Soit G_1, G_2, G_3 les centres de gravité de BMC, CNA et APB respectivement. Montrer que $G_1G_2G_3$ est équilatéral de sens direct.

Solution de l'exercice 4
Notons a, b, c, m, n, p les affixes respectives de A, B, C, M, N et P.
1)BMC est équilatéral de sens direct si, et seulement si $m + jc + j^2b = 0$ ie $m = -j^2b - jc$.
De même : $n = -j^2c - ja$ et $p = -j^2a - jb$.
Le centre de gravité de MNP a pour affixe : $\frac{m+n+p}{3} = \frac{-j-j^2}{3}(a + b + c) = \frac{1}{3}(a + b + c)$.
$\frac{1}{3}(a+b+c)$ étant l'affixe de G centre gravité de ABC ? on obtient que G est le centre de gravité commun des triangles ABC et MNP.
2) Calculons g_j, l'affixe de G_j pour $1 \leqslant j \leqslant 3$.

$$g_1 = \frac{1}{3}(m+b+c) = \frac{1}{3}(-j-j^2b+b+c) = \frac{1}{3}[(1-j^2)b+(1-j)c] = \frac{1-j}{3}((1+j)b+c) = \frac{1-j}{3}(c-j^2b)$$

De même, $g_2 = \frac{1-j}{3}(a - j^2c)$ et $g_3 = \frac{1-j}{3}(b - j^2a)$ D'où : $g_1 + jg_2 + j^2g_3 = \frac{1-j}{3}(ja - ja - j^2b + j^2b + c - c = 0$.

Exercice 5
Théorème de Van Aubel
Soit ABCD un quadrilatère de sens direct. On construit M, N, P, Q tels que MBA, NCB, PDC, QAD soient rectangles isocèles de sens direct en M, N, P, Q.
1) Montrer que MNPQ est un pseudo carré càd : MP=NQ et $MP \perp NQ$.
2) Donner une condition nécéssaire et suffisante pour que MNPQ soit un carré.

Solution de l'exercice 5
1) MBA est rectangle isocèle en M de sens direct si, et seulement si :

$$\frac{MA}{MB} = 1et(\overrightarrow{MB}, \overrightarrow{MA}) = \frac{\pi}{2}$$

Cette condition équivaut à : $\frac{z_{\overrightarrow{MA}}}{z_{\overrightarrow{MB}}} = i$ ou encore $\frac{m-a}{m-b} = i$.
Ainsi : $m - a = i(m - b)$ donc $(1 - i)m = a - ib$, d'où $m = \frac{1}{1-i}(a - ib) = \frac{1+i}{2}(a - ib)$.
De même, $n = \frac{1+i}{2}(b - ic)$,$p = \frac{1+i}{2}(c - id)$ et $q = \frac{1+i}{2}(d - ia)$.
D'où : $z_{\overrightarrow{MP}} = p - m = \frac{1+i}{2}(-a + ib + c - id)$ et $z_{\overrightarrow{NQ}} = q - n = \frac{1+I}{2}(-ia - b + ic + d)$.
Alors : $z_{\overrightarrow{NG}} = iz_{\overrightarrow{MP}}$ cad $\frac{z_{\overrightarrow{NG}}}{z_{\overrightarrow{MP}}}$=i d'où le résultat.
2) MNPQ est un carré si et seulement si MNPQ est un parallélogramme. Cette condition équivaut à : $\frac{m+p}{2} = \frac{n+q}{2}$ ie $m + p = n + q$.
Ainsi : MNPQ est un carré si, et seulement si :

$$\begin{aligned} & a - ib + c - ib = b - ic + d - ia \\ \Leftrightarrow \quad & (1 + i)(a + c) = (1 + i)(b + d) \\ & \Leftrightarrow \quad a + c = b + d \end{aligned}$$

Ainsi, MNPQ est un carré si, et seulement si, ABCD est un parallélogramme.

Exercice 6
Soit M un point d'affixe z non nul. Construire le point M′ d'affixe $z' = \frac{1}{z}$ à la règle et au compas.

Solution de l'exercice 6
Si $z \notin \mathbb{R}$:
Notons $z = re^{i\theta}$ où $r = |z|$ et $\theta = arg(z)$.
On a : $z' = \frac{1}{z} = \frac{1}{r}e^{-i\theta}$ d'où $|z'| = \frac{1}{r}$ et $arg(z') = -arg(z)[2\pi]$.
Notons A, A' les points d'affixe 1 et -1, O le point d'affixe 0 et (γ) le cercle circonscrit à A'AM.
Si P est un point du plan, notons $\gamma(P)$ la puissance du point P par rapport à (γ).
On a $\gamma(O) = \overline{OA}.\overline{OA'} = -1$ donc $\gamma(O) = \overline{OM}.\overline{ON} = -1$ où N est le deuxième point d'intersection entre (OM) et (γ).
Remarquons que $ON = \frac{1}{OM} = \frac{1}{r} = OM'$.
Il suffit alors de montrer que M' et N sont symétriques par rapport à (Oy).

Exercice 7
Cercles d'Apollonius Soit A, B deux points distincts du plan et $k \in \mathbb{R}_+^* \setminus \{-1\}$. Déterminer $\Gamma_k = \{M | MA = k.MB\}$.

Solution de l'exercice 7
On a :

$$\begin{aligned} & M \in \Gamma_k \\ \Leftrightarrow \quad & \overrightarrow{MA}^2 - k^2(\overrightarrow{MB})^2 = 0 \\ \Leftrightarrow \quad & (\overrightarrow{MA} - k\overrightarrow{MB})(\overrightarrow{MA} + k\overrightarrow{MB}) = 0 \end{aligned}$$

Soit I le barycentre de (A,1), (B,-k) et J le barycentre de (A, 1), (B,+k). Par définition du barycentre, on a, pour tout point M du plan :

$$\overrightarrow{MA} - k\overrightarrow{MB} = (1-k)\overrightarrow{MI}, \overrightarrow{MA} + k\overrightarrow{MB} = (1+k)\overrightarrow{MJ}$$

Alors :

$$\begin{aligned} & M \in \Gamma_k \\ \Leftrightarrow \quad & (1-k^2)(\overrightarrow{MI}.\overrightarrow{MJ}) = 0 \\ \Leftrightarrow \quad & \overrightarrow{MI}.\overrightarrow{MJ} = 0 \end{aligned}$$

Ainsi, Γ_k est le cercle de diamètre [IJ].

5 Exercices d'entraînement

1 Entraînement de mi-parcours

– Énoncés –

Exercice 1
Soit ABC un triangle, P un point de $[BC]$, Q un point de $[AB]$, R un point de $[AC]$. Les cercles circonscrits à AQR et BPQ se recoupent en un point X. Montrer que X est aussi sur le cercle circonscrit de CPR.

Exercice 2
Déterminer toutes les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ satisfaisant :

$$f(x)f(y) + f(x+y) = xy$$

pour tous réels x, y.

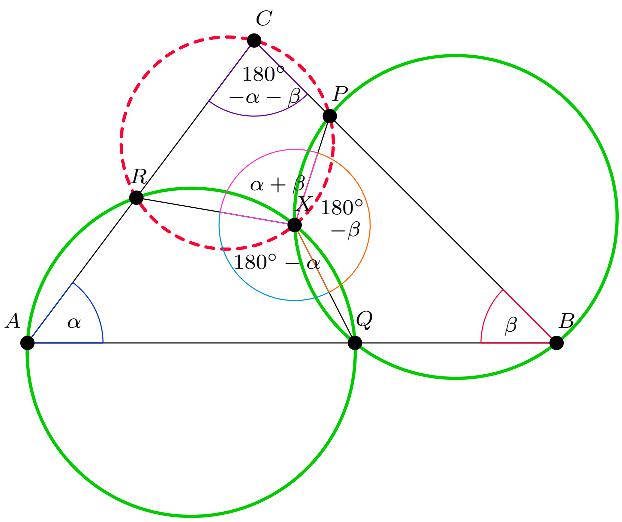
Exercice 3
Soit X à l'intérieur d'un triangle ABC. Les droites $(AX), (BX)$ et (CX) recoupent le cercle circonscrit au triangle ABC en P, Q et R respectivement. Le point U appartient au segment $[XP]$. Les parallèles à $(AB), (AC)$ passant par U coupent $(XQ), (XR)$ en V, W respectivement. Montrer que les points R, W, V, Q sont cocycliques.

Exercice 4
Soient a, b et c des réels strictement positifs tels que $a^2 + b^2 + c^2 = 3$. Montrer que

$$\frac{1}{1+ab} + \frac{1}{1+bc} + \frac{1}{1+ca} \geqslant \frac{3}{2}.$$

– Solutions –

Solution de l'exercice 1



On pose : $\alpha = \widehat{BAC}$ et : $\beta = \widehat{CBA}$. Comme les points A, Q, R, X sont cocycliques, on a : $\widehat{QXR} = 180° - \alpha$. De même, on a : $\widehat{PXQ} = 180° - \beta$. On en déduit que : $\widehat{RXP} = \alpha + \beta = 180° - \widehat{PXC}$, car : $\widehat{PXC} = 180° - \widehat{BAC} - \widehat{CBA} = 180° - \alpha - \beta$. Donc les points C, P, R, X sont également cocycliques.

Solution de l'exercice 2
En remplaçant y par 0 dans l'équation fonctionnelle on obtient

$$f(x)(f(0)+1) = 0$$

Si $f(0) \neq -1$ alors pour tout réel x, $f(x) = 0$. Cependant, réciproquement, si pour tout réel r on a $f(r) = 0$, alors en posant $x = y = 1$ par exemple, l'équation devient $0 = 1$, ce qui est absurde. On a ainsi que $f(0) = -1$. En posant $y = 1$ et $x = -1$ dans l'équation, on a :

$$f(-1)f(1) + f(0) = -1,$$

soit : $f(-1)f(1) = 0$. On a alors 2 cas, suivant que $f(1) = 0$ ou que $f(-1) = 0$.

Cas 1 : $f(1) = 0$. On pose alors $y = 1$ dans l'équation fonctionnelle :

$$f(1)f(x) + f(x+1) = x.$$

En remplaçant x par $x-1$ et en utilisant que $f(1) = 0$, on a $f(x) = x-1$ pour tout x réel. Réciproquement, la fonction qui à x associe $x-1$ est bien solution de l'équation puisque pour tous réels x, y :

$$(x-1)(y-1) + (x+y-1) = xy.$$

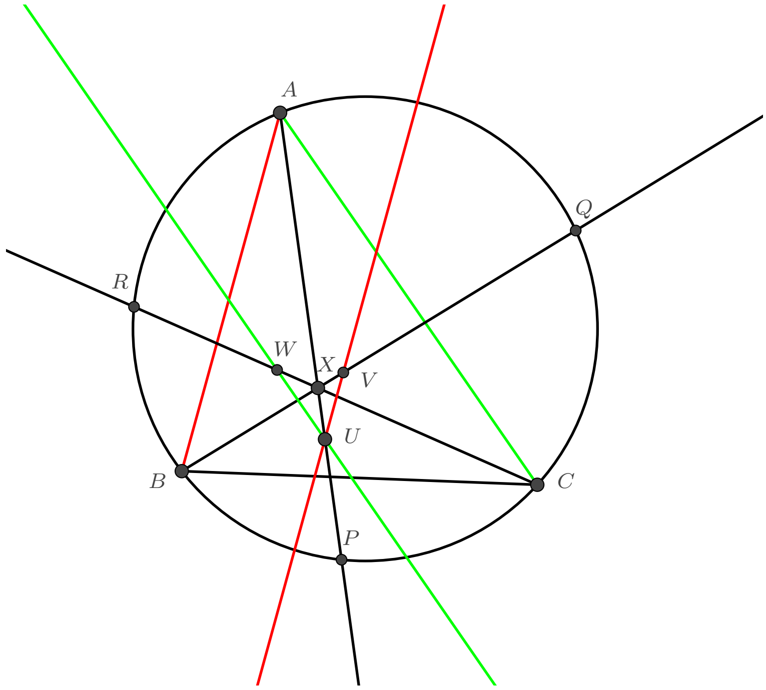
Cas 2 : $f(-1) = 0$. On fonctionne comme dans le cas précédent : on pose $y = -1$ pour obtenir :

$$f(-1)f(x) + f(x-1) = -x.$$

Alors pour tout x, $f(x-1) = -x$ et en remplaçant $x-1$ par x, on a pour tout x : $f(x) = -x-1$. Réciproquement, la fonction qui à x associe $-x-1$ est bien solution.

Les solutions sont donc : $f(x) = x-1$ pour tout réel x, et : $f(x) = -x-1$ pour tout réel x.

Solution de l'exercice 3



Comme (UV) est parallèle à (AB), d'après le théorème de Thalès on a : $\frac{XV}{XB} = \frac{XU}{XA}$. Comme (UW) est parallèle à (AC), de même on a : $\frac{XW}{XC} = \frac{XU}{XA}$. On en déduit que : $\frac{XV}{XB} = \frac{XW}{XC}$. En multipliant des deux côtés par $\frac{XB}{XW}$, on a : $\frac{XV}{XW} = \frac{XB}{XC}$. Les point B, R, Q et C sont cocycliques et (RC) et (QB) se coupent en X donc en utilisant la puissance de X par rapport au cercle circonscrit au triangle ABC, on a : $XQ \cdot XB = XR \cdot XC$, soit : $\frac{XB}{XC} = \frac{XR}{XQ}$. Ainsi $\frac{XV}{XW} = \frac{XB}{XC} = \frac{XR}{XQ}$, soit : $XV \cdot XQ = XR \cdot XW$. Par la réciproque de la puissance d'un point, les points V, Q, R, W sont cocycliques.

Solution de l'exercice 4
On utilise l'inégalité de Cauchy-Schwarz qui donne :

$$\left(\left(\sqrt{1+ab}\right)^2 + \left(\sqrt{1+bc}\right)^2 + \left(\sqrt{1+ca}\right)^2\right)\left(\left(\left(\sqrt{\frac{1}{1+ab}}\right)^2 + \left(\sqrt{\frac{1}{1+bc}}\right)^2\right) + \left(\sqrt{\frac{1}{1+ca}}\right)^2\right)$$

$$\geqslant \left(\frac{\sqrt{1+ab}}{\sqrt{1+ab}} + \frac{\sqrt{1+bc}}{\sqrt{1+bc}} + \frac{\sqrt{1+ca}}{\sqrt{1+ca}}\right)^2 = 9,$$

soit donc :

$$(3+ab+bc+ca)\left(\frac{1}{1+ab} + \frac{1}{1+bc} + \frac{1}{1+ca}\right) \geqslant 9,$$

ou encore :

$$\frac{1}{1+ab} + \frac{1}{1+bc} + \frac{1}{1+ca} \geqslant \frac{9}{3+ab+bc+ca}.$$

Il est donc suffisant de montrer que :

$$\frac{9}{3+ab+bc+ca} \geqslant \frac{3}{2},$$

soit montrer que : $3+ab+bc+ca \leqslant 6$, ou encore : $ab+bc+ca \leqslant 3$.

Or en utilisant l'inégalité de la moyenne, on a que : $ab \leqslant \frac{a^2+b^2}{2}$, $bc \leqslant \frac{b^2+c^2}{2}$ et $ca \leqslant \frac{a^2+c^2}{2}$. En sommant, on obtient :

$$ab + bc + ca \leqslant \frac{a^2+b^2}{2} + \frac{b^2+c^2}{2} + \frac{a^2+c^2}{2} = a^2 + b^2 + c^2 = 3,$$

ce qui permet de conclure.

2 Entraînement final

– Énoncés –

Exercice 1
Trouver tous les entiers positifs n tels que $n+1$ divise n^2+1.

Exercice 2

1. 4 points sont sur un cercle. Montrer qu'il existe un demi-cercle (bords compris) qui contient 3 de ces points.
2. 5 points sont sur une sphère. Montrer qu'il existe une demi-sphère (bords compris) qui contient 4 de ces points.

Exercice 3
Au départ, il y a m boules dans un sac et n dans un autre sac, où $m \geqslant 1$ et $n \geqslant 1$. Deux opérations différentes sont autorisées :

1. enlever un nombre égal de boules dans chaque sac, et
2. tripler le nombre de boules dans un sac.

Est-il toujours possible, quelles que soient les valeurs de m et n, d'enchaîner des opérations de sorte de vider les deux sacs ?

Exercice 4
Un nombre est dit *sympathique* si, pour chaque diviseur d de n, $d+2$ est un nombre premier. Trouver le nombre de diviseurs maximum d'un nombre *sympathique*.

– Solutions –

Solution de l'exercice 1
Soit n une solution éventuelle. Puisque $n \equiv -1 \pmod{n+1}$, on sait que $0 \equiv n^2+1 \equiv (-1)^2 + 1 \equiv 2 \pmod{n+1}$. Cela signifie que $n+1$ divise 2. Puisque $n+1$ est positif, et que les seuls diviseurs positifs de 2 sont 1 et 2, cela signifie que $n=0$ ou $n=1$.

Réciproquement, si $n=0$ ou $n=1$, alors $n=n^2$, donc $n+1$ divise bien $n^2+1=n+1$.

Solution de l'exercice 2

1. Soit P un des 4 points situés sur le cercle, et soit $\mathcal{D}$ le diamètre du cercle passant par P. Parmi les 3 autres points, et en vertu du principe des tiroirs, il y en a au moins 2 qui sont d'un même côté de $\mathcal{D}$ (quitte à les choisir sur $\mathcal{D}$ lui-même).

   Par conséquent, le demi-cercle qui contient ce côté de $\mathcal{D}$ contient également ces 2 points, plus P lui-même, ce qui fait bien 3 points en tout.

2. Soit P et Q deux des 5 points situés sur le cercle, et soit $\mathcal{E}$ un équateur de la sphère. Parmi les 3 autres points, et en vertu du principe des tiroirs, il y en a au moins 2 qui sont d'un même côté de $\mathcal{E}$ (quitte à les choisir sur $\mathcal{E}$ lui-même).

   Par conséquent, la demi-sphère qui contient ce côté de $\mathcal{E}$ contient également ces 2 points, plus P et Q eux-mêmes, ce qui fait bien 4 points en tout.

Solution de l'exercice 3
Chaque opération ne modifie pas la parité de $m+n$:

1. si on enlève k boules dans chaque sac, alors $m+n$ diminue de $2k$;
2. si on triple le nombre de boules d'un sac, $m+n$ augmente de $2m$ ou de $2n$, selon le sac considéré.

En particulier, si $m=2$ et $n=1$ initialement, alors on ne pourra jamais se débrouiller pour vider les deux sacs, puisque cela impliquerait d'avoir $m=n=0$.

Solution de l'exercice 4
Soit n un entier sympathique fixé, et soit d un diviseur de n. Si $d \equiv 1 \pmod 3$, alors $d+2 \equiv 0 \pmod 3$, et puisque $d+2$ est premier, cela signifie que $d+2=3$, donc que $d=1$.

Supposons maintenant qu'il existe deux nombres premiers p et q, distincts de 3, qui divisent tous les deux n. Alors $p \equiv q \equiv 2 \pmod 3$, donc $pq \equiv 1 \pmod 3$, et pq ne divise donc pas n. On en déduit que n est nécessairement de la forme 3^k ou $3^k p^\alpha$, avec $k \in \mathbb{N}$, $\alpha \in \{0,1\}$ et p un nombre premier tel que $p \equiv 2 \pmod 3$. L'entier n aura alors $\sigma_0(n) = (k+1)(\alpha+1)$ diviseurs.

Nous allons maintenant montrer que $\sigma_0(n) \leqslant 8$. Tout d'abord, puisque $3^5+2=245$ n'est pas premier, on sait que $k \leqslant 4$. Par conséquent, si $\alpha=0$, on sait que $\sigma_0(n)=k+1 \leqslant 5$, et si $k \leqslant 3$, alors $\sigma_0(n) \leqslant 2(k+1) \leqslant 8$ également. Il nous faut donc montrer que la paire (k,α) ne peut pas être égale à $(4,1)$.

Pour ce faire, procédons par l'absurde, et supposons que $n=3^4p$. Puisque $3^4 \times 5 + 2 = 407 = 11 \times 37$, on sait que $p \neq 5$, donc que p est inversible modulo 5. Or, puisque $3^2 \equiv -1 \pmod 5$, l'entier 3 est d'ordre 4 modulo 5. Par conséquent, il existe nécessairement un entier ℓ compris entre 1 et 4 tel que $3^\ell \equiv -2p^{-1} \pmod 5$, et alors $3^\ell p + 2$ n'est pas premier.

On a donc montré que $\sigma_0(n) \leqslant 8$. Réciproquement, si $n = 3^3 \times 5 = 135$, alors n a bien sûr 8 diviseurs, qui sont 1, 3, 5, 9, 15, 27, 45 et 135 lui-même. On vérifie aisément que 3, 5, 7, 11, 17, 29, 47 et 137 sont tous des nombres premiers, par exemple parce qu'ils n'ont aucun facteur premier $p \leqslant 12 = \sqrt{144}$ à part eux-mêmes.

Par conséquent, l'entier $n=135$ est sympathique, et le nombre maximum de diviseurs recherché est donc égal à 8.

V. Groupe C

Contenu de cette partie

1 Algèbre

1 Équations fonctionnelles

La notion d'équation peut être généralisée à la recherche d'objets mathématiques d'une forme quelconque, vérifiant une relation donnée.

Sont notamment présentes dans un contexte olympique les équations fonctionnelles, dont l'inconnue est une fonction, le plus souvent de $\mathbb{N}$ dans $\mathbb{N}$ ou $\mathbb{Z}$, ou de $\mathbb{R}$ dans $\mathbb{R}$.

Un problème d'équation fonctionnelle vise le plus souvent à déterminer l'ensemble exact des solutions, mais peut parfois se limiter à la recherche d'une propriété donnée des solutions, telles que la périodicité ou la continuité, ou à la recherche des solutions vérifiant une condition donnée : $f(0) = 0$, f continue, et ainsi de suite.

Nous aborderons ici les stratégies les plus classiques permettant de résoudre les différents types d'équations fonctionnelles, et citerons notamment l'équation de Cauchy sous ses différentes formes.

– Types de problèmes et méthodes classiques de résolution –

Les stratégies à appliquer face à une équation fonctionnelle reposent le plus souvent sur l'idée d'acquérir progressivement de l'information : en connaissant certains éléments du comportement de f, on peut manipuler l'équation fonctionnelle de sorte à se rapprocher d'une équation de la forme $f(x) = \ldots$, où le terme de droite ne dépend pas de f. Cependant, un argument de symétrie audacieux, par exemple, peut permettre de se passer de ce long processus (mais, hélas !, ces arguments sont rarement appliquables en-dehors d'un cas particulier. . .)

Avant de commencer la résolution

Avant même de réfléchir à une piste de résolution, la première réaction est toujours de chercher des solutions évidentes, comme par exemple :

— $x \mapsto 0$

— $x \mapsto 1$

— $x \mapsto a$

— $x \mapsto x$

— $x \mapsto x^2$

— $x \mapsto 1/x$

— $x \mapsto \frac{e^x+e^{-x}}{2}$ [1]

Dans la quasi-totalité des cas, l'équation fonctionnelle possède une ou plusieurs solutions de cette forme, qui sont généralement les seules. Avoir une idée de ce que l'on cherche à démontrer peut en effet être utile lorsque l'on cherche à le démontrer.

Parallèlement, avoir démontré qu'une équation fonctionnelle n'admet que des solutions "simples" (ou, plus généralement, que des solutions d'une certaine forme) ne suffit généralement pas à conclure : il reste encore à vérifier que toutes les solutions candidates sont (ou ne

1. Ou du moins si l'exercice 136 de la muraille vous semble trivial !

sont pas !) valables, ce qui évite notamment de passer de $7/7$ à $5/7$ sur un exercice d'équations fonctionnelles.

De plus, gardons en mémoire qu'une fonction solution n'est pas forcément simple (polynomiale, continue, dérivable…), mais peut au contraire être un objet hautement pathologique (nous verrons notamment tout à l'heure des fonctions recouvrant, dans un certain sens, le plan entier !)

Substitution

Le premier réflexe à avoir devant une équation fonctionnelle est de substituer l'une des inconnues par une valeur facilement maîtrisable, telle que 0, 1 ou $f(0)$. Cette technique possède plusieurs avantages :

— Elle permet de simplifier l'équation fonctionnelle, permettant de manipuler, par exemple, $f(x)$ au lieu de $f(x+f(y))$ en prenant $(x,y) \leftarrow (x-f(y),y)$

— Elle permet d'obtenir des informations sur le comportement de f en des valeurs particulières, permettant ainsi d'effectuer d'autres subsitutions plus efficacement (par exemple en simplifiant plus l'expression obtenue).

Cette stratégie est particulièrement utile dans le cas d'expressions de la forme $x+f(y)$ et $f(x \cdot f(y))$, qui se simplifient toutes deux en $f(0)$ en prenant $(x,y) \leftarrow (0,0)$; ou de même $x \cdot f(y)$ et $f(y \cdot f(x))$, qui se simplifient en $f(0)$ en prenant cette fois-ci $(x,y) \leftarrow (1,0)$.

Exercice 1
Trouver les $f : \mathbb{R} \to \mathbb{R}$ vérifiant $f(x-f(y)) = 1-x-y$.

Solution de l'exercice 1
On réalise la substitution $(x,y) \leftarrow (x+f(0),0)$, pour trouver $f(x) = 1-x-f(0)$. En évaluant en 0, nous trouvons alors $f(0) = 1-f(0) = \frac{1}{2}$. Réciproquement, nous avons bien $\frac{1}{2}-(x-(\frac{1}{2}-y)) = 1-x-y$: la fonction $f : x \mapsto \frac{1}{2}-x$ est l'unique solution.

Exercice 2
Trouver les fonctions polynomiales $P : \mathbb{R} \to \mathbb{R}$ vérifiant $P(x^2+1) = P(x)^2+1$ et $P(0) = 0$.

Solution de l'exercice 2
On construit par récurrence une suite (a_n) telle que $a_0 = 0$ et $a_{n+1} = a_n^2+1$. Alors, par récurrence, $P(a_n) = a_n \forall n \in \mathbb{N}$, d'où $x \mapsto P(x)-x$ admet une infinité de racines. Une fonction polynomiale admettant une infinité de racine étant forcément la fonction nulle, la fonction recherchée est $P : x \mapsto x$, dont l'on vérifie aisément la validité.

Une autre méthode similaire consiste à remplacer la ou les inconnues non pas par des valeurs déterminées mais par des expressions dépendant d'une ou de plusieurs variables, le plus souvent dans l'objectif de permettre des simplifications astucieuses. Ainsi, il peut être intéressant de choisir x en fonction de y (ou inversement), dans une équation fonctionnelle à deux variables, afin de la voir comme équation à une seule variable, sous un angle plus restreint mais parfois plus pertinent.

Ainsi, même si il est toujours bon, comme premier réflexe, de tester par exemple $f(0)$ et $f(1)$, certaines substitutions sont plus pertinentes que d'autres : notamment, $x \leftarrow x-f(y)$, $x \leftarrow f(y)$ et leurs innombrables variantes permettent de se débarasser aisément des fonctions imbriquées.

Symétrie

De nombreuses équations fonctionnelles reposent sur un principe de symétrie. Bien évidemment, la notion de symétrie est très vague, et cette méthode en est d'autant plus adaptable à une grande variété de situations.

La première symétrie, la plus classique, est celle entre x et y dans chaque membre. Elle invite notamment à des transformations de la forme $(x, y) \leftarrow (u+v, u-v)$: décomposer x et y en une partie symétrique u et une partie antisymétrique v, via une transformation qui peut facilement être inversée en $(u, v) \leftarrow (\frac{x+y}{2}, \frac{x-y}{2})$.

Pour trois variables, nous avons de même la transformation de Ravi : x, y et z sont alors considérées comme étant les côtés d'un triangle, que l'on exprime désormais à partir des distances entre les sommets et les points de tangence au cercle inscrit : $(x, y, z) \leftarrow (a+b, b+c, c+a)$.

Cependant, une situation encore plus intéressante que la symétrie d'une équation est la symétrie d'un seul de ses membres. Disons en effet que l'équation s'écrive comme $\xi(f, x, y) = \psi(f, x, y)$, avec ψ symétrique par rapport à x et y (i.e. $\psi(f, x, y) = \psi(f, y, x)$) mais pas ξ. Alors nous pouvons en déduire $\xi(f, x, y) = \xi(f, y, x)$ pour toute f solution, et ainsi restreindre drastiquement notre espace de recherche.

Plus précisément, face à des situations de la forme $\xi(f, x, y) = \xi(f, y, x)$, nous pouvons par exemple choisir $(x, y) \leftarrow (x, -x)$ ou $(x, y) \leftarrow (x, \frac{1}{x})$ afin de préserver la symétrie, ou au contraire tenter de la briser d'une façon ou d'une autre. L'on veillera cependant à ne pas poser $(x, y) \leftarrow (x, x)$, la symétrie empêchant d'obtenir une quelconque information à partir de cette substitution.

Exercice 3
Trouver les fonctions $f : \mathbb{R} \to \mathbb{R}$ vérifiant $\forall x, y \in \mathbb{R}, f(x+y) = x + f(y)$.

Solution de l'exercice 3
La demi-symétrie nous permet d'écrire $\forall x, y \in \mathbb{R}, y + f(x) = x + f(y)$, i.e. $f(x) - x = f(y) - y$, c'est-à-dire que f est de la forme $x \mapsto x + a$, pour $a \in \mathbb{R}$. Réciproquement, les fonctions de cette forme conviennent toutes.

Exercice 4
Trouver les fonctions $f : \mathbb{R} \to \mathbb{R}$ vérifiant $\forall x \neq 1, f(x) + f(\frac{1}{1-x}) = x$.

Solution de l'exercice 4
Soit $x \notin 0, 1$. Alors $f(x) + f(\frac{1}{1-x}) = x$. De plus, puisque $x \neq 0$, $\frac{1}{1-x} \neq 1$, nous pouvons donc appliquer l'identité en $\frac{1}{1-x}$ pour trouver $f(\frac{1}{1-x}) + f(1 - \frac{1}{x}) = \frac{1}{1-x}$. Enfin, nous l'appliquons encore en $1 - \frac{1}{x}$ pour trouver $f(1 - \frac{1}{x}) + f(x) = 1 - \frac{1}{x}$.

Nous avons donc trois équations fixant trois valeurs possibles pour la fonction. En ajoutant la première et la troisième, et en y soustrayant la deuxième, nous trouvons $2 \cdot f(x) = (x + 1 - \frac{1}{x}) - \frac{1}{1-x}$, ie $f(x) = \frac{1}{2}(x + 1 - \frac{1}{x} - \frac{1}{1-x})$ pour $x \notin 0, 1$. Les valeurs en 0 et 1, quant à elles, sont uniquement fixées par $f(0) + f(\frac{1}{1-0}) = 0$ i.e. $f(1) = -f(0)$.

Plus généralement, la présence d'une homographie (une fonction de la forme $x \mapsto \frac{ax+b}{cx+d}$) dans un exercice est souvent un signe d'une possibilité de transformation astucieuse : la composition de deux homographies restant une homographie, des choix pertinents des paramètres a, b, c, d révèlent facilement les intentions de l'exercice.

Périodicité

Parfois, l'objectif d'un exercice n'est pas de trouver l'ensemble exact des solutions d'une équation fonctionnelle, mais uniquement de déterminer une propriété de telles solutions. Le plus communément, cette propriété se trouve être la périodicité. Par exemple :

Exercice 5
Soit $f : \mathbb{R} \to \mathbb{R}$ vérifiant $f(x-1) + f(x+1) = \sqrt{2}f(x)$. Montrer que f est périodique.

Différentes méthodes peuvent être utiles dans ces cas-là : une substitution de x, par exemple, pour $x + a$ permet d'observer directement un comportement périodique (en faisant évoluer selon x, en quelque sorte, l'équation fonctionnelle), tandis que l'étude d'une solution donnée permet souvent d'obtenir une insight sur la structure de la solution générale (et notamment sur sa période).
Solution de l'exercice 5
Nous remarquons que la fonction $f : x \mapsto e^{ix\cdot\frac{2\pi}{8}}$, de $\mathbb{R}$ dans $\mathbb{C}$, vérifie une équation similaire (exactement la même, mais élargie aux fonctions à valeurs complexes !)[2]. Ainsi, nous avons envie de chercher des fonctions de période 8, et plus précisément telles que $f(x) = -f(x+4)$. En appliquant trois fois l'identité en x, $x+1$ et $x-1$, nous trouvons en effet $2f(x) = \sqrt{2}(f(x-1) + f(x+1)) = f(x-2) + 2f(x) + f(x+2)$, ie $f(x-2) + f(x+2) = 0$: f vérifie donc bien $f(x) = -f(x+4) = f(x+8)$ comme prévue, et est bien périodique de période 8.

Notons également qu'il n'est pas nécessaire ici de vérifier toutes les fonctions 8-périodiques : elles ne seront naturellement pas toutes solutions, et l'unique implication recherchée est ici $f(x-1) + f(x+1) = \sqrt{2}f(x) \Rightarrow f(x) = f(x+8)$, soit exactement le résultat obtenu.

Attention cependant, les solutions à une équation fonctionnelle peuvent avoir des périodes minimales distinctes, voire ne pas avoir de période minimale du tout, et pourtant être périodiques ! Comment est-ce possible ? La fonction indicatrice de $\mathbb{Q}$, définie par $f : x \mapsto \mathbf{1}_{\mathbb{Q}}(x)$, et qui associe 1 aux rationnels et 0 aux irrationnels, se répète tous les q pour tout $q \in \mathbb{Q}$. Elle n'admet donc pas de période minimale, tout en restant périodique.

Cette fonction en particulier nous révèle également un autre écueil classique des exercices d'équations fonctionnelles : les multigraphes.

Attention aux multigraphes !

Supposons en effet que vous soyez arrivés à la situation suivante :

$$\forall x, f(x) = 0 ou f(x) = 1.$$

Que pouvez-vous conclure de cela ? Pas grand-chose, malheureusement. Certes, vous seriez bien tentés de répondre que $f : x \mapsto 0$ et $f : x \mapsto 1$ sont les deux seules solutions possibles, mais cela serait faux : rien n'empêche notre fonction $f : x \mapsto \mathbf{1}_{\mathbb{Q}}(x)$ d'être solution de notre équation.

Une technique courante pour venir à bout de ces situations est de supposer, par exemple, qu'il existe x et y tels que $f(x) = 0$ et $f(y) = 1$ et d'aboutir à une contradiction, mais cela n'est pas toujours garanti de réussir : encore faut-il déjà que ces solutions soient les seules !

2. Nous pouvons notamment la retrouver en pensant à la formule de l'angle moitié.

Ainsi, une équation aussi simple que $f(x+y) = f(x) + f(y)$ (l'équation de Cauchy, que nous verrons ci-après) peut-elle avoir, en plus des $f : x \mapsto ax$, une infinité de solutions pathologiques, extrêmement contre-intuitives !

Injectivité et surjectivité

Injectivité et surjectivité sont deux outils sans aucun doute extrêmement puissants pour résoudre n'importe quelle équation fonctionnelle : savoir, respectivement, que $f(x) = f(y)$ est équivalent à (et non plus seulement une conséquence de !) $x = y$, et qu'un résultat valable pour les réels de la forme $f(x)$ est valable pour tous.

Une erreur courante, malheureusement, est de croire que ces propriétés sont vérifiées par toute fonction, alors que les démontrer est bien souvent le coeur du problème lui-même ! Une fonction aussi simple que $f : x \mapsto x^2$ ou $f : x \mapsto |x|$, en effet, ne vérifie aucne des deux : $x^2 = y^2$ n'impliquera jamais $x = y$![3]

Pourquoi ces propriétés sont-elles si importantes ? Mettons que vous avez trouvé, disons, $g(f(x)) = g(x)$, ou encore $f(g(x)) = g(x)$. Malheureusement, vous ne pouvez pour l'instant déduire $f(x) = x$ ni dans le premier cas, ni dans le deuxième...

Mais, si g se trouve être injective, x et $f(x)$, ayant la même image par g dans la première équation, sont égaux ! $g(f(x)) = g(x)$ et g injective impliquent ainsi $f(x) = x$. Et, de même, si g est surjective, l'égalité $f(g(x)) = g(x)$ est équivalente à $f(y) = y$ en prenant $y = g(x)$: tout $y \in \mathbb{R}$ pouvant s'écrire sous cette forme, $f(x) = x$ pour tout x encore une fois ! $f(g(x)) = g(x)$ et g surjective impliquent une fois de plus $f(x) = x$. L'injectivité permet donc d'éplucher, en quelque sorte, une équation fonctionnelle, tandis que la surjectivité permet de l'énoyauter[4].

Ainsi, n'importe laquelle de ces deux propriétés permet de conclure à partir de $f(f(x)) = f(x)$, une situation extrêmement courante dans un exercice d'équation fonctionnelle.

La combinaison des deux, la bijectivité, est bien plus puissante encore : elle permet en effet de considérer f^{-1}, l'inverse de la fonction f : $f^{-1}(x) = y \Leftrightarrow f(y) = x$, et ainsi de pouvoir librement simplifier des $f(f(x))$, par exemple, en faisant passer l'un des f de l'autre côté comme f^{-1}. De plus, nous pouvons tout aussi librement identifier les antécédents avec leurs images par la fonction, permettant encore une fois une plus grande aisance dans la manipulation des expressions.

– Exercices –

Exercice 6
Existe-t-il $f : \mathbb{N} \to \mathbb{N}$ vérifiant $f(f(n)) = n + 2013 \forall n \in \mathbb{N}$?

Exercice 7
Trouver les $f : \mathbb{N} \to \mathbb{N}$ vérifiant $f(f(m) + f(n)) = m + n \forall m, n \in \mathbb{N}$

Exercice 8
Trouver les $f : \mathbb{N} \to \mathbb{N}$ vérifiant $f(n+1) > f(f(n)) \forall n \in \mathbb{N}$

3. sauf, bien sûr, dans le cas où $x = y = 0$.
4. À ne pas confondre avec l'énoyautage de la fonction elle-même, qui correspond à l'injectivité !

Exercice 9
Montrer l'équivalence, pour $f : \mathbb{R} \to \mathbb{R}$ entre $f(x+y) = f(x)+f(y) \forall x, y \in \mathbb{R}$ et $f(x+y+xy) = f(x) + f(y) + f(xy) \forall x, y \in \mathbb{R}$

– L'équation de Cauchy –

Sans doute la plus classique, et en même temps la plus simple, des équations fonctionnelles est celle de Cauchy : $f(x+y) = f(x)+f(y)$. En d'autres termes, on cherche les fonctions distributives par rapport à l'addition. La simplicité de cette équation permet sa résolution sur différents domaines et codomaines [5]. Ainsi, nous pouvons aisément résoudre l'équations sur $\mathbb{N} \to \mathbb{R}$, $\mathbb{Z} \to \mathbb{R}$ et $\mathbb{Q} \to \mathbb{R}$, et, sous certaines conditions, sur $\mathbb{R} \to \mathbb{R}$ tout entier ! Cependant, la forme générale des solutions est beaucoup plus complexe, et ne sera que mentionnée ici.

Résolution pour les fonctions de $\mathbb{Q}$ dans $\mathbb{R}$

Ici, f désigne une solution de l'équation de Cauchy de $\mathbb{Q}$ dans $\mathbb{R}$.

Lemme 1.1.1. Il existe un réel a tel que $f(n) = a\,n$ pour tout entier naturel n.

Démonstration. Procédons par récurrence. Tout d'abord, $f(0) = 0$. Puis, en prenant $a = f(1)$, nous avons $f(n+1) = f(n) + f(1) = an + a = a(n+1)$ par hypothèse de récurrence. Réciproquement, ces solutions conviennent pour tout $a \in \mathbb{R}$. $\square$

Ce lemme revient à démontrer que f est linéaire sur $\mathbb{N}$. Notons que l'ordre des quantificateurs est ici crucial : placer le $\exists$ après le $\forall$ reviendrait seulement à dire que $f(0) = a \cdot 0$.

Lemme 1.1.2. Il existe un réel a tel que $f(n) = a\,n$ pour tout entier relatif q.

Démonstration. Cela est vrai pour les entiers positifs en prenant $a = f(1)$. De plus, pour $n \in \mathbb{N}$, $0 = f(0) = f(n + (-n)) = f(n) + f(-n) = an + f(-n)$, d'où $f(-n) = -an$: la fonction se prolonge à $\mathbb{Z}$. Encore une fois, ces solutions conviennent pour tout $a \in \mathbb{R}$. $\square$

Proposition 1.1.3.
Il existe un réel a tel que $f(\omega) = a\,\omega$ pour tout nombre rationnel ω.

Démonstration. Nous avons, pour tout $q \in \mathbb{N}$, $f(1) = q \cdot f(\frac{1}{q})$ ie $f(\frac{1}{q}) = \frac{1}{q} \cdot f(1)$ par récurrence, et donc, pour tout $p, q \in \mathbb{N}$, $f(\frac{p}{q}) = \frac{p}{q} \cdot f(1)$ Ce résultat s'étend aux rationnels négatifs en appliquant $\forall \omega \in \mathbb{Q}^+ f(-\omega) = -f(\omega)$, démontré de la même manière que son analogue entier. $\square$

5. Le domaine est l'ensemble des antécédents, le codomaine est l'ensemble des images acceptables (l'ensemble des images, quant à lui, est simplement nommé image et est un sous-ensemble du codomaine)

Résolution sous conditions pour les fonctions de $\mathbb{R}$ dans $\mathbb{R}$

Ici, f désigne une solution de l'équation de Cauchy de $\mathbb{R}$ dans $\mathbb{R}$.

Lemme 1.1.4. Tout réel est limite d'une suite (dé)croissante de rationnels.

Démonstration. Il suffit de regarder son écriture décimale approchée : π, par exemple, s'approche par 3, 3.1, 3.14... ainsi que par 4, 3.2, 3.15... □

Proposition 1.1.5.
Si f est croissante, alors il existe un réel a tel que $f(x) = a\,x$ pour tout réel x.

Démonstration. Soit $x \in \mathbb{R}$, et a uniquement déterminée par le comportement de f sur $\mathbb{Q}$. Soient u_n et v_n deux suites de rationnels de limite x, tels que $\forall n, u_n < x < v_n$. Alors $\forall n, f(u_n) = a \cdot u_n < a\,x < a \cdot v_n = f(v_n)$. De plus, $\forall n, f(u_n) < f(x) < f(v_n)$ par croissance. Par inégalité triangulaire, $|f(x) - a\,x| < 2 \cdot |f(v_n) - f(u_n)| \to 0$, ce qui signifie que $f(x) = a\,x$ Réciproquement, les solutions de la forme $f : x \mapsto a\,x$ conviennent toujours. □

Proposition 1.1.6.
Si f vérifie $f(xy) = f(x)f(y)$, alors f est la fonction nulle ou bien la fonction identité.

Démonstration. Déjà, remarquons que $f(1) = f(1)^2$ c'est-à-dire que $f(1) = 0$ ou $f(1) = 1$. De plus, pour $x > 0$, $f(x) = f(\sqrt{x})^2 > 0$. Ainsi, pour y quelconque, $f(x+y) = f(x)+f(y) > f(y)$: f est croissante, nous pouvons ainsi nous ramener à la proposition précédente pour trouver f de la forme $x \mapsto a\,x$. Enfin, puisque $a = f(1)$, a vaut 0 ou 1, ie $f : x \mapsto 0$ ou $f : x \mapsto x$. Nous vérifions réciproquement que ces deux solutions conviennent. □

Forme générale des fonctions de $\mathbb{R}$ dans $\mathbb{R}$

D'autres fonctions de $\mathbb{R}$ dans $\mathbb{R}$ existent, mais sont trop complexes pour pouvoir être abordées en détail ici[6]. Nous pouvons tout de même tenter d'en construire une, en supposant l'existence d'un ensemble $\mathbb{H}$ stable par addition tel que chaque $x \in \mathbb{R}$ admette une unique écriture comme $h_x + q_x$, avec $h_x \in \mathbb{H}$, $q_x \in \mathbb{Q}$.

Alors, les fonctions $f : x \mapsto h_x$ et $g : x \mapsto q_x$ vérifient toutes deux l'équation de Cauchy : en effet, pour $x, y \in \mathbb{R}$, $x+y = h_{x+y}+q_{x+y} = h_x+h_y+q_x+q_y$, d'où $h_{x+y} = h_x+h_y$ et $q_{x+y} = q_x+q_y$.

2 Polynômes – $1^{\text{ère}}$ partie

> **Introduction.** L'objectif de ce cours est de présenter l'objet « polynôme » et les propriétés remarquables associées à cet objet. Les exercices sont pour la plupart des applications directes du cours, mais contiennent les idées classiques à connaître pour aborder des exercices plus compliqués.

– Généralités –

6. Elles nécessitent notamment une notion de $\mathbb{R}$ comme $\mathbb{Q}$-espace vectoriel de dimension infinie, ainsi que la preuve de l'existence d'une base de Hamel de $\mathbb{R}$ sur $\mathbb{Q}$

Définition et propriétés

Définition 1.2.1.
Une fonction $P : \mathbb{R} \longrightarrow \mathbb{R}$ est appelée fonction polynomiale ou fonction polynôme s'il existe un entier $n \geqslant 0$ et des nombres réels $a_0, \cdots, a_n$ tels que pour tout $x \in \mathbb{R}$:

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

Si $a_n \neq 0$, alors on dit que P est de degré n et on note $\deg P = n$ et a_n est appelé le coefficient dominant de P.

Par convention, le degré du polynôme nul est $-\infty$. La constante a_0 est appelé coefficient constant de P et l'expression $a_k x^k$ son monôme. On note indifféremment P, $P(x)$ ou $P(X)$ pour désigner le polynôme.

On note respectivement $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

✌ **Explication** ✌ Dans tout ce qui suit, on ne fait pas la distinction entre polynôme et fonction polynomiale associée (une explication est disponible dans le polycoîé d'Igor Kortchemski). Il faudrait bien entendu la faire en toute rigueur.
Exemple 1 Le polynôme $P(x) = \pi x^3 - \sqrt{2}x + 4$ est de degré 3, avec pour coefficient dominant π et coefficient constant 4.

Opérations sur les degrés

Proposition 1.2.2.
On a les caractérisations suivantes :

$$\begin{aligned} P(x) = 0 \quad &\Longleftrightarrow \quad \deg P = -\infty \\ P(x) = \text{constante non nulle} \quad &\Longleftrightarrow \quad \deg P = 0 \end{aligned}$$

Pour montrer qu'un polynôme est nul, on peut montrer que son degré est $-\infty$. On utilisera ce résultat par la suite.

Proposition 1.2.3.
Soit P et Q deux polynômes. Alors $P + Q$ et PQ sont encore des polynômes.

Démonstration. *Preuve faite en classe.* □

✌ **Explication** ✌ Soit $P = 2x^3 + 5x - 3$, $Q_1 = -2X^3 + 3X + 5$, $Q_2 = X^3$ et $Q_3 = X$. Quels sont les degrés de $P + Q_1$, $P + Q_2$ et $P + Q_3$?

Proposition 1.2.4.
Avec la convention $-\infty + \text{cste} = -\infty$,

$$\begin{aligned} \deg(P+Q) &= \max(\deg P, \deg Q) && \text{si } \deg P \neq \deg Q \\ \deg(P+Q) &\leqslant \max(\deg P, \deg Q) && \text{dans tous les cas} \\ \deg(PQ) &= \deg P + \deg Q \end{aligned}$$

Démonstration. Facile. □

✌ **Explication** ✌ L'utilisation des propriétés du degré est puissante pour établir l'intégrité de $\mathbb{K}[X]$ avec $\mathbb{K}$ l'un des ensembles mentionnés plus haut. Plus précisément :

Proposition 1.2.5.
Soit $(P, Q) \in \mathbb{K}[X]^2$. Alors on a l'équivalence suivante :

$$PQ = 0 \iff \big(P = 0 \text{ ou } Q = 0\big)$$

Démonstration.

$\boxed{\Rightarrow}$ Trivial.

$\boxed{\Leftarrow}$ En passant par les degrés.

□

Unicité de l'écriture d'un polynôme

✌ **Explication** ✌ Le théorème suivant montre l'unicité de l'écriture d'un polynôme, ce qui a pour corollaire immédiat un principe d'identification entre polynômes :

Théorème 1.2.6.
Soit $P = \sum_{k=0}^{n} a_k x^k$ avec les a_k réels. Alors :

$$\forall x \in \mathbb{R},\ P(x) = 0 \iff a_0 = a_1 = \cdots = a_n$$

Démonstration. On raisonne par l'absurde. Supposons qu'il existe k tel que $a_k \neq 0$ et cherchons une contradiction. On considère alors $p = \min_k\{a_k \neq 0\}$; pour tout $x \in \mathbb{R}^*$, on a :

$$P(x) = a_p x^p + a_{p+1}x^{p+1} + \cdots + a_n x^n = 0$$

D'où en divisant par $x^p \neq 0$, il vient que pour tout $x \in \mathbb{R}^*$:

$$a_p + a_{p+1}x + \cdots + a_n x^{n-p} = 0$$

En faisant tendre x vers 0, on trouve $a_p = 0$, ce qui est absurde. □

Le corollaire immédiat de ce théorème est le principe d'identification suivant :

Théorème 1.2.7.
Soit $P = \sum_{k=0}^{n} a_k x^k$ et $Q = \sum_{k=0}^{m} b_k x^k$.

$$\forall x \in \mathbb{R},\ P(x) = Q(x) \implies \big[m = n \quad \text{et} \quad \forall k \in [\![0, n]\!],\ a_k = b_k\big]$$

Démonstration. *Preuve faite en classe.* □

✌ **Explication** ✌ Ce résultat est à la base de résolution d'équations fonctionnelles dont les solutions sont restreintes aux fonctions polynomiales. Outre les techniques propres à la résolution des équations fonctionnelles, l'utilisation du degré et l'introduction des coefficients sont des atouts supplémentaires pour leur résolution.

Exercice 1
Déterminer les polynômes réels vérifiant la relation :

$$P(x^2) = (x^2 + 1)P(x).$$

Solution de l'exercice 1
Le polynôme nul est évidemment solution.

On cherche les solutions non nulles par analyse-synthèse :

— *Analyse.* Supposons que P est solution, alors nécessairement :

$$2 \deg P = \deg P + 2 \Longleftrightarrow \deg P = 2$$

Les candidats solutions sont les polynômes de degré 2 : $P(x) = ax^2 + bx + c$ avec a, b et c réels.

— *Synthèse.* On a les équivalences suivantes :

$$\begin{aligned} P(x) = ax^2 + bx + c \text{ est solution} &\Longleftrightarrow P(x^2) = (x^2 + 1)P(x) \\ &\Longleftrightarrow ax^4 + bx^2 + c = ax^4 + bx^3 + (a + c)x^2 + bx + c \\ &\Longleftrightarrow b = 0 \quad \text{et} \quad c = -a \\ &\Longleftrightarrow P(x) = ax^2 - a = a(x^2 - 1) \end{aligned}$$

Les solutions polynomiales de l'équation fonctionnelle sont exactement les $P(x) = a(x^2 - 1)$ avec a réel quelconque.

✌ **Explication** ✌ Certains formules combinatoires peuvent se démontrer à l'aide du principe d'identification :

Exercice 2 (Formule de Vandermonde)
Soit $n \in \mathbb{N}$. Alors :

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

Solution de l'exercice 2
On identifie les coefficients devant x^n de $(1+x)^{2n} = (1+x)^n(1+x)^n$. Une preuve combinatoire serait de considérer une urne de $2n$ boules, dont n boules blanches et n boules noires, puis de compter de deux façons différentes le nombre de façons d'effectuer un tirage simultané de n boules parmi les $2n$ boules.

Dérivation polynomiale

✌ **Explication** ✌ On rappelle que P' désigne la dérivée de P et on note $P^{(k)}$ la dérivée $k^{\textit{ième}}$ de P (où $k \in \mathbb{N}$) qu'on obtient en dérivant P k fois.

Proposition 1.2.8.
Soit $(P, Q) \in \mathbb{K}[X]^2$. Alors :

$$(PQ)' = P'Q + Q'P$$

Démonstration. Laissée au lecteur. □

Exercice 3
On considère $P(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{R}[X]$ de degré n. Que vaut $P^{(j)}(0)$ pour $j \in \mathbb{N}$?

Solution de l'exercice 3
$P^{(j)}(0) = \begin{cases} 0 & \text{si } j > n \\ j! a_j & \text{si } j \leqslant n \end{cases}$

– Dualité monde de l'arithmétique/monde de l'évaluation –

Rappels d'arithmétique

✌ **Explication** ✌ Dans ce qui suit, $\mathbb{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. On exclut donc le cas $\mathbb{K} = \mathbb{Z}$.

Théorème 1.2.9.
Soit $(A, B) \in \mathbb{K}[X]^2$ avec B non nul. Alors il EXISTE UN UNIQUE couple $(Q, R) \in \mathbb{K}[X]^2$ tel que :

$$\begin{array}{c|c} A & B \\ \hline R & Q \end{array} \qquad \text{avec} \qquad \deg R < \deg B$$

$$\text{c'est-à-dire :} \quad A = BQ + R \qquad \text{avec} \qquad \deg R < \deg B$$

Démonstration.

— *Unicité* : Soit (Q_1, R_1) et (Q_2, R_2) deux couples de la division euclidienne de A par B. On en déduit alors :

$$BQ_1 + R_1 = BQ_2 + R_2 \iff B(Q_1 - Q_2) = R_1 - R_2$$

On raisonne par l'absurde. Supposons $\deg(Q_1 - Q_2) \geqslant 0$. On a alors les inégalités suivantes :

$$\deg B \leqslant \deg(B(Q_1 - Q_2)) = \deg(R_1 - R_2) \leqslant \max(\deg R_1, \deg R_2) < \deg B,$$

ce qui est absurde. Donc $\deg(Q_1 - Q_2) = -\infty$, c'est-à-dire $Q_1 = Q_2$. Il vient alors $R_1 = R_2$.

— *Existence* : On procède par récurrence pour montrer la propriété suivante :

« pour tout polynôme A de degré $\leqslant n$, il existe un couple (Q, R) tel que $A = BQ + R$ avec $\deg R < \deg B$ »

— *Initialisation.* La propriété est trivialement vraie pour $n = 0$ (attention toutefois à faire la disjonction de cas suivant la nullité de A ou pas).

— *Hérédité.* Soit $n \in \mathbb{N}$; supposons la propriété vraie. Soit A un polynôme de degré $\leqslant n + 1$.

— Si $\deg A \leqslant n$, alors l'hypothèse de récurrence permet de conclure.

— Si $\deg A = n + 1$, alors $A - \dfrac{\mathrm{dom}(A)}{\mathrm{dom}(B)} X^{n+1-\deg B} B$ est un polynôme degré $\leqslant n$, et où $\mathrm{dom}(A)$ et $\mathrm{dom}(B)$ désignent respectivement les coefficients dominants de A et B. Par hypothèse de récurrence, il existe (Q, R) avec $\deg R < \deg B$ tel que :

$$A - \frac{\mathrm{dom}(A)}{\mathrm{dom}(B)} X^{n+1-\deg B} B = BQ + R \iff A = B\big(Q + \frac{\mathrm{dom}(A)}{\mathrm{dom}(B)} X^{n+1-\deg(B)}\big) + R$$

Ce qui achève la récurrence.

□

✌ **Explication** ✌ **(Pour déterminer le reste d'une division euclidienne)**
En général, lorsque le degré de A est petit, on peut poser directement la division euclidienne de A par B.

Lorsque le degré de A est élevé ou quelconque et celui de B petit, on écrit le théorème de la division euclidienne sans chercher à calculer le quotient. Des évaluations en les racines de B permettent alors de trouver le reste.

Exercice 4 (Cas des racines simples)
Soit $n \geqslant 2$. Déterminer le reste de la division euclidienne de X^n par $X^2 - 3X + 2$.

Solution de l'exercice 4
On écrit la division euclidienne de X^n par $X^2 - 3X + 2$. Il existe alors un (unique) couple (Q, R) tel que :

$$X^n = (X^2 - 3X + 2)Q + R \quad \text{avec } \deg R < \deg B = 2 \text{ i.e. } R = aX + b \text{ avec } (a, b) \in \mathbb{K}^2$$

L'évaluation de cette relation en les racines de $X^2 - 3X + 2$, à savoir 1 et 2, permet d'établir un système de deux équations en a et b. La résolution de ce système permet alors de conclure que $R = (2^n - 1)X - (2^n - 2)$.

Exercice 5 (Cas des racines doubles)
Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{R}$. Déterminer le reste de la division euclidienne de P par $(X - a)^2$ en fonction de $P(a)$ et $P'(a)$.

Solution de l'exercice 5
Même principe que dans l'exemple précédent, à la nuance près qu'il va falloir dériver la relation, puis la réévaluer en a pour obtenir une deuxième équation. Au final, on trouve que le reste de la division euclidienne est $R = P(a) + P'(a)(X - a)$.

Exercice 6
Soit $P \in \mathbb{K}[X]$ et $(a, b) \in \mathbb{K}^2$ tel que $a \neq b$. Sachant que le reste de la division euclidienne de P par $X - a$ vaut 1 et que le reste de la division euclidienne de P par $X - b$ vaut -1, déterminer le reste de la division euclidienne de P par $(X - a)(X - b)$.

Solution de l'exercice 6
La traduction des hypothèses permet d'en déduire l'existence de polynômes Q_1 et Q_2 vérifiant le système suivant :

$$\begin{cases} P &= (X-a)Q_1 + 1 \\ P &= (X-b)Q_2 - 1 \end{cases} \quad \text{d'où} \quad \begin{cases} P(a) &= 1 \\ P(b) &= -1 \end{cases}$$

Déterminons le reste de la division euclidienne de P par $(X - a)(X - b)$:

$$P = (X - a)(X - b)Q_3 + cX + d \qquad (\bigstar)$$

où Q_3 est un certain polynôme (qu'on ne souhaite pas déterminer), et c, d des constantes à déterminer.

Évaluons $(\bigstar)$ en a et b pour écrire le système suivant :

$$\begin{cases} P(a) &= ca + d \\ P(b) &= cb + d \end{cases} \iff \begin{cases} 1 &= ca + d \\ -1 &= cb + d \end{cases} \underset{L_2 \leftarrow L_2 - L_1}{\iff} \begin{cases} 1 &= ca + d \\ -2 &= c(b - a) \end{cases} \underset{a \neq b}{\iff} \begin{cases} d &= \dfrac{b+a}{b-a} \\ c &= \dfrac{2}{a-b} \end{cases}$$

Le reste de la division euclidienne de P par $(X - a)(X - b)$ est donné par :

$$R(X) = cX + d = \frac{2}{a-b}X + \frac{b+a}{b-a}$$

Racines

Lien entre racines et divisibilité

✌ **Explication** ✌ On rappelle qu'une racine $\lambda \in \mathbb{K}$ de P est une valeur qui annule P, c'est-à-dire vérifie $P(\lambda) = 0$. Il faut faire attention à l'ensemble dans lequel on cherche les racines comme le montrent les exemples concrets suivants.
Exemple 2 $X^2 - 2$ a deux racines réelles $\pm\sqrt{2}$, mais n'a pas de racines rationnelles (puisque $\sqrt{2}$ est irrationnel). $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, mais a deux racines complexes $\pm i$.
✌ **Explication** ✌ Le résultat fondamental suivant permet de faire le lien entre deux mondes distincts (celui de l'évaluation) et celui de l'arithmétique (en terme de divisibilité) :

Proposition 1.2.10.
Soit $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Alors :

λ est racine de P (i.e. $P(\lambda) = 0$) $\iff$ P est divisible par $(X - \lambda)$ (i.e. $\exists Q \in \mathbb{K}[X],\ P = (X - \lambda)Q$)

Démonstration.

- $\boxed{\Leftarrow}$ Le sens droite-gauche est trivial.
- $\boxed{\Rightarrow}$ On effectue la division euclidienne de P par $(X - \lambda)$. L'évaluation en λ permet alors de montrer que son reste est nul.

□

Nombre maximal de racines

✌ **Explication** ✌ Un polynôme ne peut pas avoir plus de racines que son degré :

Théorème 1.2.11.
Soit $n \in \mathbb{N}$. Un polynôme de $\mathbb{K}[X]$ de degré n a au plus n racines différentes dans $\mathbb{K}$.

Démonstration. *Récurrence sur n faite en classe.* □

Exemple 3 Il existe des polynômes qui n'ont pas de racines réelles, par exemple :

$$P(x) = x^4 + 1 = (x^2)^2 + 1^2 + 2x^2 - 2x^2 = (x^2 + 1)^2 - (\sqrt{2}x)^2 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$$

puis on montre que les discriminants de ces polynômes du second degré sont strictement négatifs (en cas de besoin, on pourra se référer au paragraphe sur les rappels pour les polynômes du second degré).
Exemple 4 Un polynôme de $P \in \mathbb{R}[X]$ de degré impair a au moins une racine réelle. Il suffit, pour s'en convaincre, de regarder les limites en $\pm\infty$ et de conclure par le théorème des valeurs intermédiaires.

Corollaire 1.2.12.

- Si un polynôme P admet une infinité de racines, ALORS P est nul.
- Si un polynôme P de degré $\leqslant n$ admet $n + 1$ racines distinctes, ALORS P est nul.

— SI $P = \sum_{k=0}^{n} a_k x^k$ est de degré n et a n racines distinctes $\lambda_1, \cdots, \lambda_n$, ALORS :

$$P(x) = a_n(x - \lambda_1) \cdots (x - \lambda_n)$$

Démonstration. Les deux premiers points découlent directement du précédent théorème. Le dernier point est démontré en classe en considérant la différence. □

✌ **Explication** ✌ En dépit des apparences, ce corollaire, certes très intuitif, est l'un des plus importants de ce chapitre ! Une des recettes de cuisine pour résoudre des exercices sur les polynômes consiste à :

INTERPRÉTER LES HYPOTHÈSES EN TERME DE RACINES D'UN CERTAIN POLYNÔME

Exercice 7
Montrer que $P(x) = |x|$ n'est pas un polynôme.

Solution de l'exercice 7
Raisonnons par l'absurde en supposant que $P(x)$ soit un polynôme. ans ce cas, le polynôme $P(x) - x$ a une infinité de racines (tous les réels positifs), donc est nul. Ainsi, pour tout $x \in \mathbb{R}$:

$$P(x) - x = 0 \Longleftrightarrow |x| = x$$

Ceci est absurde.

Exercice 8
Montrer qu'il n'existe pas de polynômes P tels que :

$$\forall n \in \mathbb{N},\ P(n) = \sqrt[3]{n^2 + 1}$$

Solution de l'exercice 8
Raisonnons par l'absurde en supposant qu'un tel polynôme existe. Dans ce cas, le polynôme $P(x)^3 - (x^2 + 1)$ est nul car admet l'infinité des entiers naturels comme racines. D'où $P(x)^3 = x^2 + 1$. En passant au degré, on trouve une contradiction.

Exercice 9
Soit $P \in \mathbb{R}[X]$. On suppose que P est de degré n entier tel que pour tout $k \in [\![1, n+1]\!]$, $P(k) = 1/k$. Calculer $P(-1)$.

Solution de l'exercice 9
On considère le polynôme $xP(x) - 1$, qui est degré $n + 1$ et possède $n + 1$ racines distinctes, que sont les entiers de 1 à $n + 1$. On en déduit qu'il existe une constante $K \in \mathbb{K}$ tel que, pour tout $x \in \mathbb{R}$:

$$P(x) = K \prod_{k=1}^{n+1} (x - k)$$

L'évaluation en 0 permet de trouver que $K = \dfrac{(-1)^n}{(n+1)!}$, puis on en déduit l'expression de $xP(x)$:

$$xP(x) = 1 + \frac{(-1)^n}{(n+1)!} \prod_{k=1}^{n+1} (x - k)$$

L'évaluation de l'expression précédemment obtenue en -1 permet de trouver que $P(-1) = n + 1$.

Racines multiples

Définition 1.2.13.
Soit $P \in \mathbb{K}[X]$ $\boxed{\text{NON NUL}}$, λ un SCALAIRE et $m \in \mathbb{N}$.

$$\lambda \text{ RACINE DE MULTIPLICITÉ } m \text{ DANS P} \underset{\text{déf. 1}}{\iff} \begin{bmatrix} \exists Q \in \mathbb{K}[X],\ P = (X-\lambda)^m Q \\ \text{ET} \\ (X-\lambda)^{m+1} \text{ ne divise pas } P \end{bmatrix}$$

$$\underset{\text{déf. 2}}{\iff} \begin{bmatrix} \exists Q \in \mathbb{K}[X],\ P = (X-\lambda)^m Q \\ \text{ET} \\ Q(\lambda) \neq 0 \end{bmatrix}$$

En particulier, on a les caractérisations suivantes :

$$\begin{aligned} \lambda \text{ est racine de multiplicité } 0 &\iff \lambda \text{ n'est pas racine de } P \\ \lambda \text{ est racine de multiplicité } 1 &\iff \lambda \text{ est racine simple de } P \\ \lambda \text{ est racine de multiplicité } 2 &\iff \lambda \text{ est racine double de } P \\ \lambda \text{ est racine de multiplicité } m \geqslant 2 &\iff \lambda \text{ est racine multiple de } P \end{aligned}$$

Exemple 5 $P = (X-1)^2(X+1)(X-\pi)^{17}$ a pour racines les réels 1, -1 et π de multiplicités respectives 2, 1 et 17.

Théorème 1.2.14.
Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors :

$$\alpha \text{ est une racine multiple de } P \text{ si et seulement si } \big(P(\alpha) = 0 \text{ et } P'(\alpha) = 0\big).$$

Démonstration. *Démonstration faite en classe.* □

✌ **Explication** ✌ Plus généralement, on peut montrer par récurrence que :

Théorème 1.2.15.
Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et n un entier supérieur ou égal à 1. Alors :

$$P(\alpha) = P'(\alpha) = P''(\alpha) = \cdots = P^{(n)}(\alpha) = 0 \iff (X-\alpha)^n \text{ divise } P$$

Démonstration. Laissée au lecteur. □

Exercice 10
Montrer que pour tout $n \in \mathbb{N}^*$:

$$P_n = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$$

est divisible par $Q = (X-1)^3$.

Solution de l'exercice 10
Montrons que $(X-1)^3$ divise $P(X) = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$ i.e. que 1 est racine de multiplicité AU MOINS 3 de $P(X)$ i.e. $\begin{cases} P(1) = 0 & (i) \\ P'(1) = 0 & (ii) \\ P''(1) = 0 & (iii) \end{cases}$

(i) Calculons :

$$P(1) = n1^{n+2} - (n+2)1^{n+1} + (n+2)1 - n = 0$$

(ii) Sachant que $P'(X) = n(n+2)X^{n+1} - (n+2)(n+1)X^n + (n+2)$, calculons :

$$P'(1) = n(n+2) - (n+2)(n+1) + (n+2) = (n+2)(n+1) - (n+2)(n+1) = 0$$

(iii) Sachant que $P''(X) = n(n+1)(n+2)X^n - n(n+1)(n+2)X^{n-1}$, calculons :

$$P''(1) = n(n+1)(n+2) - n(n+1)(n+2) = 0$$

Ainsi, $(X-1)^3$ divise $P(X)$.

Exercice 11
Soit $n \geqslant 1$. Montrer que le polynôme P suivant :

$$P = \sum_{k=0}^{n} \frac{X^k}{k!}$$

est scindé à racines simples sur $\mathbb{C}$.

Solution de l'exercice 11
Supposons que P a une racine α qui n'est pas simple, ce qui signifie que

$$P(\alpha) = 0$$
$$P'(\alpha) = 0.$$

Cherchons une contradiction.

On remarque que :

$$P(X) = P'(X) + \frac{X^n}{n!}$$

En évaluant cette égalité polynomiale en α, on trouve :

$$P(\alpha) = P'(\alpha) + \frac{\alpha^n}{n!} \Longleftrightarrow \frac{\alpha^n}{n!} = 0 \Longleftrightarrow \alpha = 0$$

Mais il est clair que $P(\alpha) = P(0) = 1 \neq 0$. Contradiction !

Ainsi, P n'a que des racines simples dans $\mathbb{C}$

Cas des polynômes de degré 2

Théorème 1.2.16.
Soit $P = aX^2 + bX + c \in \mathbb{R}[X]$ un polynôme de degré 2 (i.e. $a \neq 0$) et on note $\Delta = b^2 - 4ac$.

— Si $\Delta > 0$, alors P a deux racines réelles distinctes :

$$\frac{-b \pm \sqrt{\Delta}}{2a}$$

— Si $\Delta = 0$, alors P a une racine réelle double :

$$\frac{-b}{2a}$$

— Si $\Delta < 0$, alors P n'a pas de racines réelles, mais possède deux racines complexes conjuguées :

$$\frac{-b \pm i\sqrt{-\Delta}}{2a}$$

Démonstration. *Faite en classe.* □

Exercice 12
Factoriser $X^2 + X + 1$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Solution de l'exercice 12
$X^2+X+1 = (X-j)(X-\overline{j})$ avec $j = e^{i\frac{2\pi}{3}}$ dans $\mathbb{C}[X]$ et $X^2+X+1 = X^2+X+1$ dans $\mathbb{R}[X]$.

– Formules de Viète –

✌ **Explication** ✌ Ce paragraphe poursuit l'idée selon laquelle la connaissance des racines de P donne des informations sur P.

Cas $n = 2$

Théorème 1.2.17.
Soit $P(x) = ax^2 + bx + c$ un polynôme réel de degré 2 (i.e. $a \neq 0$) ayant λ_1 et λ_2 comme racines réelles. Alors :

$$\lambda_1\lambda_2 = \frac{c}{a} \qquad \text{et} \qquad \lambda_1 + \lambda_2 = -\frac{b}{a}$$

Démonstration. Il suffit de développer $P(x) = a(x-\lambda_1)(x-\lambda_2) = ax^2+bx+c$ et d'identifier suivant les puissances de x. □

Cas général

Définition 1.2.18.
Soit $n \geqslant 1$ et $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$. Pour tout $k \in [\![1, n]\!]$, on appelle $k^{ième}$ fonction symétrique élémentaire la quantité :

$$\sigma_k(\lambda_1, \cdots, \lambda_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \lambda_{i_1} \cdots \lambda_{i_k}$$

Exemple 6 Dans le cas $n = 3$, les trois fonctions symétriques élémentaires des racines sont :

$$\begin{array}{rcl} \sigma_1(\lambda_1, \lambda_2, \lambda_3) & = & \lambda_1 + \lambda_2 + \lambda_3 \\ \sigma_2(\lambda_1, \lambda_2, \lambda_3) & = & \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 \\ \sigma_3(\lambda_1, \lambda_2, \lambda_3) & = & \lambda_1\lambda_2\lambda_3 \end{array}$$

Théorème 1.2.19.
Soit $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ avec $a_n \neq 0$. On suppose que P admet n racines réelles $\lambda_1, \cdots, \lambda_n$ (comptées avec multiplicité). Alors, pour tout $k \in [\![1, n]\!]$:

$$\sigma_k(\lambda_1, \cdots, \lambda_n) = (-1)^k \frac{a_{n-k}}{a_n}.$$

En particulier :

$$\sum_{i=1}^{n} \lambda_i = -\frac{a_{n-1}}{a_n} \qquad \sum_{1 \leqslant i < j \leqslant n} \lambda_i \lambda_j = \frac{a_{n-2}}{a_n} \qquad \prod_{i=1}^{n} \lambda_i = (-1)^n \frac{a_0}{a_n}$$

Démonstration. Il suffit de développer et d'identifier. □

Exercice 13
Chercher tous les nombres réels x, y et z tels que :

$$x + y + z = 17 \qquad xy + yz + xz = 94 \qquad xyz = 168$$

Solution de l'exercice 13
Les solutions (x, y, z) sont les six permutations possibles de $(1, -3, 4)$.

Exercice 14
Exprimer $x^2 + y^2 + z^2$ en fonction des fonction de σ_1 et σ_2.

Solution de l'exercice 14
$x^2 + y^2 + z^2 = \sigma_1^2 - 2\sigma_2$

Exercice 15
Exprimer $x^3 + y^3 + z^3$ en fonction des fonction de σ_1 ,σ_2 et σ_3.

Solution de l'exercice 15
$x^3 + y^3 + z^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

Exercice 16
Résoudre le système suivant :

$$\begin{cases} x+y+z &= 2 \\ x^2+y^2+z^2 &= 26 \\ x^3+y^3+z^3 &= 38 \end{cases}$$

Solution de l'exercice 16
On trouve après calculs que les solutions du système sont $(1,-3,4)$ et les permutations associées.

3 Polynômes – $2^{\text{ème}}$ partie

– Exercices –

Exercice 1
Soit P un polynôme tel que le reste de la division euclidienne de P par $X-1$ vaut 3 et le reste de la division euclidienne de P par $X-2$ vaut 2.

Quel est le reste de la division euclidienne de P par $(X-1)(X-2)$?

Exercice 2
Trouver tous les réels a, b tels que $(X-1)^2$ divise aX^4+bX^3+1.

Exercice 3
Soient α, β et γ les racines du polynôme X^3-3X+1.

Calculer $\alpha^4+\beta^4+\gamma^4$.

Exercice 4
Soit P un polynôme à coefficients entiers. On suppose qu'il existe quatre entiers a, b, c et d deux à deux distincts tels que $P(a)=P(b)=P(c)=P(d)=2018$.

Montrer qu'il n'existe pas d'entier x tel que $P(x)=2015$.

Exercice 5
Soient $n \in \mathbb{N}^*$ et $P \in \mathbb{R}[X]$ de degré au plus n tel que $P(k)=\frac{k}{k+1}$ pour tout $k \in [\![0,n]\!]$. Combien vaut $P(n+1)$?

Exercice 6 (BxMO 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 7
Soient P et Q des polynômes unitaires de degré 2018, tels que pour tout réel x, on ait $P(x) \neq Q(x)$. Montrer qu'il existe un réel x tel que $P(x-1)=Q(x+1)$.

Exercice 8
Soit P un polynôme de degré $n \geqslant 5$ avec n racines entières distinctes tel que $P(0)=0$. Montrer que le polynôme $P(P(X))$ a exactement n racines entières.

Exercice 9
Soit $P, Q \in \mathbb{R}[X]$ deux polynômes réels non constants ayant les mêmes racines complexes, et tels que $P-1$ et $Q-1$ aussi. Montrer que $P=Q$.

Remarque.
Les racines complexes n'ayant pas été vues en cours, l'exercice précédent n'est pas faisable avec ce qui a été vu pendant le stage.

Exercice 10 (IMO 1988, problème 4)
Montrer que l'ensemble des réels x vérifiant $\sum_{k=1}^{63} \frac{k}{x-k} \geqslant 1$ est réunion d'intervalles dont la somme des longueurs vaut 2016.

Exercice 11 (IMO 2016, problème 5)
On écrit au tableau l'égalité :

$$(x-1)(x-2)\dots(x-2016) = (x-1)(x-2)\dots(x-2016).$$

On veut effacer certains des 4032 facteurs de telle manière que l'équation au tableau n'admette aucune solution réelle. Quelle est le nombre minimal de facteur qu'on doit effacer pour y arriver ?

– Solutions –

Solution de l'exercice 1
On peut écrire $P = (X-1)Q + 3$, donc $P(1) = 3$. De même, on a $P(2) = 2$. Notons R le reste qu'on cherche : on a $\deg(R) < \deg((X-1)(X-2))$ donc $\deg(R) \leqslant 1$, donc R est une fonction affine. De plus, on a

$$P = (X-1)(X-2)Q + R$$

pour un certain polynôme Q. En évaluant en 1 et 2, on obtient $R(1) = 3$ et $R(2) = 2$, donc $R = 4 - X$.

Solution de l'exercice 2
Soit P le polynôme aX^4+bX^3+1. Dire que $(X-1)^2$ divise P revient à dire que $P(1) = P'(1) = 0$, soit $a+b+1 = 4a+3b = 0$. On a donc $b = -\frac{4}{3}a$, et $a - \frac{4}{3}a + 1 = 0$, d'où $a = 3$ et $b = -4$, qui est la seule solution.

Solution de l'exercice 3
On sait que $\alpha^3 - 3\alpha + 1 = 0$, donc $\alpha^4 = \alpha \times \alpha^3 = \alpha \times (3\alpha - 1) = 3\alpha^2 - \alpha$. On a donc

$$\begin{aligned}
\alpha^4 + \beta^4 + \gamma^4 &= 3(\alpha^2+\beta^2+\gamma^2) - (\alpha+\beta+\gamma) \\
&= 3(\alpha+\beta+\gamma)^2 - 6(\alpha\beta+\beta\gamma+\gamma\alpha) + (\alpha+\beta+\gamma) \\
&= 3 \times 0 - 6 \times (-3) + 0 \\
&= 18,
\end{aligned}$$

car les relations de Viète donnent $\alpha+\beta+\gamma = 0$ et $\alpha\beta+\beta\gamma+\gamma\alpha = -3$.

Notons que le ce calcul peut également se faire de manière bien plus "bourrine" : on sait calculer $\alpha^2+\beta^2+\gamma^2$. En mettant ce quantité au carré, il nous suffit de calculer $\alpha^2\beta^2+\beta^2\gamma^2+\gamma^2\alpha^2$. Or, on a

$$\alpha^2\beta^2+\beta^2\gamma^2+\gamma^2\alpha^2 = (\alpha\beta+\beta\gamma+\gamma\alpha)^2 - 2\alpha\beta\gamma(\alpha+\beta+\gamma),$$

donc on peut tout calculer. L'avantage de la première méthode est que la complexité du calcul explose bien moins rapidement quand on remplace α^4 par α^k avec k plus grand.

Solution de l'exercice 4
Soit $Q = P - 2018$: a, b, c et d sont des racines de Q donc il existe un polynôme R à coefficients entiers tel que $Q(X) = (X-a)(X-b)(X-c)(X-d)R(x)$. Si il existe x tel que $P(x) = 2015$, alors $Q(x) = -3$, soit $(x-a)(x-b)(x-c)(x-d)R(x) = -3$. Cependant, $x-a$, $x-b$, $x-c$ et $x-d$ sont quatre entiers deux à deux distincts qui doivent être non nuls. Il y en a donc au plus deux qui valent 1 ou -1. On peut donc supposer $|x-a| > 1$ et $|x-b| > 1$, donc $|x-a| \geqslant 2$ et $|x-b| \geqslant 2$, donc $|(x-a)(x-b)| \geqslant 4$ donc $|Q(x)| \geqslant 4$ car il est non nul, ce qui est absurde.

Solution de l'exercice 5
Soit $Q(X) = (X+1)P(X) - X$: le polynôme Q est de degré au plus $n+1$ et on a $Q(k) = 0$ pour tout $k \in \{0, 1, \ldots, n\}$. Il est donc de la forme :

$$Q(X) = cX(X-1)(X-2)\ldots(X-n).$$

De plus, on a $Q(-1) = 1$ donc $c = \frac{1}{(-1)(-2)\ldots(-n-1)} = \frac{(-1)^{n+1}}{(n+1)!}$, donc

$$P(X) = \frac{1}{X+1}\left((-1)^{n+1}\frac{X(X-1)(X-2)\ldots(X-n)}{(n+1)!} + X\right).$$

On obtient $P(n+1) = \frac{n+1+(-1)^{n+1}}{n+2}$.

Solution de l'exercice 6
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 7
Reformulons légèrement l'énoncé : on veut une racine réelle au polynôme $R(X) = P(X-1) - Q(X+1)$. A quoi peut-il ressembler ? Il est clairement de degré au plus 2017 (le coefficient du terme de degré 2018 étant nul). S'il est de degré 2017, donc impair, alors il aura bien une racine réelle (d'après le théorème des valeurs intermédiaires). Regardons de plus près, en posant $P(X) = X^{2018} + aX^{2017} + S(X)$ et $Q(X) = X^{2018} + bX^{2017} + T(X)$, où S et T sont de degré au plus 2016. Soit de plus c le coefficient de degré 2017 de R. On obtient $c = -2018 - 2018 + a - b = a - b - 4036$ (on regarde, dans $(X-1)^{2018}$, le terme de degré 2017, et de même pour $(X+1)^{2018}$). Se posent deux questions : comment gérer ce $a - b$? Et à quoi sert la condition $P(x) \neq Q(x)$ pour tout x réel ? Heureusement, elles sont liées !

$P - Q$ n'a pas de racine réelle, donc n'est pas de degré impair. Or $P - Q$ est de degré au plus 2017, et le coefficient du terme de degré 2017 est $a - b$. Donc $a - b = 0$, d'où $c \neq 0$, et R est bien de degré 2017, ce que l'on voulait.

Solution de l'exercice 8
Les racines de P sont des racines de $P(P(X))$ car $P(0) = 0$ donc il suffit de montrer que ce sont les seules. Notons $r_1 = 0, r_2, \ldots, r_n$ les racines de $P(P(X))$ et supposons que r est une racine de $P(P(X))$ différente des r_i. Alors $P(r)$ est une racine de P et n'est pas 0. On la note r_k. Sans perte de généralité (quitte à remplacer P par $-P(-X)$), on peut supposer $r_k \geqslant 0$. On a donc

$$r(r-r_2)\ldots(r-r_n) = r_k$$

et en particulier $r(r-r_k)$ divise r_k. En particulier $r \leqslant r_k$ et $r_k - r \leqslant r_k$ donc $0 < r < r_k$. En posant $s = r_k - r$ on obtient $rs | r + s$ avec $r, s > 0$ donc $r | s$ et $s | r$ donc $r = s = 1$ ou 2. Dans le premier cas on a $r_k = 2$ donc

$$-\prod_{i \neq 1,k} r - r_i = 2$$

mais ce produit contient au moins trois facteurs différents de r et de $r - r_k$, donc différents de 1 et -1, donc la valeur absolue du membre de gauche vaut au moins 8, ce que st absurde.

Dans le second cas on a

$$2 \times (-2) \prod_{i \neq 1,k} r - r_i = 4$$

mais le produit à gauche contient au moins 3 facteurs distincts, donc au moins un qui n'est pas 1 ou -1, et on obtient une nouvelle contradiction.

Solution de l'exercice 9

Soient 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 $p_0 + p_1 > n$, ce qui conclut.

Solution de l'exercice 10

L'inégalité est équivalente, après multiplication par $Q(x)^2 = (\prod_{k=1}^{63}(x-k))^2$ et passage du second membre dans le premier, à $P(x) \geqslant 0$ où $P(X) = Q(X)R(X)$ avec $R(X) = \sum_{k=1}^{63} k \prod_{1 \leqslant i \neq k \leqslant 63}(X-i) - Q(X)$.

On remarque $R(1)<0$, $R(2)>0$, $R(3)<0$, ..., $R(63)>0$ et $R(x)>0$ pour x assez grand, donc R a pour racines les r_i tels que $1 < r_1 < 2 < r_2 < \cdots < 63 < r_{63}$, et P a pour racines les r_i et les entiers compris entre 1 et 63 inclus. Or $P(x)$ est négatif pour x assez grand ou assez petit, donc P est positif sur la réunion des intervalles $[k, r_k]$ pour $1 \leqslant k \leqslant 63$, dont la longueur totale vaut $\sum_{i=1}^{63}(r_i - i)$. Par les relations coefficients racines, on déduit du coefficient de X^{62} dans R que $\sum_{i=1}^{63} r_i = 2\sum_{i=1}^{63} i$ donc la longueur totale des intervalles vaut $\sum_{i=1}^{63} i = 2016$.

Solution de l'exercice 11

Si il reste un facteur $x-1$ à droite et un à gauche, alors l'équation admet 1 comme solution et de même pour les autres facteurs. Il faut donc effacer au moins un $x-1$, au moins un $x-2$ etc... soit au moins 2016 facteurs.

Il reste à montrer que c'est possible en effaçant exactement 2016 nombres. Une manière de le faire est d'effacer $x-i$ à gauche si i est congru à 0 ou 1 modulo 4 et à droite si i est congru à 2 ou 3 modulo 4.

4 Inégalités

Le cours a porté sur les notions suivantes :

— Inégalité arithmético-géométrique

— Lemme du tourniquet : $a^2+b^2+c^2 \geqslant ab+bc+ca$

— Inégalité de Cauchy-Schwarz (preuve avec le discriminant d'un polynôme bien choisi, cas d'égalité)

— Inégalité des mauvais élèves (preuve à partir de Cauchy-Schwarz)

— Convexité : définitions, propriétés, inégalité de Jensen et preuve de l'IAG

On peut retrouver ces notions dans le très complet polycopié de Pierre Bornsztein sur le sujet.

– Exercices –

Exercice 1
Montrer que pour tout réel strictement positif x,

$$x + \frac{1}{x} \geqslant 2.$$

Exercice 2
Soient a et b deux réels positifs et n un entier. Montrer que

$$\left(1 + \frac{a}{b}\right)^n + \left(1 + \frac{b}{a}\right)^n \geqslant 2^{n+1}.$$

Exercice 3
Soient a, b, c et d quatre réels strictement positifs tels que $a + b + c + d = 1$. Montrer que

$$\frac{bcd}{(1-a)^2} + \frac{cda}{(1-b)^2} + \frac{dab}{(1-c)^2} + \frac{abc}{(1-d)^2} \leqslant \frac{1}{9}.$$

Exercice 4
Montrer que pour tous réels positifs x, y et z,

$$x^2 + y^4 + z^6 \geqslant xy^2 + y^2z^3 + xz^3.$$

Exercice 5
Soit x, y et z des réels positifs vérifiant $x^3y^2z = 1$. Quelle est la valeur minimale de $x+2y+3z$?

Exercice 6
Montrer que pour tout réel positif a, on a

$$\left(\frac{a^3+1}{a^2+1}\right)^2 \geqslant a^2 - a + 1.$$

Exercice 7
Trouver la plus grande constante K telle que pour tous réels positifs a, b et c, on ait

$$\sqrt{\frac{ab}{c}} + \sqrt{\frac{bc}{a}} + \sqrt{\frac{ac}{b}} \geqslant K\sqrt{a+b+c}.$$

Exercice 8
Montrer que si $x_0 > x_1 > \cdots > x_n$, alors

$$x_0 + \frac{1}{x_0 - x_1} + \frac{1}{x_1 - x_2} + \cdots + \frac{1}{x_{n-1} - x_n} \geqslant x_n + 2n.$$

Exercice 9
Soit a, b, x, y et z des réels positifs. Montrer que

$$\frac{x}{ay+bz} + \frac{y}{az+bx} + \frac{z}{ax+by} \geqslant \frac{3}{a+b}.$$

Exercice 10
Soient x, y et z des réels tels que $\frac{4}{x} + \frac{2}{y} + \frac{1}{z} = 1$. Trouver le minimum de $x + 8y + 4z$.

Exercice 11
Soient a, b et c des réels strictement positifs tels que $abc = 1$. Montrer que

$$\left(a + \frac{1}{b}\right)^2 + \left(b + \frac{1}{c}\right)^2 + \left(c + \frac{1}{a}\right)^2 \geqslant 3(a+b+c+1).$$

Exercice 12
Soient a, b et c des réels positifs tels que $abc = 1$. Prouver que

$$\frac{1}{a^3(b+c)} + \frac{1}{b^3(a+c)} + \frac{1}{c^3(a+b)} \geqslant \frac{3}{2}.$$

Exercice 13
Soit $x_1, \ldots, x_n$ des réels positifs tels que

$$\frac{1}{1+x_1} + \cdots + \frac{1}{1+x_n} = 1.$$

Prouver que $x_1 \cdots x_n \geqslant (n-1)^n$.

Exercice 14
Montrer que pour tout entier n,

$$\frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{2n-1} \geqslant n(\sqrt[n]{2} - 1).$$

Exercice 15
Montrer que si a, b et c sont des réels tels que $abc = 1$, alors

$$\frac{1}{2a^2+b^2+3}+\frac{1}{2b^2+c^2+3}+\frac{1}{2c^2+a^2+3}\leqslant\frac{1}{2}.$$

Exercice 16
Soient $a_2, \dots, a_n$ des réels positifs dont le produit vaut 1. Montrer que

$$(1+a_2)^2(1+a_3)^3\cdots(1+a_n)^n \geqslant n^n$$

– Solution des exercices –

Solution de l'exercice 1
On peut transformer cette inégalité en carré positif :

$$x+\frac{1}{x}\geqslant 2 \Leftrightarrow x^2+1\geqslant 2x \Leftrightarrow x^2-2x+1\geqslant 0 \Leftrightarrow (x-1)^2\geqslant 0$$

De façon équivalente, l'inégalité arithmético-géométrique appliquée à la somme de deux termes que constitue le membre de gauche donne

$$x+\frac{1}{x}\geqslant 2\sqrt{x\times\frac{1}{x}}=2$$

Solution de l'exercice 2
Première solution : Tentons d'appliquer l'IAG au membre de gauche, qui est composé d'une somme de 2 termes :

$$\begin{aligned}\left(1+\frac{a}{b}\right)^n+\left(1+\frac{b}{a}\right)^n &\geqslant 2\sqrt{\left(1+\frac{a}{b}\right)^n\times\left(1+\frac{b}{a}\right)^n}\\ &=2\sqrt{\left[\left(1+\frac{a}{b}\right)\left(1+\frac{b}{a}\right)\right]^n}\\ &=2\sqrt{\left(2+\frac{a}{b}+\frac{b}{a}\right)^n}\end{aligned}$$

D'après l'exercice précédent, la somme d'un nombre et de son inverse est toujours supérieure à 2. On a donc : $\frac{a}{b}+\frac{b}{a}\geqslant 2$, ce qui conduit enfin à

$$\left(1+\frac{a}{b}\right)^n+\left(1+\frac{b}{a}\right)^n\geqslant 2\sqrt{(2+2)^n}=2^{n+1}$$

Seconde solution : La fonction $x \mapsto (1+x)^n$ est convexe sur $\mathbb{R}^+$ donc, par l'inégalité de Jensen,

$$\left(1+\frac{a}{b}\right)^n + \left(1+\frac{b}{a}\right)^n \geqslant 2\left(1+\frac{\frac{a}{b}+\frac{b}{a}}{2}\right)^n$$

et on conclut comme précédemment en utilisant $\frac{a}{b}+\frac{b}{a} \geqslant 2$.

<u>*Solution de l'exercice 3*</u>

On remarque que $\frac{bcd}{(1-a)^2} = \frac{bcd}{(b+c+d)^2}$. L'IAG nous donne $bcd \leqslant \left(\frac{b+c+d}{3}\right)^3$. Donc $\frac{bcd}{(b+c+d)^2} \leqslant \frac{1}{27}(b+c+d)$. En faisant de même avec les autres termes et en sommant, il vient :

$$\frac{bcd}{(1-a)^2}+\frac{cda}{(1-b)^2}+\frac{dab}{(1-c)^2}+\frac{abc}{(1-d)^2} \leqslant \frac{3}{27}(a+b+c+d) = \frac{1}{9}$$

<u>*Solution de l'exercice 4*</u>

Il s'agit d'une simple application du lemme du tourniquet avec $a = x$, $b = y^2$ et $c = z^3$.

<u>*Solution de l'exercice 5*</u>

Il s'agit de minimiser la somme $x+2y+3z$ en exploitant la condition $x^3y^2z = 1$ grâce à l'IAG. Malheureusement, il n'y a pas de termes en x^3 ni en y^2 dans l'expression $x+2y+3z$. Il nous faut donc découper le terme x en trois termes, de telle sorte que l'application de l'IAG fasse apparaître un terme en x^3 qui devrait se simplifier grâce à l'hypothèse $x^3y^2z = 1$. De même, il nous faut séparer le terme $2y$ en deux pour obtenir un exposant deux et laisser le terme $3z$ tel quel car l'exposant 1 correspond déjà. Ainsi, on écrit

$$\begin{aligned} x+2y+3z &= \frac{1}{3}x+\frac{1}{3}x+\frac{1}{3}x+y+y+3z \\ &\geqslant 6\sqrt[6]{\frac{1}{3}x\times\frac{1}{3}x\times\frac{1}{3}x\times y\times y\times 3z} \text{ d'après l'IAG} \\ &= 6\sqrt[6]{\frac{1}{9}x^3y^2z} = 6\sqrt[6]{\frac{1}{9}} \text{ car } x^3y^2z = 1 \end{aligned}$$

Attention, il faut encore vérifier que la valeur $6\sqrt[6]{\frac{1}{9}}$ peut être atteinte pour conclure qu'il s'agit du minimum ! En effet, x, y et z étant positifs, on pourrait très bien dire sans trop de risque que $x+2y+3z \geqslant 0$, mais 0 n'est pas le minimum pour autant. Ici, en se rappelant du cas d'égalité de l'IAG, on vérifie aisément que prendre $\frac{1}{3}x = y = 3z = \sqrt[6]{\frac{1}{9}}$ convient.

<u>*Solution de l'exercice 6*</u>

On a $a^3+1 = (a+1)(a^2-a+1)$. L'inégalité à prouver est donc équivalente à $(a+1)^2(a^2-a+1) \geqslant (a^2+1)^2$. En développant, beaucoup de termes se simplifient : il reste à montrer que $a^3+a \geqslant 2a^2$, ce qui est une conséquence de l'IAG.

<u>*Solution de l'exercice 7*</u>

En élevant au carré, on obtient :

$$\frac{ab}{c}+\frac{bc}{a}+\frac{ac}{b}+2(a+b+c) \geqslant K^2(a+b+c)$$

D'après le lemme du tourniquet avec $x = \sqrt{\frac{ab}{c}}$, $y = \sqrt{\frac{bc}{a}}$ et $z = \sqrt{\frac{ac}{b}}$, on a $\frac{ab}{c} + \frac{bc}{a} + \frac{ac}{b} \geqslant a+b+c$.

Ainsi, $3 \geqslant K^2$. En prenant par exemple $a = b = c = 1$, la constante $K = \sqrt{3}$ est non seulement maximale mais aussi atteinte. C'est donc la réponse à cet exercice.

Solution de l'exercice 8

L'astuce est de faire apparaître les termes $x_0 - x_1, x_1 - x_2, \ldots, x_{n-1} - x_n$ grâce à un télescopage sur le terme $x_0 - x_n$. De fait, on a :

$$x_0 - x_n = (x_0 - x_1) + (x_1 - x_2) + \cdots + (x_{n-1} - x_n)$$

de sorte que l'inégalité demandée est équivalente à

$$(x_0 - x_1) + (x_1 - x_2) + \cdots + (x_{n-1} - x_n) + \frac{1}{x_0 - x_1} + \frac{1}{x_1 - x_2} + \cdots + \frac{1}{x_{n-1} - x_n} \geqslant 2n$$

ou encore, en mettant chaque terme avec son inverse, à

$$\left(x_0 - x_1 + \frac{1}{x_0 - x_1}\right) + \left(x_1 - x_2 + \frac{1}{x_1 - x_2}\right) + \cdots + \left(x_{n-1} - x_n + \frac{1}{x_{n-1} - x_n}\right) \geqslant 2n$$

ce qui est vrai en appliquant le résultat de l'exercice 1 pour $x = x_0 - x_1, x_1 - x_2, \ldots, x_{n-1} - x_n$.

Solution de l'exercice 9

On fait apparaître du degré 2 au numérateur pour pouvoir utiliser l'inégalité des mauvais élèves.

$$\begin{aligned}\frac{x}{ay+bz} + \frac{y}{az+bx} + \frac{z}{ax+by} \geqslant \frac{3}{a+b} &= \frac{x^2}{axy+bzx} + \frac{y^2}{ayz+bxy} + \frac{z^2}{azx+byz} \\ &\geqslant \frac{(x+y+z)^2}{(a+b)(xy+yz+zx)}\end{aligned}$$

Or $(x+y+z)^2 = x^2+y^2+z^2+2(xy+yz+zx) \geqslant 3(xy+yz+zx)$ d'après le lemme du tourniquet, ce qui conclut.

Solution de l'exercice 10

D'après l'inégalité de Cauchy-Schwarz,

$$\left(\frac{4}{x} + \frac{2}{y} + \frac{1}{z}\right)(x + 8y + 4z) \geqslant \left(\sqrt{\frac{4}{x}}.\sqrt{x} + \sqrt{\frac{2}{y}}.\sqrt{8y} + \sqrt{\frac{1}{z}}.\sqrt{4z}\right)$$

Vu que $\frac{4}{x} + \frac{2}{y} + \frac{1}{z} = 1$, on obtient $x + 8y + 4z \geqslant (2+4+2)^2 = 64$.

Pour montrer que ce minimum est atteint, étudions le cas d'égalité de l'inégalité de Cauchy-Schwarz : on doit avoir $\frac{\sqrt{\frac{4}{x}}}{\sqrt{x}} = \frac{\sqrt{\frac{2}{y}}}{\sqrt{8y}} = \frac{\sqrt{\frac{1}{z}}}{\sqrt{4z}}$, c'est-à-dire $\frac{2}{x} = \frac{1}{2y} = \frac{1}{2z}$. La contrainte $\frac{4}{x} + \frac{2}{y} + \frac{1}{z} = 1$ permet alors de trouver $x = 16$, $y = 4$ et $z = 4$ comme triplet qui convient.

Solution de l'exercice 11

D'après l'inégalité des mauvais élèves (ou l'inégalité de Jensen appliquée à la fonction convexe $x \mapsto x^2$), on a :

$$\left(a + \frac{1}{b}\right)^2 + \left(b + \frac{1}{c}\right)^2 + \left(c + \frac{1}{a}\right)^2 \geqslant \frac{\left(a+b+c+\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)^2}{1+1+1}$$

Par l'IAG, $\frac{1}{a}+\frac{1}{b}+\frac{1}{c} \geqslant 3$ et l'inégalité à prouver devient une inégalité en une seule variable $S=a+b+c$: $\frac{(S+3)^2}{3} \geqslant 3(S+1)$, qui est équivalente à $S(S-3) \geqslant 0$. Et on a bien $S \geqslant 3$ encore d'après l'IAG en faisant intervenir le fait que $abc=1$.

Solution de l'exercice 12
On ne se lasse pas de faire appel à l'inégalité des mauvais élèves :

$$\begin{aligned}
\frac{1}{a^3(b+c)}+\frac{1}{b^3(a+c)}+\frac{1}{c^3(a+b)} &= \frac{\left(\frac{1}{a}\right)^2}{a(b+c)}+\frac{\left(\frac{1}{b}\right)^2}{b(a+c)}+\frac{\left(\frac{1}{c}\right)^2}{c(a+b)} \\
&\geqslant \frac{\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)^2}{a(b+c)+b(a+c)+c(a+b)} \\
&= \frac{(ab+bc+ca)^2}{2(ab+bc+ca)} \text{ vu que } abc=1 \\
&= \frac{1}{2}(ab+bc+ca)
\end{aligned}$$

On termine l'exercice en remarquant finalement que $ab+bc+ca \geqslant 3\sqrt[3]{a^2b^2c^2}=3$ d'après l'IAG.

Solution de l'exercice 13
La difficulté de cet exercice est de réussir à exploiter la condition $\dfrac{1}{1+x_1}+\cdots+\dfrac{1}{1+x_n}=1$, qu'on voit mal comment faire apparaître à partir du produit $x_1\cdots x_n$. Pour y voir plus clair, posons donc $y_i=\frac{1}{1+x_i}$, de sorte que $y_1+\ldots+y_n=1$ (*), et reformulons le problème avec les y_i. Comme $x_i=\frac{1}{y_i}-1$, l'inégalité à prouver se réécrit

$$\prod_{i=1}^{n}\left(\frac{1}{y_i}-1\right) \geqslant (n-1)^n$$

ou encore

$$\prod_{i=1}^{n}(1-y_i) \geqslant (n-1)^n \prod_{i=1}^{n} y_i$$

Par ailleurs, en utilisant (*) et l'IAG, on obtient

$$1-y_i=\sum_{\substack{j=1\\ j\neq i}}^{n} y_j \geqslant (n-1)\sqrt[n-1]{\prod_{\substack{j=1\\ j\neq i}}^{n} y_j}$$

Le produit de cette inégalité pour i allant de 1 à n conduit finalement au résultat souhaité.

Solution de l'exercice 14
L'idée principale est de passer le n de l'autre côté en le réécrivant $1+1+\cdots+1$. L'inégalité se réécrit :

$$\left(1+\frac{1}{n}\right)+\left(1+\frac{1}{n+1}\right)+\cdots+\left(1+\frac{1}{2n-1}\right) \geqslant n\sqrt[n]{2}$$

soit

$$\frac{n+1}{n}+\frac{n+2}{n+1}+\cdots+\frac{2n}{2n-1} \geqslant \sqrt[n]{2}$$

Or, l'IAG donne justement :

$$\frac{n+1}{n}+\frac{n+2}{n+1}+\cdots+\frac{2n}{2n-1}\geqslant n\sqrt[n]{\frac{n+1}{n}\times\frac{n+2}{n+1}\times\cdots\times\frac{2n}{2n-1}}$$

Le produit de droite se simplifie par télescopage, fournissant ainsi le résultat annoncé.

Solution de l'exercice 15

D'après l'IAG, $a^2+b^2\geqslant 2ab$ et $a^2+1\geqslant 2a$ donc $2a^2+b^2+3\geqslant 2(ab+a+1)$. En faisant de même avec les autres termes, il vient :

$$\frac{1}{2a^2+b^2+3}+\frac{1}{2b^2+c^2+3}+\frac{1}{2c^2+a^2+3}\leqslant\frac{1}{2}\left(\frac{1}{ab+a+1}+\frac{1}{bc+b+1}+\frac{1}{ca+c+1}\right)$$

Or $abc=1$ donc d'une part $\frac{1}{ab+a+1}=\frac{1}{\frac{1}{c}+a+1}=\frac{c}{1+ca+c}$ et d'autre part $\frac{1}{bc+b+1}=\frac{1}{\frac{1}{a}+\frac{1}{ca}+1}=\frac{ca}{c+1+ca}$. On a donc la bonne surprise que

$$\frac{1}{ab+a+1}+\frac{1}{bc+b+1}+\frac{1}{ca+c+1}=\frac{c}{1+ca+c}+\frac{ca}{c+1+ca}+\frac{1}{ca+c+1}=1$$

ce qui achève la preuve.

Solution de l'exercice 16

Il s'agit de découper judicieusement chaque parenthèse pour lui appliquer l'IAG :

$$\begin{aligned}(1+a_2)^2&\geqslant 2^2\times a_2\\(1+a_3)^3=\left(\frac{1}{2}+\frac{1}{2}+a_3\right)^3&\geqslant 3^3\times\frac{1}{2}\times\frac{1}{2}\times a_3\\(1+a_4)^4=\left(\frac{1}{3}+\frac{1}{3}+\frac{1}{3}+a_4\right)^4&\geqslant 4^4\times\frac{1}{3}\times\frac{1}{3}\times\frac{1}{3}\times a_4\\&\cdots\\(1+a_n)^n=\left(\frac{1}{n-1}+\cdots+\frac{1}{n-1}+a_n\right)^n&\geqslant n^n\times\frac{1}{(n-1)^{n-1}}\times a_n\end{aligned}$$

Il ne reste plus qu'à faire le produit de ces inégalités pour que l'exercice soit terminé.

2 Arithmétique

1 Exercices divers

Exercice 1
Théorème de Wilson montrer que $(p-1)! \equiv -1 \pmod p$ ssi p est un nombre premier.

Exercice 2
A quelle condition sur le nombre premier p existe-t-il un entier a tel que $a^2 \equiv -1 \pmod p$?

Exercice 3
Résoudre l'équation $x^2 + y^2 + z^2 = 2xyz$ dans $\mathbb{Z}$.

Exercice 4
Montrer que, pour tout entier ℓ il existe un carré de largeur ℓ dans $\mathbb{Z}^2$ tel que tous les points à coordonnées entières dans ce carré soient cachés, pour un observateur situé à l'origine, par d'autres points de $\mathbb{Z}^2$.

Exercice 5
Soit a et b deux entiers. Montrer que $a^3 + b^3 + 4$ n'est pas un cube.

Exercice 6
Trouver toutes les fonctions f de $\mathbb{N}*$ dans $\mathbb{N}*$ tel que $m^2 + f(n)$ divise $mf(m) + n$ pour tous m et n.

– Solutions des exercices –

Solution de l'exercice 1
On regroupe chaque entier avec son inverse, -1 et 1 sont les seuls qui soient leurs propres inverses et restent seuls d'où le -1.

Solution de l'exercice 2
Première preuve : On regroupe de même par classe d'équivalence où y x ssi $y = -x, y = x, y = -1/x, y = 1/x$. 1 et -1 forment une classe de taille 2 les éventuelles racine de -1 formeraient une seconde classe de taille 2. Toutes les autres classes sont de taille 4, or la somme de leurs tailles fait $p-1$, donc si et seulement si $p = 1[4]$ ou p=2, on peut trouver une racine carrée de -1. Seconde preuve : lemme x est un carré mod p ssi $x^{(p-1)/2} = 1$, pour le caractère nécessaire on emploie petit fermat sur $a^2 = x$ Pour le caractère suffisant on regarde $X^{(p-1)/2} - 1$ comme un polynôme de $\mathbb{Z}/p\mathbb{Z}$ il a au plus $(p-1)/2$ racines or les carrés en sont racines et il y a exactement $(p-1)/2$ carrés (on regroupe les entiers par paire si $p|a^2 - b^2$ alors $a = b[p]$ ou $a = -b[p]$) ce qui conclut le lemme On l'applique à $-1^{(p-1)/2}$et on obtient la même conclusion qu'avec la première preuve

Solution de l'exercice 3
Soit n maximal tel que $2^n|x$ $2^n|y$ $2^n|z$ En posant les variables simplifiés $x' = x/2^n$, et en regardant mod 4 les x, y et z sont divisibles par 2 contradiction avec la maximalité de n Donc $(0, 0, 0)$ est la seule solution.

Solution de l'exercice 4
On bourrine le théorème des restes chinois Pour chaque couple (i, j) on choisit un nombre premier différent $p_{i,j}$ Puis on choisit l'origine du carré congrue $\forall(i, j)x = -i[p_{i,j}]$ et $\forall(i, j)y = -j[p_{i,j}]$ Ainsi chaque point $(x + i, y + j)$ est dissimulé par le point où on divise par $p_{i,j}$

Solution de l'exercice 5
Les cubes sont $0, 1, 8$ mod 9 donc l'expression fait de 2 à 6 mod 9 et n'est pas un cube.

Solution de l'exercice 6
Avec $m = f(n)$ on a $f(n)(f(n) + 1)|f(n)f(f(n)) + n$ donc $f(n)|f(n)f(f(n)) + n$ donc $f(n)|n$, $f(n) \leqslant n$ Avec m=n il vient $n^2 + f(n)|nf(n) + n$ donc $n^2 + f(n) \leqslant nf(n) + n$ donc $n^2 - n \leqslant (n-1)f(n)$ donc l'identité est la seule solution

2 Ordre multiplicatif et petit théorème de Fermat

– Le petit théorème de Fermat et ses démonstrations –

Comme son nom l'indique, ce cours a pour objectif la démonstration, l'étude et l'utilisation du petit théorème de Fermat ainsi que de son pendant, la notion d'ordre multiplicatif dans $\mathbb{Z}/n\mathbb{Z}$.

Commençons donc par énoncer le petit théorème de Fermat.

Théorème 2.2.1 (Petit théorème de Fermat)**.**
Soit a un entier et p un nombre premier. Alors $a^p \equiv a \pmod{p}$.

Il existe bien sûr une version équivalente de ce théorème.

Théorème 2.2.2 (Petit théorème de Fermat, version n°2)**.**
Soit a un entier et p un nombre premier. Si p ne divise pas a, alors $a^{p-1} \equiv 1 \pmod{p}$.

Remarquons que ces deux théorèmes sont bien équivalents l'un à l'autre. En effet, si le Théorème 2.2.1 est vrai, alors, pour tout élément $a \not\equiv 0 \pmod{p}$, et puisque a est inversible dans $\mathbb{Z}/p\mathbb{Z}$ en vertu du théorème de Bézout, on sait que $a^{p-1} - 1 \equiv a^{-1}(a^p - a) \equiv 0 \pmod{p}$. Réciproquement, si le Théorème 2.2.2 est vrai, alors $a^p - a \equiv a(a^{p-1} - 1) \equiv 0 \pmod{p}$ dès que $a \not\equiv 0 \pmod{p}$, et il est clair que $a^p \equiv a \pmod{p}$ quand $a \equiv 0 \pmod{p}$ également.

Nous allons maintenant donner plusieurs preuves différentes de ce théorème, basées sur des idées à chaque fois différentes.

Démonstration n°1. Tout d'abord, si $a \equiv 0 \pmod{p}$, alors $a^p \equiv 0^p \equiv 0 \equiv a \pmod{p}$. On supposera désormais que $a \not\equiv 0 \pmod{p}$. Étudions alors la fonction $\varphi_a : x \mapsto ax \pmod{p}$.

Pour tout $x \not\equiv 0 \pmod{p}$, on note que $ax \not\equiv 0 \pmod{p}$ non plus. Cela signifie que la fonction $x \mapsto ax \pmod{p}$ induit en fait une fonction φ_a de l'ensemble $(\mathbb{Z}/p\mathbb{Z})^*$ dans lui-même. Or, si $\varphi_a(x) \equiv \varphi_a(y)$, alors $x \equiv a^{-1}\varphi_a(x) \equiv a^{-1}\varphi_a(y) \equiv y \pmod{p}$. Cela signifie que φ_a est injective. Puisque $(\mathbb{Z}/p\mathbb{Z})^*$ est fini, la fonction φ_a est donc bijective.

Soit alors Δ le produit $\prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} x \equiv (p-1)! \pmod{p}$. Par construction, Δ est inversible dans $\mathbb{Z}/p\mathbb{Z}$, en tant que produit d'inversibles. Puisque φ_a est bijective, on remarque donc également que

$$\Delta \equiv \prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} \varphi_a(x) \equiv \prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} (ax) \equiv a^{p-1} \prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} x \equiv a^{p-1}\Delta \pmod{p}.$$

Comme Δ est inversible, on en déduit que $a^{p-1} \equiv 1 \pmod p$, ce qui conclut. □

Démonstration n°2. Nous allons montrer par récurrence que $a^p \equiv a \pmod p$ pour tout entier a tel que $0 \leqslant a \leqslant p-1$.

Tout d'abord, pour $a = 0$, il est clair que $0^p \equiv 0 \pmod p$. On procède donc à l'hérédité de la récurrence.

Notons que, si $1 \leqslant k \leqslant p-1$, alors p ne divise ni $k!$ ni $(p-k)!$, donc que p divise le coefficient binomial $\binom{p}{k}$. Par conséquent, si $a \geqslant 0$ est un entier tel que $a^p \equiv a \pmod p$, alors

$$(a+1)^p \equiv \sum_{k=0}^{p} \binom{p}{k} a^k \equiv \binom{p}{0} + \binom{p}{p} a^p \equiv 1 + a^p \equiv 1 + a \pmod p.$$

Ceci achève la récurrence et donc la preuve du théorème. □

Démonstration n°3. Nous allons cette fois-ci dénombrer des p-uplets d'entiers compris entre 0 et $a-1$ (cette preuve peut aussi être vue comme un dénombrement de *colliers de perles colorées*).

Notons donc Ω l'ensemble $\{0, 1, \ldots, a-1\}^p$ des p-uplets $\mathbf{x} = (x_0, x_1, \ldots, x_{p-1})$ dont chaque coordonnée x_i est un entier compris entre 0 et $a-1$. On dira qu'un p-uplet $\mathbf{x}$ est *constant* si $x_0 = x_1 = \ldots = x_{p-1}$, et *varié* sinon. Parmi les p-uplets contenus dans l'ensemble Ω, il y en a clairement a qui sont constants, et donc $a^p - a$ qui sont variés. Dans la suite, on notera Ω' l'ensemble des p-uplets variés.

On considère maintenant la fonction de *rotation* $\mathbf{T} : \Omega' \mapsto \Omega'$ telle que

$$\mathbf{T}(x_0, x_1, \ldots, x_{p-1}) = (x_1, x_2, \ldots, x_{p-1}, x_0).$$

La fonction $\mathbf{T}$ est clairement bijective, et sa composée $p^{\text{ème}}$ n'est autre que la fonction identité. Elle partitionne donc Ω' en *orbites*, c'est-à-dire en ensembles, deux à deux disjoints, de la forme $\{\mathbf{T}^k(\mathbf{x}) : k \in \mathbb{N}\}$, où $\mathbf{x}$ est un élément quelconque de Ω.

Soit $\mathbf{x}$ un p-uplet varié, et soit ω le plus petit entier naturel non nul tel que $\mathbf{T}^\omega(\mathbf{x}) = \mathbf{x}$. Soit également q et r le quotient et le reste de la division euclidienne de p par ω. Alors

$$\mathbf{T}^r(\mathbf{x}) = \mathbf{T}^r(\mathbf{T}^{q\omega}(\mathbf{x})) = \mathbf{T}^p(\mathbf{x}) = \mathbf{x}.$$

Puisque $0 \leqslant r \leqslant \omega - 1$, et par minimalité de ω, c'est donc que $r = 0$, c'est-à-dire que ω divise p.

Or, puisque les coefficients x_i ne sont pas tous égaux, il existe un entier $j \leqslant p-2$ tel que $x_j \neq x_{j+1}$. Cela montre que $\mathbf{x} \neq \mathbf{T}(\mathbf{x})$, et donc que $\omega \neq 1$, de sorte que $\omega = p$.

On montre alors, en réutilisant le raisonnement ci-dessus, que $\mathbf{T}^k(x) = \mathbf{T}^\ell(x)$ si et seulement si $k \equiv \ell \pmod p$. Par conséquent, l'orbite $\{\mathbf{T}^k(\mathbf{x}) : k \in \mathbb{N}\}$ est formée d'exactement p éléments. Puisque l'on a partitionné Ω' en ensembles à p éléments chacun, c'est donc que p divise $|\Omega'| = a^p - a$. □

Cette troisième preuve, si elle peut paraître plus compliquée, fait également apparaître de manière explicite la notion d'ordre, dont l'ordre multiplicatif est en fait un cas particulier.

– L'ordre d'une permutation et d'un élément par une permutation –

Définition 2.2.3.
Soit $\mathcal{S}$ un ensemble quelconque et soit x un élément de $\mathcal{S}$. On appelle *permutation* de $\mathcal{S}$ toute fonction $\sigma : \mathcal{S} \to \mathcal{S}$ bijective.

On appelle *orbite* de σ engendrée par x l'ensemble $\{\sigma^k(x) \ : \ x \in \mathbb{Z}\}$. Si cette orbite est de cardinal $\omega(x)$ fini, alors on dit que $\omega(x)$ est l'*ordre* de x pour la permutation σ ; sinon, on dit que x est d'ordre infini.

Par ailleurs, s'il existe un entier m tel que $\sigma^m(y) = y$ pour tout $y \in \mathcal{S}$, alors on dit que m est l'*ordre* de σ ; sinon, on dit également que σ est d'ordre infini.

On peut alors montrer facilement trois propriétés très importantes sur les orbites d'une permutation ainsi que sur l'ordre d'un élément et d'une permutation.

Proposition 2.2.4.
Soit σ une permutation d'un ensemble $\mathcal{S}$. Tout élément de $\mathcal{S}$ appartient à une unique orbite de σ.

Proposition 2.2.5.
Soit σ une permutation d'un ensemble $\mathcal{S}$ et soit x un élément de $\mathcal{S}$. Si x est d'ordre $\omega(x)$ fini, alors, pour tous $k, \ell \in \mathbb{Z}$, $\sigma^k(x) = \sigma^\ell(x)$ si et seulement si $k \equiv \ell \pmod{\omega(x)}$; sinon, alors $\sigma^k(x) = \sigma^\ell(x)$ si et seulement si $k = \ell$.

De même, si σ est d'ordre ω fini, alors, pour tous $k, \ell \in \mathbb{Z}$, $\sigma^k = \sigma^\ell$ si et seulement si $k \equiv \ell \pmod{\omega}$; sinon, alors $\sigma^k = \sigma^\ell$ si et seulement si $k = \ell$.

Proposition 2.2.6.
Soit σ une permutation d'un ensemble $\mathcal{S}$. S'il existe un élément $x \in \mathcal{S}$ d'ordre infini, ou s'il existe des éléments $x_1, x_2, \ldots \in \mathcal{S}$ d'ordres finis mais arbitrairement grands, alors σ est d'ordre infini. Au contraire, s'il existe un entier ℓ tel que tout élément $x \in \mathcal{S}$ soit d'ordre au plus ℓ, alors σ est d'ordre m, où m est le PPCM de tous les ordres $\omega(x)$ des éléments de $\mathcal{S}$.

– Ordre multiplicatif d'un élément dans $(\mathbb{Z}/n\mathbb{Z})^*$ –

On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles modulo n et $\varphi(n)$ l'indicatrice d'Euler de l'entier n, c'est-à-dire le cardinal de l'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$. Alors on peut généraliser le petit théorème de Fermat comme suit.

Théorème 2.2.7 (Théorème d'Euler-Fermat)**.**
Soit a et n deux entiers naturels non nuls premiers entre eux. Alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Démonstration. On va généraliser la démonstration n°1 du petit théorème de Fermat en faisant explicitement appel à des permutations de $(\mathbb{Z}/n\mathbb{Z})^*$. Soit φ_a la fonction définie par $\varphi_a : x \to ax \pmod{n}$. Dès lors que x est premier avec n, ax l'est également, donc φ_a induit une fonction de $(\mathbb{Z}/n\mathbb{Z})^*$ dans lui-même. Par ailleurs, puisque a est inverible modulo n, la fonction φ_a est injective, et puisque $(\mathbb{Z}/n\mathbb{Z})^*$ est fini, φ_a est en fait bijetive. C'est donc une permutation de $(\mathbb{Z}/n\mathbb{Z})^*$.

Soit alors Δ le produit $\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^*} x$. Puisque φ_a est bijective, on remarque que

$$\Delta = \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^*} \varphi_a(x) \equiv \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^*} (ax) \equiv a^{\varphi(n)} \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^*} x \equiv a^{\varphi(n)}\Delta \pmod n.$$

Or, Δ est un produit d'inversibles modulo n, donc est également inversible. On en déduit que $a^{\varphi(n)} \equiv 1 \pmod n$. ☐

Remarquons que la permutation φ_a est en fait elle-même d'ordre ω. Par ailleurs, ce théorème généralise bien le petit théorème de Fermat, puisque $\varphi(p) = p-1$ quand p est un nombre premier.

Définition 2.2.8.
Soit a et n deux entiers naturels non nuls premiers entre eux. On appelle *ordre* de a modulo n, et l'on note $\omega_n(a)$, le plus petit entier tel que $a^{\omega_n(a)} \equiv 1 \pmod n$.

Proposition 2.2.9.
Soit a et n deux entiers naturels non nuls premiers entre eux, et soit $\omega_n(a)$ l'ordre de a modulo n. Pour tous $k, \ell \in \mathbb{N}$, $a^k \equiv a^\ell \pmod n$ si et seulement si $k \equiv \ell \pmod{\omega_n(a)}$. En particulier, $\omega_n(a)$ divise $\varphi(n)$.

On peut aussi se poser des questions telles que : « Étant donnés deux entiers k et n, existe-t-il un élément d'ordre k modulo n ? » ou encore « Si x est d'ordre $\omega_n(x)$ modulo n et $\omega_m(x)$ modulo m, quel est l'ordre de x modulo mn ?

Afin de fournir des réponses partielles à cette question, on aura besoin d'utiliser le Théorème chinois.

– Théorème chinois –

La légende raconte que le Théorème chinois a été inventé par des généraux, du temps de la Chine impériale, afin de pouvoir compter rapidement combien de soldats comptaient leurs innombrables légions. Pour ce faire, ils répartissaient les soldats par groupes de 16, pour et comptaient combien ils restait de soldats n'appartenant à aucun groupe. Puis ils recommençaient en utilisant successivement des groupes de 9, de 5, de 7, de 11 et de 13. Et à la fin, ils en déduisaient rapidement combien de soldats comptait leur armée.

Pour s'aider dans leur tâche, ces généraux connaissent bien sûr la propriété suivante du PPCM de deux entiers.

Lemme 2.2.10.
Soit a, b et c trois entiers, tels que a et b soient naturels non nuls. Alors a et b divisent simultanément c si et seulement si leur PPCM, que l'on notera $a \vee b$, divise c.

Démonstration. Tout d'abord, si $a \vee b$ divise c, alors a et b divisent clairement c eux aussi. Réciproquement, soit q et r le quotient et le reste de la division euclidienne de c par $a \vee b$. Si a et b divisent c, alors ils divisent également $r = c - q \times (a \vee b)$. Puisque $0 \leqslant r \leqslant (a \vee b) - 1$, et par minimalité de $a \vee b$, cela signifie que $r = 0$, donc que $a \vee b$ divise c. ☐

Théorème 2.2.11 (Théorème chinois)**.**
Soit m et n deux entiers naturels non nuls, premiers entre eux. Il existe une fonction bijective $\psi : (\mathbb{Z}/mn\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ telle que, pour tout triplet (a, b, c) vérifiant la relation $\psi(a) = (b, c)$ et tout entier x, on ait $x \equiv a \pmod{mn}$ si et seulement si $x \equiv b \pmod{m}$ et $x \equiv c \pmod{n}$.

Démonstration. Pour tous les entiers x et y, remarquons que $x \equiv y \pmod{mn}$ si et seulement si $x \equiv y \pmod{m}$ et $x \equiv y \pmod{n}$, puisque $mn = m \vee n$. Par conséquent, et si l'on identifie les éléments de chaque ensemble $(\mathbb{Z}/\ell\mathbb{Z})$ avec les entiers compris entre 0 et $\ell - 1$, il nous suffit d'associer, à chaque élément a de $(\mathbb{Z}/mn\mathbb{Z})$, la paire $\psi(a) = (b, c)$ tel que b et c soient respectivement les restes des divisions euclidiennes de a par m et n. □

– Quelques applications –

On liste maintenant quelques résultats que l'on peut démontrer en utilisant les théorèmes ci-dessus ou en s'inspirant de leurs démonstrations. Hormis la Proposition 2.2.13 et le Théorème 2.2.16, toutes les preuves sont laissées en exercice au lecteur.

Proposition 2.2.12.
Soit $A(X)$ et $B(X)$ deux polynômes à coefficients entiers, et soit p un nombre premier. Alors tous les coefficients du polynôme $(A(X) + B(X))^p - A(X)^p - B(X)^p$ sont divisibles par p.

Proposition 2.2.13.
Soit n un entier et p un facteur premier de $\varphi(n)$. Montrer qu'il existe un entier d'ordre p modulo n.

Démonstration. Cette fois-ci, nous allons considérer l'ensemble Γ des p-uplets $\mathbf{x} = (x_0, x_1, \ldots, x_{p-1})$ d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ tels que $x_0\, x_1 \cdots x_{p-1} \equiv 1 \pmod{n}$. On dit toujours qu'un p-uplet $\mathbf{x}$ est contant si $x_0 = x_1 = \ldots = x_{p-1}$, et varié sinon. Enfin, on note Γ' l'ensemble des p-uplets variés.

Notons que $|\Gamma| = \varphi(n)^{p-1}$ et qu'il existe exactement un p-uplet constant $(x, x, \ldots, x)$ pour chaque élément x dont l'ordre divise p. Il s'agit du p-uplet $(1, 1, \ldots, 1)$ et des p-uplets $(x, x, \ldots, x)$ pour chaque x d'ordre exactement p. Si l'on note ℓ le nombre d'éléments d'ordre p, on a donc $|\Gamma| = |\Gamma'| + \ell + 1$.

La fonction de *rotation* $\mathbf{T} : \Gamma' \mapsto \Gamma'$ est toujours bijective, et sa composée $p^{\text{ème}}$ est la fonction identité. Elle partictionne donc Γ' en orbites dont le cardinal vaut p, car il divise l'ordre de $\mathbf{T}$ mais ne peut être égal à 1. Cela montre que p divise $|\Gamma'|$.

Comme p divise $\varphi(n)$, et donc $|\Gamma|$ également, on en déduit que $\ell \equiv -1 \pmod{p}$, donc que $\ell \geqslant p - 1 \geqslant 1$. □

On aurait aussi pu invoquer les résultats suivants ; la preuve du dernier ne sera pas abordée ici.

Proposition 2.2.14.
Soit a, b et n trois entiers tels que a divise b et n soit premier avec b. Alors l'ordre de n modulo a divise l'ordre de n modulo b.

Proposition 2.2.15.
Soit $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la décomposition d'un entier n en tant que produit de facteurs premiers, et soit x un entier premier avec n. Alors l'ordre de x modulo n est égal au PPCM des ordres de x modulo les $p_i^{\alpha_i}$.

Théorème 2.2.16.
Soit p un nombre premier. Il existe un entier n, non multiple de p, dont l'ordre modulo p vaut $p-1$.

– Exercices –

Exercice 1
Montrer que 13 divise $5^{60} - 3^{48}$.

Exercice 2
Montrer que 5 divise $2^{3n+5} + 3^{n+1}$ pour tout entier $n \geqslant 0$.

Exercice 3
Trouver le plus grand entier d qui divise $n^5 - n$ pour tout entier $n \in \mathbb{Z}$.

Exercice 4
Calculer 3×37 puis 27×37, puis donner un critère de divisibilité par 37.

Exercice 5
Vrai ou faux ? « Si a, b et c sont trois entiers tels que a divise bc mais ne divise pas b, alors a divise c. »

Exercice 6
Démontrer les Propositions 2.2.4, 2.2.6 et 2.2.5.

Exercice 7
Soit n un entier naturel non nul, et n le PPCM de tous les entiers inférieurs ou égaux à m. Soit également σ une permutation de l'ensemble $\{1, 2, \ldots, n\}$. Montrer que σ est d'ordre fini, et que l'ordre de σ divise m.

Exercice 8
Démontrer la Proposition 2.2.9.

Exercice 9
Pour tout entier naturel n, on note $\mathbf{S}(n)$ la somme des chiffres de n. Calculer $\mathbf{S}^5\left(2018^{2018^{2018}}\right)$.

Exercice 10
Soit k un entier premier avec 6. Montrer qu'il existe un entier $n \geqslant 0$ tel que k divise $2^n + 3^n + 6^n - 1$.

Exercice 11
Sachant que l'armée Chinoise comptait à l'époque strictement moins de 720720 soldats, comment les généraux chinois faisaient-ils pour évaluer précisément sa taille ?

Exercice 12
Démontrer la Proposition 2.2.12.

Exercice 13
Démontrer la Proposition 2.2.14.

Exercice 14
Démontrer la Proposition 2.2.15.

Exercice 15
Trouver les paires d'entiers (k, ℓ) telles que $5k + 3\ell = 32$.

– Solutions des exercices –

Solution de l'exercice 1
Le petit théorème de Fermat indique que $5^{12} \equiv 3^{12} \equiv 1 \pmod{13}$. Par conséquent,

$$5^{60} - 3^{48} \equiv (5^{12})^5 - (3^{12})^4 \equiv 1^5 - 1^4 \equiv 0 \pmod{13}.$$

Solution de l'exercice 2
Il suffit de vérifier, pour tout $n \in \mathbb{N}$, que

$$2^{3n+5} + 3^{n+1} \equiv 8^n \times 32 + 3^n \times 3 \equiv 3^n \times 2 + 3^n \times 3 \equiv 3^n \times 5 \equiv 0 \pmod{5}.$$

Solution de l'exercice 3
Tout d'abord, d doit diviser $2^5 - 2 = 30$. On va donc montrer que $d = 30 = 2 \times 3 \times 5$ convient. Pour ce faire, il suffit de constater que, si $p \in \{2, 3, 5\}$, alors $p - 1$ divise $5 - 1 = 4$, de sorte que $n^5 \equiv n \pmod{p}$ pour tout $n \in \mathbb{Z}$. Par conséquent, $n^5 - n$ est divisible par $2 \vee 3 \vee 5 = 30$.

Solution de l'exercice 4
On vérifie aisément que $3 \times 37 = 111$, puis que $27 \times 37 = 9 \times 3 \times 37 = 999$. Cela signifie que $10^3 \equiv 1 \pmod{37}$. En outre, $10^2 \equiv -11 \pmod{37}$. Par conséquent, un nombre $n = \overline{n_d n_{d-1} \dots n_1 n_0}^{10}$ est divisible par 37 si et seulement si

$$\sum_{k=0}^{d/3} (n_{3k} + 10 n_{3k+1} - 11 n_{3k+2})$$

est divisible par 37.

Solution de l'exercice 5
Cette assertion est évidement fausse, par exemple si $b = c = 2$ et $a = bc = 4$. En revanche, si a est un nombre premier, le théorème de Gauss montre qu'elle est vraie.

Solution de l'exercice 6

Tout d'abord, il est clair que tout $x \in \mathcal{S}$ appartient à l'orbite engendrée par x. D'autre part, s'il appartient également à l'orbite engendrée par y, alors il existe un $\ell \in \mathbb{Z}$ tel que $\sigma^\ell(y) = x$, et alors $\{\sigma^k(x) : k \in \mathbb{Z}\} = \{\sigma^{k+\ell}(y) : k \in \mathbb{Z}\} = \{\sigma^k(y) : k \in \mathbb{Z}\}$. Cela montre la Proposition 2.2.4.

Soit k et ℓ deux entiers naturels éventuels tels que $\sigma^k(x) = \sigma^\ell(x)$, $k < \ell$, que $k + \ell$ soit minimal. Alors $\sigma^{\ell-k}(x) = x$, donc $k = 0$ et $\omega(x)$ est fini, avec $\ell = \omega(x)$. En particulier, les éléments $\sigma^k(x)$, pour $0 \leqslant k \leqslant \omega(x) - 1$, sont deux à deux distincts. De surcroît, pour tout $a \in \mathbb{Z}$, si q et r sont le quotient et le reste de la division euclidienne de a par $\omega(x)$, alors $\omega^a(x) = \omega^r \circ \omega^{kq}(x) = \omega^r(x)$, de sorte que $\omega^k(x) = \omega^\ell(x)$ si et seulement si $k \equiv \ell \pmod{\omega(x)}$. La même preuve s'adapte immédiatement pour l'ordre de la permutation σ elle-même, ce qui conclut la preuve de la Proposition 2.2.5.

Enfin, si σ est d'ordre ω fini, alors tout élément x est d'ordre $\omega(x)$ fini, avec $\omega(x)$ un diviseur de ω. Par conséquent, m est un multiple du PPCM des ordres des éléments de $\mathcal{S}$. Réciproquement, si on note π le PPCM de ces ordres, alors il est clair que $\sigma^\pi(x) = x$ pour tout x, donc que π divise $\omega(x)$. Cela montre que $\pi = \omega(x)$, ce qui conclut.

Solution de l'exercice 7

La Proposition 2.2.4 montre que σ partitionne en orbites de tailles $t_1, \ldots, t_k$. Chaque entier t_k est inférieur ou égal à n, donc divise m. Par conséquent, les Propositions 2.2.5 et 2.2.6 montrent que l'ordre de σ divise m également.

Solution de l'exercice 8

Il s'agit là d'une simple reformulation de la Proposition 2.2.5, appliquée à la permutation $\varphi_a : x \mapsto ax$ et à l'élément 1.

Solution de l'exercice 9

Il est clair que $A \equiv B \equiv C \equiv D \equiv E \pmod 9$. Puisque 2 est d'ordre 6 modulo 9, on trouve alors

$$2018^{2018} \equiv 2^{2018} \equiv 0 \pmod 2 \text{ et } 2018^{2018} \equiv 2^{2018} \equiv (-1)^{2018} \equiv 1 \pmod 3,$$

donc $2018^{2018} \equiv 4 \pmod 6$, de sorte que

$$E \equiv 2018^{2018^{2018}} \equiv 2^{2018^{2018}} \equiv 2^4 \equiv 7 \pmod 9.$$

D'autre part, $A < 10^{4 \times 2018^{2018}}$ donc $B < 9 \times 4 \times 2018^{2018} < 10^{2+4\times 2018}$, puis $C < 9 \times 2 + 9 \times 4 \times 2018 < 73000$, donc $D < 6 + 4 \times 9 = 42$. Par conséquent, $E < 3 + 9 = 12$ et, puisque $E \equiv 7 \pmod 9$, on en déduit que $E = 7$.

Solution de l'exercice 10

Si $n \equiv -1 \pmod{\varphi(k)}$, alors $u_n \equiv 1/6 + 1/3 + 1/2 - 1 \equiv 0 \pmod k$, ce qui conclut.

Solution de l'exercice 11

Soit s le nombre de soldats dans l'armée chinoise. Le théorème Chinois indique que déterminer s modulo 5, 7, 9, 11, 13 et 16 revient à déterminer s modulo $(5 \times 9 \times 16) \times (7 \times 11 \times 13) = 720 \times 1001 = 720720$.

Solution de l'exercice 12

Il suffit de vérifier que p divise $\binom{p}{k}$ dès lors que $1 \leqslant k \leqslant p - 1$, puisque p divise $p!$ mais ne divise ni $k!$ ni $(p-k)!$. On en déduit que

$$(A(X) + B(X))^p \equiv \sum_{k=0}^{p} \binom{p}{k} A(X)^k B(X)^{p-k} \equiv \binom{p}{0} B(X)^p + \binom{p}{p} A(X)^p,$$

ce qui conclut.

Solution de l'exercice 13
Soit ω l'ordre de n modulo b. Alors $n^\omega - 1$ est un multiple de b, donc de a, ce qui conclut.

Solution de l'exercice 14
Notons ω_i l'ordre de x modulo $p_i^{\alpha_i}$ et ω l'ordre de x modulo n. D'après le théorème Chinois, $x^\ell \equiv 1 \pmod{n}$ si et seulement si $x^\ell \equiv 1 \pmod{p_i^{\alpha_i}}$ pour tout i, c'est-à-dire si et seulement si ℓ est un multiple de $\omega_{p_i^{\alpha_i}}(x)$. Ceci conclut.

Solution de l'exercice 15
Puisque 3 et 5 sont premiers entre eux, l'équation a une infinité de solutions. Évidemment, on pourrait se contenter de remarquer perfidement que $(k, \ell) = (4, 4)$ est une solution.

Mais, de manière générale, on va commencer à chercher des entiers $\hat{k}$ et $\hat{\ell}$ satisfaisant la relation de Bézout $5\hat{k} + 3\hat{\ell} = 1$. En utilisant l'algorithme d'Euclide étendu, on trouve $\hat{k} = -1$ et $\hat{\ell} = 2$, de sorte que $(k, \ell) = (-32, 64)$ est également une solution.

Par la suite, et puisque 3 et 5 sont déjà premiers entre eux, les solutions de l'équation sont en fait les paires de la forme $(k, \ell) = (3x - 32, 64 - 5x)$, où x est un entier relatif quelconque.

3 Combinatoire

1 Théorie des jeux

La théorie des jeux combinatoire est l'étude des jeux mathématiques, et de l'existence ou non d'une stratégie gagnante pour l'un des joueurs. De nombreux outils facilitent la recherche d'une telle stratégie, mais, avant d'étudier en détail ces méthodes, il faut commencer par atteindre une définition rigoureuse d'un jeu mathématique ?

Qu'est-ce qu'un jeu ? Tout d'abord un ensemble d'états, ou positions de jeu, avec des règles permettant aux joueurs de passer d'une position à une autre, et certaines positions désignées comme gagnantes pour l'un ou l'autre joueur, ou comme match nul.

Définition 3.1.1.
Soit (V, E) un graphe orienté acyclique dont chaque chemin est de longueur finie. Un jeu mathématique sur le graphe (V, E) est un quintuplet $G = (V, E, x_0, (A_1, A_2), (G_1, G_2))$, où V correspond aux sommets, E aux arêtes orientées les reliant, x_0 à la position de départ, A_1 et A_2 partitionnent les sommets non-terminaux en positions jouables par les joueurs 1 et 2 et G_1 et G_2 les sommets terminaux en positions gagnantes.

Nous étudions des stratégies gagnante sur les jeux, c'est-à-dire un choix de coups pour l'un ou l'autre des deux joueurs lui garantissant d'atteindre l'une de ses positions gagnantes quels que soient les choix de l'autre joueur.

Définition 3.1.2.
Une stratégie pour le joueur $n \in 1, 2$ est une fonction $S : A_n \mapsto V$ associant à chaque position jouable par n une position atteignable depuis celle-ci.

Définition 3.1.3.
Une partie d'un jeu est une suite de positions $J = (x_0, x_1, \ldots, x_p)$ tel qu'il existe, pour tout $k < p$, une arête reliant x_k et x_{k+1}, et tel que x_k soit un sommet terminal du graphe. Il est dit gagnant pour le joueur n si $x_k \in G_n$

Définition 3.1.4.
Une stratégie S est dite gagnante pour le joueur $n \in 1, 2$ si toute partie J tel que $\forall x_k \in A_n, x_{k+1} = S(x_k)$ est gagnant pour n.

Nous pouvons voir l'existence d'une stratégie gagnante par le biais d'une suite de quantificateurs $\forall$ et $\exists$: 1 gagne si, pour tout coup ou série de coups joués par 2, il existe un coup ou une série de coups jouables par 1 tel que pour tout... Ou, en d'autre termes, que quel que soit le jeu de 2, 1 puisse toujours jouer de sorte à atteindre une position gagnante pour lui.

Avec cette vision, le théorème suivant est facilement interprétable : la négation de $\forall x_1 \exists x_2 \exists x_3 \forall x_4, x_4 \in G_1$, par exemple, est $\exists x_1 \forall x_2 \forall x_3 \exists x_4, x_4 \in G_2$, dans l'exemple où les positions terminales sont atteintes au bout de 4 coups (en réalité, les positions terminales ne sont généralement pas atteintes au bout d'un nombre de coups prédéfini, et ce raisonnement ne sert donc bien entendu pas de preuve au théorème).

Théorème 3.1.5 (Théorème de Zermelo)**.**
Soit G un jeu mathématique à deux joueurs. Alors une et une seule des deux propositions suivantes est vraie :

— Le joueur 1 possède une stratégie gagnante.

— Le joueur 2 possède une stratégie gagnante.

Démonstration. Soit S_i l'ensemble des sommets depuis lesquels le joueur i a une stratégie gagnante, et T l'ensemble des sommets depuis lesquels aucun joueur n'a de stratégie gagnante. Supposons que x soit un sommet appartenant à T.

Sans perte de généralité, on suppose que $x \in G_1$. S'il existe une arête (x, y) telle que $y \in S_1$, alors $x \in S_1$; si, pour toute arête (x, y), le sommet y appartient à S_2, alors $x \in S_2$; par conséquent, il existe une arête (x, y) telle que $y \in T$.

Mais alors, en posant $y = f(x)$, et si chaque joueur décide, à partir d'une position $x \in S$, d'aller en position $f(x)$, on obtient ainsi une partie infinie, ce qui n'est pas possible. Donc T est en fait vide. $\square$

Ainsi, pour montrer que le joueur 1 possède une stratégie gagnante, il suffit de montrer que le joueur 2 n'en possède pas ! Et, pour montrer que le joueur 2 n'en possède pas, il suffit de montrer que, si il en possédait une, alors le joueur 1 en possèderait une également. C'est là le cœur de notre première méthode, l'argument par vol de stratégie.

Exercice 1 (Jeu de Chomp)
On considère une tablette de chocolat de dimensions $n \times m$, où le carré en position $(1, 1)$ est empoisonné. Alice et Bob mangent alternativement un nombre non nul de carrés de chocolat, correspondant à un rectangle centré sur le carré (n, m). Lequel des deux s'en sortira vivant ?

Exercice 2 (Jeu de Hex)
On considère un losange hexagonal de côté n, divisé en cases hexagonales de côté 1. Alice et Bob placent alternativement des hexagones respectivement bleus et rouges sur les cases du losange. Alice gagne si elle peut rejoindre la rive nord depuis la rive sud à l'aide d'un pont d'hexagones bleus, et Bob si il peut rejoindre la rive est depuis la rive ouest à l'aide d'un pont d'hexagones rouges. Pourquoi ce problème rentre-il dans le cadre du théorème de Zermelo ? Lequel des deux possède une stratégie gagnante ?

Malheureusement, les résultats fournis par ce genre d'arguments sont non-constructifs : on sait qui détient une stratégie gagnante, mais on ne sait pas laquelle ! Dans les cas du jeu de Chomp et du jeu de Hex, les stratégies gagnantes ne sont connues que pour des plateaux d'une dizaine de cases de côté au plus, sauf pour une disposition particulière du jeu de Chomp.

Exercice 3
Exhiber une stratégie gagnante pour le jeu de Chomp sur un plateau $n \times n$.

Une autre stratégie extrêmement courante est le jeu symétrique : l'un des deux joueurs peut décider de reproduire, en miroir, les mouvements de l'autre, de sorte à ne jamais atteindre une position finale avant lui !

Exercice 4 (Jeu de Cram)
Sur un quadrillage $n \times m$, Alice et Bob placent à tour de rôle des dominos 1×2 dans la direction de leur choix. Celui qui ne peut plus placer de dominos perd. Lequel des deux possède une stratégie gagnante :

— Si n et m sont tous les deux pairs ?

— Si n est pair et m impair ?

Les jeux mathématiques les plus étudiés comportent le plus souvent deux conditions supplémentaires :

— Les coups alternent toujours entre les deux joueurs

— Toute position terminale est gagnante pour le joueur ayant joué le coup précédent

Parmi les jeux précédents, les jeux de Chomp et de Cram vérifiaient notamment ces propriétés (à supposer que le carré $(1,1)$ ne puisse pas être mangé dans le jeu de Chomp), et tout jeu mathématique peut être ramené sous cette forme.

Dans ce contexte plus restreint, nous pouvons notamment définir les positions de type P et N.

Définition 3.1.6.
L'ensemble des positions du jeu, terminales ou non, peut être partitionné en deux sous-ensembles :

— Une position P est une position pour laquelle le joueur précédent admet une stratégie gagnante

— Une position N est une position pour laquelle le joueur suivant admet une stratégie gagnante

L'intérêt est ici que l'on peut, en raisonnant par récurrence, déterminer les positions P et N, et ainsi, en connaissant la nature de la position de départ, trouver une stratégie gagnante pour l'un ou l'autre des joueurs : cette stratégie consiste à se déplacer sur une position P si l'on est sur une position N, et à accepter de perdre si l'on est sur une position P.

L'exemple-type est celui-ci :

Exercice 5 (Jeu de soustraction)
Alice et Bob retirent, à tour de rôle, entre 1 et m objets d'une pile de n objets. Le premier qui ne peut plus jouer a perdu. Pour quelles valeurs de m et n Alice dispose-t-elle une stratégie gagnante ?

Exercice 6
Alice et Bob jouent au même jeu, mais, cette fois-ci, chacun des deux peut retirer n'importe quel nombre de pièces de la forme 2^k. Quelles sont les positions P et N ? Qu'en déduire sur les stratégies gagnantes ?

Proposition 3.1.7.
La partition de l'ensemble V des positions d'un jeu en P et N est l'unique partition vérifiant ces trois propriétés :

— $\forall x \in V, C(x) = \emptyset \Rightarrow x \in P$: on perd la partie en atteignant une position terminale[7] ;

— $\forall x \in N, C(x) \cap P \neq \emptyset$: à partir d'une position gagnante, on peut toujours atteindre une position perdante pour le prochain joueur ;

— $\forall x \in P, C(x) \cap P = \emptyset$: à partir d'une position perdante, on ne peut atteindre que des positions gagnantes pour l'autre joueur.

Démonstration. Le résultat se démontre aisément par induction structurelle sur la durée maximale du jeu à partir de la position actuelle (en nombre de coups). $\square$

Divers exercices ont par la suite été donnés, qui seront présents dans la version complète du polycopié.

– Jeu de Nim –

Un jeu particulièrement étudié, tant pour ses variantes que pour son rôle à la base d'une théorie combinatoire des jeux plus avancée[8], est le jeu de Nim, présenté ici, et dont la résolution met en jeu des outils plus avancés que celle des jeux précédents.

Définition 3.1.8.
Le jeu de Nim est un jeu à deux joueurs, joué sur n piles distinctes à $k_1, \ldots, k_n$ jetons. À tour de rôle, chacun des deux joueurs peut retirer un nombre de jetons de son choix de l'une des n piles. Le vainqueur est celui qui parvient à retirer le dernier jeton.

Essayons, pour un jeu de Nim joué sur n piles distinctes, de décrire ses positions P et N.

Définition 3.1.9.
Soient $a, b \in \mathbb{N}$. Écrivons-les comme $\sum_{i=0}^n a_i 2^i$ et $\sum_{i=0}^n b_i 2^i$. L'opérateur XOR, ou OU exclusif, est défini comme $a \oplus b = \sum_{i=0}^n (a_i + b_i - 2a_i b_i) 2^i$.

7. Dans les jeux de misère, les résultats étant inversés, cette condition devient $\forall x \in V, C(x) = \{\} \Rightarrow x \in N$.
8. Se basant notamment sur le théorème de Sprague-Grundy, affirmant que tout jeu est dans un certain sens équivalent à un jeu de Nim

Remarque 3.1.10.
Le XOR est commutatif et associatif. En effet, les opérations sur chaque chiffre binaire sont indépendantes, et chacune est commutative et associative (elles correspondent à un OU exclusif binaire).

Remarque 3.1.11.
$\forall a, b \in \mathbb{N}, (a \oplus b) \oplus b = a \oplus (b \oplus b) = a$

Théorème 3.1.12 (Théorème de Bouton).
Considérons un jeu de Nim à n piles. Une position $(x_1, \ldots, x_n)$ est de type P si et seulement si $\bigoplus_{i=1}^n x_i = 0$.

Démonstration. Vérifions que la partition des positions en $P = \{(x_1, \ldots, x_n), \bigoplus_{i=1}^n x_i = 0\}$ et $N = \{(x_1, \ldots, x_n), \bigoplus_{i=1}^n x_i \neq 0\}$ vérifie bien les trois propiétés de la définition :

— L'unique position finale, $(0, \ldots, 0)$ est dans P : $0 \oplus \ldots \oplus 0 = 0$.

— Soit $(x_1, \ldots, x_n)$ tel que $x_1 \oplus \ldots \oplus x_n = s \neq 0$, et soit d le rang du premier bit non-nul depuis la gauche dans la représentation binaire de s. Alors il existe x_k dont le d-ième bit est aussi non nul. En prenant $y_k = s \oplus x_k$, nous avons $x_1 \oplus \ldots \oplus y_k \oplus \ldots \oplus x_n = x_1 \oplus \ldots \oplus s \oplus x_k \oplus \ldots \oplus x_n = s \oplus s = 0$ par commutativité. De plus, $y_k < 2^d \leqslant x_k$: remplacer x_k par y_k est donc un coup valide, qui permet d'atteindre une position P à partir d'une position N.

— Soit $(x_1, \ldots, x_n)$ tel que $x_1 \oplus \ldots \oplus x_n = 0$. Supposons qu'il existe k, $y_k < x_k$ tel que $x_1 \oplus \ldots \oplus y_k \oplus \ldots \oplus x_n = 0 = x_1 \oplus \ldots \oplus x_k \oplus \ldots \oplus x_n$. Alors, en simplifiant, $y_k = x_k$, contradiction. Par conséquent, aucune position P n'est accessible à partir d'une position P.

□

Exercice 7
Généraliser ce résultat au cas où chaque joueur peut prendre des pièces de k des n tas différents.

– Solutions des exercices –

Solution de l'exercice 1
C'est le premier joueur à manger du chocolat qui survivra. En effet, supposons qu'Alice commence la partie et que Bob dispose d'une stratégie gagnante. Alors Alice peut commencer par manger le carré (m, n) tout seul, puis Bob choisira un carré (a, b) et mangera tous les carrés (x, y) tels que $x \geqslant a$ et $y \geqslant b$.

Mais alors Alice aurait pu manger directement tous ces carrés-là, volant la stratégie de Bob. C'est donc bien Alice, la première à manger, qui survivra.

Solution de l'exercice 2
Comme d'habitude, on suppose qu'Alice joue en premier. Si Bob avait une stratégie gagnante,

alors quitte à inverser les rôles et à s'assurer a priori la maîtrise d'un hexagone, Alice n'aurait qu'à utiliser cette stratégie pour gagner. Donc Bob n'a pas de stratégie gagnante, et c'est qu'Alice en a bien une.

Solution de l'exercice 3
Alice commence par manger tous les carrés de chocolat (x, y) tels que $x \geqslant 2$ ou $y \geqslant 2$. Ainsi, elle pourra ensuite singer les mouvements de Bob pour garder une tablette symétrique, et laisser Bob s'empoisonner en premier.

Solution de l'exercice 4

— Si m et n sont pairs, c'est Bob qui a une stratégie gagnante. En effet, à chaque fois qu'Alice pose un domino d, Bob n'a qu'à poser le symétrique d' de d par rapport au milieu du plateau de jeu. Par récurrence, à la fin de chaque coup de Bob, les dominos formerons une zone invariante par symétrie centrale, et les dominos d et d' ne peuvent se chevaucher.

— Si m et pair et n est impair, en revanche, Alice n'a qu'à commencer par poser son domino au milieu du plateau, en colonne $(n+1)/2$ et en lignes $m/2$ et $m/2+1$, pour pouvoir ensuite singer les coups de Bob à symétrie centrale près.

Solution de l'exercice 5
Alice dispose d'une stratégie gagnante dès lors que $n+1$ ne divise pas m. En effet, si c'est le cas, elle peut toujours enlever entre 1 et m jetons pour laisser à Bob un nombre de jetons divisible par $n+1$. À son tour, s'il peut jouer, Bob laissera à Alice un nombre de jetons m' qui n'est pas divisible par $n+1$, ce qui permettra à Alice de réitérer sa stratégie jusqu'à la victoire.

Solution de l'exercice 6
Cette fois-ci, Alice dispose d'une stratégie gagnante dès lors que 3 ne divise pas n. En effet, si c'est le cas, elle peut toujours enlever 1 ou 2 jetons pour laisser à Bob un nombre de jetons divisible par n. À son tour, s'il peut jouer, Bob laissera à Alice un nombre de jetons m' qui n'est pas divisible par 3.

Solution de l'exercice 7
Cette fois-ci, si $x_1, \ldots, x_n$ sont n entiers, écrivons-les en base $k+1$: $x_i = \sum_{j \geqslant 0} x_{i,j}(k+1)^j$. Pour tout j, on pose ensuite $y_j \equiv x_{1,j} + \ldots + x_{n,j} \pmod{k+1}$, et enfin on note $x_1 \bullet x_2 \bullet \ldots \bullet x_n$ l'entier $y = \sum_{j \geqslant 0} y_j (k+1)^j$. Alors une position $(x_1, \ldots, x_n)$ appartient à P si et seulement si $x_1 \bullet x_2 \bullet \ldots \bullet x_n = 0$.

2 Monovariants et invariants

– Principe –

Le concept d'invariant n'est que rarement utilisé dans des problèmes « statiques », où la situation est immuable. Par contre, certains problèmes sont « dynamiques » : il s'agit de passer d'une configuration initiale à une configuration finale, en respectant certaines règles sur les transformations effectuées. Dans ce cas, un invariant est une quantité que l'on peut associer à chaque état du problème et qui ne varie jamais lorsqu'on applique une des transformations autorisées. Si les quantités associées aux configurations initiale et finale sont différentes, on a alors démontré l'impossibilité de passer de l'une à l'autre. De même, il peut arriver qu'une quantité associée à chaque configuration croisse (resp. décroisse) à chaque transformation appliquée. On parle alors de monovariant. Il est bien entendu impossible de parvenir à une configuration où ce monovariant est plus petit (resp. plus grand) que la configuration initiale. De plus, si le monovariant est majoré et augmente d'au moins une certaine quantité non nulle fixée à chaque transformation, on peut conclure que le processus d'application des transformations prend forcément fin.

– Exercices –

Exercice 1
On se donne le tableau rempli de signes suivant :

$$\begin{array}{cccc} + & + & - & + \\ - & - & + & + \\ + & + & + & + \\ + & - & + & - \end{array}$$

Un coup consiste à choisir une ligne ou une colonne et changer les signes présents dedans. Est-il possible d'arriver à un tableau rempli de signes $+$?

Exercice 2
Sur une île se trouvent des moutons magiques. Il y en a 22 bleus, 18 rouges et 15 verts. Lorsque deux moutons de couleurs différentes se croisent, ils prennent tous deux la troisième couleur. Est-il possible qu'après un certain nombre fini de rencontres, tous les moutons soient de la même couleur ? Si oui, quelle peut être cette couleur ?

Exercice 3
Les nombres entiers de 1 à 2018 sont écrits au tableau. Une opération consiste à en choisir deux, les effacer et réécrire sur le tableau la valeur absolue de leur différence. Montrer que le dernier nombre écrit au tableau est impair.

Exercice 4
On a 2018 piles de jetons. Sur la i-ème pile, il y a p_i jetons, où p_i est le i-ème nombre premier. On s'autorise :

— à séparer une pile en deux autres et ajouter un jeton à l'une des deux piles ainsi créées.

— à fusionner deux piles et ajouter un jeton à la pile créée.

Peut-on aboutir à la situation avec 2018 piles de 2018 jetons chacune ?

Exercice 5
Dans l'espace, on part de l'ensemble de 7 sommets d'un cube. On s'autorise à remplacer un point par son symétrique par rapport à un autre point. Peut-on atteindre le huitième sommet de cette façon ?

Exercice 6
Sur un tableau, on écrit n fois le chiffre 1. Une opération consiste à choisir deux nombres a et b écrits au tableau, à les effacer et à écrire $\frac{a+b}{4}$ à la place. Montrer que le nombre écrit au tableau au bout de $n-1$ étapes est supérieur ou égal à $\frac{1}{n}$.

Exercice 7
On écrit un signe $+$ ou $-$ sur chaque case d'un tableau 8×8. Une opération consiste à choisir un carré 3×3 ou 4×4 et inverser les signes présents dedans. Peut-on toujours atteindre un tableau rempli de $+$?

Exercice 8
Sept cases d'un échiquier (8×8) sont en feu. A chaque étape, une case s'enflamme si au moins deux de ses voisines (par un côté, pas par un coin) sont en feu. Est-il possible que le feu se répande partout ? Si non, combien de cases initialement en feu faut-il au minimum pour que le feu puisse se répandre partout ?

Exercice 9
La Reine d'Angleterre veut partager la Chambre des Lords de façon originale : chaque Lord ayant au plus trois ennemis (l'inimité est réciproque), elle veut partager la Chambre en deux groupes, chaque Lord ayant au plus un ennemi dans son groupe. Est-ce possible ?

Exercice 10
n points du plan sont colriés en rouge, n autres le sont en bleu. Ces $2n$ points ne sont pas 3 à 3 alignés. Est-il possible de tracer n segments reliant un point rouge à un point bleu, chaque point étant utilisé une seule fois, de manière à ce que deux segments ne s'intersectent jamais ?

Exercice 11
Il y a 2018 mésanges qui nichent sur 120 arbres. Essayant de les déloger, un chasseur maladroit leur tire dessus. A chaque fois, il manque sa cible mais effraie une mésange qui quitte alors son arbre et se réfugie sur un arbre avec au moins autant de mésanges que son arbre de départ (elle se compte sur ce dernier). Montrer qu'après un certain nombre fini de tirs, toutes les mésanges seront sur le même arbre.

Exercice 12
Sur une ligne, on écrit 2018 entiers naturels. Ensuite, pour chaque ligne, on écrit en-dessous de chaque entier le nombre de fois qu'il apparaît dans la ligne, créant ainsi une nouvelle ligne en-dessous de la première, sur laquelle on réapplique le processus. Montrer qu'au bout d'un certain temps toutes les lignes qu'on écrit deviennent identiques.

Exercice 13
Il y a une lampe sur chaque case d'une grille 5×5. Lorsqu'on allume ou éteint une lampe, ses voisines par un côté changent également d'état. Initialement, toutes les lampes sont éteintes. Martin arrive et active certains interrupteurs. Au final, une seule lampe est allumée. Quelles sont ses positions possibles ?

Exercice 14
Sur le plan, on part du point $(1, \sqrt{2})$. Quand on est en (x, y), on peut se déplacer en $(x, y+2x)$,

$(x, y-2x)$, $(x+2y, y)$ ou $(x-2y, y)$, mais sans revenir immédiatement au point dont on venait. Montrer qu'on ne peut revenir au point de départ.

Exercice 15
2009 cartes, ayant chacune un côté bleu et un côté jaune, sont alignées côté bleu sur une table. Deux personnes situées du même côté de la table jouent alors en alternance. Un coup consiste à choisir un bloc de 50 cartes dont la carte la plus à gauche est bleue et à retourner toutes les cartes du bloc. La personne qui ne peut plus jouer perd. Le jeu se termine-t-il forcément ? Si oui, qui a une stratégie gagnante ?

Exercice 16
Des entiers positifs en nombre fini sont écrits de gauche à droite sur une ligne. Lucie choisit deux nombres voisins x et y tels que x est à gauche de y et $x > y$ et remplace la paire (x, y) par $(x-1, x)$ ou $(y+1, x)$ au choix, puis recommence tant que possible. Montrer qu'elle ne peut continuer indéfiniment.

Exercice 17
Les participants du stage Animath s'appellent $C_1, \ldots, C_n$ et font la file devant le restaurant selon les règles suivantes :

— Les animatheurs choisissent l'ordre initial des participants.

— A chaque étape, les animatheurs choisissent un entier i avec $1 \leqslant i \leqslant n$. Si le participant C_i a au moins i personnes devant lui dans la queue, il paie 1 euro aux animatheurs et avance de i places. Sinon, le restaurant ouvre et le processus se termine.

Montrer que le processus se termine forcément et déterminer la quantité maximale d'argent que les animatheurs peuvent extorquer aux participants.

– Pavages et coloriages –

Parfois, on peut montrer l'impossibilité d'une construction en coloriant la surface sur laquelle elle doit se dérouler. En voici quelques exemples :

Exercice 18
Sur une grille 2018×2018, on peut bouger un jeton d'une case vers une autre si ces deux cases ont un côté commun. Est-il possible, en partant avec le jeton dans le coin inférieur gauche, d'amener le jeton dans le coin supérieur droit en passant une et une seule fois par toutes les cases ?

Exercice 19
Un sol rectangulaire est pavé par des rectangles 4×1 et 2×2. Si l'on casse un des carreaux, peut-on le remplacer par un carreau de l'autre type et repaver le sol ?

Exercice 20
De combien de manières peut-on paver un damier 10×10 par des tétraminos en T ?

Exercice 21
Est-il possible de paver (sur plusieurs couches) un rectangle 5×7 par des trominos en L de manière à ce que chaque case soit recouverte par le même nombre de trominos ?

Exercice 22
Yakob et Baptiste jouent sur une grille 20×20 où les cases sont carrées et de côté 1. La *distance* entre deux cases est la distance entre leurs centres. Ils jouent à tour de rôle de la manière suivante : Yakob met une pierre rouge sur une case, de manière à ce que la distance entre deux cases portant des pierres rouges ne soit jamais $\sqrt{5}$, puis Baptiste met une pierre bleue sur la grille, sans restriction. Le jeu s'arrête quand un des deux ne sait plus poser de pierre. Trouver le plus grand K tel que Yakob peut toujours placer au moins K pierres, quelles que soient les réponses de Baptiste.

– Solutions –

Solution de l'exercice 1
La parité du nombre de signes $-$ est un invariant. Ce nombre est impair dans la position initiale, on ne peut donc pas atteindre une position qui aurait 0 signe $-$.

Solution de l'exercice 2
Ici, les transformations autorisées sont au nombre de 3 : on peut passer de (b, r, v) à $(b-1, r-1, v+2)$, $(b-1, r+2, v-1)$ ou $(b+2, r-1, v-1)$. En particulier, on peut remarquer que $r - v(\mod 3)$ est constant, et vaut 0 dans la position initiale. Si après les rencontres tous les moutons étaient rouges ou verts, on aurait 55 moutons d'une couleur et 0 de l'autre, et la différence vaudrait respectivement 1 ou $-1(\text{mod}3)$ ce qui est impossible. La seule couleur finale possible est donc le bleu. De fait, en faisant se rencontrer un mouton bleu et un mouton rouge, puis 17 fois un mouton rouge et un mouton vert, tous les moutons deviennent bleus. Remarquons que la construction (ou une preuve d'existence) est importante, le fait qu'un invariant soit constant entre deux positions ne garantit pas qu'on puisse passer de l'une à l'autre.

Solution de l'exercice 3
A chaque étape, la somme des nombres impliqués dans la transformation passe de $a + b$ à $a - b$ ou $b - a$, elle est donc modifiée d'une quantité paire ($2b$ ou $2a$ respectivement). La parité de la somme des nombres écrits au tableau est donc un invariant. Dans la position initiale, elle vaut $\frac{2018 \cdot 2019}{2} = 1009 \cdot 2019$ qui est impair. Après 2017 étapes, il ne reste plus qu'un nombre au tabeau, qui doit être impair.

Solution de l'exercice 4
En traitant les diverses possibilités de mouvement, on remarque que la parité du nombre de piles de hauteur paire reste inchangée. Comme ce nombre est impair dans la position initiale et pair dans la position à atteindre, il est impossible d'aboutir à cette dernière.

Solution de l'exercice 5
Plaçons-nous dans un repère orthonormé où les sept points du cube ont pour coordonnées $(0, 0, 0)$, $(0, 0, 1)$, $(0, 1, 0)$, $(1, 0, 0)$, $(0, 1, 1)$, $(1, 0, 1)$ et $(1, 1, 0)$. Le symétrique du point (a, b, c) par rapport au point (a', b', c') est le point $(2a' - a, 2b' - b, 2c' - c)$. En particulier, la parité des coordonnées est invariante par ces symétries. On ne peut donc atteindre le point $(1, 1, 1)$ puisque ses trois coordonnées sont impaires.

Solution de l'exercice 6
On peut remarquer que $\frac{1}{a} + \frac{1}{b} \geqslant \frac{4}{a+b}$ (il suffit de tout mettre au même dénominateur et de faire apparaître $(a - b)^2 \geqslant 0$). Dès lors, la somme des inverses des nombres écrits au tableau

est décroissante lorsqu'on applique une transformation. Elle vaut n dans la position initiale, donc dans la position finale elle est inférieure à n : le dernier nombre est dès lors supérieur à $\frac{1}{n}$.

Solution de l'exercice 7

Ici, la parité du nombre de signes $-$ n'est plus un invariant, mais on peut remarquer que la parité du nombre de signes $-$ en dehors des troisième et sixième colonnes en est un. La configuration demandée n'est donc pas toujours atteignable.

Solution de l'exercice 8

On peut montrer que le périmètre de la zone enflammée décroit à chaque étape. Dès lors, le feu ne peut pas se répandre sur tout l'échiquier (périmètre de 32 si les cases ont côté 1) à partir de sept cases enflammées (périmètre de 28 au maximum). Il faut au moins huit cases : si toutes les cases d'une grande diagonale sont initialement enflammées, le feu pourra se répandre partout.

Solution de l'exercice 9

Oui, c'est possible : si un Lord se trouve dans un groupe où il a deux ennemis, alors en le changeant de groupe on diminue d'au moins 1 le nombre de relations d'inimité présentes au sein des groupes. Comme ce nombre ne peut être négatif, le processus se finit, et l'état final est un état où tous les Lords ont au plus un ennemi dans leur groupe.

Solution de l'exercice 10

De même, si deux segments AB et CD, avec A et C rouges, ont une intersection, alors les segments AD et CB n'en ont pas et la somme de leurs longueurs est plus petite que celle des longueurs de AB et CD. Il n'y a que $n!$ manières d'apparier les points. En prenant celle où la somme des longueurs des segments est la plus petite, et vu la remarque précédente, il n'y aura aucune intersection. Ces deux exercices illustrent à quel point les méthodes par monovariant sont semblables aux méthodes à base d'extremum.

Solution de l'exercice 11

L'ordre lexicographique entre listes dont les éléments font partie d'un ensemble totalement ordonné est défini comme suit : on regarde le premier élément de chaque liste. Si ils sont différents, la liste ayant le plus petit premier élément est la plus petite. Si ils sont égaux, on passe au deuxième élément, et ainsi de suite. Par exemple, si on considère les mots comme des listes de lettres, l'ordre lexicographique correspond à l'ordre du dictionnaire.

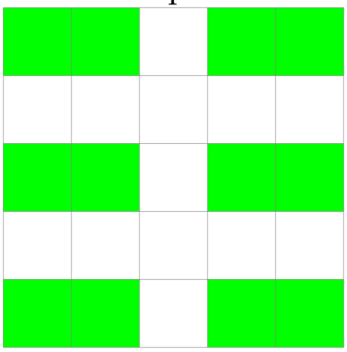
Représentons une configuration par la liste du nombre de mésanges sur chaque arbre, triée par ordre croissant. Quand le chasseur tire, un des nombres de la liste diminue de 1 et un nombre situé plus loin dans la liste augmente de 1. Dès lors, la nouvelle liste est strictement plus petite par ordre lexicographique que la première. Comme il n'y a qu'un nombre fini de listes de 120 éléments naturels dont la somme fait 2018, on finira par atteindre en un nombre fini d'étapes la plus petite, qui correspond à avoir toutes les mésanges sur un même arbre.

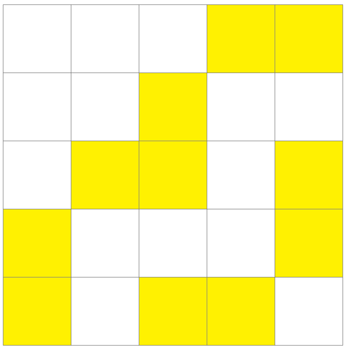
Solution de l'exercice 12

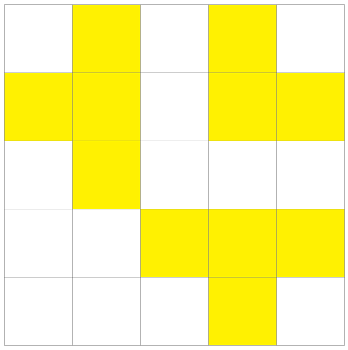
Considérons un nombre a en dehors de la première ligne. Il représente le nombre d'occurences d'un des nombres de la ligne du dessus. Ce dernier est donc présent a fois dans la ligne du dessus, et a est présent au moins a fois dans sa ligne. Dès lors, si on regarde une colonne, tous les nombres à l'exception du premier sont triés par ordre croissant. Comme de plus la somme des nombres d'une ligne autre que la première fait 2018, toutes les lignes deviennent identiques au bout d'un certain temps (sinon, la somme de chaque ligne augmenterait de 1 autant de fois que voulu, tout en restant inférieure à 2018).

Solution de l'exercice 13

Sur la première figure ci-dessus, le parité du nombre d'ampoules vertes allumés est invariante. Il en est bien sûr de même par rotation de $90°$. Ainsi, seules les ampoules du centre et entre le centre et les coins sont des solutions possibles. En appuyant sur les interrupteurs jaunes dans la deuxième figure, seule l'ampoule du centre est allumée. De même dans la troisième figure, seule l'ampoule entre le centre et le coin supérieur droit sera allumée, le reste s'en déduit par rotation.







Solution de l'exercice 14

Donnons des noms aux différentes transformations : partant de (x, y), appelons N le passage à $(x, y+2x)$, S pour $(x, y-2x)$, E pour $(x+2y, y)$ et O pour $(x-2y, y)$. La règle de ne pas revenir immédiatement en arrière signifie que l'on ne peut pas faire un déplacement N puis S, ou E puis O (et de même dans l'autre sens). On peut remarquer que les coordonnées du point sont toujours de la forme $(a+b\sqrt{2}, c+d\sqrt{2})$. De plus, puisque $\sqrt{2}$ est irrationnel, a et c sont indépendants de b et d. On peut donc montrer que partant de $(1, 0)$ et suivant les mêmes règles, on ne peut revenir au point de départ, et ce sera suffisant.

Les mouvements E et O n'ont aucun effet au point de départ, toute séquence de coups peut donc se réécrire a_1N+a_2E+a_3N+..., avec $a_i \in \mathbb{Z} \setminus \{0\}$, en notant kN le mouvement N répété k fois, si $k > 0$, et S répété k fois si $k < 0$, et de même pour E/O. Le mouvement kN correspond à passer de (x, y) à $(x, y+2kx)$ tandis que kE correspond à passer à $(x+2ky, y)$. On peut montrer par récurrence qu'après un mouvement kN on a $|c| > |a|$, et $|a| > |c|$ après un mouvement kE. Dès lors, la distance à l'origine du point (a, c) est strictement croissante (puisqu'on augmente la valeur absolue de la coordonnée la plus petite en valeur absolue, et que l'autre reste inchangée), et il est donc impossible de revenir au point de départ.

Solution de l'exercice 15

Ecrivons un 1 sur chaque face bleue et un 0 sur chaque face jaune. A toute configuration est alors associé un nombre écrit en binaire et ayant 2009 chiffres. Quand on fait un coup, on modifie 50 chiffres consécutifs, dont le plus grand passe de 1 à 0. Le nombre associé à la position baisse donc strictement. Puisqu'il ne peut être négatif, la partie finit par s'arrêter.

Pour savoir qui gagne, considérons les cartes en positon $50k$ à partir de la droite, et le nombre de cartes bleues parmi celles-ci. Au début, il est de 40, et il change de 1 à chaque coup puisqu'exactement une de ces cartes est retournée à chaque coup. Dès lors, quand c'est au tour du second joueur, le nombre de cartes bleues parmi celles considérées est impair, donc non nul. Le second joueur a donc toujors quelque chose à jouer, et ne peut donc perdre. Puisque le jeu se finit, le second joueur gagne toujours.

Solution de l'exercice 16

On peut remarquer que le maximum des entiers reste constant, et que leur somme augmente sauf si $y = x - 1$ et qu'on remplace (x, y) par $(x - 1, x)$. De plus, il n'est pas possible de faire ce coup indéfiniment, puisque si l'on considère le nombre de paires « inversées » (x est à gauche de y et $x > y$), il diminue de 1 à chaque coup de cette forme. Dès lors, si Lucie pouvait continuer indéfiniment, elle serait forcée d'augmenter régulièrement la somme des nombres de la liste, mais cette somme ne peut dépasser le maximum de la liste multiplié par sa taille, ce qui est constant.

Solution de l'exercice 17
Tout d'abord, montrons par récurrence que les animatheurs peuvent récolter $2^n - n - 1$ euros. La construction est la suivante :

Les participants sont placés dans l'ordre inverse (C_n est en premier, puis C_{n-1}, etc). Dans un premier temps, les animatheurs remettent en ordre croissant les $n - 1$ derniers élèves de la file, de la manière qui leur fait gagner le plus d'argent. On a donc l'ordre $C_n, C_1, C_2, \ldots, C_{n-1}$. Ensuite, ils font avancer une fois chaque participant de 1 à $n - 1$. On a donc l'ordre $C_{n-1}, \ldots, C_2, C_1, C_n$. Enfin, ils remettent à nouveau les $n - 1$ premiers éléments de la file dans l'ordre croissant. En notant S_n la quantité d'argent obtenue sur une file de n participants par cette méthode, on a $S_n = 2S_{n-1} + n - 1$ et $S_1 = 0$. On a donc bien $S_n = 2^n - n - 1$.

Montrons à présent qu'on ne peut récolter plus de $2^n - n - 1$ euros :

Si C_i avance, il passe devant i autres participants. En particulier, il passe devant un participant qui a un numéro supérieur au sien. Dès lors, à une configuration x de la file, associons la quantité

$$Q(x) = \sum_{\substack{i,j \in \{1,\ldots,n\} \\ i<j}} 2^i \cdot \delta_{ij} \text{ avec } \delta_{ij} = \begin{cases} 0 & \text{si } i \text{ est avant } j \text{ dans la file} \\ 1 & \text{sinon} \end{cases}$$

(il s'agit d'un comptage pondéré des paires de participants qui sont dans l'ordre inverse). Lorsque les animatheurs font avancer un participant j, il passe devant un participant avec un numéro supérieur, rétablissant ainsi l'ordre « correct » d'une paire dont j est le plus petit élément, donc Q baisse d'au moins 2^j. Il peut arriver que j passe devant des participants au numéro inférieur, mais Q ne peut de toutes façons augmenter de plus de $\sum_{i=1}^{j-1} 2^i = 2^j - 2$. Q baisse donc d'au moins 2 à chaque étape. D'autre part, Q est maximal lorsque toutes les paires sont inversées, et vaut alors $\sum_{i=1}^{n}(n - i)2^i = 2(2^n - n - 1)$, et ne peut être négatif. On ne peut donc pas faire avancer un candidat plus de $2^n - n - 1$ fois, et ce nombre est bien la somme maximale que les animatheurs peuvent percevoir.

Solution de l'exercice 18
En coloriant la grille comme un damier, on voit qu'un déplacement vers une case ayant un côté commun change la couleur de la case sur laquelle on se trouve. De plus, les cases de départ et d'arrivée sont de la même couleur, il faut donc avoir réalisé un nombre pair de mouvements pour passer de l'une à l'autre. Mais si l'on visite toutes les cases de la grille, on aura fait $2018^2 - 1$ déplacements, ce qui est impair, d'où une impossibilité.

Solution de l'exercice 19

On colorie le sol en répétant le motif

$$\begin{matrix} ABAB\ldots \\ CDCD\ldots \\ ABAB\ldots \\ CDCD\ldots \\ \vdots \quad \vdots \quad \vdots \end{matrix}$$

Un rectangle 2×2 couvre une case de chaque couleur, tandis qu'un rectangle 1×4 en couvre 2 d'une couleur et 2 d'une autre. Ils ne sont donc pas interchangeables. (La parité du nombre de cases de chaque couleur pavées doit rester constante, or elle ne le sera pas ici).

Solution de l'exercice 20
Cela est impossible. En coloriant le damier comme un damier, chaque tétramino couvre 3 cases d'une couleur et une de l'autre. En notant n le nombre de tétraminos couvrant 3 cases noires et b celui de tétraminos couvrant 3 cases blanches, on a

$$3n + b = 50$$
$$n + b = 25$$

En soustrayant, on a $2n = 25$ ce qui est impossible.

Solution de l'exercice 21
Si on réutilise le coloriage de l'exercice 19 en plaçant un A dans le coin en haut à gauche, on a 12 A sur le rectangle, mais chaque tromino ne peut recouvrir qu'un A. Si chaque case est recouverte k fois, il faut utiliser au moins $12k$ trominos pour recouvrir tous les A, mais alors on a un total d'au moins $36k$ cases recouvertes et non $35k$. Il n'est donc pas possible de réaliser un tel pavage.

Solution de l'exercice 22
Montrons que $K = 100$. Yakob peut toujours poser 100 pierres : il suffit qu'il colorie la grille en damier et qu'il joue toujours sur une case blanche. En effet, deux cases blanches ne sont jamais à distance $\sqrt{5}$ l'une de l'autre. Montrons que Baptiste peut empêcher Yakob de poser plus de 100 pierres : on pave la grille par des copies du rectangle

$$\begin{matrix} ACBD \\ BDAC \\ CADB \\ DBCA \end{matrix}$$

Si Yakob joue sur une case, Baptiste joue dans le même rectangle, sur la case de la même couleur qui n'est pas à distance $\sqrt{5}$ de la première. Ainsi, Yakob est privé des deux autres cases de même couleur du même rectangle. Au final, Yakob ne peut recouvrir plus d'un quart du rectangle qui comporte 400 cases.

3 Groupes

– Cours –

Définition 3.3.1.
Soit G un ensemble non vide avec une operation binaire :à toute paire $a, b \in G$ est associée un élément $ab \in G$. Alors on dit que G est un groupe si on a les axiomes suivants.

1. (Associativité) Pour tout $a, b, c \in G$ $(ab)c = a(bc)$.
2. (Element neutre) Il existe $e \in G$ tel que pour tout $a \in G$ $ea = a$ et $ae = a$.
3. (Inversibilité) Pour tout $a \in G$, il existe un (unique) $a^{-1} \in G$ tel que $aa^{-1} = e$ et $a^{-1}a = e$.

Définition 3.3.2.
On dit que G est un groupe abelien (ou commutatif) si il satisfait en plus la propriété suivante

1. Pour tous $a, b \in G$, $ab = ba$.

Notation.
Dans le cas des groupes abéliens, on utilisera souvent le signe $+$ pour l'opération binaire, on écrira ainsi $a + b$ au lieu de ab. Dans ce cas on notera également 0 l'élément neutre et $-a$ l'inverse de a.

Exemple 3.3.3.
Tout les exemples suivant sont des groupes :

1. L'ensemble des entiers relatifs muni de l'addition (abélien).
2. L'ensemble des réels non nuls muni de la multiplication (abélien)
3. L'ensemble des translations dans le plan forme un groupe (est-il abélien ?)
4. L'ensemble des permutations (mélange) d'un ensemble fini.
5. L'ensemble des transformations du plan formé des rotations et des translations.

Notation.
Si A et B sont deux sous-ensembles de G on notera

$$AB = \{ab \mid a \in A, b \in B\} \text{ et } A + B = \{a + b \mid a \in A, b \in B\}.$$

Définition 3.3.4.
On dit qu'un sous ensemble H de G est un sous groupe de G si c'est un groupe avec l'opération binaire de G.

Définition 3.3.5.
Si H est un sous groupe de G et $a \in G$, aH (resp. Ha) est appellé la classe à gauche (resp. à droite) engendré par H

Définition 3.3.6.
Un sous groupe G est dit normal si pour tout $a \in G$ on a $aH = Ha$.

Remarque 3.3.7.
Si G est abélien tous les sous groupes sont normaux.

Théorème 3.3.8.
Si H est un sous groupe normal de G, alors les classes engendrées par H forment un groupe avec l'opération binaire

$$(aH)(bH) = (abH).$$

On appelle ce groupe le groupe quotient et on le note G/H.

Démonstration. Il faut vérifier que la définition que l'on a donné ne dépend pas du représentant de la classe. Soit $a' \in aH$ et $b' \in bH$, montrons que $a'b' \in abH$. Soit $h_1 \in H$ et $h_2 \in H$ tel que $a' = ah_1$ et $b' = bh_2$ alors $a'b' = ah_1bh_2$. Puisque H est normal, il existe h_3 tel que $h_1b = bh_3$ et donc $a'b' = abh_3h_2$ qui appartient bien à abH. □

Exemple 3.3.9.
Soit n un entier naturel, les groupes $H = n\mathbb{Z}$ sont des sous groupes normaux à $\mathbb{Z}$. Le groupe quotient $\mathbb{Z}/n\mathbb{Z}$ sont les entiers modulo n.

Définition 3.3.10.
On appelle ordre de G le nombre d'éléments de G et on le note $|G|$

Théorème 3.3.11 (Théor de Lagrange)**.**
Si H est le sous groupe d'un groupe G fini. Alors $|H|$ divise $|G|$

Démonstration. Les classes de H définissent une relation d'équivalence

$$a \sim b \Leftrightarrow \exists h \in H, a = bh.$$

On vérifiera qu'elle est bien symétrique réflective et transitive.

Il faut maintenant faire la remarque suivante : Toutes les classes on $|H|$ éléments. En effet si $bh_1 = bh_2$ alors $h_1 = h_2$. Donc puisque G est égale à l'union disjointe de ses classes, $|G|$ est égale à $|H|$ fois le nombre de classes. □

Définition 3.3.12.
Soit $a \in G$. On appelle ordre de a (et on le note ord(a)) le plus entier k tel que $a^k = e$.

Remarque 3.3.13.
Si $a^n = e$, alors k divise n.

Remarque 3.3.14.
Pour tout $a \in G$, l'ensemble $\{a^k | k \in \mathbb{Z}\}$ forme un sous groupe de G. L'ordre de ce groupe est égale à ord(a).

Corollaire 3.3.15.
Pour tout $a \in G$, ord(a) divise $|G|$.

– Exercices –

Exercice 1
Parmi les ensembles suivants, lesquels forment un groupe ?

1. G l'ensemble des entiers relatifs muni de la soustraction.
2. $G = \{-1, 1\}$ muni de la multiplication
3. G l'ensemble des rationnels non nul muni de la division.

Exercice 2
Montrer que dans un groupe G :

1. l'élément neutre est unique
2. Pour tout $a \in G$, l'inverse a^{-1} est unique
3. $(a^{-1})^{-1} = a$ et $(ab)^{-1} = b^{-1}a^{-1}$.
4. $ab = ac \Rightarrow b = c$ et $ba = ca \Rightarrow b = c$.

Exercice 3
On suppose H un sous ensemble non nul d'un groupe G. Montrer que H est un sous groupe de G si et seulement si pour tout $a, b \in H$ $ab^{-1} \in H$.

Exercice 4
Supposons que $|G| = p$ avec p premier. Montrer qu'il existe $a \in G$ tel que $G = \{a^n | n \in \mathbb{Z}\}$.

Exercice 5
Prouver le petit théor de Fermat.

Exercice 6
Prouver le théor d'Euler-Fermat.

4 Dénombrabilité

On pourra se reporter aux cours sur le même sujet lors de la dernière journée du stage olympique d'été, en 2013 par Louis Nebout et 2014 par Matthieu Lequesne.

4 Géométrie

1 Théorèmes de l'angle inscrit et du Pôle Sud, puissance d'un point

– Résumé du cours –

Le but du cours était de rappeler quelques concepts et techniques de base en géométrie. Nous avons évoqué les propriétés suivantes :

— théorème de l'angle inscrit ;

— pôle Sud d'un triangle : dans un triangle ABC, soit S le second point d'intersection de la bissectrice de $\widehat{BAC}$ avec le cercle circonscrit. Alors S est le centre d'un cercle passant par B, C, le centre I du cercle inscrit à ABC, et le centre I_A du cercle A-exinscrit à ABC ;

— triangles semblables (l'intérêt est de transformer des informations sur des longueurs en informations sur des angles, comme l'illustre par exemple l'exercice 2 ci-dessous) ;

— puissance d'un point et axes radicaux.

– Chasse aux angles, triangles semblables, puissance d'un point –

Exercice 1
Soit ABC un triangle isocèle en A, et Γ son cercle de circonscrit. Soient D et E deux points sur $[BC]$. Les droites (AD) et (AE) recoupent Γ en F et G.

Montrer que les points D, E, F et G sont cocycliques.

Exercice 2 (IMO 2014, Problème 4)
Soit ABC un triangle dont les trois angles sont aigus, et P et Q deux points sur le côté $[BC]$ tels que $\widehat{PAB} = \widehat{BCA}$ et $\widehat{CAQ} = \widehat{ABC}$. Soient M et N les points sur (AP) et (AQ) tels que P est le milieu de $[AM]$ et Q le milieu de $[AN]$.

Montrer que le point d'intersection des droites (BM) et (CN) est sur le cercle circonscrit au triangle ABC.

Exercice 3 (IMO 2008, Problème 1)
Soit ABC un triangle dont les angles sont aigus, et soit H son orthocentre. Le cercle passant par H et dont le centre est le milieu de $[BC]$ coupe la droite (BC) en A_1 et A_2. De même, le cercle passant par H et dont le centre est le milieu de $[CA]$ coupe la droite (CA) en B_1 et B_2, et le cercle passant par H et dont le centre est le milieu de $[AB]$ coupe la droite (AB) en C_1 et C_2.

Montrer que A_1, A_2, B_1, B_2, C_1 et C_2 sont cocycliques.

Exercice 4 (IMO 2009, Problème 2)
Soit ABC un triangle et O le centre de son cercle circonscrit. Soient P et Q sur les côtés $[AC]$ et $[AB]$ respectivement. Soient K, L et M les milieux respectifs des segments $[BP]$, $[CQ]$ et $[PQ]$, et soit Γ le cercle passant par K, L et M. On suppose que la droite (PQ) est tangente au cercle Γ.

Montrer que $OP = OQ$.

– Pôle Sud d'un triangle –

Exercice 5
Soit ABC un triangle avec $\widehat{BAC} = 60°$. On note respectivement H, I et O son orthocentre, le centre de son cercle inscrit et le centre de son cercle circonscrit. Montrer que $IO = IH$.

Exercice 6
Soit ABC un triangle. On note D, E et F les pieds des bissectrices de $\widehat{A}$, $\widehat{B}$ et $\widehat{C}$, ainsi que I le centre du cercle inscrit. La médiatrice de $[AD]$ coupe (BE) en X et (CF) en Y.

Montrer que les points A, I, X et Y sont cocycliques.

Exercice 7 (IMO 2006, Problème 1)
Soit ABC un triangle et I le centre de son cercle inscrit. Un point P intérieur au triangle vérifie

$$\widehat{PBA} + \widehat{PCA} = \widehat{PBC} + \widehat{PCB}.$$

Montrer que $AP \geqslant AI$ et que l'égalité a lieu si et seulement si $P = I$.

Exercice 8 (IMO 2004, Problème 1)
Soit ABC un triangle dont les trois angles sont aigus avec $AB \neq AC$. Soient P et Q les pieds des hauteurs issues de B et C, et M le milieu de $[BC]$. Les bissectrices des angles $\widehat{BAC}$ et $\widehat{PMQ}$ s'intersectent en R.

Montrer que les cercles circonscrits à BQR et CPR se recoupent sur (BC).

Exercice 9
Soit ABC un triangle, et Γ son cercle circonscrit. On note I le centre du cercle inscrit, I_A le centre du cercle A-exinscrit et S le milieu de l'arc $\widehat{BC}$ de Γ. Soit N le milieu de l'arc $\widehat{AS}$ de Γ contenant B. Les droites (NI) et (NI_A) recoupent Γ en X et Y.

Montrer que les droites (AI), (BC) et (XY) sont concourantes.

– Solutions des exercices –

Solution de l'exercice 1
On fait une chasse aux angles :

$$\begin{aligned}\widehat{DEG}+\widehat{DFG} &= \widehat{DEA}+\widehat{DFC}\\ &= \widehat{DCF}+\widehat{BCA}+\widehat{DFC}\\ &= 180^\circ-\widehat{CDF}+\widehat{BCA}\\ &= 180^\circ-\widehat{CBA}+\widehat{BCA}\\ &= 180^\circ.\end{aligned}$$

Solution de l'exercice 2
On note α, β, γ les angles de ABC. Les égalités d'angles donnent directement deux triangles semblables : les triangles PBA et QAC (il sont aussi semblables à ABC). L'idée est de montrer que les triangles BMP et NCQ sont semblables. Pour commencer, ils ont un angle en commun : on a $\widehat{BPM} = 180^\circ - \alpha = \widehat{NQC}$. De plus, en utilisant les deux milieux et les deux triangles semblables $PBA \sim QCA$, on a

$$\frac{PB}{PM} = \frac{PB}{AP} = \frac{QA}{QC} = \frac{QN}{QC}.$$

Les triangles BMP et NCQs ont donc bien semblables.

La fin est une simple chasse aux angles. Soit X le point d'intersection de (BM) et (CN) :

$$\widehat{BXC} = 180^\circ - \widehat{MBP} - \widehat{NCQ} = 180^\circ - \widehat{MBP} - \widehat{BMP} = \widehat{BPM} = 180^\circ - \widehat{APB} = 180^\circ - \alpha,$$

donc les points A, B, C et X sont bien cocycliques.

Solution de l'exercice 3
Notons A', B' et C' les milieux de $[BC]$, $[CA]$ et $[AB]$. On note aussi Γ_A, Γ_B et Γ_C les cercles de centres A', B' et C' passant par H.

On commence par montrer que les points B_1, B_2, C_1 et C_2 sont cocycliques. Par puissance d'un point, il suffit de montrer

$$AB_1 \times AB_2 = AC_1 \times AC_2,$$

c'est-à-dire que A a la même puissance par rapport à Γ_B et Γ_C. Cela revient à dire que A est sur l'axe radical de Γ_B et Γ_C.

Or, cet axe radical passe par H. De plus, il est perpendiculaire à $(B'C')$, qui est parallèle à (BC). L'axe radical est donc perpendiculaire à (BC), donc il s'agit de la droite (AH), ce qui montre que B_1, B_2, C_1 et C_2 sont cocycliques.

Le centre du cercle passant par ces quatre points est sur la médiatrice de $[B_1B_2]$. Comme $B'B_1 = B'B_2$, cette médiatrice est aussi celle de $[AC]$. De même, le centre du cercle est sur la médiatrice de $[AB]$, donc c'est le centre O du cercle circonscrit à ABC. De même, O est le centre d'un cercle passant par A_1, A_2, B_1 et B_2, donc les six points sont cocycliques.

Solution de l'exercice 4

D'après le cas limite du théorème de l'angle inscrit, on a $\widehat{KLM} = \widehat{KMQ}$ et $\widehat{PML} = \widehat{PKL}$.

Par ailleurs, d'après le théorème de la droite des milieux, la droite (KM) est parallèle à (AB), donc $\widehat{KLM} = \widehat{KMQ} = \widehat{PQA}$. Similairement, on a $\widehat{LKM} = \widehat{LMP} = \widehat{QPA}$. Les triangles KLM et PQA sont donc semblables, donc

$$\frac{AP}{AQ} = \frac{KM}{LM} = \frac{1/2 \times BQ}{1/2 \times CP} = \frac{BQ}{CP},$$

en utilisant encore le théorème de la droite des milieux.

On a donc $PA \times PC = QA \times QB$. Cela signifie justement que les points P et Q ont la même puissance par rapport au cercle circonscrit à ABC ! On rappelle que la puissance d'un point P par rapport à un cercle de centre O et de rayon r vaut $OP^2 - r^2$. On a donc $OP^2 - r^2 = OQ^2 - r^2$, donc $OP = OQ$.

Solution de l'exercice 5

Il faut remarquer que les points B, C, H, I et O sont cocycliques. En effet, on a

$$\widehat{BOC} = 2\widehat{BAC} = 120°,$$

$$\widehat{BIC} = 180° - \frac{1}{2}\widehat{ABC} - \frac{1}{2}\widehat{ACB} = 180° - \frac{1}{2}\left(180° - \widehat{BAC}\right) = 120°,$$

et enfin

$$\widehat{BHC} = 180° - (90° - \widehat{ABC}) - (90° - \widehat{ACB}) = 180° - \widehat{BAC} = 120°.$$

On veut donc montrer que I est le milieu de l'arc $\widehat{OH}$, donc que I est le pôle Sud de BOH. Il suffit donc de montrer que $\widehat{IBO} = \widehat{IBH}$, soit $\widehat{ABO} = \widehat{CBH}$, ce qui peut se montrer par chasse aux angles.

Solution de l'exercice 6

Le point X est l'intersection de la médiatrice de $[AD]$ avec la bissectrice de $\widehat{ABD}$, donc c'est le pôle Sud du triangle BAD, donc les points A, B, D et X sont cocycliques. Il en est de même pour A, C, D et Y. On peut donc conclure par chasse aux angles :

$$\widehat{XAY} = \widehat{XAD} + \widehat{YAD} = \widehat{XBD} + \widehat{YCD} = \widehat{IBC} + \widehat{ICB} = 180° - \widehat{BIC} = 180° - \widehat{XIY},$$

donc les points A, I, X et Y sont bien cocycliques.

Solution de l'exercice 7

La condition sur les angles se réécrit

$$\widehat{PBC} + \widehat{PCB} = \widehat{ABC} + \widehat{ACB} - \widehat{PBC} - \widehat{PCB}$$

ou encore

$$\widehat{PBC} + \widehat{PCB} = \frac{1}{2}(\widehat{ABC} + \widehat{ACB}) = \frac{1}{2}(180° - \widehat{BAC}),$$

c'est à dire

$$\widehat{BPC} = \frac{1}{2}(180° + \widehat{BAC}).$$

Or, puisque I est l'intersection des bissectrices de $\widehat{ABC}$ et $\widehat{ACB}$, on a facilement

$$\widehat{BIC} = 180° - \frac{1}{2}(\widehat{ABC} + \widehat{ACB}) = \frac{1}{2}(180° + \widehat{BAC}) = \widehat{BPC}.$$

L'hypothèse de l'énoncé équivaut donc à dire que les points B, C, I et P sont cocycliques. Le centre de ce cercle est le centre du cercle circonscrit à BCI, c'est-à-dire le pôle Sud S de ABC. On a donc

$$AI = AS - SI = AS - SP \leqslant AP$$

par inégalité triangulaire, avec égalité si et seulement si $P \in [AS]$. Comme P est sur le cercle de centre S passant par I, le seul cas d'égalité est donc $P = I$.

Solution de l'exercice 8

On note X le second point d'intersection (après R) des cercles circonscrits à BQR et CPR. Commençons par une chasse aux angles :

$$\widehat{BXC} = \widehat{BXR} + \widehat{CXR} = 180° - \widehat{BQR} + 180° - \widehat{CPR} = \widehat{AQR} + \widehat{APR}.$$

Le problème équivaut donc à montrer que $\widehat{AQR} + \widehat{APR} = 180°$, c'est-à-dire que A, P, Q et R sont cocycliques.

Or, les triangles BCP et BCQ sont rectangles en P et Q, donc P et Q se trouvent sur le cercle de diamètre $[BC]$, qui a pour centre M. On a donc $MP = MQ$, donc la bissectrice de $\widehat{PMQ}$ est également la médiatrice de $[PQ]$.

Le point R est donc l'intersection de la bissectrice de $\widehat{PAQ}$ avec la médiatrice de $[PQ]$, donc c'est le pôle Sud du triangle APQ. En particulier, il est sur le cercle circonscrit à APQ, ce qui conclut.

Solution de l'exercice 9

On sait que les points A, I, S et I_A sont alignés (dans cet ordre) sur la bissectrice de $\widehat{BAC}$. En utilisant également le fait que $NA = NS$, on obtient

$$\widehat{NXS} = 180° - \widehat{NAS} = 180° - \widehat{NSA} = \widehat{NSI_A}.$$

Les triangles NXS et NSI_A sont donc (indirectement) semblables, donc $\frac{NX}{NS} = \frac{NS}{NI_A}$.

De même, on a

$$\widehat{NYS} = \widehat{NAS} = \widehat{NSA} = \widehat{NSI},$$

donc NYS et NSI sont semblables, donc $\frac{NY}{NS} = \frac{NS}{NI}$. En combinant ces deux dernières égalités, on obtient

$$NX \times NI_A = NS^2 = NY \times NI.$$

Par puissance d'un point, les points I, I_A, X et Y sont donc cocycliques. On considère donc les axes radicaux des trois cercles suivants : ce dernier cercle, Γ, et le cercle passant par B, C, I et I_A. Les trois axes radicaux sont (BC), (XY) et $(II_A) = (AI)$, donc ces trois droites sont concourantes, ce qui conclut.

2 Transformations géométriques – 1$^{\text{ère}}$ partie

Nous avons vu durant ce cours (et ses deux heures d'ϵ...) toutes les transformations classiques du plan, en commençant par les isométries (identité, translation, rotation, symétrie centrale et symétrie axiale ainsi que leur composées), en poursuivant par les similitudes du plan (homothétie et similitude directe). Nous avons fini par une ouverture sur une transformation non-classique : l'inversion.

Voici une partie des exercices traités et leur corrigé

– Isométries –

Exercice 1
Soit $ABCD$ un parallèlogramme, et P le point en son intérieur tel que $\widehat{PBC} = \widehat{PDC}$. Montrer alors que $\widehat{PAB} = \widehat{PCB}$.

Exercice 2 (Configuration de Fermat)
Soit ABC un triangle, et A' (resp. B', C') le point tels que CBA' (resp. BAC', ACB') est équilatéral direct. Montrer que $AA' = BB' = CC'$.

Exercice 3
Montrer que les centres O_A, O_B, O_C des triangles équilatéraux BCA', CAB', ABC' de la configuration de l'exercice 2 forment eux aussi un triangle équilatéral.

– Similitudes –

Exercice 4 (Monge)
Soient trois cercles. Les deux tangentes extérieures de chacun se recoupent respectivement en X, Y et Z. Montrer que ces trois derniers points sont alignés.

Exercice 5
Soit $ABCD$ un trapèze où (AB) et (CD) sont les côtés parallèles. On note X l'intersection de (AC) et (BD), ainsi que Y celle de (AD) et (BC). Montrer que les milieux M et N de $[AB]$ et $[CD]$, X et Y sont alignés.

Exercice 6 (Théorème de Miquel)
On notera $\bigcirc PQR$ le cercle circonscrit au triangle PQR.

Soient trois cercles concourants en O et se recoupant mutuellement en A, B et C. On choisit un point X sur $\bigcirc ABO$, la droite (XB) recoupe $\bigcirc BCO$ en Y. La droite (YC) recoupe $\bigcirc CAO$ en Z. Montrer que Z, A, et X sont alignés.

– Solutions –

Solution de l'exercice 1
On fait une translation de P de vecteur $\overrightarrow{AB}$, et on appelle P' ce nouveau point. Alors $\widehat{PDC} = \widehat{PP'C} = \widehat{PBC}$ donc les points P, B, C et P' sont cocycliques. Cela montre que $\widehat{PAB} = \widehat{PP'B} = \widehat{PCB}$, ce qui conclut.

Solution de l'exercice 2
On étudie la rotation

$$R_{A,60} \quad : \quad \begin{array}{l} A \to A \\ C' \to B \\ C \to B' \end{array}$$

Puisqu'elle envoie le segment $[CC']$ sur $[BB']$, ces deux segments ont donc la même longueur. En faisant de même depuis le sommet B, on trouve que $AA' = BB' = CC'$.

Solution de l'exercice 3
On va étudier la composition

$$T = R_{O_C,120} \circ R_{O_B,120} \circ R_{O_A,120}$$

On remarque que la transformation T est une "rotation" d'angle $360°$, donc c'est une translation. Comme $T(C) = C$, c'est la translation de vecteur nul, donc c'est l'identité. On en déduit que $T(O_A) = O_A$. Or,

$$O_A = T(O_A) = R_{O_C,120} \circ R_{O_B,120} \circ R_{O_A,120}(O_A),$$

donc $O_A = R_{O_C,120} \circ R_{O_B,120}(O_A)$. Ainsi, si on appelle O l'image de O_A par notre rotation de centre O_B, on a que $O_BO_A = O_BO$ et $\widehat{O_AO_BO} = 120$, et aussi que O a pour image O_A par notre rotation de centre O_C, d'où $O_CO = O_CO_A$ et $\widehat{OO_CO_A} = 120°$.

Enfin, si l'on trace la figure concernant juste les centres et O, et on s'aperçoit que (O_BO_C) est la médiatrice de $[O_AO]$, donc que $\widehat{O_BO_AO_C} = 60°$. On peut montrer de la même façon que $\widehat{O_AO_BO_C} = 60°$, et le triangle $O_AO_BO_C$ est donc équilatéral.

Solution de l'exercice 4
Soit H_1 (resp. H_2, H_3) l'homothétie de centre X (resp. Y, Z) qui envoie γ_1 sur γ_2 (resp. γ_2 sur γ_3, γ_3 sur γ_1). Son rapport est positif, et c'est le rapport des rayons, $\frac{r_2}{r_1}$ (resp. $\frac{r_3}{r_2}$, $\frac{r_1}{r_3}$). On va étudier la composition

$$T = H_3 \circ H_2 \circ H_1.$$

Elle a pour rapport $\frac{r_2}{r_1} \cdot \frac{r_3}{r_2} \cdot \frac{r_1}{r_3} = 1$ donc c'est une translation. Elle envoie γ_1 sur lui même, et en particulier son centre O sur lui même, donc c'est l'identité.

En particulier, $T(X) = X$. Donc $X = T = H_3 \circ H_2 \circ H_1(X) = T = H_3 \circ H_2(X)$. On remarque que le centre de H_2 appartient à $(H_2(X)X)$, et que le centre de H_3 appartient à $(H_2(X)X)$ puisque le centre d'une homothétie appartient toujours à la droite qui joint un point et son image. Les points X, Y et Z sont donc alignés.

Solution de l'exercice 5

Considérons l'homothétie de centre X et de rapport négatif envoyant $[AB]$ sur $[CD]$. Alors elle envoie le milieu de $[AB]$ sur le milieu de $[CD]$, donc M sur N, et X, M, N sont alignés. En considérant l'homothétie de centre Y, on trouve de la même façon que M est envoyé sur N, donc Y, M, N sont aussi alignés, ce qui conclut.

Solution de l'exercice 6

On va faire une brin de théorie : soit S l'unique similitude envoyant A sur A' et B sur B'. On sait que son centre est le point de Miquel de $(AA'), (BB'), (AB), (A'B')$, donc si l'on trace les droites (AA') et (BB') qui s'intersectent en X, on a juste à tracer les cercles circonscrits γ et γ' à ABX et $A'B'X$, et le centre de notre similitude sera leur second point d'intersection.

De là, on déduit que notre similitude envoie γ sur γ'. Mais comment trouver l'image d'un point C de γ ? Il suffit de reprendre la même construction : C' est l'intersection de (CX) avec γ'.

Soit S_1 la similitude de centre O envoyant $\bigcirc OAB$ sur $\bigcirc OBC$. Elle envoie en particulier X sur Y d'après notre théorie. De même, la similitude S_2 de centre O envoyant $\bigcirc OBC$ sur $\bigcirc OCA$ envoie en particulier Y sur Z. La composition $S_2 \circ S_1$ envoie donc $\bigcirc OAB$ sur $\bigcirc OCA$, et X sur Z, ce qui se traduit notamment par l'appartenance de A à la droite (XZ), concluant ainsi l'exercice.

3 Milieux et parallélogrammes

Une part non négligeable des problèmes de géométrie font intervenir d'une façon ou d'une autre les milieux d'un segment. Soit le milieu est déjà défini dans la figure soit une partie du problème consiste à montrer qu'un point est un milieu. Le problème des milieux de segment est qu'ils fournissent rarement une hyptohèse sur les angles, on ne peut donc pas l'utiliser dans une chasse aux angles par exemple. Le but de ce cours est d'étudier différents réflexes qui peuvent être utiles pour "intégrer" un milieu de segment dans une figure ou pour montrer que tel point est milieu d'un segment. Il ne s'agit pas d'établir une méthode infaillible, mais juste de voir quelques idées qui peuvent s'avérer utiles. Il est impensable de vouloir résoudre un problème de géométrie faisant intervenir un milieu si on n'a pas bien interpreté ce milieu.

Lorsqu'un milieu se trouve déjà placé dans une figure, on a plusieurs façons de l'interpréter :

— Par une égalité de longueurs, tout simplement : l'égalité de longueur peut permettre de trouver des triangles isométriques ou semblables, ce qui donne directement une bonne égalité d'angle.

— Introduire d'autres milieux : Introduire d'autres milieux peut permettre d'obtenir des droites parallèles ou des triangles semblables et donc des angles et des égalités de rapports. De manière générale, si on est en présence d'une condition sur des longueurs, il peut être utile d'introduire d'autres points bien choisis satisfaisant les mêmes conditions.

— Compléter un parallélogramme : Ce qu'il y a de génial avec un parallèlogramme, c'est qu'on a pleins d'égalités d'angles et de longueur (c'est d'ailleurs aussi ce qu'il y a d'embêtant avec un parallélogramme). Lorsqu'on a un point milieu de segment, introduire un autre segment dont ce point est aussi un milieu donne un beau parallélogramme et transforme donc l'hypothèse "M est le milieu d'un segment" en une égalité d'angle, un parallélisme etc...

La liste ci-dessus n'est évidemment pas exhaustive. La façon d'utiliser un milieu dépend bien sûr avant tout de la figure imposée.

Si le but du problème est de montrer que tel point est un milieu, on peut adapter els idées précédentes : tout bêtement essayer de montrer une éaglité de longueur, introduire d'autres points milieux pourrait aussi aider ou encore montrer que le point en question est intersection des diagonales d'un parallélogramme peut se montrer très efficace. Une autre idée très efficace est de faire intervenir des axes radicaux à l'aide de la propriété suivante :

Lemme 4.3.1.
Soient deux cercles k_1 et k_2 se coupant en deux points A et B. Une tangente extérieure commune aux 2 cercles touche k_1 en C et k_2 en D. Alors (AB) coupe $[CD]$ en son milieu.

Démonstration. (AB) est l'axe radical des deux cercles donc le point d'intersection M de (AB) et (CD) vérifie $CM^2 = DM^2$. □

Transformer la figure pour aboutir à cette configuration peut s'avérer très efficace.

La meilleure façon de savoir utiliser des milieux restant avant tout de pratiquer :

Exercice 1 (British math olympiad 2018, Round 2)
Soit ABC un triangle et M le milieu de $[AC]$. Le cercle tangent au segment $[BC]$ en B et passant par M recoupe (AB) en P. Montrer que $AB \cdot BP = 2BM^2$.

Solution de l'exercice 1
L'égalité à démontrer fait penser à la puisance d'un point, à ceci près qu'il y a un facteur 2 gênant. C'est ce qui nous motive à introduire le point B' tel que $ABCB'$ soit un parallélogramme. L'égalité à montrer devient $AB \cdot BP = BM \cdot BB'$, c'est-à-dire que l'on doit montrer que les points M, A, P, B' sont cocycliques. Or le cercle (MPB) est tangent à $[BC]$ donc $\widehat{MPA} = \widehat{MPB} = \widehat{MBC} = \widehat{MB'A}$ ce qui conclut.

Exercice 2 (Math Beyond limits 2018)
Soit ABC un triangle d'orthocentre H. On note D, E, F les pieds des hatueurs issues respectivement de A, B et C. La parallèle à (AC) passant par B coupe (EF) en X. Soit M le milieu de $[AB]$. Montrer que $\widehat{ACM} = \widehat{XDB}$.

Solution de l'exercice 2
Ici, l'introduction du milieu de $[AB]$ et de la parallèle à (AC) passant par B motive encore une fois à créer un parallèlogramme. Soit donc C' le point tel que $BCAC'$ soit un parallèlogramme. On a alors $\widehat{ACM} = \widehat{CC'B}$ donc l'égalité à montrer devient $\widehat{XDB} = \widehat{XC'C}$, c'est-à-dire qu'il suffit de montrer que les points C, C', D, X sont cocycliques. Les droites (BX) et (AC) sont parallèles donc Thalès donne

$$\frac{BX}{AE} = \frac{BF}{AF}$$

On se rappelle alors que les triangles BDF, BAC, EAF sont semblables (propriétés du triangles orthique), on obtient donc les égalités suivantes :

$$BX \cdot BC' = BX \cdot AC = \frac{AE}{AF} \cdot BF \cdot AC = \frac{AB}{AC} \cdot BF \cdot AC = AB \cdot BF = BD \cdot BC$$

et l'on conclut par la réciproque de la puissance d'un point.

Exercice 3 (JBMO 2013)
Soit ABC un triangle tel que $AB < AC$ et O le centre de son cercle circonscrit k. Soit D un point du segment $[BC]$ tel que $\widehat{BAD} = \widehat{CAO}$. Soit E le second point d'intersection de k avec la droite (AD). Soient M, N, P les milieux des segments $[BE]$, $[OD]$, $[AC]$. Montrez que M, N, P sont alignés.

Solution de l'exercice 3
L'idée principale est de démontrer un résultat plus fort, à savoir que M, O, D, P est un parallèlogramme, ce qui permet alors de conclure. On présente deux méthodes utilisant de deux façons différentes les différentes hypothèses sur les milieux présents.

Solution 1 utilisant des triangles isométriques : Les triangles OMB et POA sont tous les deux rectangles et $OA = OB$. Il suffit de montrer que $\widehat{MOB} = \widehat{PAO}$ pour avoir que les deux triangles sont isométriques. Or EOB est isocèle donc $\widehat{MOB} = \frac{1}{2}\widehat{BOE} = \widehat{DAB} = \widehat{PAO}$. Les triangles sont donc isométriques et $AP = OM$ et $OP = MB$. On utilise alors le fait que D est en fait pied de la hauteur issue de A dans le triangles ABC (résultat classique dont la démonstration est un bon exercice de chasse aux angles). Donc EDB et CDA sont rectangles et $DM = MB = OP$ et $DP = PA = OM$. Donc le quadrilatère $DPOM$ a les côtés opposés égaux deux à deux, c'est un parallélogramme. Donc les diagonales se coupent en leur milieu et P, N, M sont alignés.

Solution 2 utilisant une chasse aux angles un peu fastidieuse : On utilise à nouveau que EDB et ADC sont rectangles. Soit X le projeté de O sur $[CB]$. (OX) et (AD) sont parallèles. Les points P, O, X, C sont cocycliques. On commence par montrer que (OP) et (DM) sont parallèles par égalités d'angles alternes internes.

$$\widehat{ODM} = \widehat{ODA} + 90 + \widehat{MDB} = \widehat{XOD} + 90 + \widehat{DBE} = \widehat{XOD} + 90 + \widehat{CAD}$$

Or $\widehat{CAD} + 90 = 180 - \widehat{DCA}$ donc en utilisant la cocyclicité de C, P, O, D on a

$$\widehat{ODM} = 180 - \widehat{CDA} + \widehat{XOD} = \widehat{POX} + \widehat{XOD} = \widehat{POD}$$

donc (DM) et (OP) sont parallèles.

On montre ensuite que $\widehat{DPO} = \widehat{DMO}$. Il faut encore une fois voyager avec les différentes égalités d'angles dues au théorème de l'angle inscrit et au fait que CDA et EDB sont rectangles :

$$\widehat{DPO} = \widehat{DPA} - \widehat{OPA} = 180 - 2\widehat{PAD} - 90 = 180 - 2\widehat{MBD} - 90 = \widehat{DMB} - 90 = \widehat{DMO}$$

ce qui donne que $MDPO$ est un quadrilatère avec deux cotés opposés parallèles et deux angles opposés égaux, c'est un parallélogramme, on peut conclure de la même façon qu'en solution 1.

On pourra également admirer en troisisème solution la solution suivante, composée uniquement de la figure, sans plus d'explications :

Exercice 4
Soit C un point du demi-cercle de diamètre $[AB]$ et soit D le milieu de l'arc AC. Soit E la projection de D sur la droite (BC) et F l'intersection de (AE) avec le demi-cercle. Prouver que (BF) coupe le segment $[DE]$ en son milieu.

Solution de l'exercice 4

Ici, on va essayer de se ramener à la configuration du lemme donné en début de cours. (BF) est axe radical des cercles (DFB) et (EFB), il reste à montrer que (DE) est tangent à chacun de ces cercles. Une remarque préliminaire est que (DE) et (AC) sont toutes deux perpendiculaires à (BC) donc parallèles. O le centre du demi-cercle vérifie que (OD) et (AC) sont perpendiculaires car D est milieu de l'arc AC. Donc (ED) est tangente à (DFB). De plus par parallélisme, $\widehat{FED} = \widehat{FAC} = \widehat{FBC}$ donc (ED) est tangente à (FEB), on peut donc conclure par le lemme donné en début de cours.

Exercice 5

Soient A, B, C trois points d'un cercle k tels que $AB = BC$. Les tangentes en A et en B au cercle k se coupent en D. (DC) rencontre k en E. Montrer que (AE) coupe $[BD]$ en son milieu.

Solution de l'exercice 5

Une fois de plus on essaye de se ramener à la configuration du lemme. Montrons que (DB) est tangente aux cercles (AEB) et (DEA) dont (AE) est l'axe radical. (DB) est déjà tangente à (AEB) par hypothèse. Montrons l'autre tangence. (DB) est perpendiculaire à la médiatrice de $[AC]$ comme ABC est isocèle en B et (DB) est tangente à k, donc (DB) et (AC) sont parallèles. Alors, par tangence :

$$\widehat{DAE} = \widehat{ECA} = \widehat{EDB}$$

ce qui donne la tangence et conclut.

Exercice 6 (Problème 6, PAMO 2017)
Soit ABC un triangle d'orthocentre H. Le cercle de diamètre $[AC]$ recoupe le cercle circonscrit au triangle ABH en K. Montrer que (CK) coupe $[BH]$ en son milieu.

Solution de l'exercice 6
Voici deux solutions utilisant deux méthodes différentes pour montrer que (CK) coupe $[BH]$ en son milieu.

Dans la première solution, on introduit un parallélogramme dont (CK) et (BH) sont les diagonales. Soit E l'intersection de (CK) avec le cercle circonscrit à ABH. Il suffit de montrer que $CHEB$ est un parallélogramme. Soit X le pied de la hauteur issue de C. En voyageant dans les différents cercles :

$$\widehat{ECH} = \widehat{KCX} = \widehat{XAK} = \widehat{BAK} = \widehat{BEK} = \widehat{BEC}$$

donc (CH) et (BE) sont parallèles. Soit Y le pied de la hauteur issue de A Par ailleurs

$$\widehat{CEH} = \widehat{KEH} = \widehat{KAH} = \widehat{KAY} = \widehat{KCY} = \widehat{KCB} = \widehat{ECB}$$

ce qui montre que (EH) et (BC) sont parallèles. On a bien un parallélogramme et les diagonales se coupent en leur milieu.

Dans la deuxième solution, on se ramène à la configuration de la propriété énoncée au début du cours et montrer que (CK) est axe radical de deux cercles bien choisis. On montre que (BH) est tangent aux cercles KHC et BKC, et comme KC est l'axe radical de ces deux cercles il coupe le segment reliant les points de tangence en son milieu :

$$\widehat{BHK} = \widehat{BAK} = \widehat{XAK} = \widehat{XCK} = \widehat{HCK}$$

donc (BH) est tangent au cercle KHC en H.

$$\widehat{KBH} = \widehat{KAH} = \widehat{KAY} = \widehat{KCY} = \widehat{KCB}$$

donc (BH) est tangent au cercle KCB en B. (on a gardé les mêmes notations qu'en solution 1). On a donc tangence, on peut conclure par le lemme.

Exercice 7 (Problème G1, Liste courte IMO 2015)
Soit ABC un triangle d'orthocentre H et G le point tel que $ABGH$ est un parallélogramme. Soit I le point de la droite (GH) tel que (AC) coupe $[HI]$ en son milieu. La droite (AC) recoupe le cercle circonscrit du triangle GCI en J. Montrer que $IJ = AH$.

Solution de l'exercice 7
Il existe beaucoup de solutions car il y a plusieurs façon d'interpréter le fait que (AC) coupe $[HI]$ en son milieu. On présente ici deux solutions : l'une consiste à calculer patiemment plusieurs rapports de longueur, l'autre introduit astucieusement un point supplémentaire pour avoir des triangles isométriques.

Solution 1 : Dans cette solution, on utilise que (AC) coupe $[HI]$ en son milieu uniquement pour obtenir une égalité de longueurs. Quels que nouveaux points sont de mises : Soit D, E et F les pieds des hauteurs issues respectivement de A, B et C. Soit X le point d'intersection de (HI) et (AC) et soit Y le point d'intersection de (BC) et (HG). Par parallélisme, on a (BG) parpendiculaire à (BC) donc G, B, H, C sont cocycliques. Par des égalités de rapports classiques liées aux différents triangles semblables dans la figures :

$$\frac{IJ}{CG} = \frac{IX}{XC} = \frac{HX}{DX} = \frac{AF}{AC} = \frac{AH \cdot AD}{AB} \cdot \frac{1}{AC} = \frac{AH}{AB} \cdot \frac{BD}{BH} = \frac{AH}{BH} \cdot \frac{HY}{YC} = \frac{AH}{BH} \cdot \frac{BH}{GC} = \frac{AH}{CG}$$

d'où l'égalité.

Solution 2 : On note toujours X le milieu de $[IH]$. L'hypothèse que (AC) coupe $[IH]$ en son milieu peut donner envie de trouver un triangle avec dans ses sommets H et X et qui soit isométrique à IJX. Malheuresement, un tel triangle n'est pas présent dans la figure; et introduire un point Z pour compléter ce triangle ne donne pas beauocup d'informations sur ce points. Cependant, on sait que si l'énoncé est vrai, $ZH = IJ = AH$. On procède alors dans l'autre sens, on introduit Z tel que $ZH = AH$ et on montre l'isométrie. Cette discussion motive la preuve suivante :

Soit $Z \neq A$ le point de $[AC]$ tel que $HZ = AH$. De même que précédemment, on a que B, G, C, H sont cocycliques. Donc en voyageant dans les différents cercles :

$$\widehat{CJI} = \widehat{CGH} = \widehat{CBH} = \widehat{HAC}$$

C'est là que Z intervient : $\widehat{MJI} = \widehat{CJI} = \widehat{HAC} = \widehat{MDH}$. C'est suffisant pour avoir que les triangles IMJ et MHD sont semblables, et $IM = MH$ impose qu'ils sont isométriques. Donc $IJ = DH = AH$.

Exercice 8 (Problème G2, Liste courte IMO 2007)
Soit ABC un triangle tel que $AB = AC$. Le milieu de $[BC]$ est noté M. Soit X un point variable du plus petit arc AM du cercle circonscrit au triangle ABM. Soit T le point du même côté de BM que X mais dans l'autre demi-plan délimité par (AM) que X et tel que $TX = BX$ et tel que l'angle $\widehat{TMX}$ est droit. Montrer que $\widehat{MTB} - \widehat{CTM}$ ne dépend pas du choix de X.

Solution de l'exercice 8
Quelques milieux apparaissent déjà dans la figure, et l'on cherche visiblement essentiellement à travailler avec des angles. Introduire un nouveau milieu bien choisi faciliterait donc bien les choses. Parmi les différents candidats, le plus intéressant semble être le milieu de $[TB]$, nous allons expliquer pourquoi par la suite.

Soit Y le milieu de $[TB]$. On a alors non seulement (YM) et (TC) parallèles mais aussi (YX) et (TB) perpendiculaires, donc T, Y, M, X sont cocycliques. Une fois ce milieu introduit, le reste n'est plus qu'une courte chasse aux angles :

$$\widehat{MTB} - \widehat{CTM} = \widehat{YYM} - \widehat{YMT} = \widehat{YXM} - \widehat{YXT} = \widehat{YXM} - \widehat{YXB} = \widehat{BXM} = \frac{1}{2} \cdot \widehat{BAC}$$

où les deux dernières égalités viennent des différentes cocyclicités et que (YX) est bissectrice de $\widehat{TXB}$. Donc la valeur de $\widehat{MTB} - \widehat{CTM}$ est fixe et ne dépend pas de X.

Exercice 9 (Problème 1, IMO 2000)
Soient k_1 et k_2 deux cercles se coupant en deux points M et N. Une tangente commune en deux cercles touche k_1 en A et touche k_2 en B, de telle sorte que M est plus proche que N de (AB). La parallèle à (AB) passant par M coupe k_1 en C et k_2 en D. Les droites (AC) et (BD) se coupent en E, les droites (AN) et (CD) en P et les droites (BN) et (CD) en Q. Montrer que $EP = EQ$.

Solution de l'exercice 9
$\widehat{ABE} = \widehat{MBD} = \widehat{ABM}$ succiessivement par parallélisme et angle tangentiel. De même, $\widehat{MAB} = \widehat{BAE}$. Les triangles EAB et MAB sont donc semblables et ont un côté commun, ils sont isométriques. Donc $BM = ME$ et $AE = AM$, donc E est le symétrique de M par rapport à (AB). Donc (EM) et(AB) sotn perpendiculaires, donc (EM) et (CD) sont perpendiculaires. Donc on est réduit à montrer que M est le milieu de $[PQ]$. Soit X le point d'intersection de $[AB]$ et (MN). Par le lemme, X est milieu de $[AB]$. Mais les triangles ABN et PQN sont semblables et N, M, X sont alignés donc M est le milieu de $[PQ]$, ce qui conclut.

Exercice 10 (Problème 2, IMO 2009)
Soit ABC un triangle et O le centre de son cercle circonscrit. Les points P et Q sont situés sur les segments $[AC]$ et $[AB]$ respectivement. Soient K, L, M les milieux respectifs des segments $[BP], [CQ]$ et $[PQ]$. Soit k le cercle passant par K, L, M. On suppose que la droite (PQ) est tangente à k. Montrer que $OP = OQ$.

Solution de l'exercice 10
Ici, les milieux servent pour obtenir des droites parallèles..

M est le milieu de $[PQ]$ et L celui de $[QC]$ donc (ML) et (PC) sont parallèles. D'où, par tangence et parallélisme :

$$\widehat{LKM} = \widehat{LMP} = \widehat{MPA} = \widehat{QPA}$$

De même, $\widehat{PQA} = \widehat{KLM}$. Les triangles MKL et APQ sont donc semblables. Donc

$$\frac{AP}{AQ} = \frac{MK}{ML} = \frac{\frac{1}{2}QP}{\frac{1}{2}CP} = \frac{QB}{CP}$$

et on déduit $AP \cdot CP = BQ \cdot AQ$. Donc P et Q on la même puissance par rapport au cercle (ABC). La puissance du point P par rapport au cercle ABC est $OP^2 - AO^2$ et la puissance du point Q par rapport à ce même cercle vaut $OQ^2 - OA^2$ donc on a $OP^2 = OQ^2$ et $OP = OQ$.

Exercice 11 (Problème 1, EGMO 2017)
Soit $ABCD$ un quadrilatère convexe tel que $\widehat{DAB} = \widehat{BCD} = 90$ et $\widehat{ABC} > \widehat{CDA}$. Soient Q et R des points de $[BC]$ et $[CD]$ respectivement, tels que (QR) coupe les droites (AB) et (AD) en P et S respectivement et tels que $PQ = RS$. Soit M le milieu de $[BD]$ et N celui de $[QR]$. Montrer que A, N, M, C sont cocycliques.

Solution de l'exercice 11
On rappelle que dans un triangle rectangle, le milieu de l'hypothénuse est le centre du cercle circonscrit à ce triangle, ce qui occasionne de nombreux triangles isocèles.

Comme $SR = QP$, N est milieu de $[QR]$. D'où :

$$\widehat{ANC} = \widehat{PNA} = \widehat{QNC} = 2 \cdot \widehat{PSA} + 2 \cdot \widehat{QRC} = 2(180 - \widehat{SDR}) = 2 \cdot \widehat{ADC} = \widehat{AMC}$$

ce qui conclut.

Exercice 12
Soit ABC un triangle et P un point intérieur tel que $\widehat{BPC} = 90$ et $\widehat{BAP} = \widehat{BCP}$. Soinet M et N les milieux respectifs de $[AC]$ et $[BC]$. Supposons que $BP = 2PN$. Montrer que (AP) est bissectrice de l'angle $\widehat{BPM}$.

Solution de l'exercice 12
Une première grosse difficulté est la figure. Trouver un moyen de construire une figure exacte (c'est-à-dire construire le point P) permet (comme souvent pour un énoncé où la figure exacte est difficile à construire) déjà d'avancer significativement dans le problème.

Voici une façon de construire P, qui fournit en fait une solution du problème : Supposons le point P construit. Soit C' le symétrique de C par rapport à (BP). Alors $AC' = 2PM = BP$. De plus $BC = BC'$ et donc $\widehat{BC'P} = \widehat{BCP} = \widehat{PAB}$ donc C', A, P, B sont cocycliques, donc $\widehat{C'AB} = \widehat{C'PB} = 90$.

Donc pour construire P, on trace le cercle de centre B passant par C. La perpendiculaire à (AB) coupe ce cercle en un point C' situé dans l'autre demi-plan délimité par (AB) que C. On prend alors P le milieu de $[C'C]$. D'après les remarques précédentes, P vérifie toutes les conditions de l'énoncé.

Solution 1 : En gardant ces notations, on a donc $AC' = 2PM = BP$ donc $C'APB$ est trapèze isocèle, (AP) est donc parallèle à (BC'). P et N sont milieux de $[CC']$ et $[BC]$ donc (PN) et $(C'B)$ sont parallèles, donc (AP) et (PN) sont confondues. Donc P est sur la médiane de ABC issue de A. On a alors

$$\widehat{NPM} = \widehat{NPC} + \widehat{CPM} = \widehat{BCP} + \widehat{CC'A} = \widehat{BC'P} + \widehat{PC'A} = \widehat{BC'A} = \widehat{BPN}$$

puisque $C'BPA$ est cyclique et A, P, N alignés, ce qui conclut.

Solution 2 : Ici, on introduit un autre milieu et on n'utilise pas la construction exacte de P. Soit K le milieu de $[CP]$. Avec tous ces milieux, les triangles APB et MKN sont semblables. Donc $\widehat{NMK} = \widehat{BAP} = \widehat{PCN} = \widehat{NPK}$. Donc $PMKN$ est cyclique et comme $PM = \frac{1}{2}BP = NK$, ce quadrilatère est un trapèze isocèle donc (MK) et (PN) sont parallèles. On avait aussi (MK) et (AB) parallèles, donc A, P, N sont alignés. Alors $\widehat{NPM} = \widehat{PNK} = \widehat{KNC} = \widehat{PBC} = \widehat{BPN}$ ce qui conclut.

On remarquera que les deux solutions sont assez similaires : l'une agrandit la figure en introduisant un symétrique, l'autre introduit un milieu. Ainsi les deux raisonnement sont les mêmes, mais effectués à une échelle différente. Les points P, M, C, N, K sont images de C', A, C, B, P par une homotéti de rapport $\frac{1}{2}$ de centre C.

Exercice 13 (Problème 4, IMO 2017)
Soient R et S des points distincts appartenant à un cercle Ω tels que le segment $[RS]$ n'est pas un diamètre de Ω. Soit l la tangente à Ω en R. Le point T est tel que S est le milieu du segment $[RT]$. Le point J est choisi sur le plus petit arc RS de Ω de sorte que le cercle Γ circonscrit au triangle JST rencontre l en deux points distincts. Soit A le point commun de Γ et l qui est le plus proche de R. La droite (AJ) recoupe Ω en K. Prouver que la droite (KT) est tangente à Γ.

Solution de l'exercice 13
Encore une fois, la clé est de trouver comment utiliser l'hypothèse que S est le milieu de $[RT]$. On présente deux preuves, l'une se contente de transformer l'hypothèse en une égalité de longueur dans une chasse aux rapports, l'autre consiste à compléter la figure du parallélogramme.

Solution 1 : On a déjà
$$\widehat{STA} = \widehat{SJK} = \widehat{SRK}$$
par angles inscrits, donc (AT) et (KR) sont parallèles. On a donc $\widehat{KRS} = \widehat{RTA}$ et puisque (RA) est tangente à Ω en R, $\widehat{ARS} = \widehat{SKR}$ donc les triangles KRS et RTA sont semblables. Donc
$$\frac{SR}{AT} = \frac{ST}{AT} = \frac{KR}{RT}$$
et comme $\widehat{KRT} = \widehat{STA}$ par parallélisme, les triangles KRT et STA sont semblables, donc $\widehat{KTS} = \widehat{KTR} = \widehat{SAT}$, on conclut alors par angle tangentiel.

Solution 2 : Comme précédemment, on commence par trouver que (AT) et (KR) sont parallèles. On introduit X le point d'intersection de (SJ) et (KR) et Y celui de (SJ) et (AT). Comme (AT) et $KR)$ sont parallèles et que la diagonales (XY) coupe la diagonale (RT) en son milieu, le quadrilatère $TXRY$ est un parallélogramme.

Soit maintenant V le second point d'intersection de (XT) et de Γ et W celui de (YR) et de Ω. C'est le moment de remarquer que X, Y sont sur l'axe radical des deux cercles, donc V, T, K, R et W, T, A, R sont cocycliques. On voyage alors dans les différents cercles et en utilisant les droites parallèles trouvées :
$$\widehat{YWT} = \widehat{YAR} = \widehat{ARK} = \widehat{KWR}$$
donc T, K, W sont alignés. On a alors
$$\widehat{XVR} = \widehat{XKT} = \widehat{KTA} = 180 - \widehat{XTK} - \widehat{TXK} = 180 - \widehat{KRA} - \widehat{ATV} = 180 - \widehat{TAV} - \widehat{ATV}$$
et les points V, A, R sont alignés. On en déduit :
$$\widehat{TVA} = \widehat{TVR} = \widehat{ARY} = \widehat{WTY} = \widehat{KTA}$$
et on peut conclure par angle tangentiel.

Exercice 14 (BxMO 2017)
Dans le quadrilatère convexe $ABCD$, on a $\widehat{ABC} = \widehat{BCD}$ et $\widehat{ADC} = 90$. Supposons que $AB = 2 \cdot CD$. Prouver que la bissectrice de $\widehat{ACB}$ est perpendiculaire à CD.

Solution de l'exercice 14
L'égalité de longueurs interpèle. Soit N le milieu de $[AB]$. Le quadrilatère $DCBN$ est alors un trapèze isocèle (il possède une symétrie envoyant B sur C et N sur D). On trace la parallèle à (AD) passant par C, elle coupe (DN) en T. Le quadrilatère $ADCT$ a deux angles droits consécutifs et une des diagonales coupe l'autre en son milieu M, c'est un rectangle. Donc $\widehat{ACT} = \widehat{DTC} = \widehat{TCB}$ par parallélisme de (DN) et (CB), donc (CT) est la bissectrice de $\widehat{ACB}$, et elle est par définition perpendiculaire à (CD), on a gagné.

Exercice 15 (BxMO 2018)
Soit ABC un triangle dont H est l'orthocentre, et soient D, E et F les milieux respectifs des segments $[AB], [AC]$ et $[AH]$. Les symétriques de B et C par rapport à F sont P et Q respectivement.

(alph*) Montrer que les droites (PE) et (QD) se coupent sur le cercle circonscrit au triangle ABC.

(alph*) Montrer que les droite (PD) et (QE) se coupent sur le segment $[AH]$.

Solution de l'exercice 15
Avant de commencer, notons tous les triplets de parallèles (dues aux droites des milieux) : $(EF), (CH)$ et (AQ), $(FD), (BH)$ et (AP), et comme (PB) et (QC) se coupent en leur milieu, $PCBQ$ est un parallélogramme, donc $(PQ), (DE), (BC)$ sont parallèles.

(a) Soit X l'intersection de (EP) et (QD). $PQ = BC = 2ED$ et (PQ) et (ED) sont parallèles donc E et D sont milieu de $[PX]$ et $[QX]$ respectivement. Donc $(XB), (EF), (CH)$ sont parallèles, donc (XB) et (AB) sont perpendiculaires et de même (XC) et (AC). D'où $\widehat{XCA} = \widehat{XBA} = 90$ et A, B, C, X sont cocycliques.

(b) Soit Y le point d'intersection de (PD) avec (AH). (FD) et (AP) sont parallèles, donc par Thalès

$$\frac{AY}{YF} = \frac{FD}{AP} = 2$$

. De même Y' l'intersection de (EQ) et (AH) vérifie

$$\frac{AY'}{FY'} = 2$$

Donc $Y = Y'$ ce qui conclut.

Exercice 16 (Problème G3, Liste courte IMO 2017)
Soit ABC un triangle acutangle et O le centre de son cercle circonscrit. La droite (OA) coupe les hauteurs issues de B et C en P et Q respectivement. On note H l'orthocentre de ABC. Montrer que le centre du cercle circonscrit à PQH se trouve sur une médiane du triangle ABC.

Solution de l'exercice 16
On rappelle que H et O sont conjugués isogonaux. D'où

$$\widehat{PBC} = \widehat{HBC} = \widehat{HAC} = \widehat{OAB} = \widehat{PAB}$$

donc (BC) est tangente au cercle (ABP) en B et de même (BC) est tangent au cercle (AQC) en C. L'axe radical de ces deux cercles coupe donc $[BC]$ en son milieu, par le lemme. Donc cet axe radical est la médiane issue de A dans le triangle ABC. Il suffit donc que le centre (que l'on appelle G) du cercle (PQH) est sur l'axe radical des deux cercles. Or :

$$\widehat{CQG} = \widehat{HQG} = 90 - \widehat{HPQ} = 90 - (\widehat{PBA} + \widehat{PAB}) = \widehat{BAC} - \widehat{QAB} = \widehat{BAC} = \widehat{QAC}$$

Donc (GQ) est tangente au cercle (AQC) en Q et donc la puissance de G par rapport à ce cercle est GQ^2. Exactement de la même façon, on a (GP) tangent à (PBA) et donc la puissance de G par rapport à ce cercle est GP^2. Comme G est centre de QHP, $GP = GQ$, la puissance de G par rapport aux deux cercles est donc la même, G est donc sur l'axe radical des deux cercles, on a fini.

Exercice 17 (Problème G3, Liste courte IMO 2015)
Soit ABC un triangle rectangle en C et soit H le pied de la hauteur issue de C. Un point D est choisi à l'intérieur du triangle CBH de telle sorte que (CH) coupe (AD) en son milieu. Soit P le point d'intersection des droites (BD) et (CH). Soit ω le demi-cercle de diamètre $[DB]$ qui coupe $[BC]$. Une droite passant par P est tangente à ω en Q. Montrer que (CQ) et (AD) se coupent en ω.

Solution de l'exercice 17
Pour utilise le fait que (HC) coupe $[AD]$ en son milieu, il peut être intéressant d'introduire $J \neq A$ sur $[AB]$ tel que $AH = HJ$. (DJ) et (PH) son alors parallèles et les triangles PHB et DJB sont semblables.

$\widehat{DQB} = 90 = \widehat{ACB}$ car DB est un diamètre de ω. (PQ) est tangente à ω donc les triangles PDQ et PQB sont semblables. D'où

$$\frac{DQ^2}{BQ^2} = \frac{DQ}{BQ}\frac{DQ}{BQ} = \frac{PQ}{PB}\frac{PD}{PQ} = \frac{PD}{PB} = \frac{HJ}{HB} = \frac{AH}{HB} = \frac{AH}{CH}\frac{CH}{BH} = \frac{AC}{CB}\frac{AC}{CB} = \frac{AC^2}{BC^2}$$

donc $\frac{DQ}{BQ} = \frac{AC}{BC}$ et les triangles ACB et DQB sont semblables. Donc B est le centre de la similitude qui envoie Q sur C et D sur A. Si on note X le point d'intersection de (AD) et (CQ), cela signife que B appartient aux cercles (DQX) et (ACX) donc X appartient au cercle (DQB), ce que nous voulions.

Exercice 18 (Problème G4, Liste courte IMO 2006)
Soit ABC un triangle tel que $\widehat{C} < \widehat{A} < 90°$ et D un point de $[AC]$ tel que $BD = BA$. Les points de contact du cercle inscrit de ABC avec les côtés $[AB]$ et $[AC]$ sont notés respectivement K et L. Soit J le centre du cercle inscrit au triangle BCD. Montrer que la droite (KL) coupe le segment $[AJ]$ en son milieu.

Solution de l'exercice 18
La parallèle à (KL) passant par J coupe (AC) en X. On a alors $\widehat{JXA} = \widehat{KLA} = 90 - \frac{1}{2}\widehat{DAB} = \frac{1}{2}(180 - \widehat{DAB}) = \frac{1}{2}(180 - \widehat{BDA}) = \frac{1}{2}\widehat{BDC} = \widehat{CDJ}$ donc XJD est isocèle en J. On note N le projeté de J, qui est aussi le point de contact du cercle inscrit de BCD avec CD. On a alors par une chasse aux longueurs :

$$AX = AD+XD = AD+2DN = AD+2\frac{CD+CB-BD}{2} = AD+CD+CB-BD = AD+CB-AB = 2AL$$

donc L est milieu de (AX). Or (KL) et (AX) sont parallèles, donc (KL) coupe aussi (AJ) en son milieu.

Exercice 19 (Problème G3, Liste courte IMO 2006)
Soit $ABCDE$ un pentagone convexe tel que

$$\widehat{BAC} = \widehat{CAD} = \widehat{DAE}$$

et

$$\widehat{ABC} = \widehat{ACD} = \widehat{ADE}$$

Les diagonales (BD) et (CE) se coupent en P. Montrer que la droite (AP) coupe $[CD]$ en son milieu.

Solution de l'exercice 19
L'énoncé nous donne que les triangles ABC, ACD, ADe sont semblables. A est donc le centre de la similitude qui envoie B sur D et C sur E. Donc A appartient au cercle circonscrit à (PDE) et (BPC). On a donc

$$\widehat{CDP} = \widehat{CDA} - \widehat{PDA} = \widehat{DEA} - \widehat{PEA}$$

donc (CD) est tangent au cercle $(AEDP)$ en D et on a de même que (CD) est tangente en C au cercle circonscrit à $(APCB)$. On conclut alors par le lemme, appliqué aux deux cercles qui ont pour axe radical (AP).

Exercice 20 (Problème 1, EGMO 2013)
Le côté $[BC]$ d'un triangle ABC et prolongé au-delà du point C jusqu'au point D de façon que $CD = BC$. Le côté $[AC]$ est prolongé au-delà du point A jusqu'au point E de façon à ce que $AE = 2CA$. Montrer que si $AD = BE$, alors le triangle ABC est rectangle.

Solution de l'exercice 20
Dans le triangle EBD, (AC) est la médiane issue de E. $AE = \frac{2}{3}EC$ donc A est le centre de gravité de ce triangle. Donc (AD) coupe (EB) en son milieu, qu'on appelle S. Alors $SA = \frac{1}{3}DS = \frac{1}{2}AD = \frac{1}{2}EB$. Donc S est centre du cercle circonscrit de BAE, donc BAE est rectangle, et ainsi BAC aussi.

4 Transformations géométriques – $2^{\text{ème}}$ partie

Comme toujours en mathématiques, on souhaite dans tout problème de géométrie établir des relations entre des objets, qui n'apparaissent pas immédiatement dans la façon dont on les a construits ou introduits mais qui en découlent : les transformations géométriques fournissent de multiples façons de relier entre eux des éléments d'une figure, et d'en déduire déduire des propriétés utiles à la résolution.

– Similitudes directes et inversions –

Rappels

Définition 4.4.1.
Une similitude directe est une transformation du plan qui conserve les angles orientés.

Notation.
Pour deux figures $\mathcal{F}$ et $\mathcal{F}'$ *sembables* (c'est-à-dire l'une est l'image de l'autre par une similitude directe), on note souvent $\mathcal{F} \sim \mathcal{F}'$.

Remarque 4.4.2.
Deux figures sont directement semblables si l'on peut imaginer obtenir l'une à partir de l'autre « en la dilatant et en la déplaçant à plat sur le plan ». Pour deux segments quelconques, on se convainc facilement qu'ils sont toujours directement similaires. Réciproquement, une similitude est entièrement déterminée par l'image de deux points distincts.

Pour deux figures similaires $\mathcal{F}$ et $\mathcal{F}'$, on détermine alors le *centre de similitude O* comme (si la similitude n'est pas une translation) l'unique point du plan tel qu'il existe :

— Une homothétie h de centre O et de rapport $k > 0$

— Une rotation r de centre O

telles que $\mathcal{F}' = r \circ h(\mathcal{F})$.

C'est alors l'unique point fixe de la similitude $s = r \circ h$.

Inversions

Il s'agit d'une nouvelle catégorie de transformations du plan, qui ne conservent plus tout à fait les angles, les points alignés ou les rapports de longueurs, et ne sont pas à proprement parler bijectives. Néanmoins, elles ont des applications intéressantes et conservent en particulier la concourance et l'orthogonalité.

Définition 4.4.3.
Soit Γ un cercle de centre O et de rayon r. Pour un point $P \neq O$, son image par k l'*inversion par rapport à* Γ est un point P' tel que :

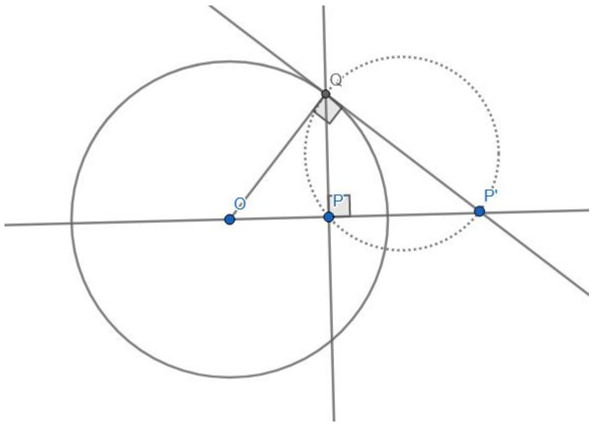
— P' appartient à la demi-droite $[OP)$

— $OP \times OP' = r^2$

On dit que « O est envoyé à l'infini » car c'est un comportement limite : quand P s'approche de O, P' s'en éloigne vers l'infini. Rigoureusement, k est une involution du plan $\mathcal{P}$ privé de O.

Voici une construction pratique : si P est à l'intérieur de Γ, soit Q une intersection de Γ avec la perpendiculaire à (OP) passant par P, et T la tangente à Γ en Q. Alors $P' = T \cap (OP)$.

Si P est à l'extérieur de Γ, on « remonte la construction » : on détermine Q le point de tangence de Γ avec sa tangente passant par P, puis on prend P' le projeté orthogonal de Q sur (OP).



On a les propriétés suivantes :

— Si $P \in \Gamma$, alors $k(P) = P$.

— Si A et B sont deux points distincts de O, d'images A' et B' par k, alors A, B, A', B' sont cocycliques (ce que l'on peut prouver en considérant la puissance de O par rapport au cercle circonscrit à ABA').

— Si D est une droite passant par O, $k(D) = D$.

— Si D est une droite ne passant pas par O, $k(D)$ est un cercle passant par O.

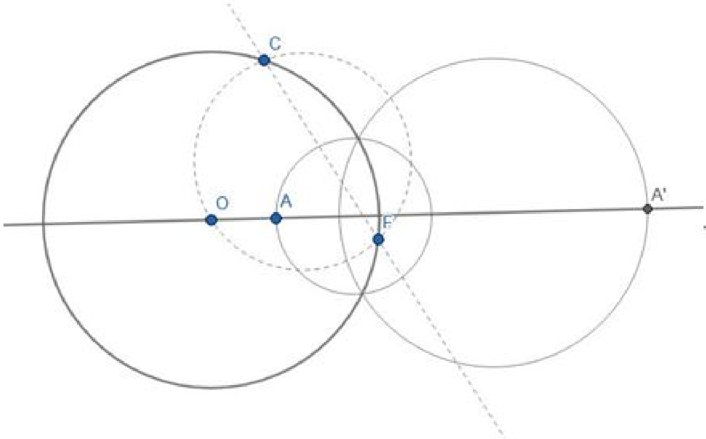
— Si $\mathcal{C}$ est un cercle passant par O, $k(\mathcal{C})$ est une droite ne passant pas par O.

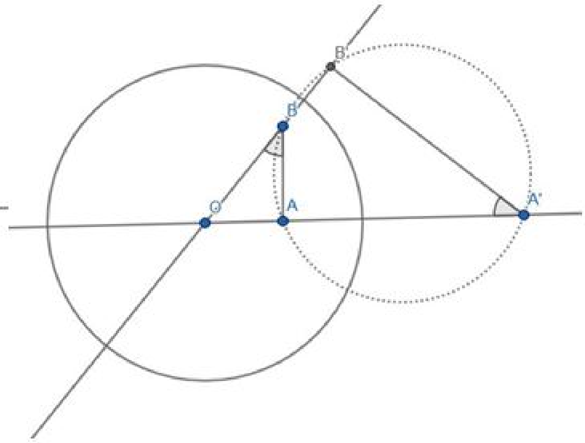
— $\mathcal{C}$ est un cercle ne passant pas par O, $k(\mathcal{C})$ est un cercle ne passant pas par O.

— Si $\mathcal{D}$ désigne le disque ouvert délimité par Γ, alors $k(\mathcal{D} \setminus \{O\}) = \mathcal{P} \setminus \mathcal{D}$

— La transformation k préserve l'orthogonalité : deux courbes quelconques se coupent orthogonalement lorsque leurs tangentes au point d'intersection sont orthogonales.

— De la même façon, un faisceau de droites parallèles est envoyé sur un faisceau de cercles tangents.





Enfin, si deux courbes $\mathcal{C}$ et $\mathcal{C}'$ s'intersectent en P, leurs images par k s'intersectent en $P' = k(P)$. On utilisera cette propriété prochainement.

– Point de Miquel –

Définition dans le cas général

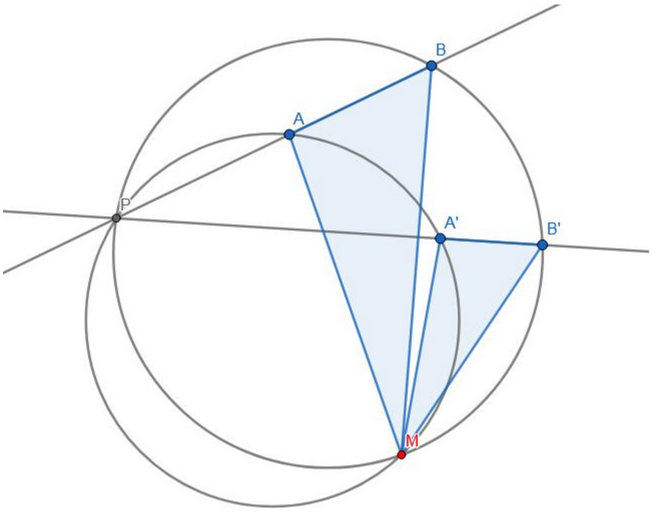
Définition 4.4.4.
Pour quatre points distincts A, B, A' et B', le *point de Miquel* du quadrilatère $ABB'A'$ est le centre M de la similitude s telle que $A' = s(A)$ et $B' = s(B)$ (défini lorsque $ABB'A'$ n'est pas un parallélogramme).

Pour le déterminer pratiquement, on a la construction suivante que l'on prouve grâce à une chasse aux angles.

Proposition 4.4.5.
Soit P le point d'intersection de (AB) et $(A'B')$; dans le cas particulier où les droites sont parallèles, alors la similitude est une homothétie, on peut considérer qu'elles intersectent à l'infini.

Alors M est le deuxième point d'intersection des cercles circoncrits à PAA' et PBB' ; si (AB) est parallèle à $(A'B')$, alors ces cercles sont dégénérés, car ce sont les droites (AA') et (BB').

Le point ainsi construit est aussi le centre de la similitude s' qui envoie A sur B et A' sur B'. On peut ainsi compléter la figure avec $Q = (AA') \cap (BB')$, avec même cas particulier que ci-dessus, et on obtient que Q ,M, A, B d'une part et Q, M, A', B' d'autre part sont aussi cocyliques.



Une figure complète est disponible en annexe de ce cours.

Point de Miquel du quadrilatère cyclique

Dans un quadrilatère cyclique, on a de nouvelles caractérisations du point de Miquel.

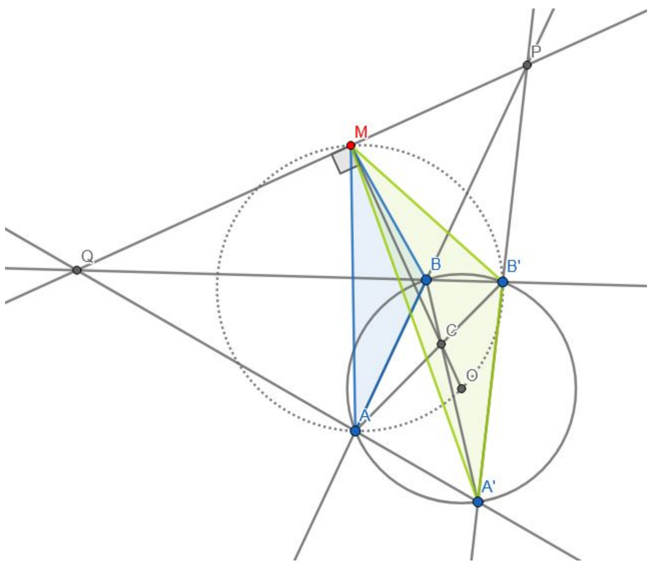
Proposition 4.4.6.
Soit $ABA'B'$ un quadrilatère (non rectangulaire) inscrit dans un cercle Γ de centre O, on introduit $P = (AB) \cap (A'B')$, $Q = (AA') \cap (BB')$, $C = (AB') \cap (A'B)$. Alors le point de Miquel M du quadrilatère est aussi :

— le projeté orthogonal de C sur (PQ) ;

— le projeté orthogonal de O sur (PQ) ;

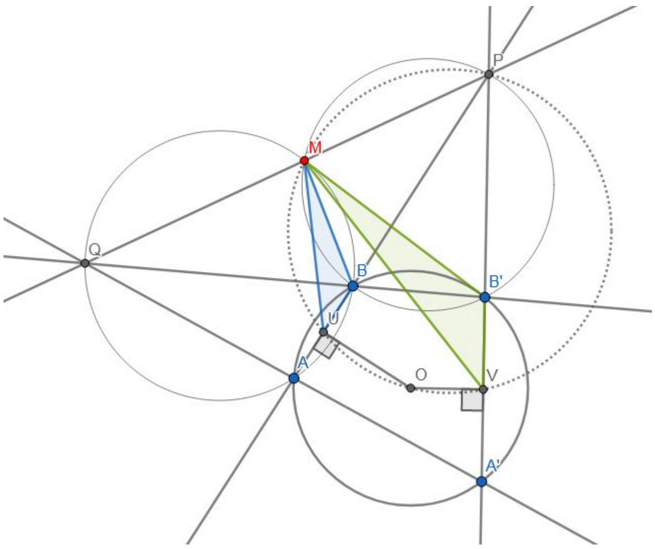
— $(OC) \cap (PQ)$.

En particulier, les points M, O, A, B' d'une part et M, O, A', B d'autre part sont cocycliques.



Démonstration. Les cercles circonscrits à QAB, PBB', $AA'B'$ sont concourants en B, où $A \in (QA')$ et $B' \in (A'P)$. Ainsi, par le théorème de Miquel, M le deuxième point d'intersection des cercles circonscrits à QAB et PBB' appartient à (PQ). Puis avec U et V les milieux de $[AB]$ et $[A'B']$, on a $s([UB]) = [VB']$ donc M est aussi point de Miquel de $UVBB'$ et M, P, U, V sont cocycliques. Comme U, P, O, V le sont aussi, les deux cercles sont les mêmes et $\widehat{OMP} = \widehat{OUP} = 90°$.

Puis C est l'inverse de M par rapport à Γ, donc $C \in (OM)$ □



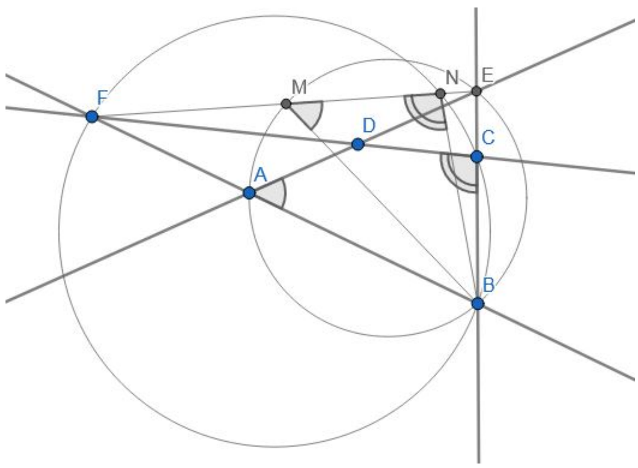
De même, une figure complète est disponible en annexe de ce cours.

Exercice 1 (De l'utilité du point de Miquel)
Soit $ABCD$ un quadrilatère convexe, $E = (AB) \cap (CD)$ et $F = (AB) \cap (CD)$. Montrer que : A, B, C, D cocycliques $\Leftrightarrow$ $EA.ED + FA.FB = EF^2$.

Solution de l'exercice 1
Soit M le second point d'intersection du cercle circonscrit à ABE (Γ_1) avec (EF) et N celui du cercle circonscrit à BCF (Γ_2) avec (EF). Par la puissance de E par rapport à Γ_1 : $EA \cdot EA = EM \cdot EF$. De même la puissance de F par rapport à Γ_2 donne $FA \cdot FB = EF \cdot NF$.

Ainsi, on s'intéresse au cas où $EM + NF = EF$, ie $M = N$. Si cela se produit, alors M est le point de Miquel de $ABCD$, et comme il appartient à (EF), on reconnaît la configuration où $ABCD$ sont cocycliques, la réciproche s'obtient de la même façon. On peut le vérifier par une simple chasse aux angles :

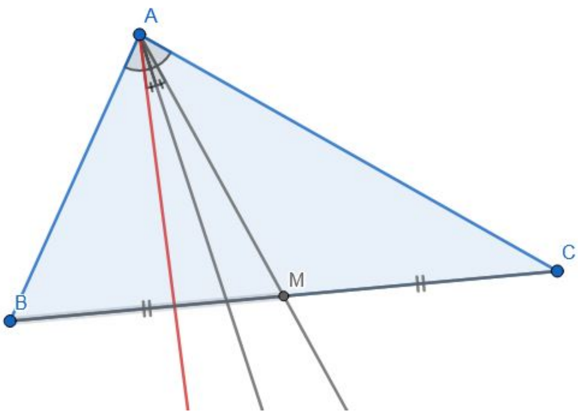
$$\widehat{DCB} + \widehat{DAB} = \widehat{FCB} + \widehat{EAB} = \widehat{FNB} + \widehat{EMB}.$$



– Symédiane –

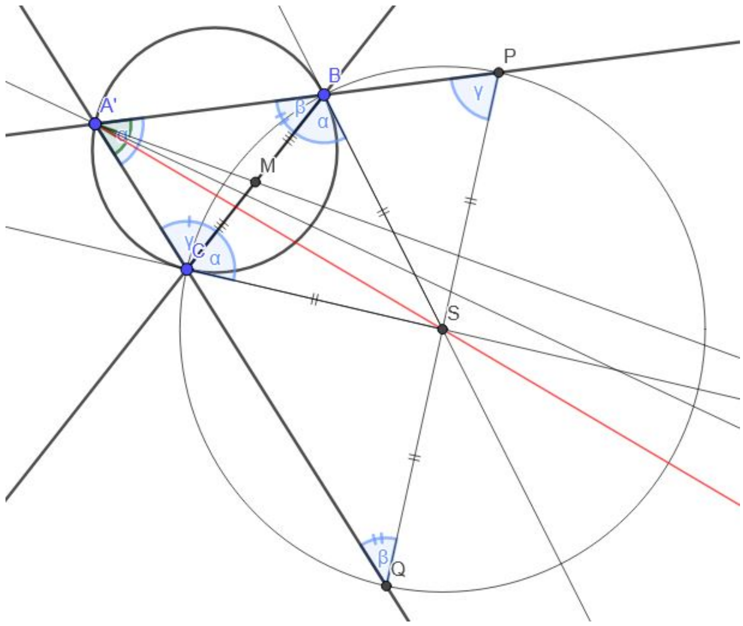
Définition et propriétés

Définition 4.4.7.
Dans le triangle ABC, inscrit dans le cercle Γ, la *symédiane issue de A* dans ABC est définie comme la droite symétrique de la médiane issue de A par rapport à la bissectrice de $\widehat{BAC}$.



On a la première propriété utile se la symédiane :

Proposition 4.4.8.
Soit S l'intersection des tangentes à Γ en B et C. Alors S appartient à la symédiane issue de A.

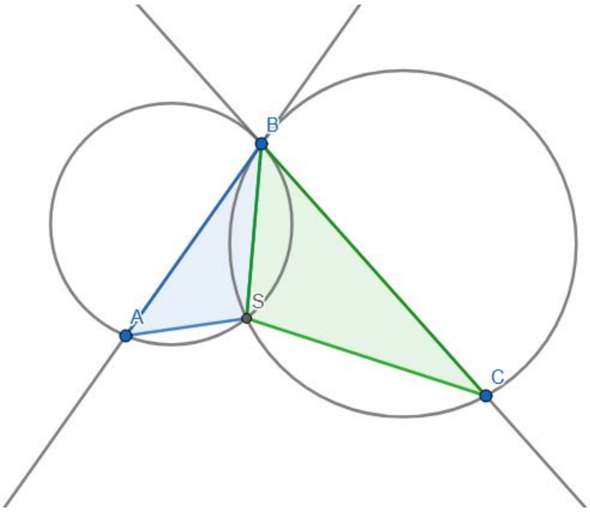


Démonstration. On considère le cercle de centre S et de rayon BS, qui recoupe (AB) et (AC) respectivement en P et en Q. Par chasse aux angles, on obtient que $\widehat{APS} = \widehat{ACB}$ et $\widehat{AQS} = \widehat{ABC}$. Ainsi, les triangles ABC et AQP sont semblables, et $S \in (PQ)$. La similitude indirecte s qui envoie l'un sur l'autre a pour centre A. s envoie alors M le milieu de $[BC]$ sur S le milieu de $[PQ]$ (centre du cercle de diamètre $[PQ]$). Par conservation des angles : $\widehat{SAB} = \widehat{SAP} = \widehat{MAC}$, donc (AS) est bien la symédiane issue de A dans ABC. $\square$

Retour du centre de similitude

On a vu comment définir le centre de similiude envoyant un segment sur un autre lorsque les quatre points sont distincts. Qu'en est-il d'une similitude qui enverrait A sur B et B sur C où A, B et C sont trois points non alignés ?

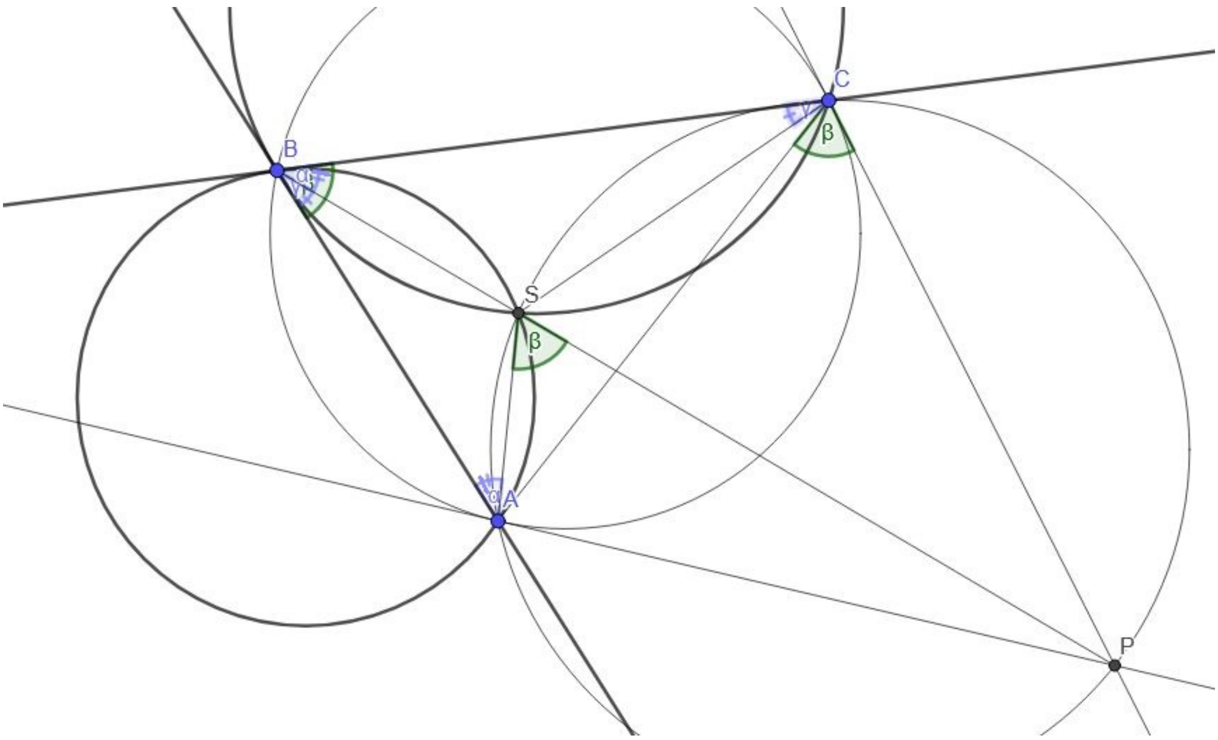
Proposition 4.4.9.
Soit S la similitude qui envoie A sur B et B sur C. Le centre de similitude S est alors la seconde intersection du cercle passant par A et B et tangent à (BC), et du cercle passant par B et C et tangent à (AB). ($\widehat{ASB} = \widehat{BSC}$ par chasse aux angles)



On obtient alors un point de la symédiane issue de B dans ABC.

Démonstration. On introduit les deux tangentes au cercle circoncrit à ABC en A et C, donc l'intersection P est sur la symédiane issue de B. On montre que B, S et P sont alignés.
Si $\alpha = \widehat{SAB}$, $\beta = \widehat{ABC}$ et $\gamma = \widehat{SBC}$, alors par similitude des triangles SAB et SBC, $\beta = \alpha + \gamma$. En outre, $\widehat{ASB} = \widehat{SAB} + \widehat{ABS} + \widehat{SBC} + \widehat{BCS} = 2\beta = 180 - \widehat{APC}$. Donc A, C, S, P sont cocycliques.

Alors par chasse aux angles : $\beta = \widehat{ACP} = \widehat{ASP} = 180 - \widehat{ASB}$. □



Exercices

Exercice 2
Soit ABC un triangle acutangle, M, N, P les milieux repectifs de $[BC]$, $[CA]$ et $[AB]$. Les médiatrices de $[AB]$ et $[AC]$ coupent (AM) en D et E respectivement. Soit $F = (BD) \cap (CE)$. Montrer que A, N, F, P sont cocycliques.

Exercice 3 (utilisant la formule de la symédiane)
Soit A, B, C trois points alignés dans cet ordre, et Γ un cercle passant par A et C. Les deux tangentes à Γ en A et C s'intersectent en T, et la droite (TB) coupe Γ en S. Enfin, soit X l'intersection de (AC) avec la bissectrice de $\widehat{CSA}$. Montrer que X est fixe lorsque Γ varie.

Exercice 4 (sur les similitudes)
Soit Γ_1 et Γ_2 deux cercles d'intersections A et D. La tangente à Γ_1 en A recoupe Γ_2 en B et la tangente à Γ_2 en A recoupe Γ_1 en C. Soit E sur $[AB)$ tel que $BE = AB$ et F la seconde intersection de (AC) avec le cercle circonscrit à ADE. Montrer que $AC = AF$.

Solutions des exercices

Solution de l'exercice 2
Soit S le centre de la similitude σ qui envoie B sur A et A sur C. On sait que S appartient à la symédiane issue de A dans ABC. Alors $\widehat{FBA} = \widehat{DBA} = \widehat{DAB} = \widehat{BAM}$ et, de même, $\widehat{ACF} = \widehat{ACS}$.

Donc $F = S$. Ainsi, la similitude de centre F σ envoie aussi P sur N (le milieu de $[BA]$ est envoyé sur le milieu $[AC]$), et par construction du point de Miquel de $[AP]$ et $[CN]$, comme $(AP) \cap (CN) = A$, on obtient que A, N, P, F sont cocycliques.

Solution de l'exercice 3
On établit d'abord le lemme suivant.

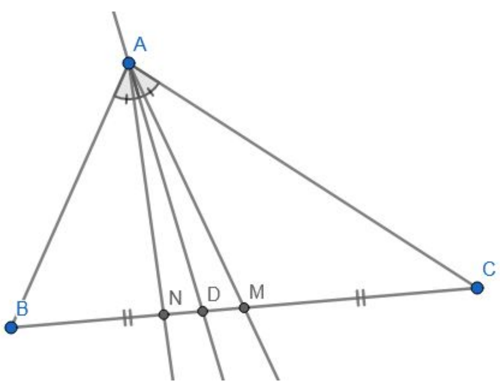
Lemme 4.4.10.
Dans un triangle ABC, soit M le milieu de $[BC]$ et N le pied de la symédiane issue de A. On a alors :

$$\frac{NB}{NC} = \left(\frac{AB}{AC}\right)^2.$$

Démonstration. D'après la loi des sinus :

$$\begin{aligned}\frac{NB}{NC} &= \frac{AB\frac{\sin\widehat{NAB}}{\sin\widehat{ANB}}}{AB\frac{\sin\widehat{NAC}}{\sin\widehat{ANC}}}\\ &= \frac{AB\sin\widehat{CAM}}{AB\sin\widehat{BAM}}\\ &= \frac{AB\frac{CM}{AC}\sin\widehat{AMC}}{AB\frac{BM}{AB}\sin\widehat{AMB}}\\ &= \left(\frac{AB}{AC}\right)^2.\end{aligned}$$

□



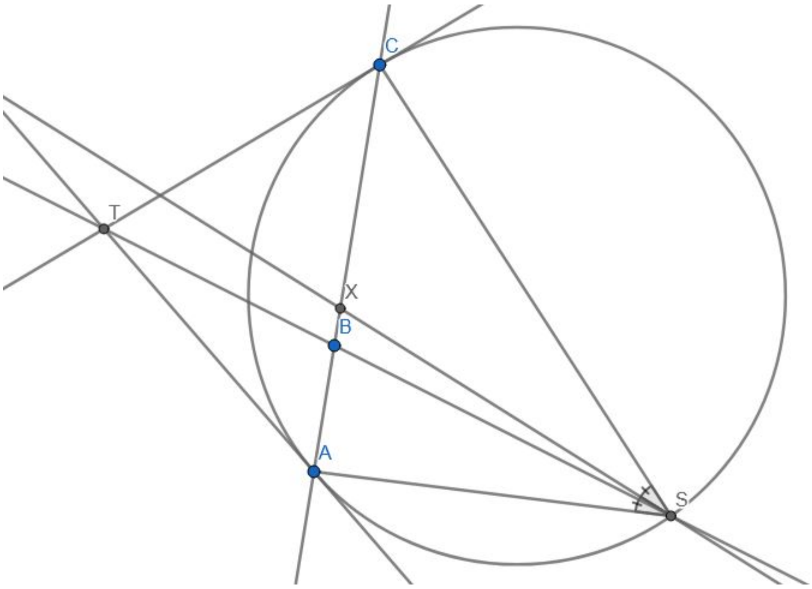
La formule de la bissectrice, qui s'obtient de façon un peu similaire, donne ensuite dans ACS :

$$\frac{AX}{CX} = \frac{AS}{CS}.$$

Puis la formule de la symédiane, en usant du fait que (SB) est la symédiane issue de S dans ASC, donne :

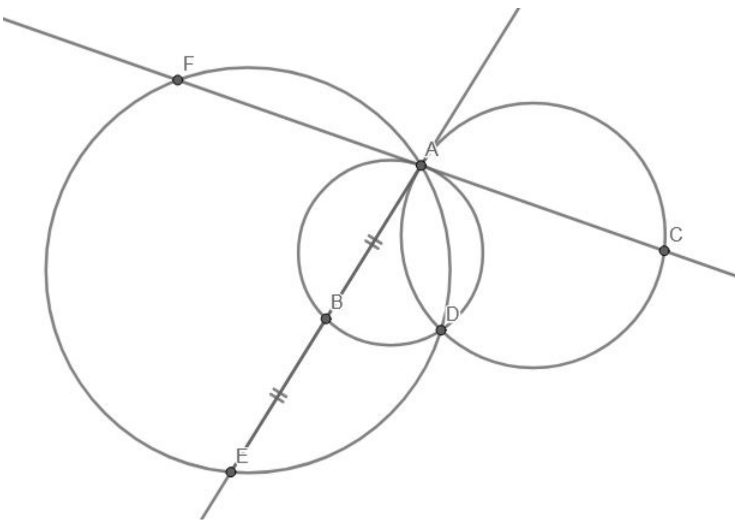
$$\frac{AB}{BC} = \left(\frac{AS}{CS}\right)^2.$$

Le rapport $\frac{AS}{CS}$ est donc fixé par les positions de A, B, C et le rapport $\frac{AX}{CX}$ l'est donc aussi en conséquence, et ne dépend pas de Γ.



Solution de l'exercice 4

Soit X le symétrique de C par rapport à A. La similitude de centre D qui envoie A sur C et B sur A envoie aussi E sur X. Donc D est le point de Miquel de $AEXC$ et comme $(XC) \cap (AE) = A$, en particulier, X, A, D, E sont cocycliques. D'où $X = F$.



– Autour des points remarquables du triangle –

Dans un triangle ABC de cercle circonscrit Γ, on nomme H_A, H_B, H_C les pieds des hauteurs issues respectivement de A, B et C ; de même on appelle A', B', C' les milieux des côtés $[BC]$, $[AC]$ et $[AB]$.

On note aussi assez conventionnellement H l'orthocentre, O le centre du cercle circonscrit et G le centre de gravité du triangle ABC. On a alors de nombreuses propriétés sur ces « points remarquables ».

Similitudes internes et symétries

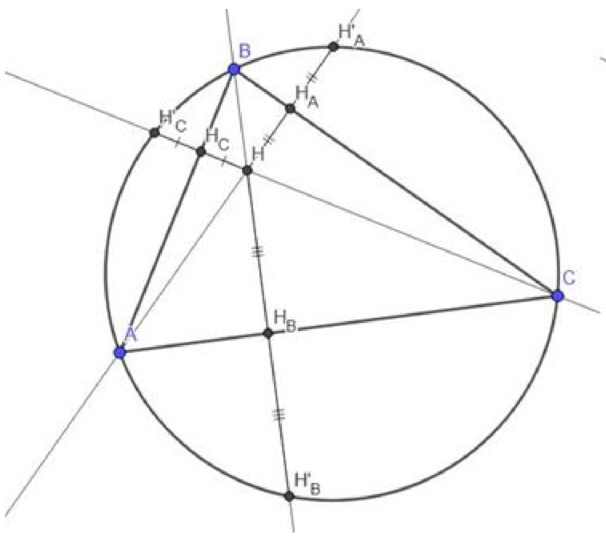
Définition 4.4.11.
Le triangle $H_AH_BH_C$ est appelé *triangle orthique* de ABC, et le triangle $A'B'C'$ est dit *triangle des milieux*.

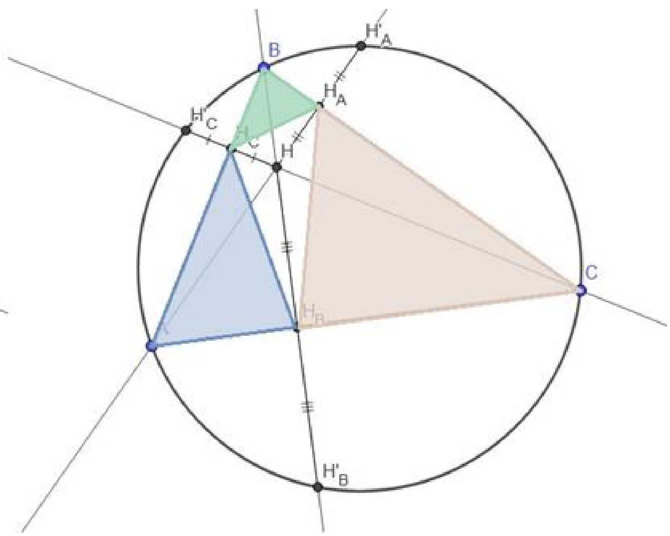
On remarque plusieurs faits utiles autour de l'orthocentre (preuve par chasse aux angles) :

— Les *symétriques de H* par rapport aux côtés (AB), (BC), (AC) sont sur le *cercle circonscrit à* ABC.

— Les triangles AH_BH_C, H_ABH_C, H_AH_BC et ABC sont *semblables*.

— Les hauteurs de ABC sont les *bissectrices* de son triangle hortique.





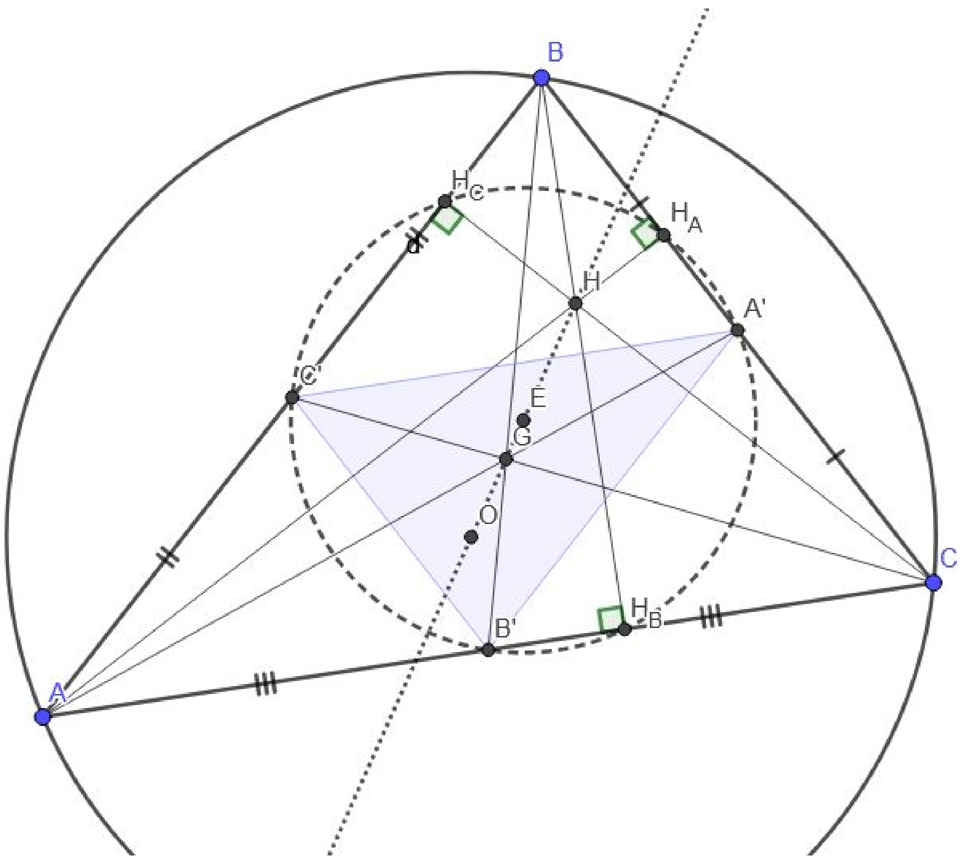
De manière plus directe encore que $A'B'C'$, $AC'B'$, $C'BA'$, $B'A'C$ et ABC sont semblables et les quatre premiers sont même isométriques (mêmes angles et mêmes longueurs).

Droite et cercle d'Euler

Proposition 4.4.12.
Les points O, G et H sont alignés dans cet ordre sur une droite appelée *droite d'Euler du triangle* ABC. De plus, on a la relation sur les distances : $GH = 20G$.

Démonstration. O est l'orthocentre de $A'B'C'$, et G est le centre de gravité commun de ABC et $A'B'C'$. C'est donc le point fixe de la similitude qui envoie un triangle sur l'autre. Or c'est aussi le point de concourance de (AA'), (BB') et CC', cette similitude est donc une homothétie et le rapport des longueurs est de $-\frac{1}{2}$. □

Remarque 4.4.13.
On obtient aussi que $AG = 2GA'$, de même $BG = 2GB'$ et $CG = 2GC'$.



Proposition 4.4.14.
Le triangle orthique et le triangle des milieux ont même cercle circonscrit, appelé *cercle d'Euler du triangle ABC*.

Le centre de ce cercle, noté E, est situé sur la droite d'Euler ; c'est en fait le milieu de $[OH]$.

Démonstration. $A'B'C'$ est le symétrique de $A'BC'$ par rapport au milieu de $[A'C']$. Le cercle circoncrit à $A'B'C'$ est donc aussi le symétrique du cercle circoncrit à $BC'A'$ par rapport à $(A'C')$ (car $[A'C']$ est une corde du cercle). Ainsi, l'image de B par cette symétrie, qui est H_B, appartient au cercle cironcrit à $A'B'C'$. On raisonne de même sur le pied des autres hauteurs.

Puis une homothétie de centre H et de rapport 2 envoie le cercle circonscrit à $H_AH_BH_C$ (c'est-à-dire le cercle d'Euler) sur Γ (auquel appartiennent les symétriques de l'orthocentre par rapport aux côtés). En particulier, E est l'image de O par une homothétie de centre H et de rapport $\frac{1}{2}$. □

Remarque 4.4.15.
On obtient également que le cercle d'Euler passe aussi par les milieux de $[AH]$, $[BH]$, $[CH]$.

Point et droite de Simpson et Steiner

Théorème 4.4.16.
Soit P un point quelconque du plan. On a les deux théorèmes suivants :

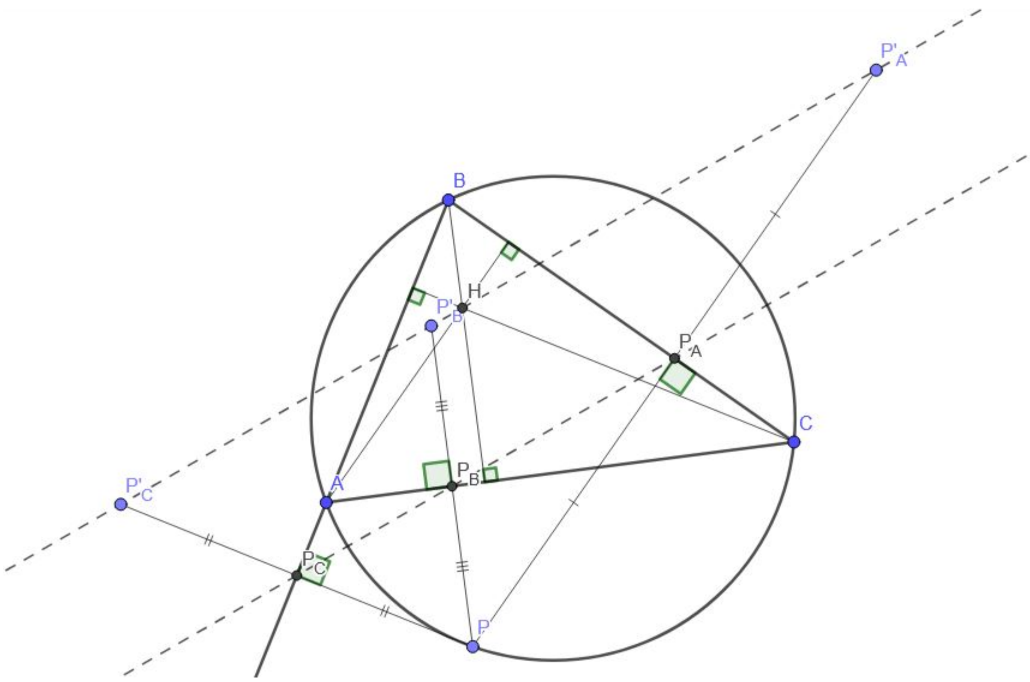
— Les projetés orthogonaux de P sur les côtés du triangle sont alignés si et seulement si $P \in \Gamma$. On appelle alors *droite de Simpson du point* P cette droite.

— Les symétriques de P par rapport aux côtés du triangle sont alignés si et seulement si $P \in \Gamma$. On appelle alors *droite de Steiner du point* P cette droite.

— Si $P \in \Gamma$, alors la droite de Steiner de P passe par H.

— Réciproquement, si D est une droite passant par H, les symétriques de D par rapport aux côtés de ABC sont concourantes en un point $P \in \Gamma$, appelé *point de Steiner* de la droite D. Il y a donc une correspondance bijective entre les points de Γ et les droites passant par H.

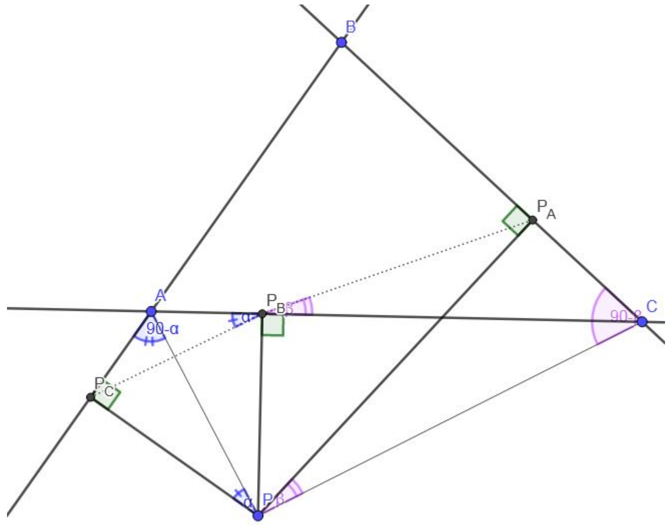
— Si $P \in \Gamma$, la droite de Steiner est parallèle à la droite de Simpson : en fait, c'est son image par une homothétie de centre P et de facteur 2.



Démonstration. On nomme P_A, P_B, P_C les projetés orthogonaux de P sur (BC), (AC), (AB), $\alpha = \widehat{P_CP_BA}$, $\beta = \widehat{CP_BP_A}$ On raisonne alors par équivalences en utilisant les cocyclicités données par les angles droits ; il faudrait faire une preuve rigoureuse avec des angles orientés, mais le principe est le suivant :

$$\begin{aligned}P_A, P_B, P_C \text{ alignés} &\Leftrightarrow \alpha = \beta \Leftrightarrow \widehat{P_CPA} = \widehat{CPP_A}\\ &\Leftrightarrow \widehat{P_CAP} = \widehat{P_ACP} \Leftrightarrow \widehat{P_CAP} = \widehat{BCP}\\ &\Leftrightarrow A, B, C, P \text{ cocycliques}\end{aligned}$$

D'où le théorème de Simpson.



Le théorème de Steiner s'en déduit alors par une homothétie de rapport 2 de centre P. Alors avec H_A le symétrique de H par rapport à (BC), on a B, C, H_A, P cocycliques, donc par la symétrie par rapport) (BC) : B, C, H, P'_A sont cocycliques. De même, B, A, H, P'_C d'une part et A, C, H, P'_B d'autre part sont cocycliques. Alors (sur notre figure) : $\widehat{BHP'_A} = \widehat{BCP'_A} = \widehat{BCP} = 180 - \widehat{PAB} = 180 - \widehat{P'_CAB} = 180 - \widehat{P'_CHB}$. Ainsi, $\widehat{P'_CHP'_B} = \widehat{P'_CHB} + \widehat{BHP'_A} = 180°$.

Par conséquent, P'_C, P'_B et H sont alignés, ce qui suffit à conclure que la droite de Steiner passe par H.

Enfin, si une droite D passe par H, on note P' son second point d'intersection avec le cercle circonscrit à BCH (symétrique de Γ par rapport à (BC)). Alors le symétrique de D par rapport à (BC) recoupe Γ en P le symétrique de P', qui est sur Γ. On sait que $D = P'H$ est alors la droite de Steiner de P, dont les symétriques par rapport aux côtés de ABC sont donc bien concourants en P. □

Exercice

Exercice 5 (Problème d'EGMO utilisant la droite d'Euler et le point de Steiner)
Soit ABC un triangle acutangle non isocèle, dont on note G le centre de gravité et O le centre du cercle circonscrit. On appelle O_1, O_2, O_3 les symétriques de O par rapport à (BC), (AC) et (AB) respectivement, on définit de même G_1, G_2, G_3.

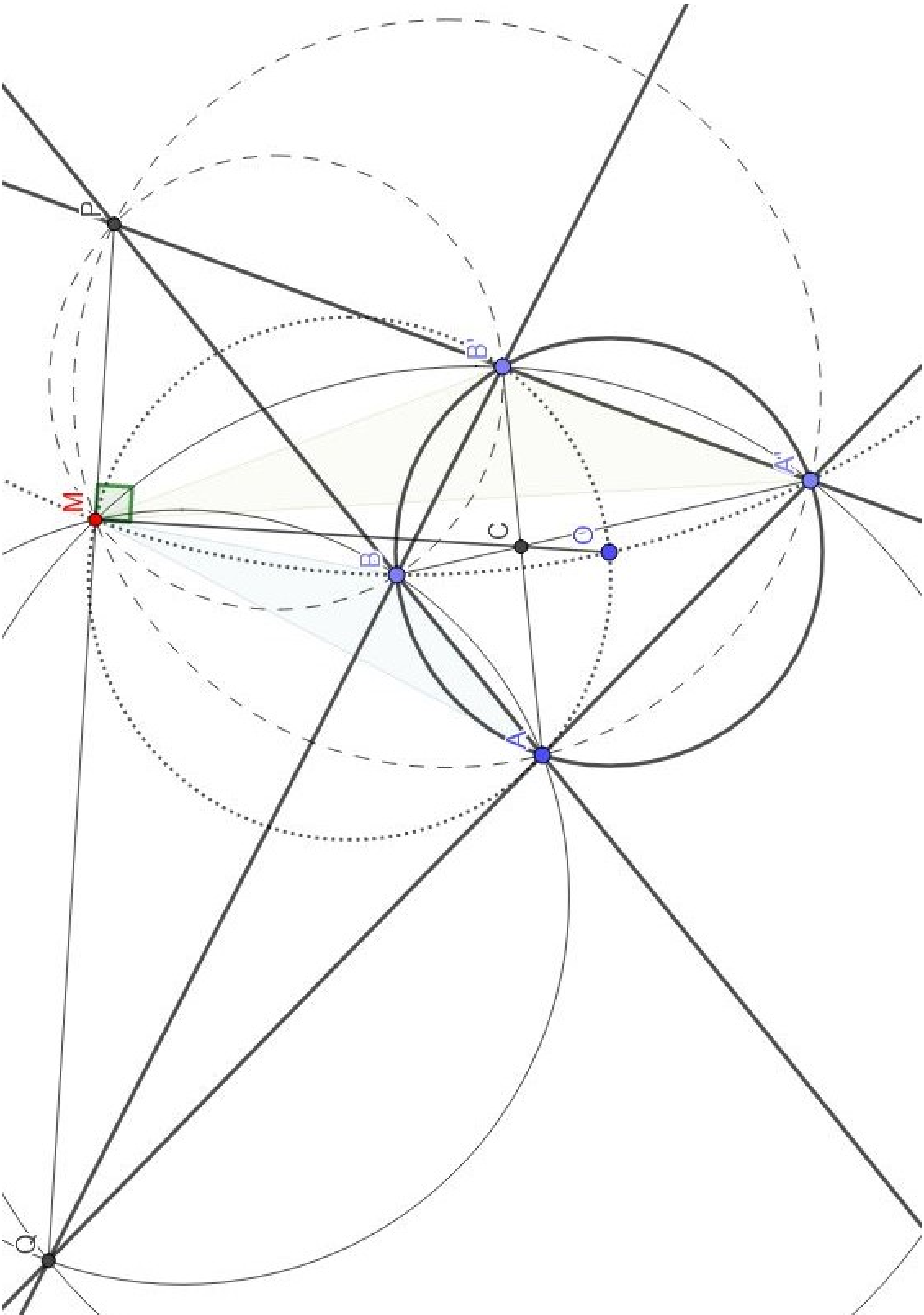
Montrer que les cercles circonscrits à G_1G_2C, G_1G_3B, G_2G_3A, O_1O_3B, O_2O_3A et ABC sont concourants.

Solution de l'exercice 5
On va plutôt trouver un point du cercle circonscrit à ABC et montrer qu'il appartient à chacun des cercles circonscrits auxquels on s'intéresse.

Ainsi, soit S le point de Steiner de la droite d'Euler dans ABC, qui passe bien par l'orthocentre. Montrons par exemple que S, C, G_1, G_2 sont cocycliques ; il s'agit du même raisonnement pour chacun des cercles. Il faudrait en toute rigueur utiliser des angles de droites, mais on peut se convaincre du résultat par une chasse aux angles comme suit, sur notre figure. On a par les symétries :

$$\widehat{SG_1C} + \widehat{CG_2S} = \widehat{O_1G_1C} + \widehat{CG_1X} = \widehat{OGC} + \widehat{CGX} = 180°.$$

– Annexe : point de Miquel du quadrilatère cocyclique –


P
B'
A'
M
C
O
B
A
Q

5 Exercices d'entraînement

1 Entraînement de mi-parcours

– Énoncés –

Exercice 1
On se donne un polynôme P à coefficients entiers tel que $P(0) \neq 0$ et $P(P(0)) = 0$. On note m le nombre de racines entières de P.

Trouver toutes les valeurs possibles de m.

Exercice 2
Déterminer toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$, telles que

$$f\big(xf(y)\big) + f\big(f(x) + f(y)\big) = yf(x) + f\big(x + f(y)\big)$$

pour tous $x, y \in \mathbb{R}$.

Exercice 3
Soit $n \geqslant 2$ un nombre entier. Alice et Bob jouent à un jeu concernant un pays constitué de n îles. Deux de ces n îles exactement possèdent une usine. Initialement il n'y a aucun pont dans le pays. Alice et Bob jouent chacun à leur tour de la manière suivante. À chaque tour, celui qui joue doit construire un pont entre deux îles différentes I_1 et I_2 telles que :

— I_1 et I_2 ne sont pas déjà reliées par un pont,

— au moins une des deux îles I_1 et I_2 possède une usine ou est reliée à une usine par une suite de ponts (en effet, un accès à une usine est nécessaire pour la construction).

Dès qu'un joueur construit un pont qui rend possible le passage d'une usine à l'autre, ce joueur perd le jeu (cela déclenche une guerre industrielle entre les deux usines). Si Alice est la première à jouer, déterminer pour quels $n \geqslant 2$ elle a une stratégie gagnante.

Exercice 4
On note $\mathbb{N}^*$ l'ensemble des entiers strictement positifs. Déterminer toutes les fonctions f de $\mathbb{N}^*$ dans $\mathbb{N}^*$ telles que, pour tous $m, n \in \mathbb{N}^*$, on ait

$$n + f(m) \mid f(n) + nf(m).$$

– Solutions –

Solution de l'exercice 1
Notons que $P(0)$ est une racine de P, donc $m \geqslant 1$. De plus, supposons que m ait au moins 4 racines distinctes. On peut supposer que $P(0)$ est l'une d'elles, et noter a_1, a_2 et a_3 les trois autres. On peut alors factoriser P et écrire

$$P = (X - a_1)(X - a_2)(X - a_3)(X - P(0))Q,$$

où Q est à coefficients entiers. En prenant $X = 0$, on obtient

$$P(0) = a_1 a_2 a_3 P(0) Q(0).$$

Comme $P(0) \neq 0$, on a $a_1 a_2 a_3 = 1$. Les nombres a_1, a_2 et a_3 divisent donc 1, donc valent ± 1, donc deux d'entre eux sont égaux, ce qui est absurde. On a donc $m \leqslant 3$.

Enfin, les valeurs $m = 1$, $m = 2$ et $m = 3$ peuvent toutes trois être atteintes, comme le montrent les exemples suivants :

$$P(X) = 1 - X,\ P(X) = (X-1)(X-2) \text{ et } P(X) = (X^2-1)(X-2).$$

Solution de l'exercice 2

On cherche à montrer que f est injective. On se donne donc y_1 et y_2 tels que $f(y_1) = f(y_2)$ et on teste (x, y_1) et (x, y_2) dans l'équation de départ. Le membre de gauche est le même pour (x, y_1) et pour (x, y_2), donc le membre de droite aussi, donc

$$y_1 f(x) = y_2 f(x).$$

On vérifie que la fonction nulle est bien solution du problème. D'autre part, si f n'est pas la fonction nulle, il existe x_0 tel que $f(x_0) \neq 0$, donc $y_1 = y_2$. Par conséquent, si f n'est pas la fonction nulle, alors elle est injective.

En prenant $x = 0$ et $y = 1$ dans l'équation de départ, on obtient

$$f(0) + f(f(0) + f(1)) = f(0) + f(f(1)),$$

donc $f(f(0) + f(1)) = f(f(1))$. Par injectivité, on en déduit $f(0) + f(1) = f(1)$, donc $f(0) = 0$. En prenant $y = 0$ dans l'équation de départ, on obtient

$$f(f(x)) = f(x)$$

donc, par injectivité, on a $f(x) = x$. Réciproquement, on vérifie facilement que l'identité est bien solution du problème. Les deux seules solutions sont donc la fonction nulle et l'identité.

Solution de l'exercice 3

Analyse générale On peut traiter des petits cas pour commencer. Un joueur est obligé de perdre quand plus personne ne peut mettre de pont sans relier les deux usines, donc si il perd si :

- la première usine est reliée à k îles et les $\binom{k}{2}$ ponts constructibles entre ces k îles ont été construits,
- la deuxième usine est reliée aux $n-k$ îles restantes et les $\binom{n-k}{2}$ ponts constructibles entre ces $n-k$ îles ont été construits.

On a donc dans tous les cas construit $T = \frac{k(k+1)}{2} + \frac{(n-k)(n-k+1)}{2}$ ponts, donc il s'est écoulé T tours, et le joueur qui doit jouer à ce moment a perdu. Nous devons maintenant chercher la parité de T.

Etude au cas par cas

— Si $n \equiv 1 \pmod{4}$ et si $k \equiv 0, 1 \pmod{4}$ alors $n - k \equiv 1, 0 \pmod{4}$; de même si $k \equiv 2, 3 \pmod{4}$ alors $n - k \equiv 3, 2 \pmod{4}$.
On en déduit après une rapide analyse que $\frac{k(k-1)}{2}$ et $\frac{(n-k)(n-k-1)}{2}$ ont la même parité, donc T est pair, et c'est Alice qui fait face à la configuration qui lui sera fatale.

— Si $n \equiv 3 \pmod{4}$ et si $k \equiv 0, 1 \pmod{4}$ alors $n - k \equiv 3, 2 \pmod{4}$; de même si $k \equiv 2, 3 \pmod{4}$ alors $n - k \equiv 1, 0 \pmod{4}$.
Il en résulte que $\frac{k(k-1)}{2}$ et $\frac{(n-k)(n-k+-)}{2}$ sont de parité différente, donc T est impair, et c'est Bob qui pleurera de désespoir devant son cuisant échec...

— Si n est pair, la parité de T dépend de k. On va donc avoir besoin d'utiliser un autre argument. Bob peut toujours jouer le symétrique d'Alice, puisqu'il y a un nombre pair d'îles. Plus précisément, on numérote les îles de 1 à n. Quand Alice joue un pont entre l'île i et l'île j, Bob joue le pont entre l'île $2n+1-i$ et l'île $2n+1-j$. Dans ce cas, si Alice peut jouer à son i-ème tour, alors Bob peut aussi jouer à son i-ème tour. Il en résulte qu'Alice sera la perdante.

Conclusion Donc Alice ne gagne que si $n \equiv 3$ [4], et Bob gagne dans tous les autres cas.

Solution de l'exercice 4
Si f est solution du problème, alors pour tous m et n, on a

$$n + f(m) | f(n) + nf(m) - n(n + f(m)) = f(n) - n^2.$$

Pour tout n_0 fixé, le nombre $f(n_0) - n_0^2$ est donc divisible par $n_0 + f(m)$ pour tout m. Supposons que $f(n_0) - n_0^2 \neq 0$. Alors ce nombre n'a qu'un nombre fini de diviseurs, donc $n_0 + f(m)$ ne peut prendre qu'un nombre fini de valeurs, donc f ne prend qu'un nombre fini de valeurs, et est bornée.

Par ailleurs, en prenant $m = 1$ dans l'énoncé, on obtient $n + f(1) | f(n) + nf(1)$, donc

$$n + f(1) | f(n) + nf(1) - f(1)(n + f(1)) = f(n) - f(1)^2.$$

On en déduit que soit $f(n) = f(1)^2$, soit $f(n) - f(1)^2 \geqslant n + 1$, donc $f(n) \geqslant n + 2$. Comme f est bornée, le second cas ne peut pas se produire pour n assez grand, donc $f(n) = f(1)^2$ pour n assez grand.

Dans ce cas, fixons m et choisissons n assez grand pour que $f(n) = f(1)^2$. Alors $n + f(m) | f(1)^2 + nf(m)$, donc

$$n + f(m) | f(1)^2 + nf(m) - f(m)(n + f(m)) = f(1)^2 - f(m)^2.$$

Pour n assez grand, on a cependant $n + f(m) > |f(1)^2 - f(m)^2|$, donc $f(1)^2 - f(m)^2 = 0$, donc $f(m) = f(1)$ pour tout m. On a donc $f(1)^2 = f(1)$ donc $f(1) = 1$, et f est la fonction constante égale à 1.

On a donc montré que s'il existe n_0 tel que $f(n_0) \neq n_0^2$, alors $f(m) = 1$ pour tout m, donc il n'existe que deux solutions possibles : la fonction carrée, et la fonction constante égale à 1. On vérifie facilement que ces deux fonctions sont solutions.

2 Entraînement final

– Énoncés –

Exercice 1
Trouver le plus petit entier naturel non nul n tel que 2016 divise $20^n - 16^n$.

Exercice 2
Soit ABC un triangle. Un cercle de centre O passant par A et C coupe les segments $[AB]$ et $[BC]$ à de nouveau aux points K et N respectivement. Les cercles circonscrits aux triangles BKN et ABC se recoupent en M. Montrer que le triangle OMB est rectangle.

Exercice 3
Soient k_1 et k_2 deux cercles de même centre, avec k_2 à l'intérieur de k_1. Soit A un point de k_1 et B un point sur k_2 tel que (AB) soit tangent à k_2. Soit C la deuxième intersection de (AB) et k_1 et soit D le milieu de $[AB]$. Une droite passant par A coupe k_2 en E et F de telle sorte que les médiatrices de $[DE]$ et $[CF]$ se coupent en un point M tel que M appartient à (AB). Trouver la valeur de $\frac{AM}{MC}$.

Exercice 4
Chaque case d'un damier de taille $n \times n$, où $n \geqslant 3$ est un nombre entier, contient une lampe. Au début, les lampes dans deux coins opposés sont allumées, et les autres sont éteintes. Une opération consiste à choisir une rangée ou une colonne du damier, et à changer l'état de toutes les lampes de cette rangée ou colonne.

Avant de commencer les opérations, Alice peut choisir d'allumer individuellement autant de lampes qu'elle veut. Elle désire s'assurer qu'il existe une suite finie d'opérations au bout de laquelle chaque lampe est éteinte. Combien de lampes, au minimum, doit-elle allumer avant le début des opérations ?

– Solutions –

Solution de l'exercice 1
On commence par factoriser 2016 en produit de facteurs premiers : $2016 = 2^5 \times 3^2 \times 7$. Il nous faut donc trouver les entiers $n \geqslant 1$ tels que l'entier $20^n - 16^n = 2^{2n}(5^n - 4^n)$ soit divisible à la fois par 2^5, 3^2 et 7. Il s'agit exactement des entiers tels que $2n \geqslant 5$, que $5^n \equiv 4^n \pmod{3^2}$ et $5^n \equiv 4^n \pmod 7$.

Puisque $4 \times 7 \equiv 1 \pmod{3^2}$ et $4 \times 2 \pmod 7$, cela revient à ce que $n \geqslant 3$, que $(-1)^n \equiv (5 \times 7)^n \equiv (4 \times 7)^n \equiv 1^n \equiv 1 \pmod{3^2}$ et que $3^n \equiv (5 \times 2)^n \equiv (4 \times 2)^n \equiv 1^n \equiv 1 \pmod 7$.

En notant ω l'ordre de -1 modulo 3^2 et ω' l'ordre de 3 modulo 7, l'entier n recherché est donc le plus petit multiple de ω et de ω' tel que $n \geqslant 3$. Or, $(-1)^1 \not\equiv 1 \pmod{3^2}$ et $(-1)^2 \equiv 1 \pmod{3^2}$, donc $\omega = 2$.

De même, $3^1 \not\equiv 1 \pmod 7$, $3^2 \equiv 2 \not\equiv 1 \pmod 7$ et $3^3 \equiv -1 \not\equiv 1 \pmod 7$, donc $\omega' > 3$, et que le petit théorème de Fermat assure que ω' divise 6. Cela signifie que $\omega' = 6$. Le plus petit entier n recherché est donc $n = 6$.

Solution de l'exercice 2
Soit X l'intersection de (KN) et (AC). M est le point de Miquel du quadrilatère complet $BNXCAK$. Or, $KACN$ est cyclique avec O le centre de son cercle circonscrit. On sait que M est le projeté de O sur (XB), ce qui montre bien que $\widehat{OMB}$ est droit.

Solution de l'exercice 3
On a $AE \cdot AF = AB^2 = 4AD^2 = AD \cdot AC$ donc E, F, C et D sont cocycliques. Les médiatrices de $[BE]$ et $[CF]$ se coupent en (CD) donc M est le centre du cercle circonscrit à $EFCD$. On déduit $\frac{AM}{MC} = \frac{AC-MC}{MC} = \frac{2 \cdot AC}{DC} - 1 = \frac{8}{3} - 1 = \frac{5}{3}$.

Solution de l'exercice 4
On suppose que les lampes allumées au départ sont celles en haut à gauche, que l'on notera $(1, 1)$, et celle en bas à droite, qui sera la case (n, n). Le coin supérieur droit sera noté $(n, 1)$.

Montrons qu'Alice peut s'en sortir en allumant $2n-4$ lampes. Elle allume toutes les lampes de la rangée du haut et de la colonne de droite, sauf $(n, 1)$. Ensuite, elle commence les opérations et choisit la rangée du haut, puis la colonne de droite, après quoi la grille est éteinte.

Montrons maintenant qu'il est nécessaire d'allumer au moins $2n - 4$ lampes. Considérons quatre coins d'un rectangle. On remarque alors que la parité du nombre de lampes allumées parmi ces quatre coins est invariante. Considérons alors tous les quadruplets de la forme $(1, 1), (a, 1), (a, b), (1, b)$ avec $1 < a, b < n$ et $(n, n), (a, n), (a, b), (n, b)$ avec $1 < a, b < n$.

Dans la configuration initiale, tous ces quadruplets ont exactement une lampe allumée, et on veut atteindre une position avec zéro lampe allumée par quadruplet. Il faut donc allumer au moins une lampe par quadruplet. Or, il y a $2 \cdot (n-2)^2$ quadruplets, et une case est commune à au plus $n - 2$ quadruplets. La conclusion s'ensuit.

VI. Groupe D

Contenu de cette partie

1 Algèbre

1 Inégalités

Ce TD a pour objet les inégalités en olympiades, au sens large du terme. Ces dernières constituent un outil récurrent, l'un des seuls qui puissent intervenir dans les quatre thèmes olympiques (malgré une prédominance naturelle en algèbre). Aussi est-il bon de savoir les maîtriser et de bien en connaître les énoncés, y compris les cas d'égalité qui ont souvent leur importance. Toutefois, devant le recul des problèmes de pures inégalités aux Olympiades Internationales de Mathématiques et dans la plupart des compétitions, nous avons préféré à un cours théorique l'approche pratique par les « listes courtes » des OIM et les techniques utiles.

À celles et ceux à la recherche d'un recueil de théorie ou d'une base de problèmes corsés, on conseille de se référer au poly de Pierre Bornsztein sur les inégalités [1] ou à celui de Thomas Mildorf [2] (en anglais).

– Inégalités en algèbre –

Exercice 1 (Inégalité de Nesbitt)
Soient $a, b, c > 0$. Montrer que :

$$\tfrac{a}{b+c} + \tfrac{b}{a+c} + \tfrac{c}{a+b} \geqslant \tfrac{3}{2} \text{ avec égalité ssi } a = b = c,$$

d'autant de façons que vous pouvez.

Exercice 2
Soient $a_1, \ldots, a_n$ des réels tels que : $\sum a_i = 0$, et : $\sum |a_i| = 1$. Montrer que : $|\sum i \cdot a_i| \leqslant \frac{n-1}{2}$.

Exercice 3
Soient a, b, c les longueurs des côtés d'un triangle. Montrer que : $\frac{a}{b+c-a} + \frac{b}{c+a-b} + \frac{c}{a+b-c} \geqslant 3$.

Exercice 4 (Problème 1, EGMO 2016)
Soit n un entier positif impair, et soit $x_1, x_2, \cdots, x_n$ des nombres réels positifs ou nuls. Montrer que :

$$\min_{i=1,\ldots,n} (x_i^2 + x_{i+1}^2) \leqslant \max_{j=1,\ldots,n} (2x_j x_{j+1})$$

où $x_{n+1} = x_1$.

Exercice 5 (Problème 1, BxMO 2014)
Trouver la plus petite valeur possible de :

$$\left\lfloor \frac{a+b+c}{d} \right\rfloor + \left\lfloor \frac{b+c+d}{a} \right\rfloor + \left\lfloor \frac{c+d+a}{b} \right\rfloor + \left\lfloor \frac{d+a+b}{c} \right\rfloor,$$

où $a,\ b,\ c$ et d varient dans $\mathbb{N}^*$.

1. disponible sur le site de la POFM.
2. disponible sur le site AoPS.

Exercice 6 (Problème 2, BxMO 2012)
Trouver tous les quadruplets (a, b, c, d) de réels strictements positifs tels que : $abcd = 1$, $a^{2012} + 2012b = 2012c + d^{2012}$, et : $2012a + b^{2012} = c^{2012} + 2012d$.

Exercice 7 (Problème 2, OIM 2012)
Soit $n \geqslant 3$ un entier et soient $a_2, \ldots a_n$ des réels strictement positifs tels que : $a_2 \cdot \ldots \cdot a_n = 1$. Montrer que :

$$(1+a_2)^2(1+a_3)^3 \cdots (1+a_n)^n > n^n.$$

Exercice 8 (Problème A1, Liste courte OIM 2017)
Soient $a_1, a_2, \ldots a_n, k$, et M des entiers strictement positifs tels que :

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = k \quad \text{et} \quad a_1 a_2 \cdots a_n = M,$$

et $M > 1$. Montrer que le polynôme $P(x) = M(x+1)^k - (x+a_1)(x+a_2)\cdots(x+a_n)$ n'a pas de racine positive.

Exercice 9 (Problème 4, RMM P4 2016)
Soient x et y des réels strictement positifs tels que : $x + y^{2016} \geqslant 1$. Montrer que : $x^{2016} + y > 1 - \frac{1}{100}$.

Exercice 10 (Problème 1, EGMO 2014)
Déterminer toutes les réels t tels que pour tout triplet (a, b, c) désignant les longueurs des côtés d'un triangle, $a^2 + bct$, $b^2 + cat$ et $c^2 + abt$ sont également les longueurs des côtés d'un triangle.

Exercice 11 (Problème A1, Liste courte OIM 2015)
On suppose que la suite $(a_n)_{n \geqslant 1}$ de réels strictement positifs satisfait :

$$a_{k+1} \geqslant \frac{k a_k}{a_k^2 + (k-1)}$$

pour tout entier strictement positif k. Montrer que pour tout $n \geqslant 2$: $a_1 + a_2 + \ldots + a_n \geqslant n$.

– Inégalités en combinatoire –

Exercice 12 (Problème 2, OIM 1998)
Dans une compétition, il y a m candidats et n juges, où $n \geqslant 3$ est un entier impair. Chaque juge choisit pour chaque candidat s'il l'accepte ou le rejette. On suppose que chaque paire de juges ont au plus k candidats sur lesquels leurs décisions coïncident. Montrer que :

$$\frac{k}{m} \geqslant \frac{n-1}{2n}.$$

Exercice 13 (Problème C2, Liste courte OIM 2009)
Pour tout entier $n \geqslant 2$, soit $N(n)$ le nombre maximal de triplets (a_i, b_i, c_i) avec $i = 1, \ldots, N(n)$, d'entiers positifs a_i, b_i and c_i vérifiant les deux conditions suivantes :

— $a_i + b_i + c_i = n$ pour tous $i = 1, \ldots, N(n)$,

— si $i \neq j$, alors : $a_i \neq a_j$, $b_i \neq b_j$ et $c_i \neq c_j$.

Déterminer $N(n)$ pour tout $n \geqslant 2$.

Exercice 14 (Problème 4, BxMO 2017)
Un n-carré Benelux (avec $n > 2$) est une grille $n \times n$ composée de n^2 cases, chacune d'elles contenant un entier strictement positif, satisfaisant les conditions suivantes :

— les n^2 entiers strictement positifs sont deux à deux distincts

— si pour chaque ligne et chaque colonne on calcule le plus grand commun diviseur des n nombres dans cette ligne ou colonne, alors on obtient $2n$ résultats différents.

1. Prouver que, dans chaque n-carré Benelux (avec $n > 2$), il existe une case contenant un nombre supérieur ou égal à $2n^2$.
2. Un n-carré Benelux est dit *minimal* si les n^2 nombres dans les cases sont inférieurs ou égaux à $2n^2$. Déterminer tous les $n > 2$ pour lesquels il existe un n-carré Benelux minimal.

– Inégalités en arithmétique –

Exercice 15 (Problème N2, Liste courte OIM 2015)
Soient a et b entiers strictements positifs tels que $a! + b!$ divise $a!b!$. Montrer que : $3a \geq 2b + 2$.

Exercice 16 (Problème N1, Liste courte OIM 2010)
Trouver $n \in \mathbb{N}^*$ minimal pour lequel il existe un ensemble $\{s_1, s_2, \ldots, s_n\}$ de n entiers strictement positifs distincts tels que :

$$\left(1 - \frac{1}{s_1}\right)\left(1 - \frac{1}{s_2}\right)\cdots\left(1 - \frac{1}{s_n}\right) = \frac{51}{2010}.$$

– Inégalités en géométrie –

Exercice 17
Existe-t-il un pavé droit tel que son périmètre, son aire et son volume soient égaux ?

Exercice 18 (inspiré du Problème 1, OIM 2006)
Soient ABC un triangle et I le centre de son cercle inscrit. Soit P un point à l'intérieur du triangle tel que

$$\widehat{PBA} + \widehat{PCA} \geqslant \widehat{PBC} + \widehat{PCB}.$$

Montrer que $AP \geqslant AI$, et qu'il y a égalité si et seulement si $P = I$.

Exercice 19 (Problème 1, OIM 2001)
Soit ABC un triangle strictement acutangle. Soient P le pied de la hauteur issue de A et O le centre du cercle circonscrit au triangle ABC. Montrer que si $\widehat{ACB} \geqslant \widehat{ABC} + 30°$ alors $\widehat{BAC} + \widehat{COP} < 90°$.

– Solutions des exercices –

Solution de l'exercice 1
Quelques façons classiques de démontrer Nesbitt :

— par l'inégalité du réordonnement

— par l'inégalité de Cauchy-Schwarz

— par l'inégalité entre les moyennes.

Solution de l'exercice 2
Comme dans la preuve de Gauss de la formule : $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, commençons par multiplier par 2 de part et d'autre. On a :

$$\begin{aligned}
2|\sum_{i=1}^{n} ia_i| &= |2\sum_{i=1}^{n}\sum_{j=1}^{i} a_i| \\
&= |2\sum_{j=1}^{n}\sum_{i=j}^{n} a_i| \\
&\leqslant \sum_{j=1}^{n} |\sum_{i=j}^{n} a_i| + |\sum_{i=1}^{j-1} a_i| \quad \text{(inégalité triangulaire et hypothèse 1)} \\
&\leqslant \sum_{j=1}^{n-1}\sum_{i=1}^{n} |a_i| \quad \text{(inégalité triangulaire et nullité du terme en } j=1\text{)} \\
&\leqslant n-1, \text{ par l'hypothèse 2.}
\end{aligned}$$

Solution de l'exercice 3
L'hypothèse de l'énoncé se traduit par la transformation de Ravi : $a = x+y$, $b = z+x$, $c = x+y$. On se ramène à montrer que :

$$\frac{y+z}{2x} + \frac{z+x}{2y} + \frac{x+y}{2z} \geqslant 3,$$

ce qui s'établit par IAG.

Solution des exercices 4 à 16
Corrigé disponible sur le site de la compétition, ou dans le forum *Contest collections* de l'inévitable site AoPS.

Solution de l'exercice 17

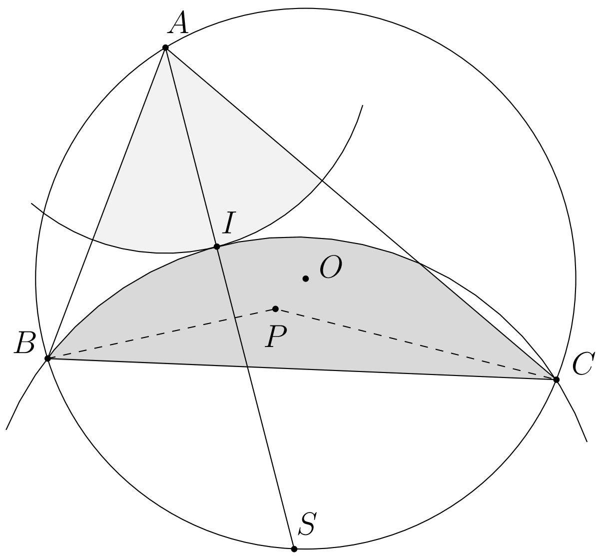
Supposons que c'est le cas. On note a, b, c les côtés du pavé droit, alors : $4(a+b+c) = 2(ab+bc+ca) = abc = x$. D'après l'inégalité de Newton sur les polynômes symétriques élémentaires :

$$\left(\frac{ab+bc+ca}{3}\right)^2 \geqslant \frac{a+b+c}{3} \cdot abc,$$

ce qui est absurde avec l'hypothèse faite. Ainsi, il n'existe pas de tel pavé droit.

Solution de l'exercice 18

On ajoute le "pôle Sud" S issu de A c'est-à-dire l'intersection de la bissectrice de l'angle $\widehat{BAC}$ avec le cercle circonscrit à ABC. On a :



$$\widehat{PBA} + \widehat{PCA} + \widehat{PBC} + \widehat{PCB} = \widehat{ABC} + \widehat{ACB} = 2(90^\circ - \frac{\widehat{BAC}}{2}),$$

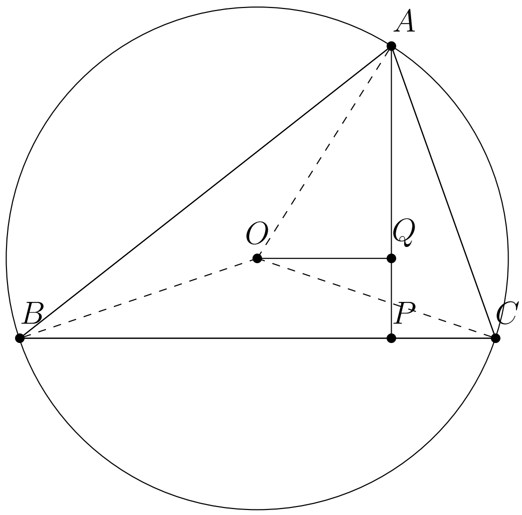
donc la condition de l'énoncé revient à : $\widehat{PBC} + \widehat{PCB} \leqslant 90^\circ - \frac{\widehat{BAC}}{2}$, ou encore à :

$$\widehat{BPC} \geqslant 90^\circ + \frac{\widehat{BAC}}{2} = \widehat{BIC}.$$

On en déduit que P est dans la zone grise foncée qui est délimitée par le cercle passant par B, I et C à cause de **l'inégalité reliant les angles inscrits à un cercle à ceux internes au disque et à ceux externe au disque**. Or $AP \leqslant AI$ si et seulement si P est dans la zone grise claire délimitée par le cercle de centre A et de rayon AI. De plus, il est bien connu que le cercle passant par B, I et C a pour centre S. A, I et S sont alignés donc le cercle de centre A et celui de centre S sont tangants en I. Le seul point appartenant aux deux zones est le point I, ce qui conclut l'inégalité.

Solution de l'exercice 19

On ajoute le projeté orthogonal Q de O sur $[AP]$. Une simple chasse aux angles donne : $\widehat{PCO} = 90^\circ - \widehat{BAC}$, et : $\widehat{OAP} = \widehat{BCA} - \widehat{ABC}$. Donc l'énoncé nous donne : $\widehat{OAP} \geqslant 30^\circ$



et l'on veut montrer : $\widehat{PCO} > \widehat{POC}$. Or, la loi des sinus nous fournit que les angles d'un triangle sont dans le même ordre que les longueurs des côtés opposés respectifs. Cette dernière inégalité équivaut donc à : $OP > PC$. Or on a : $OQ/OA = \sin(\widehat{OAP})$, donc : $OQ \geqslant R/2$, où R est le rayon du cercle circonscrit. D'un autre côté, on a : $OQ + PC < OC = R$, donc :

$$OP > OQ \geqslant R/2 \geqslant R - OQ > PC,$$

ce qui conclut.

2 Exercices divers

– Énoncés –

Exercice 1 (Problème A1, Liste courte IMO 2009)
On a 2018 triangles non plats, chaque triangle ayant une arête bleue, une blanche et une rouge. On note $b_1, \ldots, b_{2018}$ les longueurs des arêtes bleues, triées dans l'ordre croissant, et on définit de même $w_1, \ldots, w_{2018}$ pour les arêtes blanches et $r_1, \ldots, r_{2018}$ pour les arêtes rouges. Au minimum, combien y a t-il de i tels qu'on puisse former un triangles de côtés b_i, w_i et r_i ?

Exercice 2 (Problème 1, IMO 2011)
Pour tout ensemble $A = a_1, a_2, a_3, a_4$ de quatre entiers strictement positifs distincts de somme $s_A = a_1 + a_2 + a_3 + a_4$, on note p_a le nombre de couples (i, j) avec $1 \leqslant i < j \leqslant 4$ pour lesquels $a_i + a_j$ divise s_A. Parmi tous les ensembles de 4 entiers strictement positifs distincts, déterminer ceux qui maximisent p_A.

Exercice 3 (Problème A2, Liste courte IMO 2011)
Déterminer toutes les suites $(x_1, x_2, \ldots, x_{2011})$ d'entiers strictement positifs tels que pour tout entier positif n, il existe un entier a tel que $x_1^n + 2x_2^n + \ldots + 2011x_{2011}^n = a^{n+1} + 1$.

Exercice 4 (Problème 2, BMO 2018)
Soit q un rationnel positif Deux fourmis partent de l'origine d'un plan et font à chaque minute un pas vers le haut, le bas, la gauche ou la droite. La longueur du n-ième pas est q^n. Pour quelles valeurs de q est il possible que les deux fourmis se rejoignent après avoir emprunté des chemins différents ?

Exercice 5 (Problème A3, Liste courte IMO 2010)
Soient $x_1, \ldots, x_{100}$ 100 réels positifs. On prend $x_{101} = x_1$ et $x_{102} = x_2$ et on suppose que la somme de 3 x_i consécutifs est toujours au plus 1. Combien vaut au plus $\sum_{i=1}^{100} x_i x_{i+2}$?

Indice : l'hypothèse sur x_{101} et x_{102} « cache » une solution simple.

Exercice 6 (Problème A4, Liste courte IMO 2010)
Une suite $x_1, x_2, \ldots$ est définie par $x_1 = 1$ et $x_{2k} = -x_k, x_{2k-1} = (-1)^{k+1} x_k$. Montrer que, pour tout $n \geqslant 1$, $x_1 + x_2 + \ldots + x_n \geqslant 0$.

Exercice 7 (Problème 5, IMO 2016)
L'équation $(X-1)(X-2)\ldots(X-2016) = (X-1)(X-2)\ldots(X-2016)$ est écrite au tableau. On veut supprimer certains des facteurs de manière à ce qu'il reste au moins un terme de chaque côté et que l'équation obtenue n'aie aucune solution réelle. Combien de facteurs faut il supprimer au minimum ?

Exercice 8 (Problème 3, IMO 2009)
Soit $s_1, s_2 \ldots$ une suite strictement croissante d'entiers strictement positifs telle que $s_{s_1}, s_{s_2}, ..$ et $s_{s_1+1}, s_{s_2+1}, \ldots$ sont des progressions arithmétiques. Montrer que $s_1, s_2, \ldots$ est une progression arithmétique.

Exercice 9 (Problème 6, IMO 2010)
Soient $a_1, \ldots, a_r$ des réels positifs. Pour $n > r$, on pose $a_n = \max_{1 \leqslant k \leqslant n-1}(a_k + a_{n-k})$ Montrer qu'il existe des entiers positifs $l \leqslant r$ et N tels que $a_n = a_{n-l} + a_l$ pour tout $n \geqslant N$..

– Solutions –

Solution des exercices 1 à 9
Corrigé disponible sur le site de la compétition, ou dans le forum *Contest collections* de l'inévitable site AoPS.

3 Équations fonctionnelles

– Introduction –

Une équation fonctionnelle peut prendre de nombreuses formes. C'est ce qui en fait un terrain idéal pour « importer » des structures et raisonnements de différents domaines, notamment d'arithmétique (récurrence, décomposition en facteurs premiers...).

De fait, la meilleure façon de progresser est de s'exercer. Pour plus de problèmes que dans ce petit cours, on pourra notamment se reporter au polycopié en ligne de Pierre Bornsztein et Moubinool Omarjee, dont certains exercices sont reproduits ici.

Voici quelques conseils qu'il est toujours bon de rappeler. Les exemples à la suite permettent d'en bien saisir la portée :

1. Tester des valeurs particulières pour les variables, qui semblent intéressantes au vu de l'équation (en général, des valeurs simples ou menant à des simplifications dans l'équation).
2. Effectuer des substitutions : changer de variable... ou de fonction !
3. Vérifier l'injectivité ou la surjectivité.
4. Regarder les itérées d'une fonction f (c'est-à-dire les fonctions $f \circ f$, $f \circ f \circ f$, etc.) et les orbites des points (c'est-à-dire les ensembles $\{f(x), f(f(x)), f(f(f(x))), \ldots\}$ pour x fixé). En particulier :
   - chercher les points fixes (les x tels que $f(x) = x$), et
   - chercher les involutions ($f(f(x)) = x$ pour tout x), qui sont des bijections. On peut alors appliquer f des deux côtés d'une équation pour obtenir des simplifications : si $f(f(x+3)+2) = x$, alors $f(x+3)+2 = f(x)$.
5. S'intéresser à d'autres propriétés de la fonction qu'on cherche : périodicité, monotonie, parité...
6. Chercher des solutions particulières, pour déterminer s'il en existe ou non, et de ce à quoi elles pourraient ressembler. On peut en particulier tenter de montrer qu'une solution de l'équation doit nécessairement partager certaines propriétés communes aux solutions qu'on a déjà trouvées.
7. Exploiter la symétrie d'un membre de l'équation sur l'autre membre : par exemple, si $f(xy) = f(x) + y$ pour tout x, alors $f(y) + x = f(yx) = f(xy) = f(x) + y$.

8. Se ramener à une équation connue (équation de Cauchy notamment).
9. Improviser.

Quelles sont les clés pour traiter les exemples ci-dessous ?

Exercice 1
Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y,

$$f(x^{714} + y) = f(x^{2019}) + f(y^{122}).$$

Solution de l'exercice 1
Clé : substitution.

En posant $y = x^{2019} - x^{714}$, on a $f\left((x^{2019} - x^{714})^{122}\right) = 0$ pour tout réel x, donc $f(z) = 0$ pour tout $z \geqslant 0$ car la fonction $x \mapsto x^{2019} - x^{714}$ définie sur $\mathbb{R}$ est surjective sur $\mathbb{R}$ (c'est le cas de tout polynôme de degré impair) et la fonction $x \mapsto x^{122}$ définie sur $\mathbb{R}$ est surjective sur $\mathbb{R}^+$.

En choisissant $z < 0$ quelconque puis x tel que $x^{2019} = z$ (ce qui est possible car $x \mapsto x^{2019}$ est surjective sur $\mathbb{R}$) et $y = 0$, on obtient $f(z) = 0$.

Donc seule la fonction nulle peut être solution... ce qu'elle est bien, réciproquement.

Exercice 2
Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y, on ait

$$f(f(x) + 2y) = 6x + f(f(y) - x).$$

Solution de l'exercice 2
Clés : injectivité/surjectivité, alternative « injective ou périodique »

En posant $y = -f(x)/2$, on a $f(f(y) - x) = f(0) - 6x$. Le membre de droite décrit tout $\mathbb{R}$ lorsque x en fait de même, donc f est surjective. Dans nombre d'équation fonctionnelles, c'est une telle fonction « extérieure » surjective (ici $x \to f(0) - 6x$) qui permet de montrer que f est surjective.

S'il existe $a > b$ tels que $f(a) = f(b)$, alors en écrivant successivement l'équation avec $y = a$ et $y = b$, $f(f(x)+2a) = f(f(x)+2b)$ pour tout x, donc par surjectivité de f, $f(z) = f(z+2a-2b)$ pour tout réel z, donc f est $2(a-b)$ périodique.

Utilisons la non-périodicité de la fonction $x \mapsto 6x$ pour montrer que c'est absurde : en écrivant deux fois l'équation avec $x = 0$ (par exemple) et $x = 2(a-b)$, on obtient $2(a-b) = 0$.

Donc f est injective. En prenant $x = 0$ dans l'équation, on obtient $f(y) = 2y + f(0)$ pour tout réel y. Ne reste plus qu'à trouver les valeurs possibles pour $f(0)$ telles que f soit effectivement une solution : l'équation initiale devient

$$2(2x + f(0) + 2y) + f(0) = 6x + 2(2y + f(0) - x) + f(0),$$

et ceci est vrai pour tous $x, y, f(0) \in \mathbb{R}$.

Remarque 1.3.1.
L'alternative « injective ou périodique » peut apparaître lorsqu'on a des de termes comme $f(x + f(y))$: dans l'argument de f, on a une fonction de x plus une fonction de y. Dans

l'exemple ci-dessus, c'est la fonction extérieure $x \mapsto 6x$ qui a « décidé » du caractère injectif de f. Dans un registre totalement différent, lorsqu'une suite (u_n) est telle que chaque terme s'exprime comme une certaine fonction g du précédent, alors la suite est soit injective, soit périodique, car si $u_n = u_k$ pour certains $n \neq k$, $u_{n+1} = u_{k+1}$, etc.

Exercice 3
Trouver toutes les fonctions $f : [0,1] \to [0,1]$ telles que pour tout $0 \leqslant x \leqslant 1$, $f(2x - f(x)) = x$.

Solution de l'exercice 3
Clés : changement de fonction, itérées d'une fonction.

Soit $g(x) := 2x - f(x)$ pour tout x. On voit que $f \circ g$ est l'identité, qui est une fonction bijective, ce qui implique que f et g sont bijectives (c'est un fait classique assez utile). On remarque que g est à valeurs dans $[0,1]$ puisque $f(g(x))$ est bien défini pour tout x. On note, pour $n \geqslant 1$, $g^n = g \circ \ldots \circ g$ (on compose n fois g). On voit facilement par récurrence que $g^n(x) = ng(x) - (n-1)x = n(g(x) - x) + x$. S'il existe x_0 tel que $g(x_0) - x_0 \neq 0$, alors pour n assez grand $|g^n(x_0)| > 1$, or g est à valeurs dans $[0,1]$ donc g^n aussi, contradiction. Donc $g(x) = x$ pour tout x, donc $f(x) = x$ pour tout x. Réciproquement, cette fonction est solution.

Exercice 4
Trouver toutes les fonctions croissantes $f : \mathbb{R}^* \to \mathbb{R}^*$ telles que pour tous réels non nuls x, y, on ait $f(x+y)(f(x) + f(y)) = f(x)f(y)$.

Solution de l'exercice 4
Clés : changement de fonction, retour à une équation connue.

Soit $g(x) = 1/f(x)$ pour tout réel x. L'énoncé donne $g(x+y) = g(x) + g(y)$. Ainsi, g vérifie l'équation de Cauchy... sur $\mathbb{R}^*$, pas sur $\mathbb{R}$! On ne peut pas en déduire directement que g est linéaire sur $\mathbb{Q}$: une propriété standard des fonctions vérifiant l'équation de Cauchy sur un ensemble contenant au moins $\mathbb{Q}$, mais ici, on ne peut pas choisir $x = 0$ ou $y = 0$. Ainsi, on a moins de contraintes sur g. Toutefois, on peut prouver, comme pour l'équation de Cauchy sur $\mathbb{Q}$, que g est linéaire sur $\mathbb{Q}_+^*$ (prouver par récurrence sur $\mathbb{N}^*$ que $g(n) = ng(1)$, et que $g(1) = ng(1/n)$, puis écrire que $g(p/q) = pg(1/q) = p/qg(1)$ pour tous $p, q \in \mathbb{N}^*$) et de même sur $\mathbb{Q}_-^*$. Donc il existe $a, b \in \mathbb{R}^*$ tels que $g(x) = ax$ si $x > 0$ et $g(x) = bx$ si $x > 0$. En posant $x = 2$ et $y = -1$ dans l'équation $g(x+y) = g(x) + g(y)$, on obtient $a = 2a - b$ donc $a = b$.

Donc g est linéaire sur $\mathbb{Q}^*$. Or elle est croissante. Ainsi $a > 0$, et pour tout réel non nul r, pour tous rationnels $q \leqslant r \leqslant q'$, on a $aq \leqslant g(r) \leqslant aq'$. On peut prendre q et q' arbitrairement proches de r car $\mathbb{Q}$ est dense dans $\mathbb{R}$. Ainsi, $g(r) = ar$ pour tout réel non nul r.

Donc
$$f(x) = \frac{1}{ax}$$
pour tout $x \in \mathbb{R}^*$. Réciproquement, toutes ces fonctions (pour $a > 0$) sont solutions du problème.

Remarque 1.3.2.
L'équation de Cauchy $f(x+y) = f(x) + f(y)$ admet uniquement les fonctions linéaires comme solutions sur $\mathbb{Q}$. Sur $\mathbb{R}$, il existe des cas pathologiques de solutions non-linéaires... mais que l'on ne peut pas construire ! On pourra consulter ce polycopié de l'USAMO (en anglais) pour plus de détails.

– Exercices –

En cours, nous avons traité les exercices 1,4,5,8,9.

Exercice 5
Soient $a, b > 0$. Trouver toutes les fonctions $f : \mathbb{R}_+ \to \mathbb{R}$ telles que pour tous réels positifs x, y :

$$f(x)f(y) = y^a f\left(\frac{x}{2}\right) + x^b f\left(\frac{y}{2}\right).$$

Exercice 6
Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y :

$$f(x^2 - y^2) = xf(x) - yf(y).$$

Exercice 7 (BMO 2007)
Trouver toutes les fonctions réelles f telles que pour tous $x, y \in \mathbb{R}$,

$$f(f(x) + y) = f(f(x) - y) + 4f(x)y.$$

Exercice 8 (BMO 2009)
Trouver toutes les fonctions $f : \mathbb{N}^* \to \mathbb{N}^*$ telles que

$$f(f^2(m) + 2f^2(n)) = m^2 + 2n^2,$$

pour tous entiers strictement positifs m, n.

Exercice 9 (OIM 1983)
Trouver toutes les fonctions $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$ telles que, pour tous $x, y > 0$, $f(yf(x)) = xf(y)$ et $\lim_{x\to+\infty} f(x) = 0$.

Exercice 10 (APMO 2011)
Trouver toutes les fonctions réelles majorées f telles que pour tous réels x, y, on ait

$$f(xf(y)) + yf(x) = xf(y) + f(xy).$$

Exercice 11 (APMO 2016)
Trouver toutes les fonctions $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$ telles que

$$(z+1)f(x+y) = f(xf(z)+y) + f(yf(z)+x)$$

pour tous $x, y, z > 0$.

Exercice 12
Existe-t-il une fonction $f : \mathbb{N} \to \mathbb{N}$ telle que pour tout $n \geqslant 0$,

$$f(f(n)) = n + 2017\,?$$

Exercice 13
Trouver toutes les fonctions strictement croissantes $f : \mathbb{N} \to \mathbb{N}$ telles que pour tout $n \geqslant 0$, $f(f(n)) < n+1$.

Exercice 14
Trouver toutes les fonctions $f : \mathbb{N}^* \to \mathbb{N}^*$ strictement croissantes telles que $f(2) = 2$ et pour tous $m, n \geqslant 1$ premiers entre eux, ,

$$f(mn) = f(m)f(n).$$

Exercice 15 (Liste courte OIM 2014)
Trouver toutes les fonctions $f : \mathbb{Z} \to \mathbb{Z}$ telles que

$$f\big(f(m)+n\big)+f(m)=f(n)+f(3m)+2014$$

pour tous entiers m, n.

– Solutions –

Solution de l'exercice 5
Le membre de gauche est symétrique en x et y. Donc celui de droite doit l'être aussi, ainsi

$$x^a f(y/2)+y^b f(x/2)=y^a f(x/2)+x^b f(y/2)$$

pour tous réels positifs x, y. Donc si $a \neq b$, il existe c tel que $f(x/2)/(x^a-x^b)=c$ pour tout $x \neq 0, 1$. Ainsi,

$$f(x)=c(2^a x^a-2^b x^b).$$

pour tout $x>0$ différent de $1/2$ et 1. On réécrit l'équation fonctionnelle avec cette expression, et on obtient

$$c^2(2^a x^a-2^b x^b)(2^a y^a-2^b y^b)=c(y^a x^a-y^b x^b),$$

donc $c^2(2^a x^a-2^b x^b)(2^a y^a-2^b y^b)-c(y^a x^a-y^b x^b)=0$ On traite cette expression comme un polynôme en x : les coefficients de même degré doivent être égaux des deux côtés de l'équation (ceci est vrai même si a et b ne sont pas forcément entiers). Le terme en x^a donne $c^2 2^a(2^a y^a-2^b y^b)-cy^a=0$. En traitant ceci comme un polynôme en y, et en regardant le terme de degré b, on trouve $c=0$, donc $f=0$ sur $\mathbb{R}^* \setminus \{1/2, 1\}$. En injectant $x=y=1/2$ dans l'équation initiale, on a $f(1/2)=0$. Puis $x=y=1/2$ donne $f(1)=0$, donc f est la fonction nulle, qui est bien solution du problème.
Réglons le cas $a=b$: avec $x=y$ dans l'équation initiale, on obtient $f(x)^2=2x^a f(x/2)$, donc $f(x/2)$ est positive pour tout x, donc f ne prend jamais de valeur strictement négative. Donc $f(x)=\sqrt{2x^a f(x/2)}$. En remplaçant $f(x)$ et $f(y)$ par cette nouvelle expression dans l'équation initiale, on obtient

$$4x^a f\left(\frac{x}{2}\right) y^a f\left(\frac{y}{2}\right)=x^{2a} f\left(\frac{y}{2}\right)^2+y^{2a} f\left(\frac{x}{2}\right)^2,$$

qu'on peut factoriser en

$$\left(x^a f\left(\frac{y}{2}\right)-y^a f\left(\frac{x}{2}\right)\right)^2=0.$$

Le membre de gauche doit donc être nul, ce qui implique que le rapport $f(x/2)/x^a$ est constant (pour x non nul). Donc $f(x)=cx^a$ pour un certain $c \in \mathbb{R}$ (ce qui est aussi vrai en $x=0$, car en faisant $x=y=0$ dans l'équation initiale, on trouve $f(0)=0$). Réciproquement, on voit que ces fonctions sont solutions du problème.

Solution de l'exercice 6
Avec $x=y=0$, $f(0)=0$. Avec $y=-x$, $f(x)=-f(-x)$. Et pour $y=0$, on obtient $f(x^2)=xf(x)$. Ces deux dernières identités permettent d'obtenir $f(a-b)=\sqrt{a}f(\sqrt{a})-\sqrt{b}f(\sqrt{b})=f(a)-f(b)$ pour a, b positifs. Avec l'imparité de la fonction, on obtient de surcroit $f(a-b)+$

$f(-a) = f(-b)$ ainsi que $f(b-a) = f(b) + f(-a)$. Ces trois formules permettent de montrer pour *tous* x, y (positifs ou négatifs) :

$$f(x) + f(y) = f(x+y),$$

nous sommes retombés sur l'équation de Cauchy ! Maintenant, soit X réel, posons $x = \frac{X+1}{2}$ et $y = \frac{X-1}{2}$, ce qui nous donne, en utilisant l'équation de Cauchy :

$$\begin{aligned}
f(X) &= \frac{X+1}{2} f\left(\frac{X+1}{2}\right) - \frac{X-1}{2} f\left(\frac{X-1}{2}\right)\\
f(X) &= f\left(\frac{X}{2}\right) + X f\left(\frac{1}{2}\right)\\
f(X) &= X f(1)
\end{aligned}$$

Donc f est linéaire. Réciproquement, une telle fonction est solution de notre problème.

Solution de l'exercice 7

On pose $g(x) = f(x) - x^2$. L'équation devient

$$g(g(x) + x^2 + y) = g(g(x) + x^2 - y). \tag{VI.1}$$

Pour tous réels a, b, c, en prenant $x = a$ et $y = c - b^2 - g(b)$, et $x = b$, $y = c - a^2 - g(b)$, on obtient

$$g(g(a) + a^2 - g(b) - b^2 + c) = g(g(a) + a^2 + g(b) + b^2 - c) = g(g(b) + b^2 - g(a) - a^2 + c).$$

L'égalité entre le premier et le troisième membre montre que $g(c') = g(c' + 2(g(a) + a^2 - g(b) - b^2))$ pour tout $c' \in \mathbb{R}$. Ainsi, soit $g(x) + x^2$ est une fonction constante, ce qui implique que f est constante, puis $f(x) = 0$ pour tout réel x en revenant à l'équation de départ ; soit il existe $a \neq b$ tels que $g(a) + a^2 \neq g(b) + b^2$, et g est périodique. Dans ce cas, soit T sa période. Prenons $a = b + T$, on obtient $g(c') = g(c' + 2(2yT + T^2))$. Donc g est $4yT + 2T^2$-périodique. Lorsque y parcourt $\mathbb{R}$, $4yT + 2T^2$ aussi, donc $g(c') = g(c' + r$ pour tout réel r. Ainsi, g est constante, et $f(x) = x^2 + C$ où $C \in \mathbb{R}$. Réciproquement, si g est constante, elle vérifie évidemment l'équation (VI.1) qui est équivalente à celle de l'énoncé, donc ces fonctions f sont solution du problème pour tout réel C.

Solution de l'exercice 8

Il est clair que f est injective. L'identité $(x+3)^2 + 2x^2 = (x-1)^2 + 2(x+2)^2$ permet de montrer que pour tout entier $n \geqslant 2$,

$$f(n+3)^2 + 2f(n)^2 = f(n-1)^2 + 2f(n+2)^2.$$

Posons $u_n = f(n)^2$. On résout la relation de récurrence $u_{n+3} - 2u_{n+2} + 2u_n - u_{n-1} = 0$: le polynôme caractéristique est $X^3 - 2X^2 + 2X - 1 = (X-1)^3(X+1)$. On obtient $u_n = an^2 + bn + c + d(-1)^n$. Comme par ailleurs, $2u_1 + u_5 = 3u_3$ (car $2 \times 1^2 + 5^2 = 3^2 + 2 \times 3^2$), on obtient $b = 0$.

Prouvons que $c = d = 0$: Pour tout n pair, $u_n = an^2 + c + d$. Or $u_n = f(n)^2$, donc $an^2 + c + d$ est un carré parfait, donc $4(an^2 + c + d)$ aussi. Comme $2n$ est pair, $u_{2n} = 4an^2 + c + d$ et c'est également un carré parfait. Donc pour tout $n \geqslant 1$, $3(c+d)$ est la différence de deux carrés parfaits d'entiers $\geqslant n$. Or s'ils sont distincts, leur différence vaut au moins $(n+1)^2 - n^2 = 2n+1$

(prendre deux carrés consécutifs aussi petits que possible), ce qui dépasse $3(c+d)$ pour n assez grand, contradiction. Donc $u_{2n} = 4u_n$ et $c + d = 0$. Donc pour tout n pair, $u_n = an^2$ est un carré, donc a est lui-même un carré. Pour m impair, $u_m = am^2 + c - d$. De même, comme am^2 est un carré, $c - d$ est la différence de deux carrés d'entiers $\geqslant m$, et ce pour tout m, ce qui implique $c - d = 0$ comme précédemment. Comme $c + d = 0$, on obtient bien $c = d = 0$.

On a donc $f(n) = \sqrt{a}n$ pour tout entier n, a étant un carré parfait, autrement dit, f est linéaire. En injectant ceci dans l'équation initiale, on trouve que le coefficient directeur ne peut être que 1 (rappelons que f est positive, donc ce coefficient est lui-même positif). Donc f est l'identité. Réciproquement, l'identité est solution au problème.

Solution de l'exercice 9

Intéressons-nous aux points fixes de f : pour tout x, $xf(x)$ est un point fixe de f. Si 1 est le seul point fixe, alors $f(x) = 1/x$ pour tout x.

Sinon, soit z un point fixe autre que 1. Si z' est un point fixe, alors $1/z'$ aussi (faire $x = z'$ et $y = 1/z'$ dans l'équation de départ). Donc on peut supposer que $z > 1$. On prouve par récurrence sur n que si z est un point fixe, alors z^{2^n} aussi : si z^{2^n} est un point fixe, il suffit de choisir $x = y = z^{2^n}$ pour voir que $z^{2^{n+1}}$ en est un aussi. Ainsi, on a une suite de points fixes arbitrairement grands pour n grand.

Solution de l'exercice 10

En posant $x = 0$, on trouve $f(0) = 0$. Puis en posant $y = 1$, on a $f(xf(1)) = xf(1)$ or f majorée donc $f(1) = 0$.

Maintenant, avec $x = 1$ on trouve $f(f(x)) = 2f(x)$, donc $f^n(x) = 2^{n-1}f(x)$. De nouveau, comme f est majorée, on a $f(x) \leqslant 0$ pour tout x. Supposons qu'il existe r tel que $f(r) < 0$. Pour tout t, si $f(t) = 0$, alors $f(tr) = tf(r)$, donc $t \geqslant 0$.

En additionnant ce que l'on trouve pour $(x, \frac{1}{x})$ et $(\frac{1}{x}, x)$, on a pour x non nul :

$$f\left(xf\left(\frac{1}{x}\right)\right) = f\left(\frac{f(x)}{x}\right) = 0.$$

Si $x > 0$, $f(x)/x \leqslant 0$ donc $f(x) = 0$ (puisque f ne peut s'annuler sur $\mathbb{R}^{-*}$). En testant le couple $(-1, x)$, on s'aperçoit que $f(-x) = xf(-1)$, donc avec $-x = f(r)$, $f(f(r)) = -f(r)f(-1)$ or $f(f(r)) = 2f(r)$. Ainsi, $f(-1) = -2$. Donc :

$f(x) = -2x$ si $x < 0$, $f(x) = 0$ sinon. Il est facile de vérifier que cette fonction et la fonction nulle sont solution.

Solution de l'exercice 11

Ce problème a été posé à l'Olympiade du Pacifique Asiatique en 2016. Si $f(a) = f(b)$ pour deux réels a et b, en remplaçant z par a puis par b, on obtient $(a+1)f(x+y) = (b+1)f(x+y)$. Comme f est strictement positive, on en déduit $a = b$. Ainsi, f est injective.

En posant $x = y$, on obtient $f(xf(z)+x) = \frac{z+1}{2}f(2x)$. Soit s dans l'image de f, que l'on note $Im(f)$. Pour tout réel $r > 1/2$, on a que sr est aussi dans l'image de f, donc $]s/2, +\infty[\subset Im(f)$. Pour tout $u > s/4$, il existe $r > 1/2$ tel que $u/r > s/2$, donc le même raisonnement garantit que $u \in Im(f)$, d'où $]s/4, +\infty[\subset Im(f)$. En continuant ainsi, on obtient $]s/2^n, +\infty[\subset Im(f)$ pour tout $n \in \mathbb{N}^*$. Pour tout réel strictement positif r, il existe $n_r \in \mathbb{N}$ tel que $r > s/2^{n_r}$, donc $r \in Im(f)$. Finalement, $Im(f) = \mathbb{R}_+^*$, et f est surjective.

Donc f est bijective.

Ensuite, une idée consiste à prouver que pour tous a, b, c, d tels que $a + b = c + d$, on a $f(a) + f(b) = f(c) + f(d)$, en faisant $x = a, y = b$ (ou l'inverse) dans l'équation, puis

$x = c, y = d$. Si on trouve z tel que

$$\{af(z) + b, bf(z) + a\} = \{cf(z) + d, df(z) + c\},$$

c'est gagné. Il faut donc étudier ce système, en utilisant la surjectivité de f. Cela ouvre beaucoup de possibilités de substitutions pour finir l'exercice. Pour plus de détails, voir ici.

Solution de l'exercice 12
Il n'existe pas de telle fonction. Notons $A = \mathbb{N} \setminus f(\mathbb{N})$ et $B = f(\mathbb{N}) \setminus f(f(\mathbb{N}))$. A et B sont disjoints, et leur union est $\mathbb{N} \setminus f(f(\mathbb{N})) = \{0, 1, \ldots, 2016\}$. On voit aisément que f est injective, car $x \mapsto x + 2017$ est injective sur $\mathbb{N}$. Si $n \in A$, alors $f(n) \in B$. Réciproquement, si $n \in B$, il existe m tel que $f(m) = n$, mais pas de p tel que $f(p) = m$, donc $m \in A$. Ainsi, f est surjective de A vers B, donc bijective, car elle est injective. Il s'ensuit que A et B ont même cardinal, donc que la somme de leurs cardinaux devrait être paire, mais elle vaut 2017. Donc f ne peut exister.

Solution de l'exercice 13
On prouve que seule l'identité est l'unique solution, par récurrence forte sur n.

Il est clair que $f(0) = 0$. Supposons $f(j) = j$ pour tout j n'excédant pas un certain entier n. On ne peut avoir $f(n+1) \leqslant n$ car dans ce cas $f(n+1) \leqslant f(n)$, ce qui contredit la croissance de f. Si $f(n+1) = n+k$ pour un certain $k \geqslant 2$, alors $f(n+k) \leqslant n \leqslant f(n)$, ce qui entraîne le même problème. Donc $f(n+1) = n+1$.

Solution de l'exercice 14
On prouve que seule l'identité est solution. Notons $f(3) = 3 + k$ avec $k \geqslant 0$. On tâtonne en utilisant la multiplicativité de f pour les nombres premiers entre eux, et la stricte croissance pour générer des inégalités. Donc $f(6) = f(2)f(3) = 6 + 2k$, et $f(5) \leqslant 5 + 2k$. Ainsi, $f(10) \leqslant 10 + 4k$, $f(9) \leqslant 9 + 4k$, et $f(18) \leqslant 18 + 8k$, de sorte que $f(15) \leqslant 15 + 8k$. Par ailleurs, $f(5) \geqslant f(3) + 2 \geqslant 5 + k$ donc $f(15) \geqslant (5+k)(3+k) \geqslant 15 + 8k + k^2$. Donc $k = 0$. Ainsi, $f(3) = 3$, $f(6) = 6$, donc $f(4) = 4$ et $f(5) = 5$ par stricte croissance de f. Plus généralement, la stricte croissance implique que si $f(n) = n$ pour un certain n, alors $f(j) = j$ pour tout $j \leqslant n$. On prouve alors par récurrence que pour tout $m \geqslant 2$, $f(2^m + 1) = 2^m + 1$. L'initialisation vient d'être faite. Pour l'hérédité, si pour un certain $m \geqslant 2$, $f(2^m + 1) = 2^m + 1$, alors $f(2^m) = 2^m$, donc $f(2^m(2^m + 1)) = 2^m(2^m + 1)$. Or $2^m(2^m + 1) \geqslant 2^{m+1} + 1$, donc $f(2^{m+1} + 1) = 2^{m+1} + 1$.

Donc pour tout $m \geqslant 1$, pour tout $n \leqslant 2^m + 1$, $f(n) = n$. Donc seule l'identité peut être solution (ce qu'elle est effectivement).

Solution de l'exercice 15
Cet exercice est le quatrième problème d'algèbre de la liste courte des OIM 2014. Posons $f(0) = c$ et $g(n) = f(n) - f(0)$ pour tout n. L'équation fonctionnelle se réécrit :

$$g(g(m) + n + c) + g(m) = g(3m) + g(n) + 2014.$$

$m = 0$ donne $g(n + c) = g(n) + 2014$, en particulier, $g(kc) = 2014k$ pour tout $k \in \mathbb{Z}$. Prendre $n = -c$ donne $g(g(m)) + g(m) = g(3m)$. Donc $g(g(m) + n + c) = g(g(m)) + g(n) + 2014$, puis en remplaçant n par $n - c$, $g(g(m) + n) = g(g(m)) + g(n)$. En remplaçant m par c, on obtient $g(n + 2014) = g(n) + g(2014)$.

Donc $g(n + 2014c) = g(n) + cg(2014)$, or $g(n + c) = g(n) + 2014$, d'où $g(n + 2014c) = g(n) + 2014^2$. Ceci implique que $c \times g(2014) = 2014^2$. $m = n = c$ dans l'équation initiale donne $g(2014 + 2c) = 4 \times 2014$, donc $g(2014) = 2 \times 2014$, ainsi $c = 1007$, d'où $g(n + 1007) = g(n) + 2014$

et $g(1007k) = 2014k$ pour tout entier k. Par exemple, $g(1007g(m)) = 2014g(m)$. D'autre part, l'équation $g(g(m) + n) = g(g(m)) + g(n)$ permet de montrer $g(kg(m)) = kg(g(m))$ pour tout entier k, donc $g(1007g(m)) = 1007g(g(m))$. On en déduit que $g(g(m)) = 2g(m)$, puis que $g(3m) = 3g(m)$.

Maintenant, on a $3^{\varphi(1007)}g(n) = g\left(3^{\varphi(1007)}n\right)$. Et $3^{\varphi(1007)} = 1007\ell + 1$ pour un certain entier ℓ, par le théorème d'Euler (φ désigne la fonction indicatrice d'Euler), donc

$$3^{\varphi(1007)}g(n) = g(1007\ell n + n) = g(n) + 2014\ell n = g(n) + 2 \times (3^{\varphi(1007)} - 1)n.$$

Ainsi, $g(n) = 2n$ pour tout entier n.

La seule solution est donc $f(n) = 2n + 1007$, dont on vérifie aisément qu'elle satisfait l'énoncé.

2 Arithmétique

1 Polynômes cyclotomiques

Ce cours est essentiellement tiré du cours analogue proposé lors du stage olympique d'été organisé à Montpellier en 2014 et de son polycopié. Des références concernant les polynômes cyclotomiques se trouvent aux pages 116 à 141.

2 Exercices divers

Ce cours consistait en un TD uniquement constitué d'exercices tirés de listes courtes d'Olympiades Intenationales de Mathématiques. Le but était de voir des exercices d'arithmétique utilisant des petites idées simples mais bien choisies : utiliser les modulos, des comparaisons, principe des tiroirs, théorème des restes chinois, substitutions adéquates...

– Énoncés des exercices –

Exercice 1 (Problème N1, Liste courte OIM 2016)
Pour tout entier positif k, on note $S(k)$ la somme de ses chiffres. Trouver tous les polynômes à coefficients entiers tels que pour tout entier $n \geqslant 2016$, $P(n)$ est positif et $S(P(n)) = P(S(n))$.

Exercice 2 (Problème 1, OIM 2009)
Soit n un entier strictement positif et $a_1, \ldots, a_k$ avec $k \geqslant 2$ des entiers strictement positifs distincts de l'ensemble $\{1, \ldots, n\}$ tels que n divise $a_i(a_{i+1} - 1)$ pour $i = 1, \ldots, k-1$. Montrer que n ne divise pas $a_k(a_1 - 1)$.

Exercice 3 (Problème 5, OIM 2006)
Soit P un polynôme à coefficients entiers, de degré $n > 1$ et k un entier strictement positif. On considère le polynôme $Q(x) = P(P(\ldots P(P(x))\ldots))$ dans lequel P apparaît k fois. Montrer qu'il existe au plus n entiers t tels que $Q(t) = t$.

Exercice 4 (Problème N2, Liste courte 2007)
Soient $b, n > 1$ des entiers. Supposons que pour tout $k > 1$, il existe un entier a_k tel que k divise $b - a_k^n$. Montrer qu'il existe A un entier tel que $b = A^n$.

Exercice 5 (Problème 1, OIM 2017)
Pour tout entier $a_0 > 1$, on définit la suite $a_0, a_1, a_2, \ldots$ comme suit :

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{si } \sqrt{a_n} \text{ est un entier,} \\ a_n + 3 & \text{sinon.} \end{cases}$$

Déterminer toutes les valeurs de a_0 telles qu'il existe un nombre A tel que $a_n = A$ pour une infinté de valeur de n.

Exercice 6 (Problème 4, OIM 2016)
Un ensemble d'entier naturels est dit parfumé s'il contient au moins deux éléments et si chacun de ses éléments possède un facteur premier en commun avec au moins l'un des autres éléments. Soit $P(n) = n^2 + n + 1$. Déterminer le plus petit entier strictement positif b pour lequel il existe un entier positif a tel que l'ensemble

$$\{P(a+1), P(a+2), \ldots, P(a+b)\}$$

soit parfumé

Exercice 7 (Problème N1, Liste courte OIM 2015)
Déterminer tous les entiers M tels que la suite $(a_0, a_1, a_2, \ldots)$ définie par $a_0 = \frac{2M+1}{2}$ et $a_{k+1} = a_k \lfloor a_k \rfloor$ pour $k \geqslant 0$ contient au moins un terme entier.

Exercice 8 (Problème N1, Liste courte OIM 2013)
Déterminer toutes les fonctions de $\mathbb{N}*$ dans $\mathbb{N}*$ telles que

$$m^2 + f(n) \mid mf(m) + n$$

pour tous les entiers strictement positifs m et n.

Exercice 9 (Problème N2, Liste courte OIM 2011)
Soit $P(x) = (x + d_1)(s + d_2) \cdot \ldots \cdot (x + d_9)$ avec $d_1, \ldots, d_9$ des entiers distincts. Montrer qu'il existe N un entier tel que pour tous les entiers $x \geqslant N$ le nombre $P(x)$ est divisible par un nombre premier plus grand que 20.

Exercice 10 (Problème N3, Liste courte OIM 2006)
On définit pour tout entier n strictement positif $f(n)$ par

$$\frac{1}{n} \cdot \left(\lfloor \frac{n}{1} \rfloor + \lfloor \frac{n}{2} \rfloor + \ldots + \lfloor \frac{n}{n} \rfloor \right),$$

où $\lfloor x \rfloor$ est la partie entière de x.

(a) Montrer que $f(n+1) > f(n)$ pour une infinité d'entiers n.

(a) Montrer que $f(n+1) < f(n)$ pour une infinité d'entiers n.

Exercice 11 (Problème 5, OIM 2011)
Soit f une fonction des entiers relatifs vers les entiers positifs. Supposons que pour tout couple (m, n) d'entiers, $f(m) - f(n)$ est divisible par $f(m-n)$. montrer que pour tout couple d'entiers (m, n) tels que $f(m) \leqslant f(n)$, le nombre $f(n)$ est divisible par $f(m)$.

Exercice 12 (Problème N2, Liste courte OIM 2009)
Un entier strictement positif N est dit joli si $N = 1$ ou si N s'écrit comme un produit d'un nombre pair de facteurs premiers (pas forcément distincts). Pour toute paire (a, b) d'entiers strictement positifs, on pose $P(x) = (x + a)(x + b)$.

a) Montrer qu'il existe des entiers strictement positifs distincts (a, b) tels que $P(1), P(2), \ldots, P(50)$ sont jolis.

b) Montrer que si $P(n)$ est joli pour tout entier $n > 0$, alors $a = b$

Exercice 13 (Problème N5, Liste courte OIM 2008)
Pour tout $n \in \mathbb{N}$, on pose $d(n)$ le nombre des diviseurs positifs de n. Trouver toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ satisfaisant

(i) $d(f(x)) = x$ pour tout $x \in \mathbb{N}$

(ii) $f(xy)$ divise $(x-1)y^{xy-1}f(x)$ pour tout $x, y \in \mathbb{N}$

Exercice 14 (Problème N6, Liste courte OIM 2012)
Soient x et y des entiers strictement positifs. Si $x^{2^n} - 1$ est divisible par $2^n y + 1$ pour tout entier strictement positif n, montrer que $x = 1$. (Indice : on pourra commencer par montrer le résultat suivant : Pour x strictement positif, si il existe une infinité de nombres premiers $p \equiv 3 \mod 4$ divisant un nombre de la forme $x^{2^n} - 1$ avec $n \in \mathbb{N}*$, alors $x = 1$.)

Exercice 15 (Problème 5, OIM 2007)
Soietn a, b deux entiers strictement positifs. Montrer que si $4ab - 1$ divise $(4a^2 - 1)^2$, alors $a = b$.

Exercice 16 (Problème 2, OIM 2015)
Déterminer tous les triplets d'entiers (a, b, c) tels que $ab - c$, $ac - b$ et $bc - a$ sont des puissances de 2.

– Solutions –

Solution des exercices 1 à 16
Corrigé disponible sur le site des Olympiades Internationales de Mathématiques, ou dans le forum *Contest collections* de l'inévitable site AoPS.

3 Équations de Pell

Les équations de Pell n'apparaissent pas souvent aux Olympiades Internationales. Toutefois, outre le fait qu'il s'agisse d'un bel objet d'étude, les raisonnements présentés ici sont assez standard. Ce cours est fortement inspiré du livre *An Introduction to Diophantine Equations* de Titu Andreescu et Dorin Andrica, aux éditions GIL Publishing House (2002).

– Cours –

On appelle équation de Pell une équation de la forme

$$x^2 - dy^2 = 1,$$

où x et y sont les inconnues (entières) et d un entier qui n'est pas un carré parfait.

Théorème 2.3.1.
Soit d un entier qui n'est pas un entier parfait. Alors il existe une infinité de couples $(x, y) \in (\mathbb{N}^*)^2$ tels que

$$x^2 - dy^2 = 1.$$

De plus, il existe une solution $(x_0, y_0) \neq (1, 0)$ telle que $x_0 + \sqrt{d}y_0$ soit minimal, et telle que toute solution soient exactement les termes de la suite $((x_n, y_n))_{n \geqslant 0}$ définie par $x_1 = x_0$, $y_1 = y_0$, et pour tout $n \geqslant 1$, $x_{n+1} = x_0 x_n + dy_0 y_n$ et $y_{n+1} = y_0 x_n + x_0 y_n$.

Démonstration. La première partie de la preuve est un classique. Pour tout entier $c_1 \geqslant 0$, il existe $t_1, w_1 \in \mathbb{N}^*$ avec $w_1 \leqslant c_1$, tels que $|t_1 - w_1\sqrt{d}| < 1/c_1$. Qu'on considère en effet les parties fractionnaires des nombres $i\sqrt{d}$ pour tout $0 \leqslant i \leqslant c_1$: comme $\sqrt{d}$ est irrationnel, elles sont toutes distinctes et comprises entre 0 et 1 strictement, donc deux d'entre elles sont à distance strictement inférieure à $1/c_1$ par théorème des tiroirs (on rappelle que la partie fractionnaire de x est $x - \lfloor x \rfloor$, où $\lfloor x \rfloor$ est la partie entière inférieure de x, c'est-à-dire le plus grand entier ne dépassant pas x). Ainsi, il existe $0 \leqslant i_1 \neq i_2 \leqslant c_1$ tels que $(i_2 - i_1)\sqrt{d} - \lfloor (i_2 - i_1)\sqrt{d} \rfloor < 1/c_1$. Il suffit de prendre $w_1 = |i_2 - i_1|$ et $t_1 = \lfloor (i_2 - i_1)\sqrt{d} \rfloor$ si $i_2 > i_1$ $t_1 = -\lfloor (i_2 - i_1)\sqrt{d} \rfloor$ sinon, et le tour est joué.

Notons qu'alors $|t_1^2 - dw_1^2| \leqslant (t_1 + w_1\sqrt{d})/c_1 \leqslant t_1/c_1 + \sqrt{d} < 2\sqrt{d} + 1$, car $t_1 < w_1\sqrt{d} + 1$ par construction.

Choisissons un entier c_2 tel que $|t_1 - w_1\sqrt{d}| > 1/c_2$: comme précédemment, il existe un couple (t_2, w_2) tel que $|t_2 - w_2\sqrt{d}| < 1/c_2$, qui est donc différent de (t_1, w_1), et tel que $t_2^2 - dw_2^2 \in]-2\sqrt{d}-1, 2\sqrt{d}+1[$. Par récurrence, on peut construire une suite injective (t_n, w_n) vérifiant ces conditions. D'après le théorème des tiroirs « infini » (une infinité d'objets rangés dans un nombre fini de tiroirs implique qu'un tiroir contient une infinité d'objets), il existe un entier $k \in]-2\sqrt{d}-1, 2\sqrt{d}+1[$ tel que pour un certain ensemble infini $S \subset \mathbb{N}^*$, si $j \in S$, $t_j^2 - dw_j^2 = k$, et si $j, \ell \in S$, $t_j - t_\ell \equiv w_j - w_\ell \equiv 0 \pmod{|k|}$.

Prenons un tel k et deux tels entiers $j \neq \ell$. Posons $t_0 = t_j t_\ell - dw_j w_\ell$ et $w_0 = t_j w_\ell - t_\ell w_j$. Alors

$$t_0^2 - dw_0^2 = (t_j^2 - dw_j^2)(t_\ell^2 - dw_\ell^2) = k^2.$$

On remarque que t_0 et w_0 sont multiples de k, donc (t, w) est une solution à l'équation de Pell, où $t = |t_0/k|$ et $w = |w_0/k|$. Notons que si $w_0 = 0$, alors $t_j/w_j = t_\ell/w_\ell$ et $(t_j - w_j\sqrt{d})(t_j + w_j\sqrt{d}) = (t_\ell - w_\ell\sqrt{d})(t_\ell + w_\ell\sqrt{d})$ impliquent que $t_j = t_\ell$ et $w_j = w_{\ell]}$, ce qui est faux. Ainsi, $(t, w) \neq (1, 0)$.

On peut choisir $(x_0, y_0) \in (\mathbb{N}^*)^2 \setminus (1, 0)$ la solution de l'équation de Pell telle que $x_0 + y_0\sqrt{d}$ soit minimal, car il existe une solution (t, w), et il n'y a qu'un nombre finis de couples d'entiers positifs (a, b) tels que $a + b\sqrt{d} < t + w\sqrt{d}$. De plus, $a + b\sqrt{d} = c + e\sqrt{d}$ entraîne $a = b$ et $c = e$ car $\sqrt{d}$ est irrationnel, d'où l'unicité de la solution minimale.

On vérifie facilement par récurrence que tout terme de la suite définie dans l'énoncé du théorème donne une solution à l'équation de Pell, et que pour tout $n \in \mathbb{N}^*$,

$$x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^{n+1}.$$

Notons $z_n = x_n + y_n\sqrt{d}$.

Enfin, supposons qu'il existe une solution (x, y) à l'équation de Pell telle que $z_n < x + y\sqrt{d} < z_{n+1}$ pour un certain entier $n \geqslant 1$. Alors $1 < (x + y\sqrt{d})(x_n - y_n\sqrt{d}) < u_0 + v_0\sqrt{d}$. On vérifie aisément que le couple $(x_n x - y_n y d, x_n y - y_n x)$ est une solution qui contredit la minimalité de (x_0, y_0). $\square$

Remarque 2.3.2.
En lisant attentivement le dernier paragraphe de cette preuve, on constate que si (α, β) et (γ, δ) sont des solutions, alors $(\alpha\gamma + d\beta\delta, \alpha\delta + \beta\gamma)$ en est une aussi. Ce n'est pas innocent : il existe une approche plus algébrique de ces équations, où on considère l'ensemble des points (x, y) du plan qui vérifient l'équation de Pell (donc pas seulement ceux à coordonnées entières strictement positives). Il forme une courbe appelée **hyperbole**. On note $*$ l'opération telle que $(\alpha, \beta) * (\gamma, \delta) = (\alpha\gamma + d\beta\delta, \alpha\delta + \beta\gamma)$ pour tous $\alpha, \beta, \gamma, \delta$. C'est une loi de composition interne pour l'ensemble des points à coordonnées entières de l'hyperbole (*ie* elle prend deux tels points et les envoie sur un troisième).

Proposition 2.3.3.
On montre par récurrence sur n que

$$x_n = \frac{1}{2}\left((x_0 + y_0\sqrt{d})^n + (x_0 - y_0\sqrt{d})^n\right) \text{ et}$$
$$y_n = \frac{1}{2\sqrt{d}}\left((x_0 + y_0\sqrt{d})^n - (x_0 - y_0\sqrt{d})^n\right).$$

Remarque 2.3.4.
En général, il n'est pas évident de trouver x_0 et y_0. Cela peut se faire en passant par des **fractions continues** : Tout irrationnel x admet une écriture infinie de la forme

$$x = u_0 + \frac{1}{u_1 + \frac{1}{u_2 + \dots}},$$

où les u_i sont des entiers. En fait, si on note r_k le rationnel obtenu en arrêtant cette écriture à u_k, on peut prendre $u_0 = \lfloor x \rfloor$ et $u_{i+1} = \lfloor 1/x - 1/r_i \rfloor$ pour tout i. Appliquons ceci à $x = \sqrt{d}$: si on s'arrête après $\sqrt{d}$ étapes, on obtient une fraction irréductible p/q. Alors $x_0 = p$ et $y_0 = q$.

Remarque 2.3.5.
La suite (x_n, y_n) permet de donner une approximation rationnelle de $\sqrt{d}$, puisque

$$\left| \frac{x_n}{y_n} - \sqrt{d} \right| = \frac{x_n - y_n\sqrt{d}}{y_n} = \frac{1}{y_n(x_n + y_n\sqrt{d})} < \frac{1}{y_n^2}.$$

Voyons maintenant quelques équations dérivées des équations de Pell... Penchons-nous d'abord sur l'équation

$$ax^2 - by^2 = 1, \tag{VI.2}$$

où a, b sont des entiers strictement positifs.

Définition 2.3.6.
On appelle **résolvante de Pell pour l'équation (VI.2)**, l'équation

$$x^2 - aby^2 = 1. \tag{VI.3}$$

Proposition 2.3.7.
Soit $a, b \in \mathbb{N}^*$. Si ab est un carré parfait autre que 1, alors l'équation $ax^2 - by^2 = 1$ n'a pas de solution dans $(\mathbb{Z}^*)^2$ telle que $xy \neq 0$.

Démonstration. Si $pgcd(a, b) > 1$, l'équation n'a pas de solution. Sinon, il existe $c, d > 0$ tels que $a = c^2$ et $b = d^2$. Dans ce cas, l'équation devient

$$(cx)^2 - (dy)^2 = 1,$$

or 0 et 1 sont les deux seuls carrés parfaits de différence 1. Ainsi $y = 0$ et $c = x = 1$. □

Théorème 2.3.8.
Supposons que (VI.2) admette une solution et considérons la solution minimale (A, B) (ie A est minimal - remarquer que si (x, y) et (x', y') sont deux solutions, et si $x \leqslant x'$, alors $y \leqslant y'$, donc cette définition de minimalité est assez naturelle). Alors ses solutions sont exactement les couples

$$(u_n, v_n) = (Ax_n + bBy_n, Bx_n + aAy_n),$$

pour $n \geqslant 0$, où (x_n, y_n) est la suite des solutions de la résolvante (VI.3).

Démonstration. Un calcul direct montre que pour tout $n \geqslant 0$, $au_n^2 - bv_n^2 = 1$ donc que (u_n, v_n) est une solution de (VI.2). Réciproquement, si (u, v) est une solution de (VI.2), alors $(x, y) = (aAu - bBv, Bu - Av)$ est une solution de (VI.3). D'après le théorème 2.3.1, il existe $n \in \mathbb{N}$ tel que $(x, y) = (x_n, y_n)$, d'où l'on déduit que $(u, v) = (u_n, v_n)$. $\square$

Penchons nous désormais sur l'équation de Pell négative, à savoir

$$x^2 - dy^2 = -1. \tag{VI.4}$$

Théorème 2.3.9.
Si l'équation (VI.4) admet des solutions, en notant (A, B) la solution minimale, alors ses solutions sont exactement les couples ($n \geqslant 0$) :

$$(u_n, v_n) = (Bu_n + Adv_n, Au_n + Bv_n)$$

où (x_n, y_n) est la suite des solutions de l'équation de Pell $x^2 - dy^2 = 1$.

Démonstration. Multiplier les deux membres de (VI.4) par -1 et appliquer le théorème 2.3.8. $\square$

Théorème 2.3.10.
Si d est un nombre premier congru à 1 modulo 4, alors (VI.4) admet des solutions entières.

Démonstration. Soit (x_0, y_0) la solution minimale de la résolvante de Pell $x^2 - dy^2 = 1$. Si x_0 est pair, alors y_0 est impair et $d \equiv 3 \pmod 4$, contradiction. Donc x_0 est impair, et y_0 est pair. Donc $pgcd(x_0 + 1, x_0 - 1) = 2$, et $x_0 \pm 1 = 2a^2$, $x_0 \mp 1 = 2pb^2$ où a et b sont premiers entre eux et tels que $2ab = y_0$. En soustrayant ces deux égalités, on obtient $\pm 1 = a^2 - pb^2$. Comme $0 < b < y_0$, le $\pm$ ne peut être un $+$, sinon on aurait une solution de la résolvante de Pell contredisant la minimalité de (x_0, y_0). Donc $a^2 - pb^2 = -1$, et (a, b) est bien une solution de (VI.4). $\square$

– Exercices –

En cours, nous avons traité les exercices de 1 à 7.

Exercice 1
Trouver tous les entiers $n \geqslant 1$ tels que $2n + 1$ et $3n + 1$ soient des carrés parfaits.

Exercice 2
Trouver tous les nombres triangulaires qui sont des carrés parfaits (on rappelle que le n-ème nombre triangulaire est $1 + 2 + \ldots + n$).

Exercice 3
Montrer qu'il y a une infinité de triangles dont les longueurs des côtés sont trois entiers consécutifs et l'aire un entier également.

Exercice 4
Prouver qu'il y a une infinité d'entiers positifs n tels que $n, n + 1$ et $n + 2$ s'écrivent chacun comme somme de deux carrés.

Exercice 5
Prouver qu'il y a une infinité d'entiers positifs n tels que n^2+1 divise $n!$.

Exercice 6
Montrer qu'il existe deux suites (u_n) et (v_n) strictement croissantes telles que $u_n(u_n+1)$ divise v_n^2+1 pour tout $n \geqslant 0$.

Exercice 7
Soit $(x,y,z,t) \in (\mathbb{N}^*)^4$ un quadruplet vérifiant $x+y=z+t$ et $2xy=zt$, et tel que $x \geqslant y$. Trouver la plus grande valeur de m telle que $m \leqslant x/y$ à coup sûr.

Exercice 8
Montrer qu'il n'existe pas deux entiers positifs tels que la somme de leurs carrés et la différence de leurs carrés soient également des carrés parfaits.

– Solutions –

Solution de l'exercice 1
On cherche les entiers n tels qu'il existe $x,y \in \mathbb{N}^*$ vérifiant $x^2=2n+1$ et $y^2=3n+1$, ce qui équivaut à $x^2=2n+1$ et $3x^2-2y^2=1$. Cette dernière équation est une équation de Pell, dont la plus petite solution est $x=y=1$, et dont la résolvante est $X^2-6Y^2=1$. Celle-ci admet comme solution minimale $X=5$ et $Y=2$. Ainsi, les solutions de $3x^2-2y^2=1$ sont tous les termes d'une certaine suite $(X_k,Y_k)_{k\geqslant 0}$ dont la première coordonnée vérifie

$$(X_k,Y_k)=\left(\frac{1}{2}\left((5+2\sqrt{6})^k+(5-2\sqrt{6})^k\right),\frac{1}{2\sqrt{6}}\left((5+2\sqrt{6})^k+(5-2\sqrt{6})^k\right)\right)$$

Les solutions (x_k,y_k) de l'équation de Pell $3x^2-2y^2=1$ est $(x_k,y_k)=(X_k+2Y_k,X_k+3Y_k)$. Les entiers n cherchés sont donc les entiers de la forme $y_k^2-x_k^2=Y_k(2X_k+5Y_k)$, $k \geqslant 0$.

Solution de l'exercice 2
On cherche les entiers s'écrivant sous la forme $\frac{n(n+1)}{2}$ pour un certain n, et tels qu'il existe $y \in \mathbb{N}^*$ vérifiant $\frac{n(n+1)}{2}=y^2$, soit $(2n+1)^2-8y^2=1$. L'équation de Pell $X^2-8Y^2=1$ admet $(3,1)$ comme solution minimale, et donc la première coordonnée des solutions générales s'écrit

$$x_k=\frac{1}{2}\left((3+2\sqrt{2})^k+(3-2\sqrt{2})^k\right)=\frac{1}{2}\left((1+\sqrt{2})^{2k}+(1-\sqrt{2})^{2k}\right)$$

pour tout $k \geqslant 0$. Les entiers n correspondants sont ceux de la forme $\frac{x_k-1}{2}$ (on note que x_k est nécessairement impair pour tout k), donc les nombres cherchés sont les $\frac{x_k^2-1}{8}$.

Solution de l'exercice 3
Soit $a-1,a,a+1$ les longueurs d'un hypothétique triangle satisfaisant la condition demandée, où $a \geqslant 2$ est un entier. La formule de Héron stipule que l'aire d'un triangle dont les longueurs des côtés sont x,y,z et p le demi-périmètre vaut $\sqrt{p(p-a)(p-b)(p-c)}$. On cherche donc un entier y tel que

$$y^2=\frac{3a}{2}\times\frac{a+2}{2}\times\frac{a}{2}\times\frac{a-2}{2}.$$

Ce qui donne $(2y/a)^2 = 3a^2 - 12$. On pose $u = 2y/a$ et $v = a$, l'équation se réécrit $u^2 - 3v^2 = -12$. Donc u est un multiple de 3, on écrit $u = 3u'$, d'où $3u'^2 - v^2 = -4$. Si v est impair, u' aussi, et leurs carrés sont congrus à 1 modulo 4, donc l'équation n'admet pas de solution modulo 4. Ainsi, v est pair, et par suite, u' aussi. On se retrouve alors avec l'équation de Pell $V^2 - 3U^2 = 1$. Celle-ci admet une infinité de solutions (U_k, V_k) car 3 n'est pas un carré. En exprimant a en fonction de U_k et V_k, on voit que cette quantité devient arbitrairement large quand k tend vers l'infini, donc qu'il existe une infinité de valeurs satisfaisant l'énoncé.

Solution de l'exercice 4
L'équation de Pell $x^2 - 2y^2 = 1$ admet une infinité de solutions positives (x_n, y_n). Donc une infinité d'entiers positifs s'écrivent sous la forme x_k^2, qui est la somme de x_k^2 et 0^2. On a $x_k^2 - 1 = y_k^2 + y_k^2$, et $x_k^2 + 1 = x_k^2 + 1^2$. On prend alors $n = x_k^2 - 1$.

Solution de l'exercice 5
On peut prouver que pour une infinité de n, il existe u tel que $n^2 + 1 = 5u^2$, via l'équation de Pell négative $X^2 - 5y^2 = -1$ (il y a une infinité de solutions puisqu'il y a au moins une solution, car $5 \equiv 1 \pmod 4$). Un petit calcul montre que pour n assez grand, $5 < u < 2u < n$, ainsi $5, u, 2u, n$ apparaissent en des endroits tous différents de $n! = n \times \ldots \times 1$. Donc $n!$ est divisible par leur produit, ce qui permet de conclure.

Solution de l'exercice 6
Il suffit de trouver un entier $k > 0$ tel qu'il existe une suite (u_n, v_n) qui vérifie que $ku_n(u_n+1) = v_n^2 + 1$ pour tout n. Cette équation se réécrit $k(2u_n + 1)^2 - (2v_n)^2 = k + 4$. Prendre $k = 5$, et étudier $5x^2 - y^2 = 9$: si $x = 3X$ et $y = 3Y$, on tombe sur l'équation de Pell $Y^2 - 5X^2 = -1$, qui a une infinité de solutions comme vu dans l'exercice précédent.

Solution de l'exercice 7
La première équation au carré moins quatre fois la deuxième donne

$$\left(\frac{x}{y}\right)^2 - 6\left(\frac{x}{y}\right) + 1 = \left(\frac{z-t}{y}\right)^2.$$

Le membre de gauche est un trinôme en x/y, qui est positif au vu du membre de droite. Notons que $x/y > 1$ d'après l'énoncé. Or la fonction $g : m \mapsto m^2 - 6m + 1$ est négative pour $1 \leqslant m \leqslant r_1$ et positive pour $m \geqslant r_1$, où $r_1 = 3 + 2\sqrt{2}$ est la plus grande racine du trinôme. Donc $x/y \geqslant 3 + 2\sqrt{2}$. Reste à montrer qu'il existe des solutions de sorte que $\frac{z-t}{y}$ soit arbitrairement petit, ce qui impliquera que x/y est arbitrairement proche de r_1. Attention, ce n'est pas dû à la continuité de g, mais au fait que pour tout $\delta > 0$, il existe $\varepsilon > 0$ tel que si $w > r_1 + \delta$, $g(w) > \varepsilon$ (exercice : le démontrer) et on aura prouvé que $m = 3 + 2\sqrt{2}$.

On reprend l'énoncé : la première équation au carré moins deux fois la deuxième donne

$$(x-y)^2 = z^2 + t^2.$$

Quitte à diviser, on peut supposer $pgcd(x-y, z, t) = 1$, et que t est pair sans perte de généralité. Un théorème utile sur les triplets pythagoriciens (preuve laissée à qui lira ceci) affirme qu'il existe $a > b$ premiers entre eux tels que

$$x - y = a^2 - b^2,\ t = 2ab,\ z = a^2 - b^2,$$

quitte à échanger z et t. Avec $x+y = z+t$, on obtient $y = b(a-b)$. Peut-on avoir $z - t = 1$? Ceci revient à résoudre $a^2 - b^2 - 2ab = 1$, soit $(a-b)^2 - 2b^2 = 1$. L'équation de Pell $M^2 - 2N^2 = 1$

a une infinité de solutions, donc pour $b = N$ et $a = N + M$, $z - t = 1$. De plus, $y = MN$ peut être arbitrairement grand, auquel cas $\frac{z-t}{y} = \frac{1}{MN}$ est arbitrairement petit, ce qui conclut.

Solution de l'exercice 8

Cet exercice peut se résoudre sans passer par une équation de Pell. Supposons qu'il existe des entiers x, y, z, w tels que $x^2 + y^2 = z^2$ et $x^2 - y^2 = w^2$. On peut supposer $x^2 + y^2$ minimal, ce qui implique que $pgcd(x, y) = 1$, quitte à diviser par celui-ci. En additionnant ces deux équations, on obtient $2x^2 = z^2 + w^2$, donc z et w ont la même parité, donc $z + w$ et $z - w$ sont pairs, et

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

Il est clair que $pgcd(x, (z + w)/2, (z - w)/2) = 1$, car $pgcd(x, y) = 1$. Alors d'après le théorème sur les triplets pythagoriciens utilisé à l'exercice précédent, il existe $a > b$ premiers entre eux tels que $z + w = 2(a^2 - b^2)$ et $z - w = 2 \times 2ab$, ou l'inverse. Dans tous les cas,

$$y^2 = \frac{z^2 - w^2}{2} = 4ab(a^2 - b^2).$$

Donc y est pair. On écrit $y = 2y'$, ce qui donne $y'^2 = ab(a - b)(a + b)$. Les entiers $a, b, a - b, a + b$ sont tous premiers entre eux deux à deux, donc ce sont tous des carrés. En particulier, a et b sont deux carrés dont la somme et la différence sont aussi des carrés. Et $a+b < 4ab(a-b)(a+b)$, donc $a + b < y < x^2 + y^2$, ce qui contredit la minimalité de $x^2 + y^2$. Donc il n'existe pas de quadruplet x, y, z, w satisfaisant les conditions de l'énoncé.

4 Tests de primalité

Comme son nom l'indique, un test de primalité est un algorithme, prenant en entrée un entier n, et qui vise à renvoyer le résultat OUI si n est un nombre premier, ou bien NON si n est un nombre composé. Il existe bien sûr de multiples tests de primalité, mais tous ne sont aussi efficaces les uns que les autres.

– Complexité d'un algorithme –

Un algorithme consiste en une suite d'instructions que l'on considère comme élémentaires, en lisant et écrivant des informations dans un espace dédié à cet effet. De telles instructions sont, par exemple, l'addition ou la multiplication de deux nombres à 1 chiffre. Par exemple, quand on effectue la multiplication 67×89, on apprend à l'école primaire à écrire quelque chose :

$$\begin{array}{ccccl}
 & & 6 & 7 & \\
\times & & 8 & 9 & \\
\hline
 & {\scriptstyle 5} & {\scriptstyle 6} & & \triangleright \text{ retenues} \\
 & & 4 & 3 & \\
{\scriptstyle 4} & {\scriptstyle 5} & & & \triangleright \text{ retenues} \\
 & 8 & 6 & & \\
\hline
{\scriptstyle 1} & {\scriptstyle 1} & & & \triangleright \text{ retenues} \\
5 & 9 & 6 & 3 &
\end{array}$$

Ici, on effectue 4 multiplications de nombres à 1 chiffre et 6 additions de nombres à 1 chiffre, soit un total de 10 instructions élémentaires. Par ailleurs, outre l'entrée et la sortie de l'algorithme, on a dû écrire 10 chiffres, entre produits partiels et retenues.

Une manière usuelle de mesurer l'efficacité d'un algorithme est de calculer sa *complexité temporelle* et sa *complexité spatiale*. Ici, notre algorithme de multiplication aurait donc des complexités temporelle et spatiale de 10.

En pratique, cependant, on ne connaît jamais exactement les performances de la machine sur laquelle on va travailler, ni la manière dont est gérée sa mémoire ou les opérations qui sont vraiment élémentaires pour le processeur que l'on utilise. Par exemple, si on avait travaillé en base 2, comme un ordinateur, notre multiplication aurait été :

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
\times & & & & & & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
\hline
 & & & & & & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
 & & & 1 & 0 & 0 & 0 & 0 & 1 & 1 & & & \\
 & & 1 & 0 & 0 & 0 & 0 & 1 & 1 & & & & \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & & & & & & \\
\hline
 & & & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & & & & \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}$$

et nos complexités temporelle et spatiale auraient bien sûr été différentes. Cependant, on peut montrer que, étant données deux machines $\mathcal{M}_1$ et $\mathcal{M}_2$ et sous des conditions « raisonnables » que l'on n'explicitera pas ici mais que l'on pourra considérer comme étant systématiquement vérifiées, il existe un entier $\mathbf{K}$ ayant la propriété suivante :

Théorème 2.4.1.
Soit $\mathcal{A}$ un algorithme, et soit t_i et s_i ses complexités temporelle et spatiale sur la machine $\mathcal{M}_i$. Alors $t_1 \leqslant \mathbf{K}(t_2+1)$, $s_1 \leqslant \mathbf{K}(s_2+1)$, $s_1 \leqslant \mathbf{K}(t_1+1)$ et $t_1 \leqslant 2^{\mathbf{K}(s_1+1)}$.

Notons ici que l'on aurait évidemment pu intervertir les rôles de $\mathcal{M}_1$ et $\mathcal{M}_2$, quitte à changer l'entier $\mathbf{K}$. Ainsi, on se contentera ci-dessous d'évaluer les complexités temporelle et spatiale d'un algorithme à constante multiplicative près. Pour ce faire, on pourra notamment recourir aux *notations de Landau*. Si $f : X \mapsto \mathbb{R}_{\geqslant 0}$ et $g : X \mapsto \mathbb{R}_{\geqslant 0}$ sont deux fonctions de même domaine X et à valeurs dans $\mathbb{R}_{\geqslant 0}$, on écrit $f \in \mathcal{O}(g)$ s'il existe un entier $\mathbb{K}$ tel que $f(x) \leqslant \mathbf{K}(g(x)+1)$ pour tout $x \in X$, et on écrit $f \in \Theta(g)$ si $f \in \mathcal{O}(g)$ et $g \in \mathcal{O}(f)$.

Exercice 1
Montrer que les algorithmes usuels d'addition et de soustraction de deux entiers m et n, étudiés à l'école primaire, ont des complexités temporelles en $\mathcal{O}(\log(m)+\log(n))$, puis montrer que les algorithmes de multiplication et de division euclidienne ont des complexités temporelles en $\mathcal{O}(\log(m)\log(n))$.

On peut en fait trouver des algorithmes de multiplication et de division euclidienne plus efficaces, c'est-à-dire de complexité temporelle moindre, tels que les algorithmes de Karatsuba, de Toom-Cook ou la transformée de Fourier rapide. Néanmoins, de tels algorithmes ne sont pas l'objet de l'étude ci-dessous, et nous nous contenterons dorénavant d'utiliser les algorithmes usuels.

– Algorithmes de factorisation : crible d'Ératosthène –

Une première manière de tester si un entier n est de tenter de trouver un diviseur propre de n, c'est-à-dire un entier d tel que $2 \leqslant d \leqslant n-1$ et $n \equiv 0 \pmod{d}$. En effet, si un tel entier exste, alors n est composé. Si, au contraire, il n'existe aucun tel entier, cela signifie que n est premier. Notons néanmoins que trouver un diviseur d éventuel pourrait tout à fait être plus difficile que montrer l'existence d'un tel d. D'autre part, si n est premier, on risque fort de ne faire qu'échouer à trouver un d adéquat, mais sans réussir à montrer qu'il n'existe pas.

Le premier algorithme en ce sens est bien sûr le crible d'Ératosthène, dont on donne ici une version très naïve et une version plus raisonnable.

Algorithme 3 : Crible d'Ératosthène

Argument(s) : n ▷ On veut tester si n est premier

$m \leftarrow n-1$ ▷ Version naïve

$m \leftarrow \lfloor \sqrt{n} \rfloor$ ▷ Version raisonnable

pour d **allant de** 2 **à** m **:**

  si $n \equiv 0 \pmod{d}$ **alors renvoyer** « n est composé ! » ▷ d divise n

renvoyer « n est premier ! » ▷ n n'a aucun diviseur propre $d \leqslant m$

Exercice 2
Montrer que le crible d'Ératosthène, quand on lui donne l'entier n comme argument, a une complexité temporelle en $\mathcal{O}(m \log(n)^2)$.

– Algorithmes de factorisation : algorithme heuristique de Pollard –

Un second algorithme, plus compliqué, et qui vise à découvrir un petit facteur de n, est l'algorithme de Pollard. Notons que cet algorithme peut nous permettre de trouver un diviseur propre de n, et donc de prouver que n est composé (si on a de la chance), mais ne permet certainement pas de prouver que n est premier.

Algorithme 4 : Algorithme de Pollard

Argument(s) : n ▷ On veut tester si n est premier

1: $u \leftarrow$ entier choisi au hasard entre 1 et $n-1$

2: $v \leftarrow v^2+1 \pmod{n}$

3: **tant que** $u \neq v$ **:** ▷ Boucle principale

4:   $d \leftarrow (v-u) \wedge n$

5:   **si** $2 \leqslant d \leqslant n-1$ **alors renvoyer** « n est composé ! » ▷ d divise n

6:   $u \leftarrow u^2+1 \pmod{n}$ et $v \leftarrow v^4+2v^2+2 \pmod{n}$

7: **renvoyer** « n est probablement premier ! »

En ligne 4, l'algorithme utilisé pour calculer le plus grand diviseur commun à $v-u$ et à n est la variante suivante de l'algorithme d'Euclide.

Exercice 3
Montrer que l'algorithme d'Euclide modifié permet calcule le plus grand diviseur commun aux entiers a et b en un temps $\mathcal{O}(\log(a)^2 + \log(b)^2)$.

Algorithme 5 : Algorithme d'Euclide modifié

Argument(s) : (a, b) ▷ On veut calculer $a \wedge b$
si $b = 0$ **alors renvoyer** a
$\hat{a} \leftarrow a$, $\hat{b} \leftarrow b$ et $d \leftarrow 1$
tant que $\hat{a} \equiv \hat{b} \equiv 0 \pmod 2$ **:** $d \leftarrow 2d$, $\hat{a} \leftarrow \hat{a}/2$ et $\hat{b} \leftarrow \hat{b}/2$ ▷ Boucle n°1
tant que $\hat{a} \neq 0$ **:** ▷ Boucle n°2
  tant que $\hat{a} \equiv 0 \pmod 2$ **:** $\hat{a} \leftarrow \hat{a}/2$
  tant que $\hat{b} \equiv 0 \pmod 2$ **:** $\hat{b} \leftarrow \hat{b}/2$
  si $\hat{a} \geqslant \hat{b}$ **alors** $\hat{a} \leftarrow (\hat{a} - \hat{b})/2$ **sinon** $\hat{b} \leftarrow (\hat{b} - \hat{a})/2$
renvoyer $\hat{b}\, d$

Notons f la fonction $x \mapsto x^2 + 1$ définie dans $\mathbb{Z}/n\mathbb{Z}$, u_1 la valeur initiale de la variable u, et u_k l'entier $f^{k-1}(u_1) \pmod n$, où f^k désigne l'itérée $k^{\text{ème}}$ de f.

Exercice 4
Montrer que, au début du $k^{\text{ème}}$ passage dans la boucle principale, les variables u et v valent respectivement u_k et u_{2k}. En déduire, si p est un facteur premier de n, que l'on rentrera au plus $2p$ fois dans la boucle principale, puis que l'algorithme de Pollard a une complexité temporelle en $\mathcal{O}(p \log(n)^2)$.

L'heuristique sur laquelle s'appuie l'algorithme de Pollard est la suivante : les entiers $u_1, u_2, \ldots$ sont censés être répartis « au hasard » dans $\mathbb{Z}/n\mathbb{Z}$. Par conséquent, après $2p$ passages dans la boucle principale, on aurait une probabilité au plus $2p/n \leqslant 2/\sqrt{n}$ de déclarer que n est probablement premier.

En outre, si on admet notre hypothèse de répartition au hasard, le paradoxe des anniversaires indique alors qu'il y a une probabilité écrasante (c'est-à-dire qui tend vers 1 lorsque p devient arbitrairement grand) que, parmi les entiers $u_1, u_2, \ldots, u_{\lfloor \sqrt{p} \log_2(p) \rfloor}$ qui soient égaux modulo p.

Exercice 5
Montrer que, s'il existe deux entiers i et j tels que $1 \leqslant i < j \leqslant \sqrt{p} \log_2(p)$ et $u_i \equiv u_j \pmod p$, alors l'algorithme a une complexité temporelle en $\mathcal{O}(\sqrt{p} \log(n)^3)$.

Une utilisation possible de l'algorithme de Pollard est donc la suivante. On lance k instances de l'algorithme en parallèle, et on autorise chacune à effectuer au plus $n^{1/4} \log_2(n)$ passages dans la boucle principale. En effet, si n est composé et si p est son plus petit facteur premier, alors $p \leqslant \sqrt{n}$, et l'hypothèse de répartition au hasard suggère de laisser l'algorithme passer $2\sqrt{p} \log_2(p) \leqslant n^{1/4} \log_2(n)$ dans la boucle principale. Si k est raisonnablement grand, on peut espérer très fort que notre hypothèse sera vérifiée au moins une fois. . .

– Algorithme probabiliste de Miller-Rabin –

Intéressons-nous maintenant à l'algorithme de Miller-Rabin. Comme l'algorithme de Pollard, cet algorithme nous permet d'affirmer avec certitude qu'un entier n est composé, ou bien de conclure que n est probablement premier. Il a néanmoins deux avantages sur l'algorithme de Pollard : tout d'abord, il va beaucoup plus vite ; en outre, si n est composé, on peut en fait montrer que l'on a au moins une chance sur deux de s'en rendre compte.

Algorithme 6 : Algorithme de Miller-Rabin

Argument(s) : n ▷ On veut tester si n est premier

$\ell \leftarrow 0$
$m \leftarrow n-1$
tant que $m \equiv 0 \pmod 2$ **:** $\ell \leftarrow \ell + 1$ et $m \leftarrow m/2$ ▷ Boucle n°1
$u \leftarrow$ entier choisi entre 1 et $n-1$
$v \leftarrow u$
tant que $m \neq 0$ **:** ▷ Boucle n°2
  si $m \equiv 1 \pmod 2$ **alors** $u \leftarrow uv \pmod n$
  $v \leftarrow v^2 \pmod n$ et $m \leftarrow \lfloor m/2 \rfloor$
si $u \equiv 1 \pmod n$ **alors renvoyer** « n est probablement premier ! »
sinon
  tant que $u \not\equiv -1 \pmod n$ et $\ell \neq 0$ **:** $u \leftarrow u^2 \pmod n$ et $\ell \leftarrow \ell - 1$ ▷ Boucle n°3
  si $u \equiv -1 \pmod n$ **alors renvoyer** « n est probablement premier ! »
  sinon renvoyer « n est composé ! » ▷ On sait que n est composé

Exercice 6
Montrer que l'algorithme de Miller-Rabin a une complexité temporelle en $\mathcal{O}(\log(n)^3)$.

Dans la suite, on notera α la valuation 2-adique de $n-1$, β l'entier $(n-1)/2^\alpha$ et $\hat{u}$ la valeur initiale de la variable u.

Exercice 7
Montrer que, après l'exécution de la boucle n°1, les variables ℓ et m valent respectivement α et β.

La boucle n°2 consiste en ce que l'on appelle une *exponentiation rapide* (ici, modulo n).

Exercice 8
Montrer que, après l'exécution de la boucle n°2, la variable u vaut $\hat{u}^\beta \pmod n$.

Exercice 9
Montrer que, si n est premier, alors l'algorithme de Miller-Rabin indique nécessairement que n est probablement premier.

Réciproquement, nous allons montrer que, si n est composé, alors l'algorithme de Miller-Rabin indiquera avec une probabilité raisonnable que n est bien composé. Deux notions cruciales pour aboutir à cet objectif sont les notions de groupe, d'anneau et de corps, que nous retrouverons plus tard.

Définition 2.4.2.
Un ensemble $\mathbb{K}$, muni d'une loi d'addition $(+)$ commutative et associative, est un *groupe commutatif* s'il existe un élément, que l'on notera 0, tel que :

— pour tout $x \in \mathbb{K}$, $0 + x = x$;

— pour tout $x \in \mathbb{K}$, il existe un élément $y \in \mathbb{K}$ tel que $x + y = 0$.

Plus succinctement, on dira que $(\mathbf{K}, +, 0)$ est un groupe commutatif.

Définition 2.4.3.
Un ensemble $\mathbb{K}$, muni de deux lois d'addition $(+)$ et de multiplication $(\times)$ associatives et commutatives, est un *anneau commutatif* s'il existe deux éléments, que l'on notera respectivement 0 et 1, tels que :

- $(\mathbb{K}, +, 0)$ soit un groupe ;
- pour tout $x \in \mathbb{K}$, $x \times 1 = x$;
- pour tous $x, y, z \in \mathbb{K}$, $x \times (x + y) = (x \times y) + (x \times z)$.

On dit alors que la multiplication est *distributive* sur l'addition, et on dira plus succinctement que $(\mathbf{K}, +, \times, 0, 1)$ est un anneau commutatif. En général, on notera $\mathbb{K}^*$ l'ensemble des éléments *inversibles* de $\mathbb{K}$, c'est-à-dire l'ensemble $\{x \in \mathbb{K} \,:\, \exists y \in \mathbb{K}$ tel que $x \times y = 1\}$.

Définition 2.4.4.
Un anneau commutatif $(\mathbb{K}, +, \times, 0, 1)$ est un *corps commutatif* si tout élément $x \neq 0$ de $\mathbb{K}$ est un élément inversible.

Exercice 10
Soit p un nombre premier. Montrer que $(\mathbb{Z}/p\mathbb{Z}, +, \times, 0, 1)$ est un corps commutatif.

Exercice 11
Soit $(\mathbb{K}, +, \times, 0, 1)$ un corps commutatif et soit $P(X)$ un polynôme de degré $d \geqslant 0$, à coefficients dans $\mathbb{K}$. Montrer que P a au plus d racines, comptées avec leur multiplicité, et que, si $P(X)$ divisible par un polynôme $Q(X)^2$ non constant, alors $Q(X)$ divise à la fois $P(X)$ et $P'(X)$.

Exercice 12
Soit a et b deux entiers premiers avec n, d'ordres respectifs ω_a et ω_b modulo n. Montrer que, si ω_a et ω_b sont premiers entre eux, alors ab est d'ordre $\omega_a\omega_b$.

Exercice 13
Soit p un nombre premier. Montrer qu'il existe un entier k d'ordre $p - 1$ modulo p et d'ordre $p(p - 1)$ modulo p^2.

Supposons maintenant que n est composé. On dira qu'un entier $x \in Z/n\mathbb{Z}$ est *loyal* si choisir $u = x$ en ligne 6 montre que n est composé, et que x est *déloyal* sinon.

Exercice 14
Montrer que, s'il existe un nombre premier p tel que $n \equiv 0 \pmod{p^2}$, alors il existe au plus $(n - 1)/p$ nombres déloyaux.

Exercice 15
Montrer que, si n est le produit de $k \geqslant 2$ nombres premiers $p_1, \ldots, p_k$ deux à deux distincts, alors il existe au plus $(n - 1)/2$ nombres déloyaux.

Exercice 16
Montrer que, si n est composé, alors l'algorithme de Miller-Rabin a au moins une chance sur deux d'indiquer que n est effectivement composé.

– Test de Lehmer et certificat de Pratt –

On dispose maintenant d'algorithmes efficaces permettant de détecter, avec une probabilité aussi grande qu'on le souhaite, les nombres composés, et qui ne déclarent comme composés que des nombres qui sont effectivement composés. Réciproquement, on souhaiterait disposer d'un algorithme qui nous permette de vérifier de manière certaine qu'un nombre est effectivement premier.

Le test de Lehmer, que l'on présente ci-dessous, est un premier pas dans cette voie.

Exercice 17
Soit n un entier et soit $p_1, \ldots, p_k$ les facteurs premiers de $n-1$. Montrer que l'entier n est premier si et seulement s'il existe un entier $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $x^{n-1} \equiv 1 \pmod n$ et tel que, pour tout $\ell \leqslant k$, $x^{(n-1)/p_\ell} \not\equiv 1 \pmod n$.

Ces tests peuvent alors être utilisés dans le cadre de ce que l'on appelle un certificat de Pratt, et qui est défini récursivement comme suit.

Définition 2.4.5.
Soit p un nombre premier et $q_1 \cdots q_k$ une factorisation de $p-1$ en nombres premiers, avec $k \geqslant 1$ si et seulement si $p \geqslant 3$. Soit également x un entier d'ordre $p-1$ modulo p.

Un *certificat de Pratt* de p est un tuple $\mathbf{C}(p)$ défini récursivement par

$$\mathbf{C}(2) = \langle 2 \rangle, \mathbf{C}(3) = \langle 2 \rangle \text{ et } \mathbf{C}(p) = \langle p, x, \mathbf{C}(q_1), \mathbf{C}(q_2), \ldots, \mathbf{C}(q_k) \rangle \text{ si } p \geqslant 4.$$

On encode ci-dessous chaque entier en base 2. Ainsi, quitte à changer d'unités d'espace, on suppose que l'encodage d'un entier $n \geqslant 2$ prend une place au plus $\log_2(n)$, et que l'encodage de chaque symbole $\langle$ ou $\rangle$ et de chaque virgule prend une place 1. De manière analogue, quitte à changer d'unité de temps, on suppose que calculer $m+n$ et $m-n$ prend un temps au plus $\log_2(m) + \log_2(n)$, et que calculer mn et la division euclidienne de m par n prend un temps au plus $\log_2(m)\log_2(n)$.

Exercice 18
Montrer que le certificat de Pratt d'un nombre premier p prend une place $\lambda(p) \leqslant 6\log_2(p)^2$.

Exercice 19
Montrer qu'il existe un algorithme permettant de vérifier, étant donnés un entier n et un tuple $\mathbf{T}$, si $\mathbf{T}$ est un certificat de Pratt de n en temps $\mathcal{O}(\log(n)^5)$.

Évidemment, si les certificats de Pratt ont le double avantage d'être courts et d'être faciles à vérifier, il n'est a priori pas évident du tout d'en construire un. En particulier, discuter de la primalité de n nécessite ici de savoir factoriser $n-1$. Cela semble peu efficace, puisque l'on avait mentionné plus haut que tester si un nombre n est premier avait de fortes chances d'être plus facile que de factoriser n.

– Algorithme AKS –

L'algorithme AKS a été inventé en 2003 par Manindra Agrawal, Neeraj Kayal et Nitin Saxena ; le premier était le professeur d'informatique des deux autres, alors étudiants en licence. Il s'agit d'un algorithme déterministe permettant de tester si un entier n est premier en

Algorithme 7 : Algorithme AKS

Argument(s) : n ▷ On veut tester si n est premier

pour b **allant de** 2 **à** $\log_2(n)$ **:** ▷ Boucle n°1

  si $n^{1/b}$ est un entier **alors renvoyer** « n est composé ! »

$r \leftarrow 2$ ▷ Ci-dessous, on note $\omega_r(n)$ l'ordre de n modulo r

tant que $n \not\equiv 0 \pmod{r}$ et $\omega_r(n) \leqslant 4\log_2(n)^2$ **:** $r \leftarrow r+1$ ▷ Boucle n°2

si $r^2 \geqslant n$ **alors renvoyer** « n est premier ! »

sinon si $n \equiv 0 \pmod{r}$ **alors renvoyer** « n est composé ! »

pour a **allant de** 1 **à** $2\sqrt{r}\log_2(n)$ **:** ▷ Boucle n°3

  si $(X+a)^n \not\equiv X^n + a \pmod{X^r - 1, n}$ **alors renvoyer** « n est composé ! »

renvoyer « n est premier ! »

temps $\mathcal{O}(\log(n)^{12})$. Cet algorithme est affreusement lent en pratique, mais il constitue néanmoins le seul exemple connu à ce jour de test de primalité fonctionnant en temps polynomial en $\log(n)$. L'algorithme est le suivant.

Dans un premier temps, nous allons étudier la complexité de cet algorithme. Nous montrerons ensuite qu'il renvoie toujours un résultat correct.

Exercice 20
Montrer que chaque exécution de la boucle n°1 prend un temps $\mathcal{O}(\log(n)^4)$.

Exercice 21
Montrer que chaque exécution de la boucle n°2 prend un temps $\mathcal{O}(\log(n)^3)$.

Exercice 22
Montrer que chaque exécution de la boucle n°3 prend un temps $\mathcal{O}(r^2\log(n)^3)$.

Une clé de l'efficacité de l'algorithme AKS réside dans le fait que l'entier r obtenu à la fin de la boucle n°2 n'est pas trop grand. C'est ce que l'on peut montrer en procédant comme suit.

Exercice 23
Pour tout entier $n \in \mathbb{N}^*$, on note $\ell(n)$ le plus petit multiple commun à tous les entiers $k \leqslant n$ et $\hat{\ell}(n)$ le produit $n\binom{2n}{n}$. Montrer que que $\hat{\ell}(n)$ divise $\ell(2n)$ et que, dès lors que $n \geqslant 4$, $\hat{\ell}(n) \geqslant 2^{2n}$. En déduire que $\ell(n) \geqslant 2^n$ pour tout entier $n \geqslant 7$.

Exercice 24
Soit $n \geqslant 2$ un entier. Montrer qu'il existe un entier $r \leqslant \lceil 16\log_2(n)^5 \rceil$ tel que l'ordre de n modulo r soit un entier $\omega_r(n) > 4\log_2(n)^2$.

Exercice 25
Montrer que l'algorithme AKS a une complexité temporelle en $\mathcal{O}(\log(n)^{16.5})$.

Nous allons maintenant montrer que le résultat de l'algorithme AKS est correct.

Exercice 26
Montrer que, si n est un nombre premier, alors l'algorithme AKS indique bien que n est premier.

Réciproquement, il ne nous reste plus qu'à montrer le résultat suivant.

Théorème 2.4.6 (Théorème AKS)**.**
Soit $n \geqslant 2$ un entier, soit p le plus petit facteur premier de n, soit $r < p$ un entier tel que n soit d'ordre $\omega_r(n) > 4\log_2(n)$ modulo r, et soit $H(X)$ un facteur irréductible du polynôme cyclotomique $\phi_r(X)$ dans $\mathbb{Z}/p\mathbb{Z}$. Si $(X+a)^n \equiv X^n + a \pmod{H(X), p}$ pour tout $a \leqslant 2\sqrt{r}\log_2(n)$, alors n est une puissance de p.

On va procéder par l'absurde. On supposera désormais que les entiers n, p et r et le polynome $H(X)$ sont fixés une fois pour toutes, de sorte que n ne soit pas une puissance de p mais que $(X+a)^n \equiv X^n + a \pmod{H(X), p}$ pour tout $a \leqslant 2\sqrt{r}\log_2(n)$. On notera d le degré de $H(X)$ et λ l'entier $\lfloor 2\sqrt{r}\log_2(n)\rfloor$.

Montrons tout d'abord que l'on peut travailler directement modulo p et $H(X)$ sans se poser trop de questions.

Exercice 27
Soit $\mathcal{F}$ l'ensemble des éléments de $(\mathbb{Z}/p\mathbb{Z})[X]$, considérés modulo $H(X)$. Montrer que $\mathcal{F}$, muni des lois $+$ et $\times$ usuelles, est un corps commutatif.

Puisque les éléments de $\mathcal{F}$ sont des classes de congruences de polynômes en la variable X, on se restreindra ci-dessous, dès que l'on considérera des polynômes à coefficients dans $\mathcal{F}$, à prendre des polynôme en la variable T.

Exercice 28
Soit $(G, 0, +)$ un groupe commutatif de cardinal k. Montrer que, pour tout élément x de G, on a $k\,x = 0$.

Exercice 29
Montrer que X est un élément de $\mathcal{F}^*$ d'ordre r.

On introduit ensuite la notion d'introspection, due aux auteurs de l'algorithme AKS.

Définition 2.4.7.
On dit qu'un entier k est *introspectif* pour un polynôme $P(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ si $P(X^k) \equiv P(X)^k \pmod{H(X), p}$.

Exercice 30
Montrer que, si k et ℓ sont introspectifs pour un même polynôme $P(X)$, alors $k\,\ell$ est également introspectif pour $P(X)$. Montrer ensuite que, si k est introspectif pour deux polynômes $P(X)$ et $Q(X)$, alors k est également introspectif pour $PQ(X)$.

Dans la suite, on notera $\mathcal{G}_1$ l'ensemble des entiers de la forme $n^{\gamma_1}p^{\gamma_2}$ et $\mathcal{H}_1$ l'ensemble des polynômes de $(\mathbb{Z}/p\mathbb{Z})[X]$ de la forme $\prod_{a_1}^{\lambda}(X+a)^{\theta_a}$. On note également $\mathcal{G}_2$ l'ensemble des résidus des éléments de $\mathcal{G}_1$ modulo r, et $\mathcal{H}_2$ l'ensemble des résidus des éléments de $\mathcal{H}_1$ modulo $H(X)$. Enfin, on pose $t = |\mathcal{G}_2|$.

Exercice 31
Montrer que tout élément de $\mathcal{G}_1$ est introspectif pour tout élément de $\mathcal{H}_1$.

Exercice 32
Monter que, si $A(X)$ et $B(X)$ sont deux éléments distincts de $\mathcal{H}_1$ de degré strictement inférieur à t, alors $A(X) \not\equiv B(X) \pmod{H(X)}$, puis en déduire que $|\mathcal{H}_2| \geqslant \binom{t+\lambda-1}{\lambda}$.

Exercice 33
En considérant l'ensemble $\mathcal{G}' = \{n^i \cdot p^j \ : \ 0 \leqslant i, j \leqslant \sqrt{t}\}$, montrer que $|\mathcal{H}_2| \leqslant n^{3\sqrt{t}/2}$.

Exercice 34
Montrer le Théorème 2.4.6.

– Solutions des exercices –

Solution de l'exercice 1
Si l'on travaille en base b, alors les nombres m et n sont des nombres à au plus $c_m = \log_b(m)+1$ et $c_n = \log_b(n) + 1$ chiffres. En supposant que $m \leqslant n$, on a donc $c_m \leqslant c_n$ Lors du calcul de $m+n$ ou de $m-n$, on effectue au plus $2c_n$ additions ou soustractions de nombres à un chiffre, en tenant compte des retenues, d'où un coût de $\mathcal{O}(c_n) = \mathcal{O}(\log(m) + \log(n))$.

De même, lors du calcul de $m \times n$, on effectue d'abord $c_m\, c_n$ multiplications de nombres à un chiffre, puis c_m additions en chaîne de nombres à au plus $c_m + c_n$ chiffres, d'où un coût de $\mathcal{O}(c_m^2 + c_m\, c_n) = \mathcal{O}(\log(m)\log(n))$.

Enfin, lors de la division euclidienne de n par m, on va successivement soustraire à n un nombre de la forme $k\, b^\ell\, m$, avec $1 \leqslant k \leqslant b-1$ et $\ell = c_n, c_n - 1, \ldots, 0$. Chaque soustraction a en fait un coût de l'ordre de $\mathcal{O}(bc_m)$, donc le coût total de la division est de $\mathcal{O}(bc_m c_n) = \mathcal{O}(\log(m)\log(n))$.

Solution de l'exercice 2
Pour chaque entier $d \leqslant m$, on teste si $n \equiv 0 \pmod d$ en temps $\mathcal{O}(\log(d)\log(n))$, donc $\mathcal{O}(\log(n)^2)$. On effectue au plus m de ces tests, d'où le résultat.

Solution de l'exercice 3
Si les entiers a et b sont écrits en binaire, alors la boucle n°1 permet, en temps $\mathcal{O}(\log(a)+\log(b))$, de se ramener au cas où $a \wedge b$ est un entier impair. On supposera désormais que c'est le cas.

Par la suite, chaque exécution de la boucle n°2 permet, en un temps $\mathcal{O}(\log(\hat{a})+\log(\hat{b}))$ donc $\mathcal{O}(\log(a)+\log(b))$, de diminuer la quantité $\log(\hat{a})+\log(\hat{b})$ de 1, sans modifier la valeur de $\hat{a} \wedge \hat{b}$. Cela montre que l'algorithme renvoie bien un résultat correct en temps $\mathcal{O}((\log(a)+\log(b))^2) = \mathcal{O}(\log(a)^2 + \log(b)^2)$.

Solution de l'exercice 4
Une récurrence immédiate montre que, au début du $k^{\text{ème}}$ passage dans la boucle principale, les variables u et v valent effectivement u_k et u_{2k}.

Puis, en vertu du principe des tiroirs, il existe deux entiers i et j tels que $1 \leqslant i < j \leqslant p+1$ et $u_i \equiv u_j \pmod p$. Mais alors, pour $k = (j-i)\lceil i/(j-i) \rceil \leqslant j-1 \leqslant p$, on a nécessairement $u_k \equiv u_{2k} \pmod p$, ce qui montre bien que l'on rentre au plus $2p$ fois dans la boucle principale.

Enfin, chaque passage dans la boucle principale prend un temps $\mathcal{O}(\log(n)^2)$, ce qui conclut.

Solution de l'exercice 5
De même que précédemment, s'il existe deux entiers i et j tels que $1 \leqslant i < j \leqslant \sqrt{p}\log_2(p)$ et $u_i \equiv u_j \pmod p$, alors on rentre au plus $2(j-1)$ fois dans la boucle principale. Puisque $j - 1 \leqslant \sqrt{p}\log_2(p) \leqslant \sqrt{p}\log_2(n)$ et que chaque passage dans la boucle principale prend un temps $\mathcal{O}(\log(n)^2)$, on a bien une complexité temporelle en $\mathcal{O}(\sqrt{p}\log(n)^3)$.

Solution de l'exercice 6
La boucle n°1 prend un temps $\mathcal{O}(\log(n))$. Puis on rentre au plus $\log_2(n)$ fois dans la boucle n°2, ce qui prend un temps $\mathcal{O}(\log(n)^2)$ à chaque fois. De même, en ligne 10, on a $\ell \leqslant \log_2(n)$, et on rentre donc au plus $\log_2(n)$ fois dans la boucle n°3, ce qui prend un temps $\mathcal{O}(\log(n)^2)$ à chaque fois. Au total, l'algorithme prend donc un temps $\mathcal{O}(\log(n)^3)$.

Solution de l'exercice 7
Une récurrence immédiate montre que, après la $k^{\text{ème}}$ exécution de la boucle n°1, on a $\ell = k$ et $m = (n-1)/2^k$. Par conséquent, on exécute cette boucle α fois, à l'issue desquelles $\ell = \alpha$ et $m = \beta$.

Solution de l'exercice 8
Pour tout entier $k \geqslant 1$, on note β_k l'unique entier tel que $0 \leqslant \beta_k < 2^k$ et $\beta \equiv \beta_k \pmod{2^k}$. Une récurrence tout aussi immédiate que précédemment montre que, après la $k^{\text{ème}}$ exécution de la boucle n°2, on a $u \equiv \hat{u}^{\beta_k} \pmod{n}$, $v \equiv \hat{u}^{2^k} \pmod{n}$ et $m = \lfloor \beta/2^k \rfloor$. Par conséquent, on passe $k = \lfloor \log_2(\beta) \rfloor + 1$ fois dans la boucle. Après ce passage, on a bien $\beta_k = \beta$, donc $u \equiv \hat{u}^\beta \pmod{n}$.

Solution de l'exercice 9
Si n est premier, alors $\hat{u}^{n-1} \equiv \hat{u}^{2^\alpha \beta} \equiv 1 \pmod{n}$. Soit alors ℓ le plus petit entier naturel tel que $\hat{u}^{2^\ell \beta} \equiv 1 \pmod{n}$. Si $\ell = 0$, l'algorithme indique déjà en ligne 9 que n est probablement premier.

Si $\ell \geqslant 1$, soit $x \equiv \hat{u}^{2^{\ell-1}\beta} \pmod{n}$. Alors $x \not\equiv 1 \pmod{n}$ mais $x^2 \equiv 1 \pmod{n}$, donc n divise $x^2 - 1 = (x-1)(x+1)$. Puisque n est premier et ne divise pas $x-1$, c'est donc que n divise $x+1$, ce qui signifie que $x \equiv -1 \pmod{n}$. Par conséquent, l'algorithme indique dans ce cas aussi que n est probablement premier.

Solution de l'exercice 10
Il est clair que $(\mathbb{Z}/p\mathbb{Z}, +, \times, 0, 1)$ est un anneau commutatif. D'autre part, tout entier $x \not\equiv 0 \pmod{p}$ est nécessairement premier avec p, donc le théorème de Bézout indique qu'il existe un entier y tel que $x\,y \equiv 1 \pmod{p}$, ce qui montre que x est inversible, et conclut donc l'exercice.

Solution de l'exercice 11
On montre, par récurrence sur $d \geqslant 0$, que P a au plus d racines. Soit r une racine éventuelle, et soit $Q(X)$ et $R(X)$ le quotient et le reste dans la division euclidienne de $P(X)$ par $X - r$. Alors $P(X) = (X-r)Q(X) + R(X)$ et R est de degré au plus 0, donc R est le polynôme constant égal à $R(r) = P(r) - (r-r)Q(r) = 0$. Cela signifie que $P(X) = (X-r)Q(X)$, et puisque Q a au plus $d-1$ racines, la première partie de l'exercice s'ensuit.

D'autre part, si un polynôme $T(X)^2$ divise P, alors on peut en fait écrire $P(X) = T(X)^2 U(X)$, et alors $T(X)$ divise également $P'(X) = T(X)(2T'(X)U(X) + T(X)U'(X))$, ce qui conclut.

Solution de l'exercice 12
Si $\omega_a = 1$ ou $\omega_b = 1$, le résultat est évident. On suppose donc que $\omega_a > 1$ et $\omega_b > 1$. Soit alors p un facteur premier de ω_a. Puisque ω_a et ω_b sont premiers entre eux, on en déduit que ω_a ne divise pas $\omega_a\omega_b/p$. Cela montre que

$$(ab)^{\omega_a\omega_b/p} \equiv a^{\omega_a\omega_b/p}(b^{\omega_b})^{\omega_a/p} \equiv a^{\omega_a\omega_b/p} \not\equiv 1 \pmod{n},$$

donc que ω_{ab} ne divise pas $\omega_a\omega_b/p$. De même, si q est un facteur premier de ω_b, ω_{ab} ne divise pas $\omega_a\omega_b/q$. Cependant, puisque $(ab)^{\omega_a\omega_b} \equiv (a^{\omega_a})^{\omega_b}(b^{\omega_b})^{\omega_a} \equiv 1 \pmod{n}$, on sait également que ω_{ab} divise $\omega_a\omega_b$. On en conclut que $\omega_{ab} = \omega_a\omega_b$.

Solution de l'exercice 13

On montre tout d'abord que, si a et b sont deux entiers d'ordres α et β modulo n, il existe un entier c d'ordre $\gamma = \alpha \wedge \beta$. En effet, pour tout facteur premier p de γ, on pose

$$\alpha_p = \begin{cases} p^{v_p(\alpha)} & \text{si } v_p(\alpha) \geqslant v_p(\beta) \\ 1 & \text{sinon} \end{cases} \text{ et } \beta_p = \begin{cases} 1 & \text{si } v_p(\alpha) \geqslant v_p(\beta) \\ p^{v_p(\beta)} & \text{sinon.} \end{cases}$$

Puis on pose $\hat{\alpha} = \prod_{p|\gamma} \alpha_p$ et $\hat{\beta} = \prod_{p|\gamma} \beta_p$. Alors $\hat{\alpha}$ et $\hat{\beta}$ sont premiers entre eux, $\gamma = \hat{\alpha}\,\hat{\beta}$ et les entiers $\hat{a} = a^{\alpha/\hat{\alpha}}$ et $\hat{b} = b^{\beta/\hat{\beta}}$ sont respectivement d'ordres $\hat{\alpha}$ et $\hat{\beta}$ modulo n. Par conséquent, il existe nécessairement un entier, disons ρ_n, d'ordre maximal ϖ_n modulo n.

Remarquons alors que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est une racine du polynôme $P(X) = X^{\varpi_p+1} - X$, qui est donc de degré $\varpi_p + 1 \geqslant p$. Le petit théorème de Fermat indique que ϖ_p divise $p-1$. On en déduit que $\varpi_p = p - 1$.

D'autre part, pour tout entier $a \in \{1, 2, \ldots, p-1\}$, puisque $(a\,p+1) \not\equiv 1 \pmod{p^2}$ et que $(a\,p+1)^p \equiv \sum_{k=0}^{p} \binom{p}{k} a^k\, p^k \equiv \binom{p}{p} a\,p + 1 \equiv 1 \pmod{p^2}$, on sait que $a\,p+1$ est un entier d'ordre p modulo p^2. Cela montre que $p-1$ et p sont deux diviseurs de ϖ_{p^2}, qui divise $p(p-1) = \varphi(p^2)$, et qui vaut donc $p(p-1)$.

On pose alors $k = \rho_{p^2}$, et on note κ l'ordre de k modulo p. Il existe un entier a tel que $k^\kappa \equiv a\,p + 1 \pmod{p^2}$, ce qui montre que $k^{p\,\kappa} \equiv 1 \pmod{p^2}$. On en déduit que $p(p-1)$ divise $p\,\kappa$, ce qui signifie que $\kappa = p - 1$ et conclut l'exercice.

Solution de l'exercice 14

. Tout d'abord, nul entier x n'est déloyal s'il n'est premier avec n. Il suffit donc de montrer que, parmi les $\varphi(n)$ éléments de $(\mathbb{Z}/n\mathbb{Z})^*$, il y en a au plus $\varphi(n)/p$ qui sont déloyaux. Soit a un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre $p(p-1)$ modulo p^2 et soit $\mathcal{D}$ l'ensemble des éléments déloyaux.

Si x et x' sont deux éléments déloyaux, et pour tous les entiers $k \leqslant k'$ compris entre 0 et $p-1$, si $a^k x = a^{k'} x'$, alors $a^{(k'-k)(n-1)} \equiv x^{n-1}/(x')^{n-1} \equiv 1 \pmod{p^2}$. Cela montre que $p(p-1)$, donc en particulier p, divise $(k'-k)(n-1)$, de sorte que $k = k'$ et donc que $x = x'$. On en déduit que $n - 1 \geqslant \varphi(n) \geqslant p|\mathcal{D}|$, ce qui conclut.

Solution de l'exercice 15

Une fois encore nul entier ayant un facteur commun avec n n'est déloyal. On va donc montrer que, parmi les $\varphi(n)$ éléments de $(\mathbb{Z}/n\mathbb{Z})^*$, il y en a au plus $\varphi(n)/p$ qui sont déloyaux.

Soit p un facteur premier de n. D'après le théorème Chinois et l'exercice 13, il existe un élément k de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre $p-1$ modulo p et tel que $k \equiv 1 \pmod{n/p}$.

Pour tout facteur premier q de n, y compris p, et tout élément x de $(\mathbb{Z}/n\mathbb{Z})^*$, on note $\ell(q,x)$ la valuation 2-adique de l'ordre de x modulo q. Remarquons alors que $\ell(p,x) \neq \ell(p,k\,x)$ et que $\ell(q,x) = \ell(q,k\,x)$ pour tout $q \neq p$.

Or, on constate aisément que, si x est déloyal, les entiers $\ell(q,x)$ ne dépendent pas de q. Par conséquent, si x est déloyal, $k\,x$ ne l'est pas. Ainsi, au plus un élément de $(\mathbb{Z}/n\mathbb{Z})^*$ sur deux est déloyal, ce qui conclut l'exercice.

Solution de l'exercice 16

Si n est composé, alors il existe au plus $(n-1)/2$ nombres déloyaux compris entre 1 et $n-1$, que n soit divisible par le carré d'un nombre premier ou pas. Puisque l'entier x est choisi au hasard parmi les entiers compris entre 1 et $n-1$, le résultat s'ensuit.

Solution de l'exercice 17
On souhaite en fait montrer que n est premier si et seulement s'il existe un entier d'ordre $n-1$ modulo n. Si tel est le cas, alors $n-1$ divise $\varphi(n)$, donc n est bien premier. Réciproquement, si n est premier, l'exercice 13 montre qu'il existe bien un élément d'ordre $n-1$, ce qui conclut.

Solution de l'exercice 18
Nous allons procéder par récurrence (forte, bien sûr). Remarquons déjà que $\lambda(2) \leqslant \lambda(3) \leqslant 6 \leqslant \Lambda(2) \leqslant \Lambda(3)$. et que $\lambda(3) \leqslant 4 \leqslant \Lambda(3)$.

Comme $p-1$ est nécessairement un entier pair différent de 2, on sait que $2 \leqslant k \leqslant \log_2(p)$. En outre, puisque $\sum_{i=1}^k \log_2(q_i) = \log_2(p)$, que la fonction $x \mapsto x^2$ est convexe et que $1 \leqslant \log_2(q_i)$ pour tout $i \leqslant k$, on sait également que

$$\sum_{i=1}^k \log_2(q_i)^2 \leqslant (k-1) + (\log_2(p)+1-k)^2 \leqslant (\log_2(p)-1) + (\log_2(p)-1)^2 = \log_2(p)^2 - \log_2(p).$$

On conclut alors en vérifiant, pour tout nombre premier $p \geqslant 5$, que

$$\lambda(p) \leqslant \log_2(x) + \log_2(p) + k + 3 + \textstyle\sum_{i=1}^k \lambda(q_i) \leqslant 6\log_2(p) + \sum_{i=1}^k \Lambda(q_i) \leqslant \Lambda(p).$$

Solution de l'exercice 19
Notre algorithme fonctionne comme suit, pour $n \geqslant 4$: on vérifie d'abord que $n = q_1 q_2 \cdots q_k + 1$, puis on vérifie que $\mathbf{C}(q_1), \ldots, \mathbf{C}_(q_k)$ sont bien des certificats de Pratt, et enfin on vérifie que x passe le test de Lehmer.

Soit alors $\tau(n, \mathbf{T})$ le temps requis pour vérifier si un tuple $\mathbf{T}$ est un certificat de Pratt de n. Quitte à rechanger encore une fois d'unité de temps, on peut supposer que $\tau(n, \mathbf{T})$ vaut au plus 1 pour tout $n \leqslant 15$. On va maintenant montrer par récurrence que $\tau(n, \mathbf{T}) \leqslant T(n)$ pour tout $n \geqslant 2$, où l'on a posé $T(n) = 2\log_2(n)^4$. Notons que, si $n \leqslant 15$, c'est déjà le cas, et qu'il suffit donc de s'intéresser au cas où $n \geqslant 16$.

La première phase de l'algorithme consiste à calculer $n-1$, donc on effectue alors successiveent les divisions euclidiennes par $q_1, q_2, \ldots, q_k$, sous réserve que chaque q_i soit inférieur à n. Cela prend un temps au plus $k\log_2(n)^2$, c'est-à-dire au plus $\log_2(n)^3$, puisque l'on rappelle que $2 \leqslant k \leqslant \log_2(n)$. Par conséquent, si $n \neq q_1 \cdots q_k + 1$, on a déjà $\tau(n, \mathbf{T}) \leqslant \log_2(n)^3 \leqslant T(n)$. On suppose donc désomais que $n = q_1 \cdots q_k + 1$.

La deuxième phase consiste à vérifier des certificats de Pratt de $q_1, \ldots, q_k$, ce qui prend un temps au plus $T(q_1) + \ldots + T(q_k)$. Puis, si cette phase est un succès, on calcule, pour tout $i \leqslant k$, les entiers $(n-1)/q_i$ en temps $\log_2(n)^2$, et $x^{(n-1)/q_i} \pmod n$ en temps $2\log_2(n)^3$, grâce à l'algorithme d'exponentiation rapide modulo n. Enfin, on calcule $x^{n-1} \pmod n$ en temps $2\log_2(n)^3$ également. On déduit de tout ceci que $\tau(n, \mathbf{T}) \leqslant (3+k)\log_2(n)^3 + \sum_{i=1}^k T(q_i)$.

Or, la fonction $x \mapsto x^4$ est convexe, et l'on sait que $1 \leqslant \log_2(q_i)$ pour tout $i \leqslant k$ et que $\sum_{i=1}^k \log_2(q_i) \leqslant \log_2(n)$, de sorte que $\sum_{i=1}^k \log_2(q_i)^4 \leqslant (k-1) + (\log_2(n)+1-k)^4$. Il ne nous reste donc plus qu'à montrer que $T(n) \geqslant \hat{\tau}(n,k)$, où l'on a posé

$$\hat{\tau}(n,k) = (3+k)\log_2(n)^3 + 2(k-1) + 2(\log_2(n)+1-k)^4.$$

Puisque $2 \leqslant k \leqslant \log_2(n)$ et que $k \mapsto \hat{\tau}(n,k)$ est une fonction convexe, il suffit de vérifier que $\hat{\tau}(n,2) \leqslant T(n)$ et que $\hat{\tau}(n,\log_2(n)) \leqslant T(n)$. Or, on a supposé que $n \geqslant 16$, c'est-à-dire que $\log_2(n) \geqslant 4$. On conclut alors en vérifiant que

$$\begin{aligned}
\hat{\tau}(n,2) &= 5\log_2(n)^3 + 2 + 2(\log_2(n)-1)^4 \\
&= T(n) + 3(4-\log_2(n))\log_2(n)^2 + 4(1-2\log_2(n)) \\
&\leqslant T(n) \\
\hat{\tau}(n,\log_2(n)) &= 3\log_2(n)^3 + \log_2(n)^4 + 2\log_2(n) \\
&\leqslant \log_2(n)^4 + 4\log_2(n)^3 \\
&\leqslant T(n).
\end{aligned}$$

Solution de l'exercice 20

Soit $b \leqslant \log_2(n)$ un entier, et soit $n_b = \lfloor n^{1/b} \rfloor$. Encodons l'entier n_b sur $\log_2(n)$ bits. Pour tout $k \geqslant 1$, on peut déterminer en k mises à la puissance b les k bits de poids fort de n_b. Chaque mise à la puissance b peut être effectuée en temps $\mathcal{O}(\log(n)^2\log(b))$, sous réserve de s'arrêter dès qu'un résultat intermédiaire dépasse n. Puique $b \leqslant n$, on calcule donc n_b en temps $\mathcal{O}(\log(n)^4)$, et on teste en temps $\mathcal{O}(\log(n)^3)$ si $n_b^b = n$. Le résultat désiré s'ensuit.

Solution de l'exercice 21

Posons $\ell = \lfloor 4\log_2(n) \rfloor$. On peut tester sans finesse si $\omega_r(n) \leqslant \ell$ en calculant $n^k \pmod r$ successivement pour $k = 1, 2, \ldots, \ell$ et en testant à chaque fois si $n^k \equiv 1 \pmod r$. On procède donc à au plus ℓ multiplications de complexité $\mathcal{O}(\log(r)^2)$ chacune, ce qui prend bien un temps $\mathcal{O}(\log(r)^2\log(n))$. Puisque $r \leqslant n$ par construction, le résultat s'ensuit.

Solution de l'exercice 22

Soit s l'unique entier tel que $0 \leqslant s \leqslant r-1$ et $n \equiv s \pmod r$. Il s'agit ici de calculer $(X+a)^n \pmod{X^r - 1, n}$ et de vérifier si le résultat obtenu est égal à $X^s + a$. L'algorithme d'exponentiation rapide nous permet de n'utiliser que $\mathcal{O}(\log(n))$ multiplications de polynômes modulo n et $X^r - 1$.

Chaque multiplication nécessite de multiplier r^2 paires de coefficients dans $\mathbb{Z}/n\mathbb{Z}$, pour un coût unitaire de $\mathcal{O}(\log(n)^2)$, et d'effectuer $\mathcal{O}(r^2)$ additions dans $\mathbb{Z}/n\mathbb{Z}$, pour un coût unitaire de $\mathcal{O}(\log(n))$. Chaque exécution de la boucle n°3 prend donc un temps $\mathcal{O}(r^2\log(n)^3)$.

Solution de l'exercice 23

Soit p un nombre premier et soit k le plus grand entier tel que $p^k \leqslant 2n$. Pour tout entier $i \leqslant k$, on sait que $\lfloor (2n)/p^i \rfloor \leqslant 2\lfloor n/p^i \rfloor + 1$, et même que $\lfloor (2n)/p^i \rfloor = 2\lfloor n/p^i \rfloor$ si $i \leqslant v_p(n)$, puisque alors les deux fractions $(2n)/p^i$ et n/p^i sont en fait des entiers. On en déduit que $v_p(\hat{\ell}(n)) = v_p(n) + \sum_{i=1}^{k} \lfloor (2n)/p^i \rfloor - 2\lfloor n/p^i \rfloor \leqslant k$, de sorte que $\hat{\ell}(n)$ divise $\ell(2n)$.

On montre ensuite par récurrence que $\hat{\ell}(n) \geqslant 2^{2n}$ pour tout $n \geqslant 4$. En effet, on a déjà $\hat{\ell}(4) = 280 > 2^8$ puis, pour tout $n \geqslant 4$, $\hat{\ell}(n+1) = 2(2n+1)\hat{\ell}(n)/n \geqslant 4\hat{\ell}(n) \geqslant 2^{2n+2}$.

Par conséquent, pour tout entier pair $n \geqslant 8$, on a bien $\ell(n) \geqslant \hat{\ell}(n/2) \geqslant 2^n$. En outre, on sait que $\ell(n) \leqslant 2\ell(n-1)$, avec égalité si et seulement si n est une puissance de 2. Cela signifie que $\ell(n-1) \geqslant 2^{n-1}$, ce qui conclut l'exercice.

Solution de l'exercice 24

Soit r un entier tel que $\omega_r(n) \leqslant 4\log_2(n)^2$. Cela signifie que r divise $n^{\omega_r(n)} - 1$, donc divise également l'entier $\Delta = \prod_{k=1}^{4\log_2(n)^2} (n^k - 1)$.

Puisque $16\log_2(n)^5 \geqslant 16$, on observe en outre que

$$\Delta < \prod_{k=1}^{4\log_2(n)^2} n^k \leqslant n^{(4\log_2(n)^2)^2} = 2^{16\log_2(n)^5} \leqslant \ell(\lceil 16\log_2(n)^5 \rceil).$$

Par conséquent, il existe un entier $\rho \leqslant \lceil 16\log_2(n)^5 \rceil$ qui ne divise pas Δ, et donc tel que $\omega_\rho(n) > 4\log_2(n)^2$.

Solution de l'exercice 25

On exécute $\log_2(n)$ fois la boucle n°1, pour un temps total $\mathcal{O}(\log(n)^5)$. Puis, d'après le résultat de l'exercice 24, on exécute au plus $\lceil 16\log_2(n)^5 \rceil$ fois la boucle n°2, pour un temps total $\mathcal{O}(\log(n)^8)$. Enfin, en ligne 7, on a $r \leqslant \lceil 16\log_2(n)^5 \rceil$, et on exécute $2\sqrt{r}\log_2(n)$ fois la boucle n°3, pour un temps total $\mathcal{O}(r^{5/2}\log(n)^4)$, donc $\mathcal{O}(\log(n)^{33/2})$, ce qui conclut.

Solution de l'exercice 26

Si n est premier, l'algorithme ne va évidemment pas indiquer que n est composé avant la boucle n°3. Or, $\binom{n}{k}$ est divisible par n si $1 \leqslant k \leqslant n-1$. Par conséquent, pour tout entier a, on a

$$(X+a)^n \equiv \sum_{k=0}^{n} \binom{n}{k} a^{n-k} X^k \equiv \binom{n}{0} a^n + \binom{n}{n} X^n \equiv X^n + a^n \pmod{n},$$

ce qui conclut.

Solution de l'exercice 27

On procède comme pour l'exercice 10. Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif, on y dispose d'une division euclidienne, d'un algorithme d'Euclide, et donc d'une relation de Bézout. En particulier, si $G(X)$ est élément non nul de $\mathcal{F}$, alors il est premier avec $H(X)$, et il existe donc un polynôme $A(X)$ tel que $AG(X) \equiv 1 \pmod{H(X)}$. Cela signifie que $\mathcal{F}$ est bien un corps.

Solution de l'exercice 28

Soit x un élément de G fixé. La fonction $\psi : t \mapsto t + x$ définit une permutation de G, de sorte que $\sum_{t \in G} t = \sum_{t \in G} \psi(t) = k\,x + \sum_{t \in G} t$, donc que $k\,x = 0$.

Solution de l'exercice 29

Soit ω l'ordre de X dans $\mathcal{F}$. Puisque $H(X)$ divise $\phi_r(X)$ donc $X^r - 1$ dans $\mathbb{Z}/p\mathbb{Z}$, on en déduit que $X^r \equiv 1 \pmod{H(X), p}$. Par ailleurs, le polynôme $Q(X) = X^r - 1$ est premier avec son polynôme dérivé $Q'(X) = X^{r-1}$, puisque $r^{-1}XQ'_r(X) - Q_r(X) \equiv 1 \pmod{p}$. En vertu de l'exercice 11, et puisque H divise déjà ϕ_r, il ne peut diviser aucun polynôme $X^\ell - 1$ tel que $\ell < r$. Cela signifie que $X^\ell \not\equiv 1 \pmod{H(X), p}$ pour tout $\ell < r$, donc que $\omega = r$.

Solution de l'exercice 30

Si k et ℓ sont tous deux introspectifs pour $P(X)$, alors, en posant $Y = X^k$, on a

$$P(X^{k\ell}) \equiv P(Y^\ell) \equiv P(Y)^\ell \equiv P(X^k)^\ell \equiv P(X)^{k\ell} \pmod{p},$$

ce qui signifie que $k\,\ell$ est également instrospectif pour $P(X)$.

Par ailleurs, si k est instrospectif pour $P(X)$ et $Q(X)$, alors

$$PQ(X^k) \equiv P(X^k)Q(X^k) \equiv P(X)^k Q(X)^k \equiv PQ(X)^k \pmod{p},$$

ce qui signifie que k est également instrospectif pour $PQ(X)$.

Solution de l'exercice 31
Soit $P(X)$ un polynôme de la forme $X + a$, avec $1 \leqslant a \leqslant \lambda$. Par hypothèse, on sait déjà que n est introspectif pour $X + a$. Par ailleurs, on a également

$$(X + a)^p \equiv \sum_{k=0}^{p} \binom{p}{k} X^k a^{p-k} \equiv \binom{p}{0} a^p + \binom{p}{p} X^p \equiv X^p + a^p \pmod{p},$$

ce qui signifie que p est également introspectif pour $X + a$, et donc que tout élément m de $\mathcal{G}_1$ est introspectif pour $X + a$. Enfin, puisque l'ensemble des polynômes pour lesquels m est introspectif est stable par produit, cela montre bien que m est introspectif pour tout élément de $\mathcal{H}_1$.

Solution de l'exercice 32
Soit A et B deux éléments de $\mathcal{H}_1$ de degré au plus $t-1$ et tels que $A(X) \equiv B(X) \pmod{H(X)}$. On note alors, pour tout $m \in \mathcal{G}_1$, que $A(X^m) \equiv A(X)^m \equiv B(X)^m \equiv B(X^m) \pmod{H(X)}$, ce qui signifie que X^m est une racine de $A(T) - B(T)$.

Or, X est d'ordre r dans $\mathcal{F}$, ce qui signifie que $\{X^m : m \in \mathcal{G}_1\}$ est un sous-ensemble de $\mathcal{F}^*$ de cardinal $|\mathcal{G}_2| = t$. Le polynôme $A(T) - B(T)$ a donc t racines distinctes dans $\mathcal{F}$, ce qui signifie que $A - B$ est de degré au moins t, ou encore que $A = B$.

Pour conclure l'exercice, il suffit donc en fait de montrer que $\mathcal{H}_1$ compte au moins $\binom{t+\lambda}{\lambda-1}$ éléments de degré au plus $t - 1$. Tout d'abord, puisque $r > \omega_r(n) > 4\log_2(n)^2$, on en déduit que $\sqrt{r} > 2\log_2(n)$, donc que $p > r > 2\sqrt{r}\log_2(n) \geqslant \lambda$. Par conséquent, les polynômes $X + a$, où $1 \leqslant a \leqslant \lambda$, sont deux à deux distincts modulo p.

Choisir un élément $\mathcal{H}_1$ de degré $t - 1$ revient donc à choisir une collection d'entiers $\kappa = (\kappa_0, \ldots, \kappa_\lambda)$ dont la somme vaut $t-1$, puis à identifier κ au polynôme $P_\kappa(X) = \prod_{a=1}^{\lambda}(X+a)^{\kappa_a}$. Puisqu'il existe $\binom{t+\lambda-1}{\lambda}$ telles collections κ, le résultat désiré s'ensuit immédiatement.

Solution de l'exercice 33
Puisque n n'est pas une puissance de p, les éléments de $\mathcal{G}'$ sont deux à deux distincts. On en déduit que $|\mathcal{G}'| = (\lfloor\sqrt{t}\rfloor + 1)^2 > \sqrt{t}^2 = t$, c'est-à-dire que $|\mathcal{G}'| \geqslant t + 1$. Puisque tout élément de $\mathcal{G}'$ est congru à un élément de $\mathcal{G}_2$ modulo r, il existe donc $k_1 < k_2$ dans $\mathcal{G}'$ tels que $k_1 \equiv k_2 \pmod{r}$.

Alors $X^{k_1} \equiv X^{k_2} \pmod{X^r - 1, p}$, donc $X^{k_1} = X^{k_2}$ dans $\mathcal{F}$. Or, k_1 et k_2 sont introspectifs pour tout polynôme $P(X) \in \mathcal{H}$, de sorte que $P(X)^{k_1} = P(X^{k_1}) = P(X^{k_2}) = P(X)^{k_2}$. Par conséquent, tout élément de $\mathcal{H}$ est racine du polynôme $R(Y) \in \mathcal{F}[Y]$, défini par $R(Y) = Y^{k_2} - Y^{k_1}$, de sorte que $|\mathcal{H}| \leqslant k_2$.

Enfin, puisque p est le plus petit facteur premier de n et que $n \neq p$, on en déduit que $p \leqslant \sqrt{n}$, d'où l'on conclut que $|\mathcal{H}| \leqslant k_2 \leqslant (pn)^{\sqrt{t}} \leqslant n^{3\sqrt{t}/2}$.

Solution de l'exercice 34
Notre hypothèse selon laquelle le Théorème 2.4.6 était faux nous a amené à montrer que $n^{3\sqrt{t}/2} \geqslant |\mathcal{H}_2| \geqslant \binom{t+\lambda-1}{\lambda}$. Or, on sait que $r \geqslant t \geqslant \omega_r(n) > 4\log_2(n)^2$. Cela montre que $t-1 \geqslant \Lambda$ et que $\lambda = 2\sqrt{r}\log_2(n) \geqslant \Lambda$, où $\Lambda = \lfloor 2\sqrt{t}\log_2(n)\rfloor$. Remarquons au passage que $\sqrt{n} \geqslant p > r \geqslant \Lambda$.

Notons alors que $n \geqslant 4$, car n est composé, de sorte que $\Lambda \geqslant \lfloor 2\log_2(n)\rfloor \geqslant 4$. En vertu de l'exercice 23, il s'ensuit que $\hat{\ell}(\Lambda) \geqslant 2^{2\Lambda}$. Puisque la fonction $(a, b) \mapsto \binom{a+b}{a}$ est croissante par rapport à chacun de ses arguments, on en déduit que

$$n^{3\sqrt{t}/2} \geqslant \binom{t+\lambda-1}{\lambda} \geqslant \binom{2\Lambda}{\Lambda} = \hat{\ell}(\Lambda)/\Lambda \geqslant 2^{2\Lambda}/\sqrt{n} \geqslant n^{4\sqrt{t}-1/2}/4.$$

Cela signifie que $4 \geqslant n^{(5\sqrt{t}-1)/2} \geqslant 4^{(5\sqrt{t}-1)/2} \geqslant 4^2$, ce qui est évidemment impossible, prouvant l'absurdité de notre hypothèse et concluant donc la preuve du Théorème 2.4.6.

3 Combinatoire

1 Géométrie combinatoire

– Quelques idées utiles –

— Tester des petits cas (comme dans tous les problèmes de combinatoire)

— Toujours commencer par la méthode la plus brutale possible (exercice 9)

— Penser à la récurrence (exercices 4,6,7)

— Ordonner les points par abscisse croissante (exercices 1,2,3)

— Considérer l'enveloppe convexe (exercices 6,7,8,11)

— Trianguler les polygones : pour diviser un polygone en triangles, il faut tracer $n-3$ diagonales, on obtient $n-2$ triangles (exercice 10)

– Exercices –

Exercice 1
On donne 2016 points dans le plan, trois quelconques jamais alignés. Démontrer que l'on peut construire 504 quadrilatères deux à deux disjoints, non nécessairement convexes, et dont les sommets sont les points données.

Exercice 2
On considère 2018 droites du plan, deux à deux non parallèles et trois à trois non concourantes. On appelle E l'ensemble de leurs points d'intersection. On veut attribuer une couleur à chacun des points de E de sorte que deux quelconques de ces points qui appartiennent à une même droite et dont le segment qui les relient ne contient aucun autre point de E, soient de couleurs différentes.

Combien faut-il au minimum de couleurs pour pouvoir réaliser une telle coloration ?

Exercice 3
Soit $\mathcal{P}$ un polygone convexe à n côtés. Montrer qu'il existe un ensemble S de $n-2$ points tels que tout triangle dont les sommets sont des sommets de $\mathcal{P}$ contient exactement un point de S.

Exercice 4 (Théorème de Helly)
On considère quatre parties convexes du plan telles que l'intersection de trois d'entre elles est toujours non vide.

a) Montrer que l'intersection des quatre convexes est non vide.
b) Le théorème reste-t-il vrai en remplaçant 4 par $n \geqslant 4$?

Exercice 5
Soit $A_1 \dots A_n$ un polygone convexe fixé. On considère X à l'intérieur du polygone. Pour tout i, on note B_i la deuxième intersection de (A_iX) avec le bord du polygone. Montrer qu'il est possible de choisir X de telle manière que pour tout i :

$$\frac{XA_i}{XB_i} \leqslant 2.$$

Exercice 6
Soit $n \geqslant 1$: on place dans le plan $2n$ points, trois quelconques non alignés. On en colorie n en bleu et n en rouge. Montrer qu'il est possible de tracer n segments qui ne se croisent pas, chaque segment reliant un point bleu à un point rouge, de telle manière que chaque point soit utilisé une seule fois.

Exercice 7 (IMO 2013, Problème 2)
On considère un ensemble S de 4035 points dans le plan, trois quelconques non alignés, dont 2017 coloriés en bleu et 2018 en rouge. Montrer qu'il est possible de tracer 2017 droites dans le plan de telle manière que :

(i) aucune droite ne passe par un point de S,
(ii) aucune des régions délimitées par les 2017 droites ne contient deux points de S de couleurs différentes.

Exercice 8 (IMO 1995, Problème 3)
Trouver tous les entiers $n > 3$ pour lesquels il existe n points $A_1, \dots, A_n$ du plan et des réels $r_1, \dots, r_n$ tels que :

(i) trois quelconques des points ne sont jamais alignés,
(ii) pour tout $\{i, j, k\}$, l'aire du triangle $A_iA_jA_k$ est égale à $r_i + r_j + r_k$.

Exercice 9 (IMO 2014, Problème 6, version facile)
On considère un ensemble de n droites tracées dans le plan, deux quelconques non parallèles, trois quelconques non concourantes. Elles divisent le plan en un certain nombre de régions, certaines finies et certaines infinies. Montrer qu'il est possible de colorier au moins $\sqrt{\frac{n}{2}}$ de ces droites en bleu de manière à ce qu'il n'y ait aucune région finie dont le périmètre soit entièrement bleu.

Exercice 10 (Problème de la galerie d'art)
Soit $\mathcal{P}$ un polygone non croisé (pas forcément convexe). Montrer qu'il existe un ensemble $\mathcal{A}$ de $\lfloor \frac{n}{3} \rfloor$ sommets de $\mathcal{P}$ tel que pour tout X à l'intérieur de $\mathcal{P}$, il existe un point $C \in \mathcal{A}$ tel que le segment $[CX]$ soit entièrement à l'intérieur de $\mathcal{P}$.

Exercice 11
Soit S un ensemble fini de points du plan avec $|S|$ pair. Montrer qu'il est possible de partitionner S en deux ensembles S_1 et S_2 tels que le bord de l'enveloppe convexe de S_1 contienne autant de points que le bord de l'enveloppe convexe de S_2.

– Solutions des exercices –

Solution de l'exercice 1
Quitte à faire tourner la figure, on peut supposer que les points ont des abscisses deux à deux distinctes. On note P_i avec $1 \leqslant i \leqslant 2016$ les points ordonnés par abscisse croissante et, pour tout k entre 0 et 503, on considère un quadrilatère dont les sommets sont P_{4i+1}, P_{4i+2}, P_{4i+3} et P_{4i+4}.

Solution de l'exercice 2
La configuration contient au moins un triangle. Cela peut par exemple se prouver par récurrence sur le nombre de droites : trois droites forment un triangle et si on ajoute une droite, soit elle laisse le triangle intact, soit elle le sépare en un triangle et un quadrilatère. Par conséquent, il est impossible d'effectuer un coloriage avec deux couleurs.

On va maintenant montrer qu'un coloriage à trois couleurs est possible : on ordonne les points par abscisse croissante comme dans l'exercice précédent, et on les colorie dans cet ordre. Au moment où on doit colorier un point $P = (d_i) \cap (d_j)$, on a déjà colorié au plus un de ses voisins sur (d_i) (celui qui est à gauche) et un sur (d_j) (aussi celui de gauche). On a donc au plus deux couleurs interdites et on peut toujours choisir la troisième. La réponse est donc 3 couleurs.

Solution de l'exercice 3
On choisit S comme suit : notons A le point le plus à gauche de $\mathcal{P}$ (qui est unique quitte à "tourner" la figure) et Z le plus à droite.

— Pour tout sommet X de $\mathcal{P}$ sur l'arc de $\mathcal{P}$ au-dessus de A et Z, on prend dans S un point "juste en-dessous" de X.

— Pour tout sommet X de $\mathcal{P}$ sur l'arc de $\mathcal{P}$ en-dessous de A et Z, on prend dans S un point "juste au-dessus" de X.

On a donc pris 1 point par sommet de $\mathcal{P}$ différent de A et Z, soit $|S| = n - 2$.

Enfin, soient I, J et K des sommets de $\mathcal{P}$. On peut supposer qu'ils sont ordonnés par abscisse croissante, donc J est différent de A et Z. Il y a alors à l'intérieur du triangle IJK un petit segment issu de J partant vers le haut (si J est sur l'arc bas) ou vers le bas (si J est sur l'arc haut). Ceci garantit que le point de S placé juste au-dessus ou juste en-dessous de J est bien dans IJK.

Solution de l'exercice 4

a) On note $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ et $\mathcal{C}_4$ les quatre convexes. Soit $A_1 \in \mathcal{C}_2 \cap \mathcal{C}_3 \cap \mathcal{C}_4$. On définit de même A_2, A_3 et A_4. Si A_1, A_2, A_3 et A_4 sont les sommets d'un quadrilatère convexe, peut supposer que $[A_1A_2]$ et $[A_3A_4]$ s'intersectent. On a $[A_1A_2] \subset \mathcal{C}_3 \cap \mathcal{C}_4$ et $[A_3A_4] \subset \mathcal{C}_1 \cap \mathcal{C}_2$, donc le point d'intersection des deux segments est simultanément dans les quatre convexes. Sinon, on peut supposer que A_1 est à l'intérieur du triangle $A_2A_3A_4$ donc $A_1 \in \mathcal{C}_1$, donc A_1 est dans les quatre convexes.

b) Oui : on fait une récurrence sur n en utilisant le cas $n = 4$. Si le théorème est vrai pour n, on prend $n + 1$ convexes : n quelconques ont toujours une intersection non vide. On prend 4 points dans ces intersections et on applique la preuve précédente.

<u>*Solution de l'exercice 5*</u>
La condition $\frac{XA_i}{XB_i} \leqslant 2$ équivaut à $\frac{A_iX}{A_iB_i} \leqslant \frac{2}{3}$, ce qui revient à dire que X est dans l'image du polygone par l'homothétie de centre A_i et de rapport $\frac{2}{3}$. On note P_i cette image. Alors P_i est un polygone convexe, et il suffit de vérifier :

$$\bigcap_{i=1}^{n} P_i \neq \emptyset$$

D'après le théorème de Helly, il suffit de vérifier que l'intersection de trois P_i n'est jamais vide. C'est vrai car pour tous i, j et k le centre de gravité de $A_iA_jA_k$ se trouve dans P_i, P_j et P_k.

<u>*Solution de l'exercice 6*</u>
On raisonne par récurrence forte sur n : le résultat est trivial pour $n = 1$. Supposons le résultat vrai jusqu'au rang $n-1$, et considérons n points bleus et n points rouges. Il suffit de séparer les $2n$ points par une droite de manière à avoir de chaque côté de la droite autant de points bleus que de rouges, et de traiter séparément chaque côté de la droite par hypothèse de récurrence.

On considère le bord de l'enveloppe convexe des $2n$ points : si elle contient deux points de couleurs différentes, alors elle contient deux points consécutifs de couleur différente. On peut isoler ces deux points par une droite et on a gagné.

Sinon, on suppose que le bord de l'enveloppe convexe est entièrement bleu. Quitte à faire une rotation, les ordonnées des points sont deux à deux distinctes. On fait descendre une droite horizontale : le point le plus haut A_1 et le plus bas A_{2n} sont sur le bord donc sont bleus. On a donc un point bleu "en trop" au-dessus de la droite juste après avoir passé A_1 et un point rouge en trop juste avant A_{2n}. Comme on passe les points un par un, on aura donc à un moment autant de points bleus que de rouges au-dessus de la droite, donc on a gagné !

<u>*Solution de l'exercice 7*</u>
On raisonne par récurrence sur 4035. Plus précisément, on montre par récurrence sur n qu'avec $2n + 1$ points on peut tracer n droites vérifiant la condition voulue, le nombre de points rouges et de points bleus n'ayant en fait aucune importance. Avec 3 points, si il y en a 2 bleus et 1 rouge, il est facile de tracer une droite qui isole le point rouge. Si le problème est résolu pour n, considérons $2n + 3$ points. Soient A et B deux sommets consécutifs de l'enveloppe convexe. Par hypothèse de récurrence, il existe n droites qui marchent pour $S \setminus \{A, B\}$.

Si A et B sont de la même couleur, on ajoute une droite qui isole A et B du reste et on a gagné. Sinon, on suppose A bleu et B rouge : si A et B sont dans la même région, tous les points de S dans cette région autres que A et B sont de la même couleur, par exemple rouge. On ajoute un droite qui isole A et on a gagné. Si A et B sont dans des régions différentes :

— Si la région de A ne contient que des bleus et celle de B que des rouges, on a gagné.

— Si la région de A ne contient que des rouges et celle de B que des rouges, on ajoute une droite qui isole A.

— Si la région de A ne contient que des bleus et celle de B que des bleus, on ajoute une droite qui isole B.

— Si la région de A ne contient que des rouges et celle de B que des bleus, on ajoute une droite qui isole A et B.

Solution de l'exercice 8

Supposons que l'enveloppe convexe contienne quatre points A_i, A_j, A_k, A_ℓ dans cet ordre. En écrivant de deux manières différentes l'aire du quadrilatère convexe $A_iA_jA_kA_\ell$, on obtient $r_i+r_k = r_j+r_\ell$. Si elle contient 5 points, en appliquant ce résultat à plusieurs quadrilatères on obtient que tous les r_i pour A_i sur le pentagone sont égaux, et on obtient une contradiction. Le bord de l'enveloppe convexe contient donc au plus 4 points.

Notons maintenant $A_1 \dots A_\ell$ (avec $\ell = 3$ ou $\ll= 4$) l'enveloppe convexe, et soit A_k à l'intérieur. Alors on peut décomposer l'enveloppe convexe en triangles en traçant les segments $[A_iA_k]$ avec $1 \leqslant i \leqslant \ell$. L'aire de l'enveloppe convexe s'écrit alors

$$2(r_1 + r_2 + \dots r_\ell) + \ell r_k.$$

On en déduit que r_k est le même pour tous les points à l'intérieur de l'enveloppe convexe, donc si A_k et $A_{k'}$ sont à l'intérieur de l'enveloppe convexe alors pour tout $1 \leqslant i \leqslant \ell$, les triangles $A_iA_{i+1}A_k$ et $A_iA_{i+1}A_{k'}$ ont la même aire, donc $(A_kA_{k'})$ est parallèle à tous les côtés (A_iA_{i+1}), ce qui est impossible, donc $A_k = A_{k'}$. Il y a au plus un point à l'intérieur, soit 5 points au maximum.

On peut construire des exemples avec 4 points (parallélogramme par exemple). Si il y a un exemple à 5 points, on a 4 points sur le bord et 1 à l'intérieur. Supposons que c'est A_5. Il est à l'intérieur de deux triangles, supposons $A_1A_2A_3$ et $A_1A_2A_4$. En décomposant le triangle $A_1A_2A_3$ en trois triangles $A_1A_2A_5$, $A_2A_3A_5$ et $A_3A_1A_5$, on obtient

$$r_1 + r_2 + r_3 + r_5 = 0.$$

De même, en décomposant $A_1A_2A_4$, on obtient $r_1 + r_2 + r_4 + r_5 = 0$, donc $r_3 = r_4$. La droite (A_3A_4) est donc parallèle aux droites (A_1A_2), (A_1A_5) et (A_2A_5), donc les points A_1, A_2 et A_5 sont alignés, ce qui est absurde.

Solution de l'exercice 9

On utilise un algorithme glouton : supposons qu'on ait déjà colorié k droites et cherchons s'il est possible d'en colorier une $(k+1)$-ème. On appelle une région finie *dangereuse* si tout son bord sauf un côté est déjà colorié en bleu. Une telle région a au moins deux côtés consécutifs bleus donc un de ses sommets est une intersection de deux droites bleues. Il y a $\binom{k}{2}$ telles intersections. De plus, une intersection touche au plus 4 régions finies, donc il y a au plus $4\binom{k}{2} = 2k(k-1)$ régions dangereuses. Chaque région dangereuse interdit d'ajouter une droite donc il y a au plus $2k(k-1)$ droites interdites. On peut donc ajouter de nouvelles droites tant que $2k(k-1) < n$, donc tant que $2k^2 < n$ donc il est possible d'en colorier $\sqrt{\frac{n}{2}}$.

Solution de l'exercice 10

On trace $n-3$ diagonales de $\mathcal{P}$ de manière à le diviser en $n-2$ triangles. Il suffit de sélectionner

$\lfloor \frac{n}{3} \rfloor$ sommets de manière à avoir au moins sommet de chaque triangle. On va montrer qu'il est possible de colorier en bleu, rouge et jaune les sommets de $\mathcal{P}$ de manière à ce que chaque triangle contienne exactement un sommet bleu, un rouge et jaune. Une fois ce lemme montré, il suffit de prendre tous les sommets de la couleur la moins utilisée. Il y en a au plus $\frac{n}{3}$, et il y en a exactement un par triangle.

On montre ce lemme par récurrence sur le nombre de sommets. Il est trivial pour $n = 3$. De plus, il y a $n-2$ triangles et n côtés de $\mathcal{P}$ donc il existe au moins un triangle dont 2 côtés sont des côtés de $\mathcal{P}$. Ces côtés sont forcément consécutifs et ont un sommet X en commun. On peut appliquer l'hypothèse de récurrence au polygone obtenu en supprimant X puis, comme X est dans un seul triangle, on n'a seulement deux couleurs interdites pour X et on peut colorier X.

Solution de l'exercice 11

Pour tout ensemble fini X de points, on notera $|\partial X|$ le nombre de points de X sur le bord de l'enveloppe convexe de X.

On note $A = A_1 \ldots A_k$ le bord de l'enveloppe convexe de S. L'idée est la suivante : on commence en mettant d'un côté les sommets de A, et de l'autre côté les autres, puis on change de côté les A_i un par un.

Plus précisément, soit $T = S \setminus A$. Pour tout $0 \leqslant i \leqslant n$, on pose $X_i = \{A_1, \ldots, A_i\} \cup T$ et $Y_i = \{A_{i+1}, \ldots, A_n\}$. Notons que $X_n = S$ et $Y_n = \emptyset$, donc il existe des i pour lesquels $|\partial X_i| \geqslant |\partial Y_i|$. On considère le plus petit i tel que $|\partial X_i| \geqslant |\partial Y_i|$.

Si $i = 0$, alors $|\partial T| \geqslant |\partial S|$. On supprime alors des points de T un par un pour les ajouter à A. Cela ne change pas l'enveloppe convexe de A. De plus, le bord de l'enveloppe convexe de T va passer de $|\partial T|$ à 0 et ne peut jamais diminuer de plus de un en un coup, donc à un certain moment les deux parties auront des enveloppes convexes de même taille.

Si $i \geqslant 1$, alors on a $|\partial X_{i-1}| < |\partial Y_{i-1}|$. D'autre part, on a $|\partial X_{i-1}| \geqslant |\partial X_i| - 1$ (ajouter un point à X_{i-1} augmente son bord d'au plus 1), et $|\partial Y_{i-1}| \leqslant |\partial Y_i| + 1$ (pour la même raison). On a donc

$$|\partial Y_i| \leqslant |\partial X_i| \leqslant |\partial X_{i-1}| + 1 \leqslant |\partial Y_{i-1}| \leqslant |\partial Y_i| + 1,$$

donc $|\partial X_i|$ vaut $|\partial Y_i|$ ou $|\partial Y_i| + 1$. Dans le premier cas, (X_i, Y_i) est la partition qu'on recherche.

Dans le second cas, notons que $|\partial X_i| + |\partial Y_i| = 2|\partial Y_i| + 1$ est impair, donc différent de $|S|$. Il existe donc un point B de S qui n'est ni sur le bord de l'enveloppe convexe de X_i, ni sur celui de Y_i. Par construction, les points de Y_i forment un polygone convexe, donc $B \in X_i$. Si B n'est pas dans l'enveloppe convexe de Y_i, on peut faire passer B de X_i à Y_i. On a alors $|\partial(X_i \setminus B)| = |\partial X_i|$ (car B n'est pas au bord de l'enveloppe convexe de X_i). De plus, on a

$$|\partial(Y_i \cup B)| = |Y_i \cup B| = |Y_i| + 1 = |\partial Y_i| + 1.$$

En effet, B n'est pas dans l'enveloppe convexe de Y_i, donc il est sur le bord de celle de $Y_i \cup B$. Tous les autres points de Y_i sont sur A, donc en particulier au bord de l'enveloppe convexe de $Y_i \cup B$. La partition $(X_i \setminus B, Y_i \cup B)$ convient donc.

Enfin, il reste le cas où tous les points de X_i qui ne sont pas sur ∂X_i sont dans l'enveloppe convexe de Y_i. Dans ce cas, notons X' l'ensemble des points de X_i qui ne sont pas dans l'enveloppe convexe de Y_i. Alors tous les points de X' sont sur ∂X et le point B précédent n'est pas dans l'enveloppe convexe de X', donc $\partial X' \subset \partial X_i$, et l'inclusion est stricte. Par conséquent, on a $|\partial X'| < |\partial X_i|$, donc

$$|\partial X'| \leqslant |\partial Y_i| = |\partial(S \setminus X')|.$$

La deuxième égalité vient du fait que tous les points de $S \setminus X'$ qui ne sont pas dans Y_i sont à l'intérieur de son enveloppe convexe. On peut maintenant ajouter un à un les points de $S \setminus X'$ à X', jusqu'à avoir un ensemble dont le bord de l'enveloppe convexe a $|\partial Y_i|$ sommets.

2 Théorie des graphes

Ce cours est en deux parties. La première tourne autour du théorème de Turan et la seconde s'intéresse au théorème max-flow min-cut et à son application à des démonstrations des théorème de König, Hall et Dilworth.

– Définitions –

Un **graphe non-orienté** G est un couple (S, A) où S est un ensemble fini dont les éléments sont appelés **sommets** et A est un ensemble de paires d'éléments de S appelées **arêtes**. Il est dit que $u \in S$ est relié à $v \in S$ si $\{u, v\}$ est une arête. L'on peut représenter un graphe dans le plan en représentant les sommets par des points du plan et les arêtes par des courbes les reliant. Les voisins d'un sommet u sont les éléments de $D(u) = \{v \in S \mid \{u, v\} \in A\}$. Le dégré d'un sommet u est $d(u) := |D(u)|$.

Un **graphe orienté** G est un couple (S, A) où S est un ensemble fini dont les éléments sont appelés **sommets** et A est un sous-ensemble de $S^2 - \{(s, s) \mid s \in S\}$ dont les éléments sont appelées **arêtes**.

– Relation d'équivalence et relation d'ordre –

Un bref rappel sur les relations d'ordre et d'équivalence ainsi que leurs représentations par des graphes est fait ici.

Une relation $\sim$ sur un ensemble E est **d'équivalence** si elle respecte les trois conditions suivantes :

(1) $\forall x \in E,\ x \sim x$;

(2) $\forall x, y \in E,\ x \sim y \Leftrightarrow y \sim x$;

(3) $\forall x, y, z \in E,\ x \sim y$ et $y \sim z \Rightarrow x \sim z$.

Une relation d'équivalence induit une partition de E en ensembles appelés **classes d'équivalence**. Le graphe d'une relation d'équivalence est un graphe non-orienté de sommets E tel que pour tout x et y distincts dans E, $\{x, y\}$ est une arête si et seulement si $x \sim y$. C'est une réunion de cliques à sommets disjoints. Chaque clique correspond à une classe d'équivalence.

Définition 3.2.1.
Le graphe k-partite complet $\mathcal{K}_{n_1,\ldots,n_k}$ est le complémentaire du graphe de la relation d'équivalence de cardinaux de classes $n_1, \ldots, n_k$.

Cette définition caractérise les graphes k-partites comme les complémentaires des graphes d'équivalence. Cela se traduit dans le lemme suivant :

Lemme 3.2.2.
Soit $G = (S, A)$ un graphe. Il existe k tel que G soit k-partite si et seulement si pour tout $\{u, v\} \in A$ et $w \in S - \{u, v\}$, $\{u, w\} \in A$ ou $\{v, w\} \in A$.

Une **relation d'ordre** $\leqslant$ sur un ensemble E est une relation vérifiant les trois relations suivantes :

(1) $\forall x \in E,\ x \leqslant x$;

(2) $\forall x, y \in E,\ x \leqslant y$ et $y \leqslant x \Rightarrow y = x$;

(3) $\forall x, y, z \in E,\ x \leqslant y$ et $y \leqslant z \Rightarrow x \leqslant z$.

Pour tout ensemble X, $(\mathcal{P}(X), \subset)$ est un ensemble ordonné.

Exercice 1
Soit $(E, \leqslant)$ un ensemble ordonné. Montrer qu'il existe un ensemble finie F et et des ensembles $X_e \subset F$ pour tout $e \in E$ tels que pour tout $e_1, e_2 \in E$, $e_1 \leqslant e_2$ si et seulement si $X_{e_2} \subset X_{e_2}$. (toute relation d'ordre s'incarne dans l'inclusion)

Le graphe d'une relation d'ordre est un graphe orienté de sommets E et tel que pour tout x et y disctincts dans E, (x, y) est une arête si et seulement si $x \leqslant y$. Ce graphe est acyclique. Réciproquement, tout graphe orienté acyclique $G = (S, A)$ définit un ordre sur S par : $u \leqslant v$ si et seulement si il existe un chemin de u à v dans G. Le graphe $\bar{G}$ associé à $\leqslant$ définit par (u, v) est une arête de $\bar{G}$ si et sulement si il existe un chemin de u à v dans G est la **clôture transitive** de G.

Pour G un graphe, on appelle **orientation** de G un graphe orienté $\overrightarrow{G}$ de mêmes sommets que G tel que $\{u, v\}$ est une arête de G si et seulement si (u, v) ou (exclusif) (v, u) est une arête de $\overrightarrow{G}$.

Exercice 2
Montrer que tout graphe admet une orientation acyclique.

– Théorème de Turan et applications –

Théorème 3.2.3 (Mantel)**.**
Un graphe sans triangles à n sommets a au plus $\lfloor \frac{n^2}{4} \rfloor$ arêtes. Le seul graphe sans triangle avec n sommets et $\lfloor \frac{n^2}{4} \rfloor$ arêtes est $K_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil}$.

Démonstration. (Par récurrence en supprimant une arête)
On traite les cas $n \leqslant 4$ à la main puis on procède par récurrence. Soit $\{u, v\}$ une arête de G. Comme le graphe est sans triangles, les voisins de u et v forment des ensembles disjoints. En particulier $d(u) + d(v) \leqslant n$. Soit G' le graphe obtenu en supprimant u et v. G' a au plus $\lfloor \frac{(n-1)^2}{4} \rfloor$ arêtes. Donc G a au plus $\lfloor \frac{(n-2)^2}{4} \rfloor + n + 1 = \lfloor \frac{n^2}{4} \rfloor$ arêtes.
Si nous sommes dans le cas d'égalité, G' est bipartite et $d(u)+d(v) = n$. Comme il n'y a pas de triangles dans G, G est également biparti de parties $D(u) \cup \{v\}$ et $D(v) \cup \{u\}$. Or $K_{a,(n-a)}$ a $a(n-a)$ arêtes, quantité maximale pour $a = \lfloor \frac{n}{2} \rfloor$ ou $a = \lceil \frac{n}{2} \rceil$, soit $G = K_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil}$. $\square$

Exercice 3
Soit G un graphe à n sommets et T le nombre de triangles dans G. Montrer que :

$$T \geqslant \frac{1}{3} \sum_{\{u,v\} \in A} (d(u) + d(v) - n)$$

En déduire une autre démonstration du théorème.

Théorème 3.2.4 (Turan)**.**
Le nombre d'arête d'un graphe à n sommets sans p-cliques est majoré par :

$$\left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}$$

Tout graphe à n sommets sans p-cliques avec un nombre maximal d'arêtes est $(p-1)$-partite complet.

Exercice 4
Démontrer le second point du théorème.

Exercice 5
Montrer que $\mathcal{K}_{n_1,\ldots,n_k}$ a au plus $(1 - \frac{1}{k})\frac{n^2}{2}$ arêtes, où $n := n_1 + \cdots + n_k$.

Exercice 6
Soit G un graphe à n sommets de degrés respectifs $d_1, \ldots, d_n$. Montrer que le cardinal maximal d'une clique de G est minoré par :

$$\sum_i \frac{1}{n - d_i}$$

En déduire une preuve du premier point du théorème.

Remarque 3.2.5.
En passant au graphe complémentaire, l'exercice ci-dessous nous donne la proposition suivante.

Si G est un graphe dont les sommets sont de degrés $d_1, \ldots, d_n$, alors il existe un ensemble I de sommets indépendants tel que :

$$|I| \geqslant \sum_i \frac{1}{d_i + 1}$$

Exercice 7
Soit $p \geqslant 1$ et G un graphe sans p-cliques à n sommets. Montrer que G admet un sommet de degré inférieur ou égal à :

$$\left(1 - \frac{1}{p-1}\right)n$$

Donner une seconde démonstration sans utiliser le théorème de Turan.

Maintenant quelques exercices...

Exercice 8
On dispose 2017 points dans le plan tel que pour tout triplet de points, au moins deux d'entre eux soient à distance inférieure à 1. Montrer qu'il existe un disque de rayon 1 contenant au moins 1009 de ces points.

Exercice 9
Soit n points dans le plan. Montrer que le nombre de segments de longueur 1 formé par ces points est inférieur à $\frac{n^2}{3}$.

Exercice 10
On définit le graphe étoilé K_r comme le graphe de sommets $x, u_1, \dots, u_r$ et d'arêtes $\{x, u_1\}, \dots, \{x, u_r\}$. Montrer que tout graphe à n sommets et m arêtes contient au moins $n\binom{\frac{2m}{n}}{r}$ sous-graphes isomorphes à K_r. (on pose $\binom{x}{r} = \frac{1}{r!}x(x-1)\cdots(x-r+1)$)

Exercice 11
Montrer qu'un graphe dont le degré moyen est supérieur à d admet un sous-graphe dont tous les sommets sont de degré supérieur à $\frac{d}{2}$. En déduire que tout graphe G de degré moyen supérieur à $2n$ admet tous les arbres à n sommets comme sous-graphes.

Exercice 12
On dispose 2^{500} points numérotés $1, \dots, 2^{500}$ dans un certain ordre sur un cercle. Montrer que l'on peut trouver 100 cordes disjointes joignant des points tel que la somme des extrémités soit la même pour chaque corde.

– Théorème max-flow min-cut et applications –

Un **graphe de flot** $G = (S, A)$ est un graphe orienté tel que :

(1) Si (u, v) est une arête, (v, u) n'est pas une arête ;

(2) à chaque arête (u, v) est associé un entier non nul $c(u, v)$ appelé **capacité** ;

(3) Deux sommets sont particuliers : la source s et le puit p.

Si (u, v) n'est pas une arête, on a la convention $c(u, v) = 0$. Un flot f associé à G est une fonction de S^2 dans $\mathbb{N}$ tel que :

(1) Pour tout u,v, $f(u, v) \leqslant c(u, v)$;

(2) Pour tout $u \in S$ différent de s et p, le flot entrant est égal au flot sortant, ie :

$$\sum_v f(v, u) = \sum_v f(u, v)$$

(3) Le flot sortant en s est positif :

$$\sum_v f(s, v) \geqslant \sum_v f(v, s)$$

La **valeur du flot** f, notée $|f|$ est le flot sortant en s :

$$|f| = \sum_v f(v,s) - \sum_v f(s,v)$$

Le **graphe résiduel** G_f associé au flot f est un graphe de sommets S et définit par la capacité c_f :

$$c_f(u,v) = \begin{cases} c(u,v) - f(u,v) & \text{si } (u,v) \text{ est une arête de } G \\ f(v,u) & \text{si } (v,u) \text{ est une arête de } G \end{cases}$$

On remarque que le graphe résiduel n'est pas nécessairement un graphe de flot (condition (1) non respectée). On peut cependant y définir un flot sans problème en ajoutant la condition :

$$\forall u,v \ f'(u,v) = 0 \text{ ou } f'(u,v) = 0$$

Proposition 3.2.6.
Si f est un flot sur un graphe de flot G et f' un flot sur G_f, alors $f + f'$ est un flot sur G de taille :

$$|f + f'| = |f| + |f'|$$

Un **chemin augmentant** pour un flot f est un chemin de s à p sur le graphe résiduel G_f. Un chemin augmentant fourni un flot f' de valeur non nulle sur G_f et donc un flot $f + f'$ sur G de valeur strictement supérieure à celle de f. Une **coupe** C d'un graphe de flot G est une partition de ses sommets en U et V avec $s \in U$ et $p \in V$. La valeur $|C|$ de la coupe est donnée par :

$$|C| = \sum_{(u,v)\in U\times V} c(u,v)$$

Un flot f est dit maximal si $|f|$ est maximal parmis les flots du graphe de flot G. Une coupe C est dite minimale si $|C|$ est minimal parmis les coupes de G.

Proposition 3.2.7.
Pour toute coupe C et flot f d'un graphe de flot G :

$$|f| \leqslant |C|$$

Démonstration. La coupe C est associée à un partiton en U et V. Par relation de Chasles (propriété (2) des flots) :

$$|f| = \sum_{(u,v)\in U\times V} f(u,v) - \sum_{(v,u)\in V\times U} f(v,u) \leqslant \sum_{(u,v)\in U\times V} f(u,v) \leqslant \sum_{(u,v)\in U\times V} c(u,v) = |C|$$

□

Théorème 3.2.8 (max-flow min-cut)**.**
Soit f un flot d'un graphe G, il y a équivalence entre les trois propositions suivantes :

(i) f est maximal ;

(ii) il n'y a pas de chemin augmentant pour f ;

(iii) il existe une coupe C telle que $|f| = |C|$.

Démonstration. $(i) \Rightarrow (ii)$ est traité plus haut.

$(iii) \Rightarrow (i)$ est donnée par la proposition ci-dessus.

$(ii) \Rightarrow (iii)$: on se place sur G_f. On pose U l'ensemble des sommets atteignables depuis s et $V = S - U$. Soit C la coupe associée. D'après l'hypothèse (ii), $p \in V$. Comme on ne peut aller de U à V, $\forall (u, v) \in U \times V$, $c_f(u, v) = 0$. Soit :

$$\forall (u, v) \in (U \times V) \cap A \ f(u, v) = c(u, v) - c_f(u, v) = c(u, v)$$

$$\forall (v, u) \in (V \times U) \cap A \ f(v, u) = c(v, u) - c_f(v, u) = c_f(u, v) = 0$$

Et donc :

$$|f| = \sum_{(u,v) \in U \times V} f(u, v) - \sum_{(v,u) \in V \times U} f(v, u) = \sum_{(u,v) \in U \times V \cap A} c(u, v) = |C|$$

□

Dans la suite, toutes les arêtes ont une capacité de 1.

Remarque 3.2.9.
Si toutes les capacités valent 1, le théorème 3.2.8 se reformule de la façon suivante : le flot maximal est égal au nombre minimal d'arêtes qu'il faut supprimer pour qu'il n'y ai plus d'arêtes de s à p.

Nous allons maintenant appliquer le théorème 3.2.8 à des problèmes de couplage de graphe biparti. Soit K un graphe biparti et L et M sa partiton des sommets. On définit le graphe de flot G sur $L \cup M \cup \{s\} \cup \{p\}$ comme suit :

(1) Pour tout $(u, v) \in L \times M$, (u, v) est une arête si et seulement si $\{u, v\}$ est une arête de K ;

(2) Pour tout $u \in L$, (s, u) est une arête de K et pour tout $v \in M$, (v, p) est une arête de K.

Il y a alors clairement une bijection entre couplages de K et flots de G : à chaque flot f on associe le couplage $\{ \{u, v\} \mid u \in L, \ v \in M, \ f(u, v) > 0 \}$.

Un **transveral** d'un graphe est un ensemble de sommets tel que toute arête soit incidente à un sommet de l'ensemble. Il y a une injection des transversales de K dans les ensemble d'arêtes de G induisant des coupes donnée par : à T un transversal de K, on asssocie l'ensemble $(\{s\} \times T \cap L) \cup (T \cap M \times \{p\})$.

Théorème 3.2.10 (König)**.**
Le cardinal du couplage maximal d'un graphe biparti est égal au cardinal de son transversal minimal.

Exercice 13
Montrer le théorème 3.2.10.

Théorème 3.2.11 (Hall)**.**
K un graphe biparti et L et M sa partiton des sommets. À chaque $E \subset L$ on associe $C(E)$ l'ensemble des sommets de M reliés à un sommet de E. K admet un couplage de cardinal $|L|$ si et seulement si pour tout $E \subset L$, $|E| \leqslant |C(E)|$.

Exercice 14
Montrer le théorème 3.2.11.

Voici un petit complément sur les couplages. Le problème des mariages est le suivant. Il y a n enfants et n peluches, l'on veut attribuer une peluche à chaque enfant. Pour cela, chaque enfant ordonne les peluches par ordre de préférence et chaque peluche ordonne les enfants par ordre de préférence. L'objectif est de trouver une attribution tel qu'il n'existe pas un enfant et une peluche qui auraient tout deux préférés être ensemble qu'avec leurs partenaires attribués.

Théorème 3.2.12 (Existence d'un mariage stable)**.**
Il existe toujours un mariage stable.

Exercice 15
Montrer le théorème 3.2.12 en construisant un mariage stable par stratégie gloutonne.

Théorème 3.2.13 (Dilworth)**.**
Soit $(E, \leqslant)$ un ensemble partiellement ordonné. Une chaîne est un ensemble $\{u_1, \ldots, u_k\} \subset E$ tel que $u_1 \leqslant \cdots \leqslant u_k$. Une antichaîne est un sous ensemble de E formé d'éléments incomparables via $\leqslant$. Le cardinal maximal d'une antichaîne est égal au cardinal minimal d'une partition en chaînes.

Exercice 16
Montrer le théorème 3.2.13.

Théorème 3.2.14 (Mirsky)**.**
Soit $(E, \leqslant)$ un ensemble ordonné. Le cardinal minimal d'une partition en antichaînes est égal au cardinal maximal d'une chaîne.

Exercice 17
Montrer le théorème 3.2.14.

Remarque 3.2.15.
Une conséquence directe du théorème 3.2.13 est que si h est le cardinal maximal d'une chaîne et w le cardinal maximal d'une antichaîne :

$$|E| \leqslant hw$$

Voici maintenant un certain nombre d'exercices...

Exercice 18
Soit G un graphe orienté, A et B deux ensembles de ses sommets (non nécessairement disjoints). Montrer que le nombre minimal de sommets qu'il faut supprimer pour qu'il n'existe plus de chemins de A à B est égal au nombre maximal de chemins à sommets disjoints entre A et B (un chemin peut ne contenir qu'un sommet).

Exercice 19
Montrer qu'un graphe biparti dont tous les sommets ont même degré $d > 0$ admet un couplage maximal (ie. tous les sommets sont couplés).

Exercice 20
On écrit m fois chaque entier $1, \ldots, n$ dans un tableau à m colonnes et n lignes. On se donne le droit de permuter les nombres dans chaque colonne. Montrer que l'on peut arriver à un tableau où chaque ligne contient exactement une fois chaque entier.

Exercice 21
Montrer que toute suite réelle de taille $mn+1$ contient une sous-suite croissante de taille $n+1$ ou une sous suite décroissante de taille $m+1$. Montrer que $mn+1$ est optimal.

Exercice 22
Soit E un ensemble de cardinal n. Soit $\mathcal{A}$ une antichaîne de $(\mathcal{P}(E), \subset)$. Montrer que :

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{n}{|A|}} \leqslant 1$$

Et en déduire $|\mathcal{A}| \leqslant \binom{n}{\lfloor \frac{n}{2} \rfloor}$. Trouver un cas d'égalité.

– Solutions des exercices –

Solution de l'exercice 1
On choisit $F = \mathcal{P}(E)$ et pour $e \in E$, on pose $X_e = \{f \in E \mid f \leqslant e\}$. Soit $e_1, e_2 \in E$ tels que $e_1 \leqslant e_2$. Il est alors clair que $X_{e_1} \subset X_{e_2}$. Réciproquement, si $X_{e_1} \subset X_{e_2}$, alors, comme $e_1 \in X_{e_1}$, d'où $e_1 \in X_{e_2}$ et donc $e_1 \leqslant e_2$.

Solution de l'exercice 2
Soit G un graphe quelconque à n sommets. On numérote ses sommets de 1 à n. On oriente chaque arête de G du plus petit sommet au plus grand. Cette orientation est clairement acyclique.

Solution de l'exercice 3
Soit m le nombre d'arêtes dans G. Pour chaque arête $\{u, v\}$ et sommet w, les sommets u, v et w forment un triangle si et seulement si $w \in D(u) \cap D(v)$. On a donc :

$$\begin{aligned}
T &= \frac{1}{3} \sum_{\{u,v\} \in A} |D(u) \cap D(v)| = \frac{1}{3} \sum_{\{u,v\} \in A} (d(u) + d(v) - |D(u) \cup D(v)|) \\
&\geqslant \frac{1}{3} \sum_{\{u,v\} \in A} (d(u) + d(v) - n) = \frac{1}{3}\Big(\Big(\sum_{u \in S} d(u)^2\Big) - nm\Big) \\
&\geqslant \frac{1}{3}\Big(\frac{1}{n}\Big(\sum_{u \in S} d(u)\Big)^2 - nm\Big) = \frac{m}{12n}\Big(m - \frac{n^2}{4}\Big) \text{ d'après Cauchy-Schwarz}
\end{aligned}$$

Ainsi, si G n'a pas de triangles, $T = 0$ et $m \leqslant \frac{n^2}{4}$.

Solution de l'exercice 4
Soit G un graphe à n sommets sans p-cliques avec un nombre maximal d'arêtes. Il s'agit de

montrer que tous sommets u,v et w distincts tel que $\{u,v\}$ soit une arête vérifient que $\{u,w\}$ ou $\{v,w\}$ soit une arête. Supposons par l'absurde l'existence de u,v et w tels que seul $\{u,v\}$ soit une arête.

Si $d(u) \geqslant d(w)$ (ou $d(v) \geqslant d(w)$ par symétrie), on supprime w et on duplique u en u' et u'' sans les relier pour obtenir un graphe G' qui a plus d'arêtes et toujours pas de p-cliques. Contradiction.

Si $d(w) > d(u)$ et $d(w) > d(v)$, on supprime u et v, et on triple w en w_1,w_2 et w_3, sans les relier. On a à nouveau un graphe sans p-cliques avec plus d'arêtes. Contradiction.

Solution de l'exercice 5
Avec m le nombre d'arête du graphe :

$$m = \frac{1}{2}\sum_i n_i(n-n_i) = \frac{n^2}{2} - \frac{1}{2}\sum_i n_i^2 \leqslant \frac{n^2}{2} - \frac{1}{2k}(\sum_i n_i)^2 = (1-\frac{1}{k})\frac{n^2}{2} \text{ d'après Cauchy-Schwarz}$$

Solution de l'exercice 6
On note $1,\dots,n$ les sommets du graphe et $T(G)$ la taille maximale d'une clique de G. Pour toute permutation $\sigma \in S_n$, on crée une clique C_σ comme suit : pour i de 1 à n, si $\sigma(i)$ est relié à $\sigma(j)$ pour tout $j < i$, $\sigma(i) \in C_\sigma$; $\sigma(i) \notin C_\sigma$ sinon. Remarquons que :

$$|C_\sigma| = \sum_i f_{\sigma(i)}(\sigma) = \sum_j f_j(\sigma)$$

Où f_j est l'indicatrice de : « j apparait dans σ avant tous ses non-voisins ». Or, comme j a exactement $n-d_j-1$ non-voisins, il apparaît avant ceux-ci dans 1 permutation sur $n-d_j$. Donc :

$$T(G) \geqslant \frac{1}{n!}\sum_\sigma |C_\sigma| = \frac{1}{n!}\sum_\sigma\sum_j f_j(\sigma) = \sum_j \frac{1}{n!}\sum_\sigma f_j(\sigma) = \sum_j \frac{1}{n-d_j} \text{ d'après la remarque ci-dessus}$$

Si on suppose que G n'a pas de p-clique, avec m son nombre d'arêtes, l'on a :

$$(p-1) \geqslant \sum_i \frac{1}{n-d_i} \geqslant \frac{n^2}{n^2 - \sum_i d_i} = \frac{1}{1-\frac{2m}{n^2}} \text{ d'après Cauchy-Schwarz, et donc :}$$
$$m \leqslant \left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}$$

Solution de l'exercice 7
Première démonstration en appliquant le théorème de Turan.

Soit $d_1,\dots,d_n$ les degrés des sommets du graphe et m le nombre d'arête du graphe. Comme le graphe n'a pas de p-cliques, d'après le théorème 3.2.4 :

$$\frac{1}{n}\sum_i d_i = \frac{2m}{n} \leqslant \frac{2\left(1-\frac{1}{p-1}\right)\frac{n^2}{2}}{n} = \left(1 - \frac{1}{p-1}\right)n$$

Donc un des degrés est inférieur ou égal à $\left(1 - \frac{1}{p-1}\right)n$.

Seconde démonstration sans utiliser Turan :

Montrons la contraposée. Soit G un graphe à n sommet dont tous les degrés sont strictement supérieurs à $\left(1 - \frac{1}{p-1}\right)n$. Soit u_1 un sommet quelconque. On peut choisir u_2 dans $D(u_1)$ si $p \geqslant 2$. Si $p \geqslant 3$, $|D(u_1) \cap D(u_2)| \geqslant |D(u_1)| + |D(u_2)| - n > \left(1 - \frac{2}{p-1}\right)n \geqslant 0$ et l'on peut choisir u_3 dans $D(u_1) \cap D(u_2)$. Ainsi, tant que $k \leqslant p$, on peut trouver par ce procédé $u_1, \ldots, u_k$ qui forment une clique et tel que $|D(u_1) \cap \cdots \cap D(u_k)| > \left(1 - \frac{k}{p-1}\right)n$. En particulier, il existe une p-clique.

Solution de l'exercice 8

On construit un graphe G dont les sommets sont les points. Deux sommets sont reliés si et seulement si leur distance excède strictement 1. Ce graphe est sans triangle et il existe donc un point s de degré inférieur ou égal à $\lfloor \frac{2017}{2} \rfloor = 1008$. Ainsi, au moins 1008 points sont à distance inférieure ou égale à 1 de s. Alors, le cercle de centre s et de rayon 1 convient.

Solution de l'exercice 9

On note G le graphe formé par les n points et les segments de longueur 1. Ce graphe ne peut contenir de 4-clique. Il a donc au plus $\frac{n^2}{3}$ arêtes d'après le théorème 3.2.4.

Solution de l'exercice 10

Soit $d_1, \ldots, d_n$ les degrés des sommets du graphe. Le graphe K_r apparaît $\sum_i \binom{d_i}{r}$ fois. Or la fonction $x \mapsto \binom{x}{r}$ est convexe sur $\mathbb{R}_+$. Donc, par Jensen :

$$\sum_i \frac{1}{n}\binom{d_i}{r} \geqslant \binom{\sum_i \frac{d_i}{n}}{r} = \binom{\frac{2m}{n}}{r}$$

Le nombre de sous-graphes isomorphes à K_r est donc minoré par $n\binom{\frac{2m}{n}}{r}$.

Solution de l'exercice 11

Le degré moyen est $\frac{2m}{n}$. On a donc $m \geqslant n\frac{d}{2}$. On supprime les sommets de degré strictement inférieur à $\frac{d}{2}$ tant qu'il y en a. Si il n'y en avait pas, G convient. Sinon, ce processus conserve l'inégalité $m > n\frac{d}{2}$ entre le nombre n se sommets restant et m d'arêtes restantes. En particulier $m > 0$. Donc, à la fin des suppressions, le graphe n'est pas vide et ne contient que des sommets de degré supérieur à $\frac{d}{2}$. C'est ce que nous voulions.

Solution de l'exercice 12

Les sommes sont $3, \ldots, 2^{501} - 1$. Pour chaque somme s, on définit le graphe G_s de sommets les cordes de somme s et tels que deux cordes soient reliées par une arête si et seulement si elles s'intersectent. On cherche à montrer qu'un des graphes G_s admet une partie indépendante de taille $\geqslant 100$. Nous allons pour cela montrer que la moyenne sur les graphes G_s de la quantité $\sum_i \frac{1}{d_i+1}$ donné par la remarque 5 est minorée par 100.

On remarque que deux cordes de même somme ne peuvent avoir d'extrémité en commun. Soit l une corde. Cette cordes sépare les points en deux ensembles A_l et B_l (on ne compte pas les extrémités). Soit $N(s)$ l'ensemble des voisins de s dans G_s. On dispose d'une injection de $N(s)$ dans A_l et d'une injection de $N(s)$ dans B_l. l a donc au plus $m_l = \min(|A_l|, |B_l|)$ voisins. À m fixé, il existe 2^{500} cordes l tels que $m_l = m$. Il reste donc à montrer que :

$$\frac{1}{(2^{501} - 1) - 3 + 1} \sum_{i=0}^{2^{449}-2} \frac{2^{500}}{i+1} \geqslant 100$$

Ce qui est impliqué par :

$$\sum_{i=1}^{2^{449}-1} \frac{1}{i} \geqslant \sum_{k=1}^{499} \sum_{i=2^{k-1}}^{2^k-1} \frac{1}{i} \geqslant 1 + \sum_{k=2}^{499} \frac{2^{k-1}}{2^k} = 1 + \frac{498}{2} \geqslant 200$$

Solution de l'exercice 13

(König) Il s'agit de montrer que l'injection décrite ci-dessus atteint une coupe minimale, puis conclure avec le théorème 3.2.8. Or, à tout $E \subset A$ induisant une coupe, l'on peut associer $(E \cap ((\{s\} \times L) \cup (M \times \{p\}))) \cup \{\{s\} \times L \mid \exists v,\ (u,v) \in E\}$ qui est de cardinal inférieur et dans l'image de l'injection.

Solution de l'exercice 14

(Hall) Si il existe un couplage de cardinal $|L|$, alors la condition est clairement vérifiée. Supposons maintenant que la condition soit vérifiée. D'après le théorème 3.2.10, il suffit de montrer que tout transversal est de cardinal $\geqslant |L|$. Soit $T = T_L \cup T_M$ un transversal avec $T_L \subset L$ et $T_M \subset M$. Alors :

$$|T_M| \geqslant |C(L - T_L)| \geqslant |L| - |T_L| \text{ et donc } |T| = |T_L| + |T_M| \geqslant |L|$$

Ce qui conclut.

Solution de l'exercice 15

(mariages stable) On se place dans le contexte de n enfants et n peluches. On procède avec l'algorithme suivant en plusieurs tours de propositions :

(1) Au premier tour, chaque enfant demande sa peluche préférée. Chaque peluche est alors provisoirement appariée à l'enfant qu'elle préfère parmis ceux qui l'ont demandé ;

(2) À chaque tour suivant, les enfants qui n'ont pas de peluche provisoire demande leur peluche préférée parmis celles qui ne leurs ont pas été refusé. Chaque peluche non appariée choisie provisoirement l'enfant qu'elle préfère parmis ceux qui la demande. Les peluches déjà appariées qui reçoivent une proposition qu'elles préfèrent à leur enfant actuel changent d'enfant provisoir (elles prennent la meilleure de ces propositions) ;

(3) Quand tout le monde est apparié, le couplage obtenu est stable.

On associe à chaque peluche p d'un couplage provisoir le rang de l'enfant apparié (dans $\{1, \dots, n\}$) si elle est appariée, $n + 1$ sinon. La somme de ces quantités diminue à chaque étape, donc l'algorithme termine. De plus, tout le monde est apparié à la fin : chaque peluche reçoit au moins une proposition au cours de l'algorithme. Ce couplage est optimal : en effet, si e et p se préfèrent à leurs partenaires p' et e' dans le couplage final, e a proposé à p avant p' et donc p a choisit p ou mieux à ce tour, contradiction.

Solution de l'exercice 16

(Dilworth) Soit A une antichaîne. Toute partition en chaîne contient ses éléments et ce dans des chaînes différentes. Ainsi, le cardinal d'une antichaîne minore le cardinal de toute partition en chaînes. Soit E' et E'' des copies de E et K le graphe biparti de parties E' et E'' où : pour $u \in E'$ et $v \in E''$, $\{u, v\}$ est une arête si et seulement si $u < v$. D'après le théorème 3.2.10 on dispose d'un couplage C de même cardinal qu'un transversal T. L'ensemble $A \subset E$ des élements n'apparaissant pas dans T est une antichaîne, de cardinal au moins $|E| - |T|$ (certains éléments peuvent appraître deux fois dans T). Du couplage C se déduit une partition en chaînes en mettant bout à bout les relations données par les arêtes. Cette partition est de cardinal $|E| - |C|$ (nombre de composantes connexes d'un arbre). On a donc une partiton en chaînes de même cardinal qu'une antichaîne.

Solution de l'exercice 17
(Mirsky) Soit h le cardinal maximal d'une chaîne. On observe que toute partition en antichaînes est de cardinal supérieur ou égal à h. Pour chaque $x \in E$, on pose $N(x)$ le cardinal maximal de plus grand élément x. Pour tout $1 \leqslant i \leqslant h$, $N^{-1}(i)$ est une antichaîne. En effet, si $x < y$, alors $N(y) > N(x)$. Donc $N^{-1}(1), \ldots, N^{-1}(h)$ est une partition de E en h antichaînes.

Solution de l'exercice 18
Soit $S = \{a_1, \ldots, a_n\}$ les sommets du graphe. On définit $S' = \{a_1^{\rightarrow}, \ldots, a_n^{\rightarrow}, a_1^{\leftarrow}, \ldots, a_n^{\leftarrow}\}$. On définit le graphe de flot H sur $S' \cup \{s, p\}$ par :

(1) s est la source, p est le puit ;

(2) $(a_i^{\leftarrow}, a_i^{\rightarrow})$ est une arête pour tout i ;

(3) $(a_j^{\rightarrow}, a_i^{\leftarrow})$ est une arête pour toute arête (a_j, a_i) de G ;

(4) $(s, a_i^{\leftarrow})$ est une arête pour $a_i \in A$ et $(a_j^{\rightarrow}, p)$ est une arête pour $a_j \in B$.

Il y a clairement une bijection conservant le cardinal entre les flots de H et les chemins à sommets disjoints de A à B sur G. De plus, pour séparer s et p en coupant des arêtes, il est toujours optimal de couper des arêtes $(a_i^{\leftarrow}, a_i^{\rightarrow})$, ce qui reviens à supprimer des sommets dans G. Le théorème 3.2.8 conclut.

Solution de l'exercice 19
Il s'agit de vérifier la condition du théorème 3.2.11. Soit L et M les deux parties du graphe et C comme définies dans le théorème 3.2.11. Tout $E \subset L$ engendre $d|E|$ arêtes qui relient au moins $\lfloor \frac{d|E|}{d} \rfloor = |E|$ sommets de M (tiroirs). Donc $|C(E)| \geqslant |E|$, comme souhaité.

Solution de l'exercice 20
On travaille par récurrence sur m. Le cas $m = 1$ est directment vérifié. Pour établir l'hérédité, il suffit de montrer que l'on peut placer exactement un seul des entiers $1, \ldots, n$ sur la dernière colonne. Pour cela, on définit les graphe biparti K sur $L \cup M$ où $L = \{1, \ldots, n\}$ représente les entiers et $M = \{L_1, \ldots, L_n\}$ les n lignes du tableau. On relie k à L_i si la ligne i contient l'entier k. Un couplage maximal de K nous permetterait de conclure. Vérifions la condition du théorème 3.2.11 : pour un ensemble $E \subset \{1, \ldots, n\}$, les entier de E dans le tableau sont au nombre de $m|E|$ et intersectent donc au moins $\lfloor \frac{m|E|}{m} \rfloor = |E|$ lignes (tiroirs). Donc $|C(E)| \geqslant |E|$.

Solution de l'exercice 21
Soit $u_1, \ldots, u_{nm+1}$ une suite réelle. On pose $E = \{(i, u_i) | 1 \leqslant i \leqslant mn+1\}$ et on définit la relation d'ordre $\preceq$ sur E par :

$$(i, u_i) \preceq (j, u_j) \Leftrightarrow i \leqslant j \text{ et } u_i \leqslant u_j$$

Une antichaîne est alors une suite décroissante et une chaîne une suite croissante. D'après la remarque sur le théorème 3.2.13, si il n'y a ni d'antichaînes de cardinal $m+1$ ni de chaînes de cardinal $n+1$, $mn+1 = |E| \leqslant mn$, contradiction. Donc u admet une sous suite croissante de cardinal n ou une sous suite décroissante de cardinal m.

La suite à mn termes $u_0, \ldots u_{mn-1}$ définie par $u_{km+r} = -km+r$ pour $0 \leqslant k < n$ et $0 \leqslant r < m$ montre l'optimalité de la borne $mn + 1$.

Solution de l'exercice 22
Pour tout $A \in \mathcal{A}$, on note $S_A = \{\sigma \in S_n \mid A = \{\sigma(1), \ldots, \sigma(|A|)\}\}$. On a, par un rapide dénombrement, $|S_A| = |A|!(n - |A|)! = \frac{n!}{\binom{n}{|A|}}$. Or, comme $\mathcal{A}$ est une antichaîne, Pour tout $A \neq B \in \mathcal{A}$, $S_A \cap S_B = \varnothing$. Donc :

$$1 \geqslant \frac{1}{|S_n|}\Big(\sum_{A \in \mathcal{A}} |S_A|\Big) = \sum_{A \in \mathcal{A}} \frac{1}{\binom{n}{|A|}}$$

Or, pour tout k, $\binom{n}{k} \leqslant \binom{n}{\lfloor \frac{n}{2} \rfloor}$. Donc :

$$1 \geqslant \sum_{A \in \mathcal{A}} \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} = \frac{|\mathcal{A}|}{\binom{n}{\lfloor \frac{n}{2} \rfloor}}$$

Soit $|\mathcal{A}| \leqslant \binom{n}{\lfloor \frac{n}{2} \rfloor}$, valeure atteinte, par exemple, pour $\mathcal{A} = \{A \subset E \mid |A| = \lfloor \frac{n}{2} \rfloor\}$.

3 Groupes

– Introduction –

La notion gén'erale de groupe est apparue au XIXème siècle, introduits par Évariste Galois dans le contexte de la résolution des équations algébriques. Vers la fin du XIXème, le concept de groupe avait pris une place centrale en mathématiques, au point que le mathématicien Henri Poincaré pouvait écrire, en 1881 : "les mathématiques ne sont qu'une histoire de groupes".

Si la notion de groupe est de nature algébrique, et les premiers exemples de groupe appartiennent au domaine de l'algèbre et aux domaines proches de la combinatoire et de la théorie des nombres, les groupes ont un rôle important en géométrie (où ils incarnent la notion la plus générale de symétrie), en topologie, en physique (cristallographie, mécanique quantique), mais aussi, à un légèrement moindre degré, en l'analyse.

Comme M. Jourdain pour la prose, vous manipulez des groupes sans le savoir :

> "Par ma foi, il y a plus de quarante ans que je dis de la prose
> sans que j'en susse rien, et je vous suis le plus obligé du monde
> de m'avoir appris cela."

Comme Monsieur Jourdain, vous aussi connaissez des exemples de groupes (mais probablement, en ce qui vous concerne, depuis un peu moins de quarante ans), sans avoir eu l'occasion d'étudier le concept abstrait de groupe. À la fin des années 1970 et dans les années 1980, les groupes abstraits étaient au programme du lycée, et même du collège, ce qui n'était pas une bonne chose. Mais maintenant, leur étude a presque disparu des programmes des classes préparatoires et souvent des deux premières années à l 'université, et c'est dommage !

Avant de donner une définition abstraite, nous allons commencer par donner des exemples de groupes.

– Exemples de groupes –

$\mathbb{Z}$

Les propriétés de l'addition dans $\mathbb{Z}$ sont bien connues :

— $\forall a, b, c \in \mathbb{Z}, a + (b + c) = (a + b) + c$ (associativité)

— $\forall a \in \mathbb{Z}, a + 0 = 0 + a = a$ (0 est un élément neutre)

— $\forall a \in \mathbb{Z}, a + (-a) = (-a) + a = 0$ ($-a$ est l'opposé de a)

— $\forall a, b \in \mathbb{Z}, a + b = b + a$ (commutativité).

$\mathbb{Q}$

Les propriétés de l'addition dans $\mathbb{Q}$ sont bien connues :

— $\forall a, b, c \in \mathbb{Q}, a + (b + c) = (a + b) + c$ (associativité)

— $\forall a \in \mathbb{Q}, a + 0 = 0 + a = a$ (0 est un élément neutre)

— $\forall a \in \mathbb{Q}, a + (-a) = (-a) + a = 0$ ($-a$ est l'opposé de a)

— $\forall a, b \in \mathbb{Q}, a + b = b + a$ (commutativité).

$\mathbb{Q}^* = \mathbb{Q}^* \backslash \{0\}$

Les propriétés de la multiplication dans $\mathbb{Q}^*$ sont bien connues :

— $\forall a, b, c \in \mathbb{Q}^*, a \times (b \times c) = (a \times b) \times c$ (associativité)

— $\forall a \in \mathbb{Q}^*, a \times 1 = 1 \times a = a$ (1 est un élément neutre)

— $\forall a \in \mathbb{Q}^*, a \times (\frac{1}{a}) = (\frac{1}{a}) \times a = 1$ ($\frac{1}{a}$ est l'inverse de a)

— $\forall a, b \in \mathbb{Q}^*, a \times b = b \times a$ (commutativité).

Remarque 3.3.1.
Notez que dans ce dernier cas, on a considéré $\mathbb{Q}^*$! Notez aussi l'utilisation de deux termes différents : opposé et inverse, pour éviter l'ambiguité.

$\mathbb{R}$

Les propriétés de l'addition dans $\mathbb{R}$ sont bien connues :

— $\forall a, b, c \in \mathbb{R}, a + (b + c) = (a + b) + c$ (associativité)

— $\forall a \in \mathbb{R}, a + 0 = 0 + a = a$ (0 est un élément neutre)

— $\forall a \in \mathbb{R}, a + (-a) = (-a) + a = 0$ ($-a$ est l'opposé de a)

— $\forall a, b \in \mathbb{R}, a + b = b + a$ (commutativité).

$\mathbb{R}^* = \mathbb{R} \backslash \{0\}$

Les propriétés de la multiplication dans $\mathbb{R}^*$ sont bien connues :

— $\forall a, b, c \in \mathbb{R}^*, a \times (b \times c) = (a \times b) \times c$ (associativité)

— $\forall a \in \mathbb{R}^*, a \times 1 = 1 \times a = a$ (1 est un élément neutre)

— $\forall a \in \mathbb{R}^*, a \times (\frac{1}{a}) = (\frac{1}{a}) \times a = 1$ ($\frac{1}{a}$ est l'inverse de a)

— $\forall a, b \in \mathbb{R}^*, a \times b = b \times a$ (commutativité).

$\mathbb{R}^{*+} =$

Les propriétés de la multiplication dans $\mathbb{R}^*$ sont bien connues :
- $\forall a, b \in \mathbb{R}^{*+}, a \times b \in \mathbb{R}^{*+}$
- l'associativité est vraie dans $\mathbb{R}^*$, donc dans $\mathbb{R}^{*+}$
- $\forall a \in \mathbb{R}^*, a \times 1 = 1 \times a = a$ (1 est un élément neutre)
- $\forall a \in \mathbb{R}^*, a \times (\frac{1}{a}) = (\frac{1}{a}) \times a = 1$ ($\frac{1}{a}$ est l'inverse de a)
- la commutativité est vraie dans $\mathbb{R}^*$, donc dans $\mathbb{R}^{*+}$.

$\mathbb{C}$

Les propriétés de l'addition dans $\mathbb{C}$ sont bien connues :
- $\forall a, b, c \in \mathbb{C}, a + (b + c) = (a + b) + c$ (associativité)
- $\forall a \in \mathbb{C}, a + 0 = 0 + a = a$ (0 est un élément neutre)
- $\forall a \in \mathbb{C}, a + (-a) = (-a) + a = 0$ ($-a$ est l'opposé de a)
- $\forall a, b \in \mathbb{C}, a + b = b + a$ (commutativité).

$\mathbb{C}^* = \mathbb{C}\backslash\{0\}$

Les propriétés de la multiplication dans $\mathbb{C}^*$ sont bien connues :
- $\forall a, b, c \in \mathbb{C}^*, a \times (b \times c) = (a \times b) \times c$ (associativité)
- $\forall a \in \mathbb{C}^*, a \times 1 = 1 \times a = a$ (1 est un élément neutre)
- $\forall a \in \mathbb{C}^*, a \times (\frac{1}{a}) = (\frac{1}{a}) \times a = 1$ ($\frac{1}{a}$ est l'inverse de a)
- $\forall a, b \in \mathbb{C}^*, a \times b = b \times a$ (commutativité).

$\mathbb{C} = \{z \in \mathbb{C}^*, |z| = 1\}$

Les propriétés de la multiplication dans $\mathbb{C}$ sont bien connues :
- $\forall a, b \in U, a \times b \in \mathbb{C}$
- l'associativité est vraie dans $\mathbb{C}^*$, donc dans $\mathbb{C}$
- $1 \in \mathbb{C}$, donc 1 est un élément neutre pour $(\mathbb{C}, \times)$
- $\forall a \in \mathbb{C}, \frac{1}{a} \in \mathbb{C}$ ($\frac{1}{a}$ est l'inverse de a dans $\mathbb{C}$)
- la commutativité est vraie dans $\mathbb{C}^*$, donc dans $\mathbb{C}$

$\mathbb{R}^n$ (n un entier $\geqslant 0$)

Les propriétés de l'addition dans $\mathbb{R}^n$ sont bien connues :
- $\forall a, b, c \in \mathbb{R}^n, a + (b + c) = (a + b) + c$ (associativité)
- $\forall a \in \mathbb{R}^n, a + 0 = 0 + a = a$ (0 est un élément neutre)
- $\forall a \in \mathbb{R}^n, a + (-a) = (-a) + a = 0$ ($-a$ est l'opposé de a)
- $\forall a, b \in \mathbb{R}^n, a + b = b + a$ (commutativité).

Vers une définition

On voit que les propriétés que tous ces situations ont en commun sont :

— on a un ensemble muni d'une opération

— les propriétés 1, 2, 3 (associativité, élément neutre, inverse) sont vérifiées

— de manière facultative, il peut y avoir commutativité (propriété 4).

Tous les ensembles précdents sont donc des groupes commutatifs. Pour bien être au clair, on inclut dans la notation l'opération. Ainsi, $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times), (\mathbb{R}^n, +)$ sont des groupes commutatifs.

Mais attention ! Dans tous les cas ci-dessus, il y a une propriété essentielle qui est *implicite* : on prend deux éléments de l'ensemble, on leur applique une certaine opération (ici, $+$ ou $\times$, et on trouve un élément du *même* ensemble ; l'élément neutre est dans l'ensemble, l'inverse d'un élément est dans l'ensemble. La question devient très importante quand on considère un sous-ensemble d'un des ensemble pr'ecédents. Par exemple, $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-ensembles de $\mathbb{R}$, qui sont eux-mêmes des groupes.

Exercice 1
Montrer que les sous-ensembles suivants de $(\mathbb{R}, +)$ ne sont pas des groupes

1. $\mathbb{R}^+$
2. $]0, 1[$
3. $\mathbb{N}$

Exercice 2
Montrer que les sous-ensembles suivants de $(\mathbb{R}^*, \times)$ ne sont pas des groupes

1. $\mathbb{Z}$
2. $]0, 1[$

Un exemple plus intéressant : $\mathbb{Z}/n\mathbb{Z}$

Exercice 3

1. Montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe
2. Est-ce que $(\mathbb{Z}/n\mathbb{Z}, \times)$ est un groupe ?
3. Est-ce que $(\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe ?
4. Montrer que $(\mathbb{Z}/p\mathbb{Z}, \times)$ est un groupe si p est premier.

Pour d'autres exemples, voir dans la section suivante.

– Définitions et propriétés générales –

Définitions

On appelle *loi de composition interne* sur un ensemble A une application de $A \times A$ dans A. On note $a * b$ l'image de (a, b) par cette application.

Soit G muni d'une loi de composition interne $*$. On dit que $(G, *)$ est un groupe si

1. $\forall a, b, c \in G, a * (b * c) = (a * b) * c$ (associativité)
2. $\exists e \in G, \forall a \in G, a * e = e * a = a$ (e est un élément neutre)
3. $\forall a \in G, \exists b, a * b = b * a = e$

On dit que ce groupe est commutatif si, de plus

$$\forall a, b \in G, a * b = b * a.$$

Notation.

1. Lorsque la loi $*$ est sans ambiguïté, on parle du groupe G.
2. Le symbole $*$ est générique ; on peut utiliser ce qu'on veut, par exemple aussi †. Mais le plus souvent, on utilise $+$ si le groupe est commutatif, et on note l'élément neutre 0 et $-a$ pour l'inverse de a, et $\times$, ou $\cdot$, ou même on "oublie" le $\cdot$ pour un groupe qui n'est pas commutatif, et l'élément neutre est noté 1, l'inverse de a étant noté a^{-1}, ou parfois $1/a$. Mais **attention !** Si l'ensemble est muni de deux opérations, comme $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$... on note $\times$ poir la deuxième opération, alors que cette deuxième opération peut être commutative, comme c'est le cas dans les exemples déjà mentionnés !

Proposition 3.3.2. Soit $(G, *)$ un groupe. Montrer les propriétés suivantes

— e vérifiant (2) ci-dessus est unique

— $\forall a \in G$, b vérifiant (3) ci-dessus est unique.

[Indication : pour (2), supposer qu'il y a deux éléments e, e' vérifiant la propriété, et calculer $e * e'$. Pour (3), supposer deux éléments b, b' et calculer $b' * a * b$.]

On peut alors dire que e est **l'**élément neutre et que b est **l'**inverse de a (articles définis). On note $b = a^{-1}$.

Proposition 3.3.3. Soit G un groupe et $g \in G$. Les applications λ_g, ρ_g définies par

$$\lambda_g(x) = g^{-1}x$$
$$\rho_g(x) = xg$$

sont des bijections de G dans G.

Exercice 4
Le démontrer.

Sous-groupes

Soit maintenant H un sous-ensemble de G. H est un *sous-groupe* de $(G, \circ)$ si $(H, \circ)$ est un groupe.

Proposition 3.3.4. 1. H est un sous-groupe de $(G, \circ)$ si et seulement si les deux propriétés suivantes sont vérifiées
(i) $\forall a, b \in H, a * b \in H$
(ii) $\forall a \in H, a^{-1} \in H$.
2. H est un sous-groupe de G si et seulement si

$$\forall a, b \in H, a * b^{-1} \in H.$$

Exercice 5
Le démontrer.

Exercice 6
Soit $(G, *)$ un groupe, et H, H' deux sous-groupes.

1. Montrer que $H \cap H'$ est un sous-groupe.
2. Généraliser à une intersection quelconque
3. Montrer que $H \cup H'$ est un sous-groupe ssi $H \subset H'$ ou $H' \subset H$.

Soit maintenant X un sous-ensemble d'un groupe G. On appelle emphsous-groupe engendré par X, parfois noté $\langle X \rangle$, le plus petit sous-groupe de G contenant X (ou "plus petit" est au sens de l'inclusion"-.

Exercice 7
Montrer que $\langle X \rangle$ existe.

Une question intéressante est, pour un sous-ensemble $X \subset G$ donné, donner une description explicite de $\langle X \rangle$. Une autre est, pour un groupe G doonné, donner des ensembles explicites X, de préférence petits, tels que $G = \langle X \rangle$.

Morphismes

On va maintenant donner un sens à la notion de ressemblance de deux groupes.

Soit $(G, *)$ et $(G', \dagger)$ deux ensembles munis de lois de composition interne. Une application $G \to G'$ est un *morphisme* si

$$\forall a, b \in G, f(a * b) = f(a) \dagger f(b).$$

On dit aussi *homomorphisme*.

Exemples.

(1) Soit n un entier relatif, et f l'application de $\mathbb{C} \to \mathbb{C}$ définie par $f(z) = z^n$. Montrer que f est un morphisme $\mathbb{C}^* \to \mathbb{C}^*$.

(2) L'application $z \mapsto \overline{z}$ est un morphisme de $(\mathbb{C}, +)$ dans lui-même et de $(\mathbb{C}^*, \times)$ dans lui-même.

(3) L'application $z \mapsto |z|$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^{*+}, \times)$

(4) Soit $(G, *)$ un groupe, et $g \in G$. L'application $n \in \mathbb{Z} \mapsto g^n$ est un morphisme de $(\mathbb{Z}, +)$ dans $(G, *)$ [On commencera par construire proprement l'application $n \mapsto g^n$.]

(4 bis) Comment noter le morphisme précédent lorsque le groupe est noté additivement ?

(5) Soit $n \in \mathbb{N}^*$. L'application $\pi\colon (\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$ définie par

$$\pi(x) = \dot{x},$$

où $\dot{x}$ est la clase de x modulo n, est un morphisme.

(6) L'application de $(\mathbb{R}, +) \to (\mathbb{R}^*, \times) : x \mapsto e^x$ est un morphisme

(7) L'application de $(\mathbb{R}, +) \to (\mathbb{C}, \times) : x \mapsto e^{ix}$ est un morphisme.

(8) Les applications $g \mapsto \lambda_g, g \mapsto \rho_g$ définies ci-dessus sont des morphismes de G dans $\mathcal{S}(G)$.

Revenons à la situation générale d'un morphisme $f\colon (G, *) \to (G', \dagger)$, mais en supposant maintenant que G, G' sont des groupes. On définit *le noyau de* f : $\ker f = \{g \in G, f(g) = e'\}$ (ou e' est l'Ĺément neutre de G')et *l'image de* f $\operatorname{Im} f = \{f(g), g \in G\}$.

La proposition suivante est très importante

Proposition 3.3.5. 1. Le noyau $\ker f$ est un sous-groupe de G. Plus généralement, si H' est un sous-groupe de G', alors $f^{-1}(H')$ est un sous-groupe de G.

2. f est *injective* ssi $\ker f = \{e\}$.
3. L'image $\operatorname{Im} f$ est un sous-groupe de G'. Plus généralement, si H est un sous-groupe de G, $f(H)$ est un sous-groupe de G'.
4. f est surjective ssi $\operatorname{Im} f = G'$.

Un morphisme bijectif s'appelle *isomorphisme*.

Exercice 8
Le démontrer.

Proposition 3.3.6. Soit G un groupe, et $g \in G$. Le sous-groupe engendré par G est l'image du morphisme $n \in \mathbb{Z} \mapsto g^n$.

Exercice 9
Le démontrer.

On dit que g st un *générateur* de G si $\langle g \rangle = G$.

Exercice 10
Déterminer les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$. On explicitera le cas particulier où n est premier, ainsi que le cas $n = 12$. Les musiciens fourniront une interprétation de ce cas.

Exercice 11
Soit G un groupe, et $g \in G$. Montrer que le sous groupe $\langle g \rangle$ est isomorphe soit à $\mathbb{Z}$, soit à $\mathbb{Z}/d\mathbb{Z}$ pour un d unique dans $\mathbb{N}^*$. Dans ce deuxième cas, on dit que g est d'ordre fini d; montrer que l'application $n \mapsto g^n$ est périodique de période d. Montrer que si $g^n = e$, alors n est un multiple de d.

Exemples de groupes

L'ensemble des bijections d'un ensemble dans lui-même

Soit E un ensemble, et $\mathcal{S}(E)$ l'ensemble des bijections de E dans E. L'ensemble $\mathcal{S}(E)$ muni de la loi $\circ$ est un groupe **Exercice 12**

Le démontrer. Un cas particulier : $E = \{1, 2, \ldots, n\}$. On note $\mathcal{S}_n$ au lieu de $\mathcal{S}(E)$.

Exercice 13
Montrer que $\mathcal{S}_n$ a $n!$ éléments.

Exercice 14
$(\mathcal{S}_n, \circ)$ est-il commutatif ?

Exercice 15
Décrire l'ensemble des éléments de $\mathcal{S}_2, \mathcal{S}_3, \mathcal{S}_4$ et disposer, sous forme d'une table, le produit de tous les éléments 2 à 2.

Groupe des isométries d'un triangle équilatéral, d'un tétraèdre

De manière générale, quand on parle d'une figure (triangle, tétraèdre...), il s'agira ici de l'ensemble de ses sommets.

Exercice 16
Dans le plan euclidien, soit abc un triangle équilatéral. Décrire l'ensemble de ses isométries.

Exercice 17
Remarquer la ressemblance entre ce dernier ensemble et $\mathcal{S}_3$. Justifier cette ressemblance en utlisant la notion de morphisme

Exercice 18
Traiter les deux exercices précédents en remplaçant triangle par tétraèdre régulier

– Quotients de groupes –

Cette notion est de loin la plus difficile, même si un exemple important, $\mathbb{Z}/n\mathbb{Z}$, est déjà connu. On va se placer d'abord dans le cas G commutatif, et on indiquera dans la sous-section suivante ce qui se passe dans le cas g
'enéral.

Quotients : cas commutatif

Soit $(G, +)$ un groupe commutatif, et H un sous-groupe. On montre (le faire !) que la relation $\mathcal{R}$

$$x\mathcal{R}y \iff x - y \in H$$

est une relation d'équivalence.

Montrer que la classe déquivalence contenant un $X \in G$, notée $\dot{x}$ est

$$\dot{x} := x + H = \{x + h, h \in H\}.$$

Comme dans le cas général d'une relation d'équivalence sur un ensemble, on peut définir un nouvel ensemble, l'ensemble des classes déquivalence. On le note G/H (le *quotient* de G par H), et on note π l'application qui a un élément $x \in G$ associe sa classe $\dot{x} = x + H$.

Théorème 3.3.7.
On définit une loi de composition interne sur G/H par

$$\dot{x}\dot{+}\dot{y} = \overset{\cdot}{\overbrace{x + y}}.$$

Muni de cette loi, G/H est un groupe commutatif et l'application π est un morphisme de groupes dont le noyau est H.

Exercice 19
Le démontrer. La seule difficulté est de comprendre que la définition n'a pas de sens *a priori* : il faut démontrer que $\overset{\cdot}{\overbrace{x + y}}$ ne dépend que de $\dot{x}$ et $\dot{y}$, et pas du choix de $x \in \dot{x}, y \in \dot{y}$.

Exemples. $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{R}/2\pi\mathbb{Z}$.

Remarque 3.3.8.
Selon la situation, il faut soit se représenter G/H comme un ensemble formé d'éléments dont la nature exacte n'a pas d'importance; mais on dispose du morphisme $\pi\colon x \mapsto \dot{x}$, soit se représenter les éléments de G/H comme les sous-ensembles $x + H$. L'addition est alors

$$(x + H) \cdot +(x' + H) = x + x' + H.$$

On vérfie dans ce cas la double inclusion $(x + H) \cdot +(x' + H) \subset x + x' + H$ et $x + x' + H \subset (x + H) \cdot +(x' + H)$.

Quotients : cas général

Si on veut faire exactement la même chose dans le cas non-commutatif que dans le cas commutatif, il faudrait avoir légalité

$$(x' * H)\dot{*}(x * H) = x' * x * H.$$

Si l'inclusion $x' {*} x {*} H \subset x' {*} H {*} x {*} H$ est toujours vraie, il n'y a aucune raison que $x' {*} H {*} x {*} H \subset x' * x * H$: en effet, pour mettre un élément $x' * h' * x * h$ sous la forme $x' * x * h$", il faudrait pouvoir faire "sauter" x au dessus de h', en d'autres termes avoir la propriété

$$\forall x \in G, \forall h' \in H, \exists h" \in H, h' * x = x * h".$$

Il est plus commode de formuler cette derière propriété sous la forme

$$\forall x \in G, x^{-1}Hx \subset H.$$

Un groupe H possédant cette propriété est dit *distingué*.

Théorème 3.3.9.
Soit H un sous-groupe distingué de G. On définit la relation d'équivalence sur G

$$x\mathcal{R}y \iff x^{-1}y \in H.$$

On note G/H l'ensemble des classes d'équivalence ; l'application qui a un éleément $x \in G$ associe sa classe est notée π ou encore $x \mapsto \dot{x}$.

1. On a
$$x\mathcal{R}y \iff xy^{-1} \in H.$$

2. On définit une loi de composition interne sur G/H par
$$\dot{x}\dot{*}\dot{y} = \dot{\overbrace{x * y}}.$$

Muni de cette loi, G/H est un groupe et l'application π est un morphisme de groupes dont le noyau est H.

Même si H n'est pas distingué, on peut quand même faire quelque chose d'intéressant. On considère *deux* relations d'équivalence distinctes :

$$x\mathcal{R}_d y \iff x^{-1}y \in H$$
$$x\mathcal{R}_g y \iff xy^{-1} \in H.$$

On note G/H l'ensemble des classes d'équivalence pour $\mathcal{R}_d$, $H\backslash G$ l'ensemble des classes d'équivalence pour $\mathcal{R}_g$. Dans les deux cas, on a une application qui à un élément associe sa classe.

Ces ensembles n'ont pas de structure naturelle de groupe, mais on a dans les deux cas une action de G sur eux (la notion d'action de groupe sortant du cadre de cette présentation).

– Groupes finis –

Le cardinal d'un groupe fini G s'appelle *ordre* de G. Dans ce paragraphe, on va noter $|X|$ le cardinal de l'ensemble fini $|H|$.

Théorème 3.3.10 (Lagrange)**.**
Soit H un sous-groupe de G. L'ordre de H divise l'ordre de G, et on a $|G| = |H||G/H|$.

Corollaire 3.3.11.
Tout élément g de G est d'ordre fini qui *divise* l'ordre de G.

Corollaire 3.3.12 (Petit théorème de Fermat)**.**
Soit p un nombre premier et $x \neq 0$ premier avec p. Alors

$$x^{p-1} \equiv 1.$$

– Arithmétique –

Dans ce paragraphe, on va démontrer des propriétés que vous connaissez bien (pgcd, ppcm, Bézout...).

Proposition 3.3.13. Soit $a \in \mathbb{N}$; $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Les sous-groupes de $(\mathbb{Z}, +)$ sont tous de cette forme.

Proposition 3.3.14. Soit a, b des entiers strictement positifs. les deux propriétés suivantes sont équivalentes :
(i) a divise b
(ii) $b\mathbb{Z} \subset a\mathbb{Z}$.

Proposition 3.3.15. La relation binaire $a|b$ (a divise b) est une relation d'ordre.

Dans un ensemble E muni d'une relation d'ordre $\prec$. Soit X un ensemble non-vide. Un majorant de X est un élément $M \in E$ tel que pour tout $x \in X$, $x \prec M$. **Si** l'ensemble des majorants de X est non-vide, et si cet ensemble admet un plus petit élément, ce plus petit élément est unique et s'appelle *borne supérieure* de X, et est notée $\sup X$. De même, on définit, si elle existe, la borne inférieure de X, notée $\inf X$.

Soit $a, b \in \mathbb{N}^*$, qu'on munit de la relation de divisibilité. On veut démontrer que $\sup(\{a, b\})$ et $\inf(\{a, b\})$ existent. Reconnaissez-vous $\sup(\{a, b\})$ et $\inf(\{a, b\})$?

Proposition 3.3.16. On considère l'ensemble $\mathcal{G}$ des sous-groupes de $\mathbb{Z}$. On munit $\mathcal{G}$ de l'inclusion. Soit $A, B \in \mathcal{G}$.

(i) $A \cap B \in \mathcal{G}$
(ii) $A + B = \{a + b, a \in A, b \in B\} \in \mathcal{G}$
(iii) $A \cap B = \inf(\{A, B\})$
(iv) $A + B = \sup(\{A, B\})$.

Corollaire 3.3.17.
Soit $a, b \in \mathbb{N}^*$, muni de la relation de divisibilité. Alors $\sup(\{a, b\})$ et $\inf(\{a, b\})$ existent.

Corollaire 3.3.18 (Relation de Bézout)**.**
$a, b \in \mathbb{N}^*$ sont premiers entre eux ssi il existe $u, v \in \mathbb{Z}$ tels que

$$ua + vb = 1.$$

Exercice 20
Démontrer les assertions de cette section.

– Le groupe symétrique –

On rappelle que $\mathcal{S}_n$ est le groupe des bijections de $\{1, \dots, n\}$ dans $\{1, \dots, n\}$, et qu'il est d'ordre $n!$. Ses éléments s'appellent permutations de $\{1, \dots, n\}$.

Soit $i, j \in \{1, \dots, n\}$. On appelle transposition l'élément $\tau_{i,j} \in \mathcal{S}_n$ tel que $\tau(i) = j, \tau(j) = i$, et $\tau(k) = k$ si $k \neq i, j$.

Théorème 3.3.19.
Soit T l'ensemble de toutes les transpositions. Alors $\langle T\rangle = \mathcal{S}_n$.

Soit $i_1, i_2, \ldots, i_k$ une suite d'éléments tous distincts de $\{1,\ldots,n\}$. A cette suite correspond une permutation σ, appelée *cycle*, telle que $\sigma(i_q) = i_{q+1}$ pour $q \leqslant k-1$, $\sigma(i_k) = i_1$, $\sigma(j) = j$ pour $j \notin \{1,\ldots,n\}$. L'ensemble $\{i_1,\ldots,i_k\}$ s'appelle le support de σ.

Soit σ, σ' deux cycles disjoints (de supports disjoints). Alors $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Théorème 3.3.20.
Toute permutation est un produit de cycles disjoints. Cette décomposition est unique à l'ordre près.

Soit $\sigma \in \mathcal{S}_n$. On définit
$$\epsilon(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}.$$
Montrer que σ est un morphisme de $\mathcal{S}_n$ dans $\{-1,1\}$.

4 Géométrie

1 Exercices divers

– Exercices Faciles –

Exercice 1
Soit ABC un triangle dont les bissectrices sont (AD), (BE) et (CF) et I le centre de son cercle inscrit. La médiatrice de $[AD]$ coupe (BE) et (CF) en X et Y respectivement. Montrer que le quadrilatère $AXYI$ est cyclique.

Exercice 2
Soit ABC un triangle et M le milieu de $[BC]$. On note D et E les points des côtés $[AC]$ et $[AB]$ de telle sorte que $MC = MB = ME = MD$. La bissectrice issue de A coupe (BC) en F et la bissectrice de $\widehat{EMD}$ recoupe (AF) en X. Montrer que les quadrilatères $BEXF$ et $DXFC$ sont cycliques.

Exercice 3
Soit ABC un triangle. On place P et Q avec $P \neq Q$ deux points sur $[BC]$. On note O_1, O_2, O_3 et O_4 les centres des cercles circonscrits de ABP, ABQ, ACP et ACQ. Montrer que $O_1O_2O_3O_4$ est cyclique si et seulement si $\widehat{BAP} = \widehat{CAQ}$.

Exercice 4
Soit ABC un triangle et I le centre de son cercle inscrit. On place un point P à l'intérieur du triangle de tel sorte que $\widehat{PBC} + \widehat{PCB} = \widehat{PCA} + \widehat{PBA}$. Montrer que $AP \geqslant AI$.

Exercice 5
Soit ABC un triangle, ω son cercle inscrit, de centre I. D, E et F les points de tangence de ω sur (BC), (CA) et (AB) respectivement. Soit X la projection orthogonale de C sur $[BI]$. Montrer que $X \in (EF)$.

Exercice 6
Soit ABC un triangle acutangle, H son orthocentre. Soit W un point sur $[BC]$. on note M et N les pieds des hauteurs issues de B et C. ω_1 est le cercle circonscrit de BWN et X le point diamétralement opposé à W. ω_2 est le cercle circonscrit de CWM et Y le point diamétralement opposé à W. Montrer que les points X, Y et H sont alignés.

Exercice 7
Soit ABC un triangle acutangle $D \in [AB]$ et $E \in [AC]$ tel que $AD = AE$. La médiatrice de $[CE]$ coupe le petit arc $\widehat{AB}$ en F et la médiatrice de $[CE]$ coupe le petit arc $\widehat{AC}$ en G. Montrer que $(FG)//(DE)$.

– Exercices un peu plus durs mais tout aussi simple –

Exercice 8
Soit $A_1A_2\dots A_n$ un n-gone régulier. Pour tout $i \in \{1, 2, \dots, n\}$ on note X_i l'intersection des droites $(A_{i-2}A_{i-1})$ et (A_iA_{i+1}). On suppose que les points X_i sont tous dans un cercle Γ. On note ω_i le cercle tangent aux demi-droites $[A_{i-1}X_i)$ et $[A_iX_i)$ au delà de X_i et intérieurement tangent à Γ en T_i. On note Ω_i le cercle tangent aux demi-droites $[A_{i-1}X_i)$ et $[A_iX_i)$ au delà de X_i et extérieurement tangent à Γ en S_i.
a) Montrer que les droites (X_iT_i) sont concourantes.
b) Montrer que les droites (X_iS_i) sont concourantes.

Exercice 9
Soit $ABCD$ un quadrilatère cyclique et P un point sur le côté de $[AB]$. La diagonale (AC) coupe (DP) en Q. La droite parallèle à (CD) passant par P coupe (BC) en K et la droite parallèle à (DB) passant par Q coupe (CB) en L. Montrer que les cercles de BKP et CLQ sont tangents.

Exercice 10
Soit ABC un triangle et O le centre de son cercle circonscrit, on prend P et Q deux points sur les côtés $[AC]$ et $[AB]$. On note K, L et M les milieux de $[PB]$, $[QC]$ et $[PQ]$. Montrer que si le cercle KLM est tangent à (PQ) alors $OP = OQ$.

Exercice 11
Soit $ABCD$ un quadrilatère tel que les demi-droites $[AB)$ et $[DC)$ se coupent en E. $[BC)$ et $[AD)$ se coupent en F. On note X_1, X_2, X_3 et X_4 les points de tangences du cercle inscrit de EBC, du cercle inscrit de FCD, du cercle E-exinscrit de EAD, du cercle F-exinscrit de FAB sur (BC), (CD), (DA) et (AB) respectivement. Montrer que les points X_1, X_3 et E sont alignés si et seulement si les points X_2, X_4 et F sont alignés.

Exercice 12
Soit $ABCD$ circonscriptible. On prend (g) une droite passant par A, elle recoupe l'intérieur du segment $[BC]$ en M et (DC) en N. On note I_1, I_2 et I_3 les centres des cercles inscrits des triangles de ABM, MCN et ADN. Montrer que l'orthocentre du triangle $I_1I_2I_3$ est sur la droite (g).

Exercice 13
Soit ABC un triangle rectangle en C, H le pied de la hauteur issue de C. Un point D est choisi à l'intérieur du triangle CBH de tel sorte que la droite (CH) coupe le segment $[AD]$ en son milieu. P est l'intersection des droites (BD) et (CH). Soit ω le demi-cercle de diamètre $[BD]$ qui coupe le segment $[CB]$ en son intérieur. Une droite passant par P est tangente à ω en Q. Montrer que les droites (CQ) et (AD) se coupent sur ω.

– Exercices encore un peu plus durs –

Exercice 14
Soit ABC un triangle, H son orthocentre, M le milieu de $[BC]$ et F le pied de la hauteur issue de A. On note D le point du cercle ABC tel que $\widehat{HDA} = 90$. On note K le point du cercle ABC tel que $\widehat{DKH} = 90$ Montrer que les cercles DKH et FKM sont tangents en K.

Exercice 15

Un quadrilatère $ABCD$ admet un cercle inscrit de centre I. Soit I_a, I_b, I_c et I_d les centres des cercles inscrits de DAB, ABC, BCD et CDA respectivement. On suppose que les tangentes commune extérieurs des cercles AI_bI_b et CI_bI_d se coupent en X, et les tangentes communes extérieures de BI_aI_c et DI_aI_c en Y. Montrer que $\widehat{XIY} = 90$.

Exercice 16

Soit ABC un triangle et ω son cercle inscrit. D est le point de tangence de ω sur $[BC]$. H est le pied de la hauteur issue de A. On note M le milieu de $[AH]$. (DM) recoupe ω en N. Montrer que le cercle circonscrit de BCN est tangent à ω.

Exercice 17

Soit $ABCD$ un quadrilatère convexe tel qu'il existe un cercle ω tangent à (AB) et (BC) au delà de A et C ainsi qu'à (AD) et (DC). On note ω_1 le cercle inscrit de ABC, ainsi que ω_2 le cercle inscrit de ADC. Montrer que les tangentes communes extérieurs de ω_1 et ω_2 se coupent sur ω.

Exercice 18

Soit ABC un triangle et Ω son cercle circonscrit. on prend une tangente (t) à Ω. On note (t_a), (t_b) et (t_c) les symétriques de t par rapport à BC, CA et AB. Montrer que le cercle circonscrit du triangle formé par (t_a), (t_b) et (t_c) est tangent à Ω.

– Solutions des exercices faciles –

Solution de l'exercice 1

On note M le milieu du segment $[AD]$. On sait alors que (YM) est la médiatrice de $[AD]$ et que (CY) est a bissectrice de l'angle $\widehat{ACD}$, ainsi d'après le théorème du pôle Sud on trouve que les points A, Y, D et C sont cocycliques. Cela permet d'affirmer que $\widehat{YAI} = \widehat{YAD} = \widehat{YCD} = \frac{\gamma}{2}$. On trouve de la même manière que $\widehat{XAI} = \frac{\beta}{2}$. Cela donne $\widehat{YAX} = \frac{\gamma+\beta}{2}$. On trouve ainsi $\widehat{YAX} + \widehat{YIX} = \frac{\gamma+\beta}{2} + \widehat{BIC} = \pi$ car ces derniers sont les angles du triangle BIC. Ainsi, $\widehat{YAX} + \widehat{YIX} = \pi$ ce qui conclut.

Solution de l'exercice 2

On trouve tout d'abord que BD et CE sont des hauteurs du triangle. On sait que $MX = MX$, que $ME = MD$ et que $\widehat{XME} = \widehat{XMD}$, donc les triangles EXM et DXM sont isométriques ce qui montre que $XE = XD$. On peut ainsi définir X comme l'intersection de la médiatrice de $[ED]$ avec la bissectrice de $\widehat{EAD}$, d'après le théorème du pôle sud les points A, E, X et D sont cocycliques. Maintenant on peut finir en chasse aux angles. $\widehat{AXD} = \widehat{AED} = \widehat{ACB} = \widehat{ACF}$ donc le quadrilatère $DXFC$ est cyclique, par symétrie le quadrilatère $BEXF$ est également cycliques.

Solution de l'exercice 3

On va passer aux directions perpendiculaires. On sait que le droites qui relie le centre de deux cercles est perpendiculaire à leur axe radical. On trouve ainsi $(O_1O_2) \perp (AB)$, $(O_1O_3) \perp (AP)$, $(O_3O_4) \perp (AC)$ et $(O_2O_4) \perp (AQ)$. Le quadrilatère $O_1O_2O_3O_4$ est cyclique si et seulement si $(O_2O_1, O_1O_3) = (O_2O_4, O_4O_3)$ qui par passage à la perpendiculaire devient $(AB, AP) = (AQ, AC)$.

Solution de l'exercice 4

On va montrer que P est sur le cercle antarctique. On va pour cela raisonner en terme d'angles orientés. On note alors $(PB, BI) = x$, alors $(AB, BP) = \frac{\beta}{2} - x$ et $(PB, BC) = \frac{\beta}{2} + x$. De la même manière en posant, $(PC, CI) = y$ on trouve, $(PC, CA) = \frac{\gamma}{2} + y$ et $(PC, CB) = \frac{\gamma}{2} - y$. La relation de l'énoncé devient alors $2x = 2y$ ou encore $x = y$. Donc $(PB, BI) = (PC, CI)$ et donc les points B, C, I et P sont cocycliques. Ainsi, P est sur le cercle antarctique mais le cercle antarctique admet (AI) comme diamètre donc $AP \geqslant AI$ et $AP = AI$ si et seulement si $P = I$.

Solution de l'exercice 5

Soit Y l'intersection des droites (AB) et (CX). On sait que $\widehat{IBC} = \frac{\beta}{2}$, que $\widehat{ICB} = \frac{\gamma}{2}$ et que $\widehat{BXC} = 90$, ainsi on trouve $\widehat{XCI} = \frac{\alpha}{2}$. On a aussi $\widehat{BAI} = \frac{\alpha}{2}$ donc les points A, Y, X et C sont cocycliques. Ainsi, les projections orthogonales de I sur les trois côtés du triangle AYC sont alignés, il s'agit là des points F, E et X qui sont donc bien alignés.

Solution de l'exercice 6

On note H_A le pied de la hauteur issue de A. On note Z l'intersection des cercles BWN et CWM, alors $\widehat{XZW} = 90$ et $\widehat{WZY} = 90$ cela montre que les points X, Y et Z sont alignés. On sait que les points M, N, B et C sont cocycliques. Ainsi en regardant les axes radicaux des cercles BWN, CWM et $BCMN$ on trouve que les droites BN, CM et WZ sont concourantes ou encore que X, Z et A sont alignés. On a de plus, $AZ \cdot AW = AN \cdot AB = AH \cdot AH_A$ donc les points Z, W, H et H_A sont cocycliques. Ainsi, $\widehat{HZW} = \widehat{HH_AW} = 90$. Et ainsi, les points X, Y et H sont alignés.

Solution de l'exercice 7
On note S le pôle Sud depuis A. On note D' le point de l'arc $\widehat{AB}$ tel que $AD' = AD$. On définit E' de manière symétrique. Soit F' le milieu de l'arc $\widehat{D'B}$, alors F' est sur la médiatrice de $[BD']$ et sur la bissectrice de $\widehat{D'AB}$ soit sur la médiatrice de $[D'D]$ car $AD' = AD$. Le point F' est sur deux médiatrices du triangle $D'DB$ il est donc sur la troisième, soit la médiatrice de $[BD]$, ainsi $F' = F$. De la même manière G est le milieu de l'arc $\widehat{E'C}$.

On démontre maintenant le lemme suivant. Soit quatre points X_1, X_2, X_3 et X_4 sur un cercle, on note Y_i le milieu de l'arc $\widehat{X_iX_{i+1}}$, alors $(Y_1Y_3) \perp (Y_2Y_4)$. La preuve du lemme est trivial il suffit de montrer que $\widehat{Y_1Y_2Y_4} + \widehat{Y_2Y_1Y_3} = 90$, mais l'angle $\widehat{Y_1Y_2Y_4}$ est proportionnel à la longueur d'arc entre Y_1 et Y_4. De même l'angle $\widehat{Y_2Y_1Y_3}$ est proportionnel à la longueur d'arc entre Y_2 et Y_3. Or $\widehat{Y_1Y_4} + \widehat{Y_2Y_3} = \dfrac{\widehat{ABC} + \widehat{ADC}}{2} \sim \dfrac{\pi}{2}$. En posant $\{D', E', C, B\} = \{X_1, X_2, X_3, X_4\}$ et alors $\{A, G, S, F\} = \{Y_1, Y_2, Y_3, Y_4\}$. On trouve $(FG) \perp (AS)$, or $(DE) \perp (AS)$ donc $(FG)//(DE)$.

– Solutions des exercices moyens –

Solution de l'exercice 8
a) On note Ω le cercle inscrit de $A_1A_2 \dots A_n$ et T le centre d'homothetie négative qui envoie Ω sur Γ. X_i est ainsi le centre d'homothetie négative qui envoie Ω sur ω_i, T_i est le centre d'homothetie positive qui envoie ω_i sur Γ, donc d'après Monge, les points T_i, X_i et T sont alignés. T est donc un point commune aux n droites, elles sont donc concourantes.

b) On reprend les notations précédentes, on note de plus S le centre d'homothetie positive qui envoie Ω sur Γ. On montre, également en utilisant Monge, que les points S, S_i et X_i sont alignés. S est donc un point commun à toutes les droites, elles sont donc concourantes.

Solution de l'exercice 9
On note X l'intersection de (DP) et du cercle ABD, alors $(PX, XB) = (DX, XB) = (DC, CB) = (PK, CB) = (PK, KB)$, ce qui montre que les points P, X, B et K sont cocycliques, en échangent les rôles de B et C on montre également que les points X, L, Q et C sont cocycliques. Cela permet d'oublier les points L et K de l'énoncé. Comme X, P et Q sont alignés il suffit de démontrer que la tangente, t_P en P au cercle PXB et la tangente, t_Q en Q au cercle XQC sont parallèle. Ou encore que $(t_P, PX) = (t_Q, QX)$. Or, $(t_P, PX) = (XB, PB) = (XB, AB) = (XC, AC) = (t_Q, QX)$ ce qui conclut.

Solution de l'exercice 10
On note M_B et M_C les milieux des côtés de $[AC]$ et $[AB]$ respectivement. Le cercle KLM est tangent à la droite (PQ) si et seulement si $\widehat{QMK} = \widehat{MLK}$ et $\widehat{PML} = \widehat{MKL}$. On sait que $(MK)//(PB)$ et que $(ML)//(PC)$. Donc $\widehat{KML} = \widehat{BAC} = \alpha$, $\widehat{QMK} = \widehat{AQP}$ et $\widehat{LMP} = \widehat{APQ}$. Si la droite (PQ) est tangente au cercle KLM, on a donc $\widehat{KML} = \widehat{BAC}$, $\widehat{AQP} = \widehat{MLK}$ et

$\widehat{APQ} = \widehat{MKL}$. Ce qui implique donc $APQ \sim MKL$, on sait que $\widehat{KML} = \widehat{QAP}$ également dans le cas où la droite (PQ) n'est pas tangente au cercle KLM, il faut et il suffit donc d'avoir $\frac{AP}{AQ} = \frac{MK}{ML} = \frac{2MK}{2ML} = \frac{BQ}{CP}$. On trouve donc $BQ \cdot AQ = AP \cdot PC$. Soit P' et Q' les symétriques de P et Q par M_B et M_C respectivement. Alors on trouve $AQ \cdot AQ' = AP \cdot AP'$ ou encore que Q, Q', P et P' sont cycliques. Mais alors le centre de ce cercle est l'intersection des médiatrice de $[QQ']$ et $[PP']$ soit OM_B et OM_C, donc O est le centre du cercle et ainsi : $OP = OQ$.

Solution de l'exercice 11

Comme la conclusion est symétrique il suffit de montrer que si X_1, X_3 et E sont alignés alors X_2, X_4 et F le sont également. On note Y_1, Y_2, Y_3 et Y_4 les points de tangences respectifs de ω_1, ω_2, ω_3 et ω_4 (ω_i est le cercle inscrit dont le point de tangence est X_i) sur les côtés AB, BC, CD et DA. On note aussi Z_1, Z_2, Z_3 et Z_4 les points de tangences respectifs de ω_1, ω_2, ω_3 et ω_4 sur les côtés CD, DA, AB et BC. On prend γ_1 le cercle tangent extérieurement à ω_1 en X_1 et à ω_3 en T, alors d'après le théorème de Monge, les centres d'homothetie extérieurs des cercles ω_1, ω_3 et γ_1 sont alignés, soit E, X_1 et T alignés. Comme par hypothèse les points E, X_1 et X_3 sont alignés (et pour des raisons de positions évidentes) on trouve bien $X_3 = T$. Donc γ_1 est tangent au cercle ω_1 en X_1 et ω_3 en X_3. les tangentes communes sont donc (BC) et (AD). On obtient ainsi $FX_1 = FX_3$, on sait aussi que $FY_2 = FZ_2$ et $FZ_4 = FY_4$, donc $X_1Y_2 = X_3Z_2$ et $Z_4X_1 = X_3Y_4$. Or, $Z_4X_1 = Y_1X_4$, $Y_4X_3 = Z_3X_4$ donc $Y_1Z_3 = 2Z_4X_1$. De la même manière, $Z_1Y_3 = 2X_1Y_2$. On a cependant $Z_1Y_3 = Y_1Z_3$ ce qui montre que $Z_4X_1 = X_1Y_2$, ou encore $Y_1X_4 = Z_1X_2$ et donc $EX_4 = EX_2$. Il existe donc un cercle γ_2 tangent à (AB) et (CD) en X_4 et X_2. D'après le théorème de Monge appliqué aux cercles ω_4, ω_2 et γ_2, les points X_4, X_2 et F sont bien alignés.

Solution de l'exercice 12

On note ω_i le cercle inscrit de centre I_i. On va démontrer que la seconde tangente intérieure de ω_1 et ω_3, que l'on appellera g' passe par C. La seconde tangente de ω_1 depuis C recoupe g en X. on va alors montrer que le quadrilatère $ADCX$ est circonscriptible. On peut établire deux relations sur les quadrilatères $ABXC$ et $ABCD$ au vu de leur circonscraptibilité. On trouve

$$AD - AB + BC - CD = 0 \quad (1)$$

et

$$CX - XA + AB - BC = 0 \quad (2)$$

On somme les relations (1) et (2) pour obtenir $CX - XA + AD - DC = 0$ cette dernière relation implique que le quadrilatère $ADCX$ est circonscriptible. Cela montre bien que la seconde tangente intérieure de ω_1 et ω_3 passe par C. Dans l'optique de démontrer que l'orthocentre de $I_1I_2I_3$ se trouve sur g on va montrer que les symétriques de g par les trois côtés de $I_1I_2I_3$ sont concourants, on finira ensuite en utilisant la droite de Steiner. Le symétrique de g par I_1I_2 est la droite (BC), le symétrique de g par I_2I_3 est (DC) et enfin le symétrique de g par I_1I_3 est g'. Or les droites (BC) et (DC) se coupe en C mais comme démontré plus haut g' passe également par C, on conclut en disant que la droite de steiner d'un point (la droite formé par les symétriques d'un point sur le cercle circonscrit) par un triangle passe par l'orthocentre du triangle.

Solution de l'exercice 13

On va essayer de regarder l'exemple d'un point D pour comprendre un petit peu. Le point D reste toujours sur une droite qui est une homothetie de centre A et de facteur 2, on nomme cette droite (l). On va regarder le cas où D est le symétrique de A par D, c'est-à-dire l'intersection de (l) avec (AB), on nomme cette position particulière de D le point D_1. On prend X la projection orthogonale de D_1 sur (BC). Le point P correspondant à D_1 est H. On va ici montrer que le point X correspond au point Q pour le point D_1. On a tout d'abord X est clairement sur le cercle de diamètre BD_1. On va maintenant montrer que la droite (HX) est tangente au cercle D_1XB. On sait pour cela que $HC^2 = HA \cdot HB$, comme le triangle CHX est isocèle en H (la projection de H sur (BC) est le milieu de $[CX]$ par Thalès) on trouve $HX^2 = HA \cdot HB = HD_1 \cdot HB$ donc la droite (HX) est bien tangente au cercle D_1XB ce qui montre que $X = Q_1$ le point Q correspondant au point D_1. On note ω_1 le cercle D_1XB. On peut maintenant regarder la configuration général. On regarde maintenant la similitude de centre B qui envoie D_1 sur D, comme $BHP \sim BD_1D$ cette similitude envoie aussi H sur P, elle envoie B sur B et envoie ainsi ω_1 sur ω, elle envoie donc la tangente depuis H à ω_1 sur la tangente depuis P à ω. Ainsi, $BD_1D \sim BQ_1Q$. On sait de plus que $BQ_1C \sim BD_1A$. On note Y le point d'intersection des droites (AD) et (CQ). Alors $\widehat{YDB} = 180 - \widehat{ADB} = 180 - \widehat{CQB} = \widehat{YQB}$, ce qui montre que les points D, B, Q et X sont cocycliques, ce qui conclut.

– Solutions des exercices durs –

<u>*Solution de l'exercice 14*</u>

On note H_B et H_C les pieds des hauteurs issues de B et C respectivement dans ABC. On va tout d'abord démontrer le lemme suivant : Les symétriques de H par F et M sont sur le cercle circonscrit. On sait pour cela que les points A, H_B, H et H_C sont cocycliques. Donc $\widehat{H_BHH_C} = 180 - \alpha$, On note H' le symétrique de H par F, alors $\widehat{BH'C} = \widehat{BHC} = \widehat{H_BHH_C} = 180 - \alpha$ ce qui montre que H' est bien sur le cercle ABC. On note A' le symétrique de H par M, alors $\widehat{BA'C} = \widehat{BHC} = \widehat{H_BHH_C} = 180 - \alpha$, ce qui montre de la même manière que A' se trouve bien sur le cercle ABC. On trouve ainsi que $(H'A')$ est parralèle à (BC) et donc $\widehat{A'H'A} = 90$ ce qui montre que $[AA']$ est un diamètre de ABC, on sait que $\widehat{ADH} = 90$ donc les points D, H, M et A' sont alignés.

On veut démontrer que les cercles DKH et FKM sont tangents, on pense donc tout naturellement à regarder le deuxième cercle passant par F et M qui est tangent au cercle DKH, il s'agit en fait du cercle HFM en effet les diamètre des cercles DKH et HFM, respectivement $[DH]$ et $[HM]$ sont alignés. On prend la tangente commune à ces deux cercles en H, il s'agit aussi de la perpendiculaire en H à la droite (HM). Cette droite recoupe (BC) en un point que l'on notera X. Soit Y le milieu de $[DH]$ la projection orthogonale de H sur (XY) est notée Z, on note T le symétrique de H par Z, alors $YD = YH = YT$ ce qui montre que $\widehat{DTH} = 90$. On sait que $XZ \cdot XY = XH^2 = XF \cdot XM$ donc les points Y, Z, M et F sont cocycliques. l'homthetie de centre H et de facteur 2 envoie Y sur D, Z sur T, M sur A' et F sur H', cela montre que le point T est cocyclique avec D, H' et A' donc que T est également sur le cercle ABC d'après ce qui est dit au dessus. Tout cela démontre que $T = K$. On peut maintenant conclure.

On sait que $XK = XH$ par construction du point $T = K$. Donc, $XK^2 = XH^2 = XF \cdot XM$ ce qui montre que la droite (XK) est tangente au cercle KFM ce plus par symétrie axiale d'axe (XY) la droite (XK) est tangente au cercle DKH. Cela montre donc que les cercle DKH et FKM sont tangents.

Solution de l'exercice 15

On note ω_i le cercle inscrit de centre I_i et de rayon r_i, on note aussi O_A, O_B, O_C et O_D les centres des cercles AI_bI_d, BI_aI_c, CI_bI_d et DI_aI_c. On va commencer par démontrer que les cercles ω_a et ω_c sont tangents tous les deux en le même point sur (AC). Soit X_a le point de tangence de ω_a sur (BD) et X_c le point de tangence de ω_c sur (BD). On sait que $ABCD$ est circonscriptible, cela implique que $AB - AD = BC - CD$. On Peut calculer la distance BX_a elle vaut $\frac{AB - AD + BD}{2} = \frac{BC - CD + BD}{2} = BX_c$ ce qui montre que $X_a = X_c$. On renomme ce dernier point T. Alors les points I_a, T et I_c sont alignés et $(I_aI_c) \perp (BD)$. On note $\widehat{ABT} = 2x$ et $\widehat{TBC} = 2y$, alors $\widehat{ABI} = x + y$ et $\widehat{ABI_a} = x$, ce qui montre que $\widehat{I_aBI} = y$ et ainsi que les droites (BT) et (BI) sont conjuguées isogonales dans le triangle BI_aI_c, or (BT) est la hauteur dans ce même triangle et son conjugué est, il est connu, la droite passant par B et le centre du cercle circonscrit. Donc O_B est sur la droite (BI). De la même manière O_D se trouve sur la droite (DI). On sait aussi que $(O_BO_D) \perp (I_aI_c)$ donc $(DB)//(O_BO_D)$. On va maintenant démontrer que la droite (IY) bissecte l'angle $\widehat{BID}$. X se trouve sur la droite O_BO_D de telle sorte que $\frac{XO_B}{XO_D} = \frac{r_b}{r_d}$, par le lemme de la bissectrice on veut montrer que $\frac{IO_B}{IO_B} = \frac{r_b}{r_d}$, or comme $(DB)//(O_BO_D)$ on a $\frac{IO_B}{IO_D} = \frac{IB}{ID}$. On va maintenant calculer $X := r_b \cdot \frac{1}{r_d} = \frac{\sin(\widehat{IAB}) \cdot AI}{\sin(\widehat{ABI})} \frac{\sin(\widehat{ADI})}{\sin(\widehat{IAD}) \cdot AI}$ d'après la loi des sinus dans les triangles IAB et IAD, $X = \frac{\sin(\widehat{ADI})}{\sin(\widehat{ABI})}$. On trouve d'autre part, $X' := r_b \cdot \frac{1}{r_d} = \frac{2I_aI_c}{\sin(\widehat{I_aDI_c})} \cdot \frac{\sin(\widehat{I_aBI_c})}{2I_aI_c} = \frac{\sin(\widehat{I_aDI_c})}{\sin(\widehat{I_aBI_c})}$, or, $\widehat{ADI} = \frac{\widehat{ADC}}{2} = \widehat{I_aDI_c}$ et également $\widehat{ABI} = \widehat{I_aBI_c}$ ce qui montre que $X = X'$ et ainsi que la droite (IY) est la bissectrice extérieure de l'angle $\widehat{BID}$. On montre de la même manière que la droite (XI) est la bissectrice extérieure de l'angle $\widehat{AIC}$. Dans le but de démontrer que $\widehat{XIY} = 90$ il faut démontrer que les angles $\widehat{AIC}$ et $\widehat{BID}$ ont les même bissectrice. Si la proposition suivante est vraie alors, $(DI, IC) = (AI, IB)$. Ou encore $(CI, ID) + (AI, IB) \equiv 0 \pmod{180}$. On va démontrer cette dernière relation, on appelle E le point d'intersection des droites (AD) et (BC), Alors $(AI, IB) = 90 + \frac{(BE, EA)}{2}$ et $(CI, ID) = 90 - \frac{(BE, EA)}{2}$, donc $(AI, IB) + (BE, EA) = 180 \equiv 0 \pmod{180}$, ce qui conclut.

Solution de l'exercice 16

On note ω_1 le cercle A-exinscrit, de centre J, on note D' le point de tangence de ω_1 sur $[BC]$ et D'' le point diamétralement opposé à D' dans ω_1. on regarde maintenant l'homothetie de centre A qui envoie ω sur ω_1. Elle envoie I sur J et envoie également la droite (BC) sur une droite parallèle à elle-même et tangente à ω_1 se point de tangence est donc D'' ce qui montre que les points A, D et D'' sont alignés. On sait que la droite (Ah) et la droite $(D'D'')$ sont parrallèles et que les points A, D et D'' sont alignés ainsi que les points H, D et D' on trouve que les milieux de $[AH]$ et $[D'D'']$ sont alignés avec D. On sait ainsi que la droite (MD) passe par J.

On prend maintenant la tangence en N à ω elle recoupe la droite (BC) en X, la droite (IX) recoupe la droite (DN) en le milieu de $[DN]$, que l'on appellera Y. Alors $\widehat{IYJ} = 90$ ce qui montre que Y est sur le cercle antarctique (de diamètre $[IJ]$) depuis A dans ABC, ce cercle passe ausi par B et C. on a alors $XN^2 = XY \cdot XI$ (car $\widehat{IYN} = \widehat{INX} = 90$) et $XY \cdot XI = XB \cdot XC$ (car les points I, Y, B et C sont cocycliques), donc $XN^2 = XB \cdot XC$ ce qui montre que la droite (XN) est une tangente commune des cercles ω et BNC ce qui montre que ces deux cercles sont bien tangents.

Solution de l'exercice 17

On nomme T_1 le point de tangence de ω_1 sur $[AC]$, on note également T_2 le point de tangence de ω_2 sur $[AC]$. On va tout d'abord démontrer que $AT_2 = CT_1$. La condition de tangence de ω donne $AD - DC = CB - BA$, Donc $AT_2 = \dfrac{AD + AC - DC}{2} = \dfrac{CB - AB + AC}{2} = CT_1$. Cette relation permet de motiver les trace de nouveaux cercles. Ainsi, on trace ω_3 le cercle B-exinscrit dans le triangle ABC, alors comme $AT_2 = CT_1$ le cerlce ω_3 est tangente à (AC) en T_2. Introduisons maintenant la parallèle (d_1) à (AC) tangente à ω_1 en X. Alors une homothetie de centre B envoie ω_1 sur ω_3 elle envoie ainsi (d_1) sur (AC) et X sur T_2, donc les points B, X et T_1 sont alignés. Il existe aussi une homothetie de centre B qui envoie ω_3 sur ω elle envoie (AC) sur la droite parrallèle à (AC) "la plus proche de B" tangente ω en Z, donc les points B, T_2 et Z sont alignés. Cela montre que les points T_2, X et Z sont alignés sur une droite g. Soit Z' le point d'intersection des tangentes communes extérieures de ω_1 et ω_2, alors il s'agit du centre d'homthetie positive qui envoie ω_1 sur ω_2, en appliquant Monge aux cercles ω_1, ω_2 et ω_3 on remarque que le point Z' est sur la droite (T_2X). On introduit de la même manière la droite (d_2) parrallèle à (AC) et tangente à ω_2 en Y. On trouve alors par argument de symétrie que les points T_1, Y, Z' et Z sont alignés sur une droite g'. Les droites g et g' se coupent en deux points Z et Z' mais elles ne sont pas confondues (en tout cas pas une suffisement de fois) donc $Z = Z'$ or Z est sur ω sont Z', l'intersection des deux tangentes communes extérieures de ω_1 et ω_2 également, cela conclut.

Solution de l'exercice 18

Avec $\{I, J, K\}$ une permutation de $\{A, B, C\}$, on note T_I le symétrique de T par la droite (JK), on note X_I l'intersection des droite (t_j) et (t_k). D'après le droite une homothetie de facteur 2 de la droite de Simson les points T_A, T_B et T_C sont alignés.

Lemme 4.1.1.
Les points T_A, T_B, C et X_C sont cocycliques.

On va compose la symétrie d'axe (AC) et la symétrie d'axe (BC), on appelle cette composition R, la composition de ces deux symétrie axiale est une rotation d'angle $2\widehat{ACB} = 2\gamma$. R envoie t_b sur t_a et plus précisément T_B sur T_A. Ainsi par nature de R on trouve $(T_BC, CT_A) = 2\gamma$ mais aussi X_C étant l'intersection de t_b et t_c que $(T_BX, XT_A) = (t_b, t_c) = 2\gamma$, donc $(T_BC, CT_A) = (T_BX, XT_A)$ ce qui montre bien que les points T_B, T_A, C et X_C sont cycliques, on note ω_c le cercle circonscrit de ce quadrilatère.

On définit de la même manière ω_a et ω_b.

Lemme 4.1.2.
Les cercle ω_a et ω_c se coupent sur Ω

On note X la deuxième intersection des cercle ω_a et ω_c autre que T_B. On veut monter que $(AX, XC) = (AB, BC)$. Or $(AX, X) = (AX, XT_B) + (XT_B, XC) = (AT_C, T_CT_B) + (T_AT_B, T_AC)$ On note maintenant Y_B l'intersection des droites (T_CA) et (T_AC). Alors comme les points T_A, T_B et T_C sont alignés on trouve $(AT_C, T_CT_B) + (T_AT_B, T_AC) = (AT_C, T_CT_A) + (T_AT_C, T_AC) =$

$(AT_C, T_AC) = (AY_B, Y_BC)$. On veut ainsi montrer que $(AY_B, Y_BC) = (AB, BC)$ ou encore que les points, A, B, C et Y_B sont cocycliques. Comme le point T est sur Ω, on trouve $(TC, CB) = (TA, AB)$ et par symétrie axiale on trouve $(TC, CB) = -(T_AC, CB)$ ainsi que $(TA, AB) = -(T_CA, AB)$. donc $(Y_BA, AB) = (T_CA, AB) = (T_AC, CB) = (Y_BC, CB)$ ce qui montre bien que le point Y_B se trouve sur Ω et donc que $(AY_B, Y_BC) = (AB, BC)$ et donc que X est sur Ω.

On remarque que dans le quadrilatère complet formé par les droites (t_a), $(t_b$, (t_c) et T_AT_C on a les cercles ω_a et ω_c qui contiennent le point de Miquel du quadrilatère donc X est aussi sur ω_b (trivial par argument de symétrie) mais également sur $X_AX_BX_C$ ainsi le point X est sur les deux cercles dont nous ovulons montrer la tangence il s'agit donc du point de tangence. on remarque que l'on a pas utilisé le fait que la droite t est tangente au cercle Ω.

On peut maintenant finir de deux manières :

a) On peut tout d'abord introduire la tangente (l) au cercle $X_AX_BX_C$ en X et montrer qu'elle est également tangente au cercle Ω. On a $(X_CX, l) = (X_CX_A, X_AX)$, comme les points X_A, T_B et X_C sont alignés on trouve $(X_CX_A, X_AX) = (T_BX_A, X_AX) = (T_BA, AX)$. On a aussi $(CX, X_CX) = (CT_B, X_CT_B) = -(CT, t)$ par symétrie axiale. $-(CT, t) = -(CA, AT) = (CA, T_BA)$ pr symétrie. Donc $(CX, l) = (CX, X_CX) + (X_CX, l) = (T_BA, AX) + (CA, T_BA) = (CA, AX)$ donc la droite l est tangente à Ω et à $X_AX_BX_C$ en X, ces deux cercles sont donc tangents.

b) On va utiliser que avant un état avancé de la preuve la condition que t est tangente à Ω n'est pas utile. Prenons maintenant une droite (t) qui n'est pas tangente à Ω mais qui coupe ce cercle en T et T', alors d'après ce que l'on a vu plus tôt on peut introduire X en correspondance à T comme fait précédemment, on peut aussi introduire X' pour le point T, on a montré que le cercle $X_AX_BX_C$ passe par X, il passe donc aussi par argument de symétrie par X'. Ainsi, les deux cercles $X_AX_BX_C$ et Ω ont X et X' en commun. On fait maintenant tourner la droite t autour du point t de tel sorte que T' se rapporte vers T. En même temps que T' se rapproche de T le point X' se rapproche du point X, on passe maintenant à la limite, lorsque $T' = T$ la droite t est tangente à Ω mais alors $X' = X$ donc les cercles $X_AX_BX_C$ et Ω sont alors tangents ce qui conclut.

2 Géométrie projective

– Énoncés –

Exercice 1 (Problème 4, IMO 2014)
Des points P et Q sont choisis sur le côté $[BC]$ d'un triangle acutangle de tel sorte que $\widehat{PAB} = \widehat{ACB}$ et $\widehat{QAC} = \widehat{CBA}$. Les points M et N sont choisis sur les droites (AP) et (AQ) de tel sort que $AP = PM$ et $AQ = QN$. Montrer que les droites (BM) et (CN) se coupent sur le cercle circonscrit de ABC.

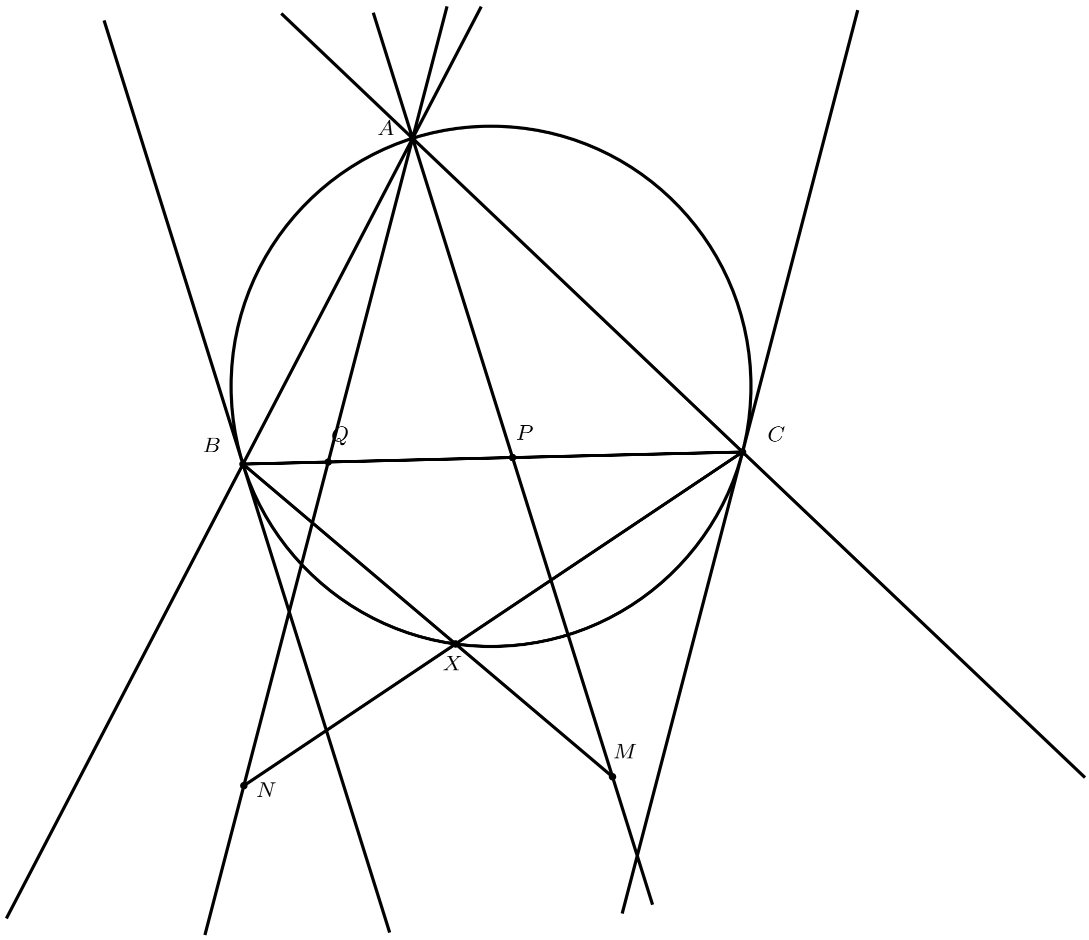
Exercice 2 (Problème 5, IMO 2005)
Soit $[AB]$ et $[CD]$ deux segments tel que $AB = CD$, on prend des points P et Q sur ces segments de tel sorte que $AP = CQ$. Les droites (AC) et (BD) se coupent en X et la droite (PQ) recoupe les droites (AC) et (BD) en E et F respectivement. Montrer que lorsque le point P bouge le cercle circonscrit passe par un point fixe autre que X.

Exercice 3 (Problème G7, Liste courte IMO 2015)
Soit $ABCD$ un quadrilatère convexe et P, Q, R et S des points sur les côtés $[AB]$, $[BC]$, $[CD]$ et $[DA]$. Les droites (PQ) et (SR) se coupent en O. On suppose que les quadrilatère $APOS$, $BQOP$, $CROQ$ et $DSOR$ admettent des cercles inscrit. Montrer que les droites (AC), (PQ) et (RS) sont concourantes.

Exercice 4 (Problème 3, RMM 2011)
Soit ABC un triangle acutangle, on prend une droite ℓ parallèle à (BC), elle coupe (AB) en D et (AC) en E, elle recoupe le petit arc $\widehat{AB}$ et $\widehat{AC}$ en F et G. On appelle γ_1 le cercle tangent à $[BD]$, $[DF]$ et $\widehat{FB}$, et γ_2 le cercle tangent à $[CE]$, $[EG]$ et $\widehat{GC}$. Les tangentes intérieures de γ_1 et γ_2 se coupent en X, trouver le lieu des points X lorsque la droite ℓ bouge.

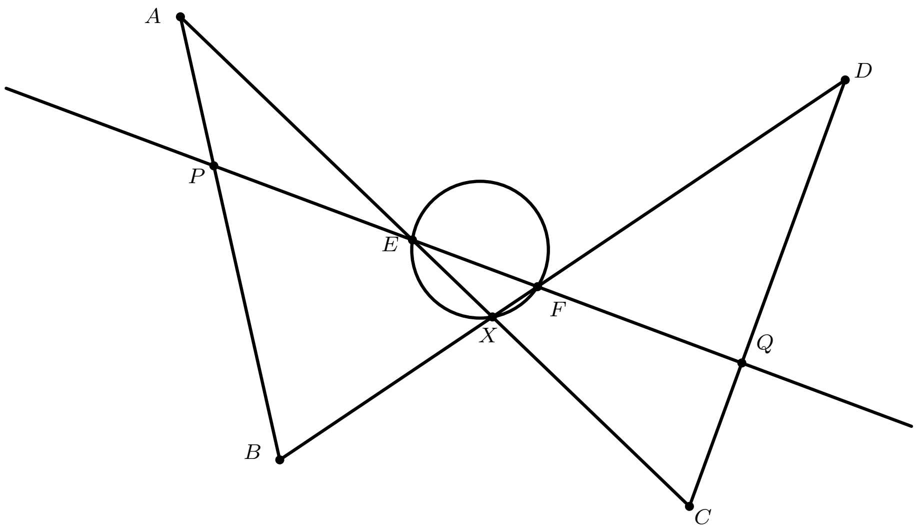
– Solutions –

<u>*Solution de l'exercice 1*</u>



On note X (resp. Y) l'intersection de BM (resp. CN) avec le cercle circonscrit de ABC. On veut montrer que $X = Y$. Une chasse aux angles rapide montre que (t_b) la tangente en B au cercle circonscrit de ABC est parallèle à la droite (AP), donc en projetant depuis B de la droite (AP) sur le cercle circonscrit de ABC. $-1 = b_{AMP\infty} = b_{AXCB} = b_{BCAX}$ de la même manière $b_{BCAY} = -1$ donc par unicité du birapport $X = Y$. Cela conclut.

<u>*Solution de l'exercice 2*</u>



On regarde la transformation qui envoie (AB) sur (DC) et P sur Q, A sur C et enfin B sur D, il s'agit d'une transformation affine, donc projective mais qui échange le point à l'infini de (AB) avec le point à l'infini de (DC). Si on démontre que la transformation affine qui envoie (AC) sur (BD) et E sur F (défini grâce à des droites (PQ) successives). Pour cela on prend la conique tangente aux droites (AB), (CD), (AC), (BD) et (PQ) cette coniques définie uniquement la transformation qui envoie AB sur AD. Elle définit la transformation de la manière suivante : soit P_1 un point de (AB) on prend la tangente à (c) et on recoupe avec (CD) en Q_1, cette transformation est la transformation que l'on veut car elle envoie P sur Q, A sur C et B sur D, comme la transformation est affine elle échange ∞_{AB} avec ∞_{CD}, donc la droite à l'infini est tangente à (c). Cela montre que (c) est une parabole. On regarde maintenant la transformation induite par cette conique qui envoie (AC) sur (BD), cette transformation envoie E sur F et ∞_{AC} et ∞_{BD} donc la transformation qui envoie E sur F est une transformation affine. Si on prend deux positions de P les deux cercles correspondants se coupent en un second point Y, alors Y est le point de Miquel de la similitude direct qui envoie E sur F, comme la transformation E sur F est une transformation affine on trouve que tout les cercles XEF passent par Y également, ce qui conclut.

Remarque 4.2.1.
La transformation construite avec la conique est bien une transformation projective si AB et CD sont bien tangents à la conique.

Solution de l'exercice 3
On rappelle le théorème de Brianchon : Soit (1), (2), (3), (4), (5) et (6) six droites. Les points

$((1)\cap(2),(4)\cap(5))$, $((2)\cap(3),(5)\cap(6))$ et $((3)\cap(4),(6)\cap(1))$ sont alignés si et seulement si les six droites sont tangentes à une même conique. Ainsi, en nommant les droites (1), (2), (3), (4), (5) et (6) comme (QS), (BC), (DC), (PR), (AB) et (AD) la condition de l'énoncé est équivalente à (QS), (BC), (DC), (PR), (AB) et (AD) tangentes à une conique.

Lemme 4.2.2.
Le quadrilatère $ABCD$ admet un cercle inscrit.

Démonstration. Une chasse au tangente démontre ce lemme. □

On nomme ω_1, ω_2, ω_3 et ω_4 les cercles inscrits de $APOS$, $BQOP$, $CROQ$ et $DSOR$. Et ω le cercle inscrit de $ABCD$. On note maintenant $X_1 = (PR)\cap(AD)$, $X_2 = (SQ)\cap(AB)$, $X_3 = (PR)\cap(BC)$ et $X_4 = (SQ)\cap(DC)$. On note enfin X le centre d'homothetie extérieur de ω_1 et ω_3. En appliquant Monge à ω, ω_1 et ω_3 on trouve que A, C et X alignés. En appliquant Monge aux cercles ω_1, ω_4 et ω_3 on trouve X_1, X_4 et X alignés. en appliquant Monge aux cercles ω_1, ω_2 et ω_3, on trouve X_2, X_3 et X alignés. Donc les droites (X_2X_3), (X_1X_4) et (AC) sont concourantes. En posant, (1), (2), (3), (4), (5) et (6) comme (AB), (SQ), (DC), (CB), (RP) et (AB) on trouve d'après le théorème de Brianchon que ces droites sont concourantes.

Solution de l'exercice 4
On va démontrer que X se situe sur la bissectrice de $\widehat{BAC}$.

Soit O_1 et O_2 les centres de γ_1 et γ_2 de rayon r_1 et r_2 respectivement. On regarde l'involution de centre A qui échange B et F ainsi que D et C. Elle échange F et G. Elle échange donc γ_1 et γ_2. Donc elle échange les droites (AO_1) et (AO_2), $\widehat{ABC}$ et $\widehat{O_1AO_2}$ ont la même bissectrice. Comme l'inversion échange γ_1 et γ_2 on a $\frac{AO_1}{AO_2} = \frac{r_1}{r_2}$. On sait que $\frac{r_1}{r_2} = \frac{O_1X}{O_2X}$ donc $\frac{AO_1}{AO_2} = \frac{XO_1}{XO_2}$ ce qui montre que (AX) bissecte $\widehat{O_1AO_2}$ et donc $\widehat{BAC}$.

3 Points de Miquel et similitudes

– Géométrie projective dynamique –

Prérequis

Pour cette partie, il est nécessaire de bien connaitre les différents espaces projectifs unidimensionnels réels, et savoir passer de l'un à l'autre par des transformations conservant le birapport.

Nous avons bien souvent à faire à des exercices laissant la position d'un point assez libre. Il s'agit typiquement d'exercices commençant par la phrase « soit machin un point/un cercle/une droite passant par tel bidule ». Rien de plus horripilant, dans cette situation, que de savoir résoudre une bonne quinzaine de cas particuliers sans savoir résoudre le cas général !

L'innovation majeure de la géométrie dynamique est de ramener une configuration générale à l'étude de cas particuliers, bien plus aisée. Cependant, ne nous voilons pas la face, il faut respecter certaines conditions pour appliquer ce génial principe. . .

Principe d'utilisation

Théorème 4.3.1.
Soit $\mathfrak{P}$ une transformation projective (ou bien une composition de transformations projectives) envoyant les éléments X_i d'un espace projectif unidimensionnel réel E_1 sur les éléments Y_i d'un autre E_2. On note cette transformation $X_i \mapsto Y_i$.

Alors si l'on trouve une transformation projective $\mathfrak{P}'$ envoyant X_1 (resp. X_2, X_3) sur Y_1 (resp. Y_2, Y_3), on peut affirmer que $\mathfrak{P} = \mathfrak{P}'$.

Démonstration. Il suffit de savoir qu'une transformation projective est uniquement définie par l'image de trois points, les autres points étant fixés par leur birapport par rapport aux premiers. □

En pratique

1. Il faut impérativement savoir ce qui peut bouger et ce qui ne le peut pas ! En effet, les espaces projectifs unidimensionnels réels utilisés doivent être des espaces fixes.
2. On essaye de passer de X_i à Y_i en sautant d'un espace projectif unidimensionnel réel à l'autre et *en conservant le birapport* pour montrer l'existence de la transformation *projective* $\mathfrak{P}$.
3. On montre pour trois cas (particuliers et simples) que la transformation mal définie $\mathfrak{P}$ est en fait la transformation projective simple (et qui, accessoirement, résout l'exercice) $\mathfrak{P}'$!
4. On conclut l'exercice, et on se relit pour vérifier qu'on n'essaye pas de truander le correcteur, ce qui le mettrait de mauvais poil.

– Involutions projectives –

Montrons ici quelques résultats phares issus des involutions.

Théorème 4.3.2 (Rappel sur les involutions)**.**

1. Une involution est une transformation $\mathfrak{I}$ qui est sa propre réciproque, ce qui signifie que $\mathfrak{I} \circ \mathfrak{I} = Id$.
2. Une transformation projective complexe qui échange une paire de points est toujours une involution.
3. Il existe une unique involution qui échange deux paires de points quelconques.
4. Une involution peut toujours s'écrire comme la composition d'une symétrie axiale et d'une inversion.
5. Une involution projective complexe peut toujours prendre la forme $X \to \frac{1}{X}$.
6. Le centre de notre involution est le point de Miquel des quatre points considérés.
7. L'axe réel et l'axe imaginaire sont fixes par l'involution ; ce sont des bissectrices pour les paires de droites $(MX; MX')$.

8. L'involution a l'effet d'une inversions sur les objets géométriques.

Démonstration.

1. C'est la définition d'une involution.
2. On définit la transformation projective $\mathfrak{P}$ qui échange X sur X', Y sur Y' et on va chercher l'image de Y', notée K. Alors

$$b_{XX'YY'} \overset{\text{par } \mathfrak{P}}{=} b_{X'XY'K} \overset{\text{manip'}}{=} b_{XX'KY'}.$$

Donc par unicité du birapport, $K = Y$. Ceci est valable pour tout point supplémentaire, donc la transformation est involutive.
3. $\mathfrak{P}$ est l'unique transformation qui échange X et X' et envoie Y sur Y', et on a vu qu'elle échangeait en réalité Y et Y'.
4. Soit $\mathfrak{I}$ l'unique involution qui échange X et X' ainsi que Y et Y'. On considère la transformation $S_{(b)} \circ \mathcal{I}_M$, composée de la symétrie d'axe (b), la bissectrice de $\widehat{XMX'}$ où M est le point de Miquel du quadrilatère $(XY), (XY'), (X'Y), (X'Y')$, et de l'inversion de centre M et de rapport $r^2 = MX \cdot MX'$.
En choisissant M comme centre du plan projectif complexe, en confondant la droite réelle avec (b), et en posant $r^2 = 1$ par une homothétie appropriée, on fait en sorte Quel $S_{(b)} : M(z) \mapsto M(\overline{z})$ et que $\mathcal{I}_M : M(z) \mapsto M\left(\frac{1}{\overline{z}}\right)$ De ces choix judicieux, on déduit que $S_{(b)} \circ \mathcal{I}_M : M(z) \mapsto M\left(\frac{1}{z}\right)$. On vérifie alors aisément que cette composition conserve le birapport, et que c'est une transformation projective.
Maintenant, démontrons que c'est $\mathfrak{I}$: elle échange par définition X et X'. Par propriété du point de Miquel, $MXY \sim MY'X'$, donc l'inversion laisse (MY) fixe et la symétrie échange (MY) et (MY'). Pour les longueurs, $MY \cdot MY' = MX \cdot MX'$, ce qui conclut que Y et Y' sont échangés. Or, $\mathfrak{I}$ est l'unique transformation projective qui fait cela ! Donc $\mathfrak{I} = S_{(b)} \circ \mathcal{I}_M$. On prouve aussi le point suivant, et que le centre de notre involution est le point de Miquel des quatre points échangés.
5. Voir 4.
6. Le centre de l'involution est le point qui est échangé avec l'infini, c'est à dire M d'après notre composition.
7. La paire de droite $(MX; MX')$ est laissée invariante par l'inversion, tandis qu'elle est échangée par la symétrie axiale d'axe réel, d'où la propriété.
8. Rappelons juste que la symétrie axiale est une isométrie.

$\square$

– Théorèmes essentiels –

Théorème 4.3.3 ($1\mathbb{R}$ - Espaces projectifs unidimensionnels réels et leurs involutions)**.**
Liste non exhaustive.

1. *Points sur une droite* :

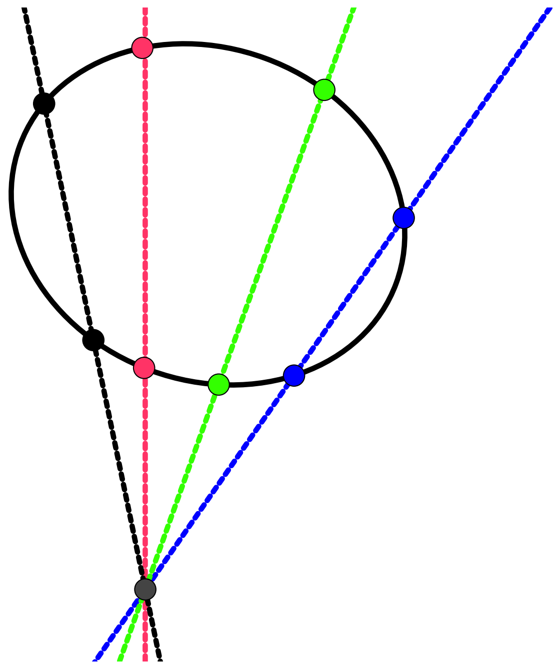
   Les involutions possibles sont au nombre de 3 : celle qui envoie X sur son opposé, sur son inverse et sur l'opposé de son inverse (correspondant respectivement à la symétrie centrale, l'inversion et leur composition).

2. *Droites par un point* :

   Elles sont très variées. Citons la symétrie axiale et le « passage à l'orthogonale ».

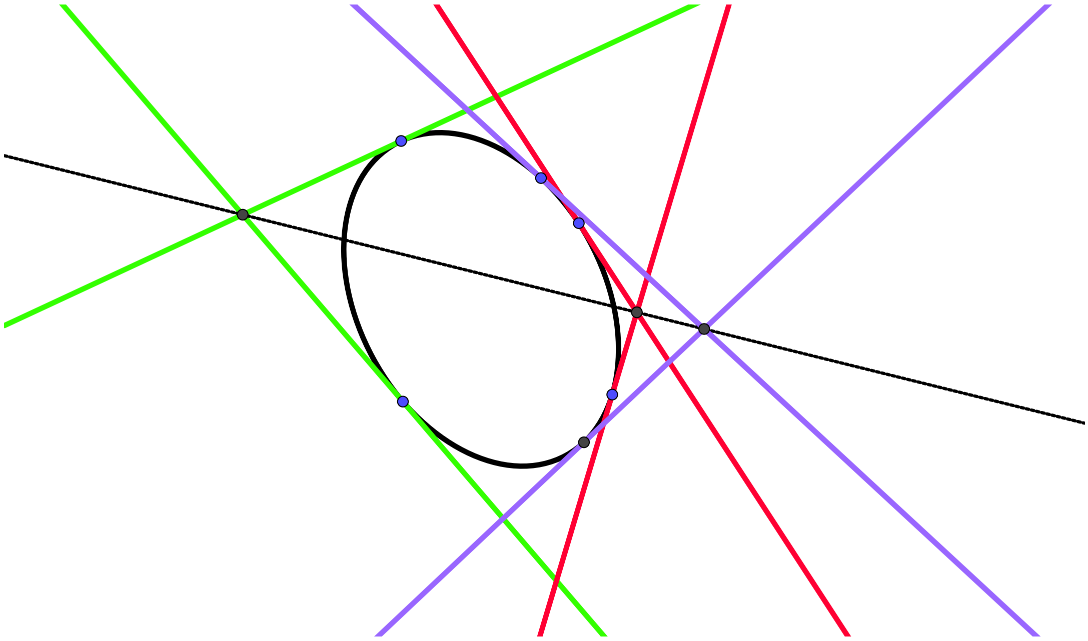
3. *Points sur une conique* :

   Elles ont toujours la forme suivante ; cela traduit que les droites joignant deux points échangés par l'involution sont toujours concourantes. Cette situation est une équivalence : la concourance implique l'involution, et l'involution implique la concourance.



4. *Tangentes à une conique* :

   Elles ont toujours la forme suivante ; cela traduit que les intersection de deux tangentes échangées sont alignées sur une droite. Cette situation est encore une équivalence : l'alignement donne l'involution, et l'involution donne l'alignement.



Théorème 4.3.4 (1$\mathbb{R}$ – Second théorème de Desargues)**.**
Soient A, B, C, D les sommets principaux d'un quadrilatère complet, et (d) une droite qui évite ces sommets. On note $(d) \cap (AB) = X, (d) \cap (CD) = X', (d) \cap (AC) = Y, (d) \cap (BD) = Y', (d) \cap (AD) = Z, (d) \cap (BC) = Z'$.

Alors il existe une involution des points sur la droite (d) qui échange X et X', Y et Y', ainsi que Z et Z'.

Théorème 4.3.5 (1$\mathbb{R}$ – Troisième théorème de Desargues)**.**
Soit K un faisceau de coniques (κ_i) défini par quatre points et (d) une droite qui évite ces quatre points. On définit $(d) \cap \kappa_i = \{X_i; X_i'\}$.

Il existe une involution qui échange les paires de points X_i et X_i'.

Remarque 4.3.6.
Le Théorème 4.3.4 est une généralisation du Théorème 4.3.3. L'intérêt de ces théorèmes est toujours de montrer l'existence d'une transformation projective échangeant des éléments, et de lui trouver une meilleur définition, qui coïncide bien souvent avec l'énoncé. L'avantage des involutions, c'est qu'elle ne peuvent adopter que certaines formes (voir le théorème 1), et qu'il faut montrer la forme particulière qu'elle adopte pour seulement 2 paires de points.

Théorème 4.3.7 (1$\mathbb{C}$ – Condition d'involutions complexes)**.**
Toutes les propositions suivantes traduisent des involutions :

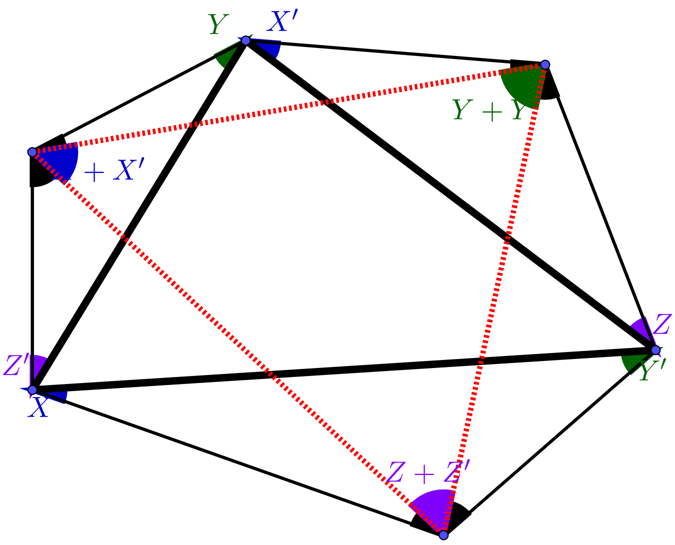
1. Si nous avons un quadrilatère complet, il existe une involution de centre M échangeant ses sommets opposés.
2. Si nous trouvons une transformation projective échangeant une paire de points, c'est une involution.

3. Le point 2 arrive si $b_{BAA'C'} = b_{B'A'AC}$ par exemple. Dans ce cas, l'involution échange A et A', B et B' ainsi que C et C'.
4. Le point 3 arrive si et seulement si
$$\frac{BA'}{CA'} \cdot \frac{CB'}{AB'} \cdot \frac{AC'}{BC'} = 1 \text{ et } \widehat{(A'B, A'C)} + \widehat{(B'C, B'A)} + \widehat{(C'A, C'B)} \equiv 0 \ [2\pi],$$
ce que l'on peut réinterpréter comme étant l'égalité des complexes $b_{BAA'C'} \cdot b_{A'B'AC} = 1$ issue de 3.

Notons que le phénomène observé au point 3 peut en fait se généraliser. En particulier, on peut créer de nombreuses égalités de birapport de cette sorte, le but étant de prouver l'existence d'une transformation projective échangeant une paire de points, et d'autres choisies. Pour démontrer ces égalités de birapport, tout (ou presque...) est permis : triangles semblables, calcul brutal, complexes, Ceva et Ménélaüs, transmission par des espaces projectifs unidimensionnels réels, remarquer leur harmonicité...

Théorème 4.3.8 (1$\mathbb{C}$ – Théorème des triangles fantômes)**.**
En supposant être dans son cadre d'application, et exploitant plusieurs fois le point 4 ci dessus, on obtient ce théorème dans son cas général.

Ce théorème est extrêmement riche, et peut être caché dans bien des exercices. Il faut donc chercher un peu les différentes situations qui peuvent survenir : triangles ajoutés isocèles/équilatéraux/plats/rectangles...



– Braderie d'exercices –

Exercice 1 (Dualité)
Regarder le dual du second théorème de Desargues, de Pappus et du lemme suivant.

Lemme 4.3.9.
Soit $\mathfrak{P}$ une transformation projective envoyant le faisceau de droites $A_{(a_i)}$ sur le faisceau de droite $B_{(b_i)}$. Alors $(a_i) \cap (b_i) = X_i$ parcourt une conique passant par A et B.

.

Exercice 2 (Birapport de 4 coniques d'un faisceau)
Dans cet exercice, on se propose de donner une définition du birapport de quatre coniques.

1. Transformer par une projection adéquate le faisceau de conique en faisceau de cercle.
2. Soit P un point du plan quelconque. Montrer que les polaires p_1, p_2, p_3, p_4 de P par rapport à quatre cercles Γ_i de centre O_i du faisceau sont concourantes.
3. En passant à la perpendiculaire, noter que $b_{p_1,p_2,p_3,p_4} = b_{PO_1,PO_2,PO_3,PO_4}$
4. En projetant sur L'axe de symétrie du faisceau, montrer que ce birapport ne dépend pas de P, donc qu'il est justifié de parler d'un birapport de coniques. On pourra dorénavant poser $b_{\Gamma_1,\Gamma_2,\Gamma_3,\Gamma_4} = b_{p_1,p_2,p_3,p_4}$.
5. Noter que, de retour dans le cadre général, le birapport de quatre coniques peut être assimilé à celui des quatre points d'intersection d'avec une 5ème conique passant par trois des points fixés du faisceau.

Exercice 3
Démontrer qu'une transformation projective complexe a toujours pour forme complexe $z \mapsto \frac{az+b}{cz+d}$ avec a, b, c, d des complexes. En déduire qu'une telle transformation admet toujours deux points fixes.

Exercice 4 (pour s'entraîner)
Montrer la concourance des hauteurs par géométrie dynamique.

Exercice 5
Soit $ABCD$ un parallèlogramme, et P et Q des points de (BC) et (CD) tels que $ABP \sim ADQ$. Montrer que $(BD), (PQ)$ et la tangente au cercle circonscrit à APQ sont concourantes.

Exercice 6 (Théorème du papillon)
Soit $ABCD$ un quadrilatère cyclique de centre O, $X = (AC) \cap (BD)$, et $[EF]$ la corde perpendiculaire à OX passant par X. Elle coupe (AD) et (BC) en Y et Z. Montrer que $XY = XZ$.

Exercice 7
Soit Γ un cercle, et P un point à l'extérieur. On trace les tangentes à γ par P, qui le touchent en A et B. On trace aussi une droite par P qui coupe le cercle en C et D. Montrer que (AB) et les tangentes au cercle en C et D sont concourantes.

Exercice 8
Montrer le théorème de Napoléon.

Exercice 9
Soit ABC un triangle de cercle circonscrit Γ. Une droite d varie, parallèle à (BC), elle coupe $(AB), (AC)$, et Γ respectivement en D, E, K et L. Soit γ_1 (resp. γ_2) le cercle tangent intérieurement à $\Gamma, [KD]$ et $[DB]$ (resp. $\Gamma, [LE]$ et $[EC]$).

Quel est le lieu de l'intersection des tangentes internes aux deux cercles inscrits ?

Exercice 10
Soient ABX et CDX deux triangles directs rectangles en X. On pose $(AC) \cap (BD) = Y$ et $(AD) \cap (BC) = Z$. Montrer que XYZ est rectangle.

Exercice 11 (Algèbre projective)
Résoudre dans $\mathbb{C}^3$ le système

$$\begin{cases} a^2+ab+c=0; \\ b^2+bc+a=0; \\ c^2+ca+b=0. \end{cases}$$

– Correction des exercices –

Solution de l'exercice 1

1. *Dual du second théorème de Desargues* : Soient a, b, c, d les droites principales d'un quadrangle complet (on note P_{uv} l'intersection des droites u et v) et D un point qui n'est sur aucune des droites précédentes. On note $x = (DP_{ab}), x' = (DP_{cd}), y = (DP_{ac}), y' = (DP_{bd}), z = (DP_{ad}), z' = (DP_{bc})$.
   Alors il existe une involution projective du faisceau de droites passant par D qui échange x et x', y et y', ainsi que z et z'.
2. *Dual de Pappus* : On prend trois droites a, b, c passant par un point A dans cet ordre, et trois autres d, e, f passant par un point B dans cet ordre. Alors $a \cap f$, $b \cap e$, $c \cap d$ sont alignés.
3. *Dual du Lemme 4.3.9* : S'il existe une transformation projective des points de la droite d sur les points de la droite d', avec X_i envoyé sur X_i', alors les droites (X_iX_i') sont tangentes à une même conique.

Solution de l'exercice 2

1. On envoie deux des points du faisceau sur les deux points cycliques $(1 : i : 0)$ et $(1 : -i : 0)$, et toutes nos coniques deviennent des cercles passant par deux points.
2. On sait que les axes radicaux de κ_i, κ_j et P sont concourants. En fixant i et en faisant varier j, les axes radicaux de P et des cercles de K sont tous concourants. L'axe radical de P et κ_i est la droite passant par le milieu des tangentes au cercle passant par P, donc en appliquant une homothétie de centre P et de facteur 2, on envoie l'axe radical sur la polaire de P. En conclusion, toutes les polaires de P par rapport aux cercles de K sont concourantes.
3. On sait que la polaire de P par rapport à κ_i est perpendiculaire à PO_i, donc le passage à la perpendiculaire par P envoie p_i sur (PO_i), d'où l'égalité de birapport.
4. On a $b_{PO_1,PO_2,PO_3,PO_4} = b_{O_1O_2O_3O_4}$ donc le birapport des polaires est indépendant du choix de P.

Solution de l'exercice 3
Soit f l'unique transformation projective complexe qui envoie $A(a)$ sur $A'(a')$, $B(b)$ sur $B'(b')$ et $C(c)$ sur $C'(c')$. On va commencer par montrer qu'une homographie conserve le birapport :

$$f(z) = \frac{az+b}{cz+d} = \frac{b-\frac{ad}{c}}{cz+d} + \frac{a}{c} = \frac{\alpha}{cz+d} + \beta.$$

Donc f est la composition de la similitude directe $z \mapsto cz + d$, de l'involution $z \mapsto \frac{1}{z}$ et de la similitude directe $z \mapsto \alpha z + \beta$. Or ces trois transformations conservent le birapport donc f conserve le birapport.

Ensuite, remarquons que multiplier les constantes de f par un scalaire ne change pas la fonction, donc on peut poser $d = 1$. En écrivant le système d'équation des égalités $f(x) = x'$, on trouve 3 équations linéaires à 3 inconnues, qui admettent en général une unique solution (sauf cas particuliers comme $a' = b'$, etc). Donc f est l'unique fonction qui envoie A, B, C sur A', B', C' en conservant le birapport, c'est donc notre transformation projective !

Pour finir, cherchons les points fixes de notre transformation projective :

$$\frac{az+b}{cz+d} = z, \text{ c'est-à-dire } cz^2 + (d-a)z - b = 0.$$

Cette équation du second degré admet toujours deux solutions, parfois confondues, donc une involution projective complexe a deux points fixes.

Solution de l'exercice 4

1. On va laisser la direction (AC) fixée, ainsi que A et B. (BH) est alors aussi fixée. On définit

   $$\mathfrak{P} : (BC_i) \xrightarrow{\text{intersection avec } (AC)} C_i \xrightarrow{\text{projection sur } (BH) \text{ perpendiculaire à } (AB)} H_i \xrightarrow{\text{droite passant par} A} (AH_i).$$

   On a donc une transformation projective envoyant les droites par B sur les droites par A.

   Reste à montrer que cette transformation est le passage à l'orthogonal, en vérifiant cela pour trois choix de C_i. Par exemple, $C_1 = A$, $C_2 =$ le pied de la hauteur issue de B, et $C_3 =$ le symétrique de A par (BH).

Solution de l'exercice 5

On peut démonter ce problème de bien de façons, mais voici une preuve instructive ; ce n'est pas la plus simple.

On fait varier (B_iC_i) parallèlement à (AD). B_i, C_i et P_i se baladent respectivement sur $(AB), (DC)$ et (AP). On va définir une transformation projective envoyant (DB_i) sur (QP_i) :

$$\mathfrak{P} : (DB_i) \xrightarrow{\text{point sur } (AB)} B_i \xrightarrow{\text{droite par } \infty_{(AD)}} (B_iP_i) \xrightarrow{\text{point sur } (AP)} P_i \xrightarrow{\text{droite par } Q} (QP_i).$$

D'après le Lemme 4.3.9, l'intersection de (DB_i) et (QP_i) se balade sur une unique conique. On sait que cette conique passe par D et Q. Cherchons trois autres points pour fixer cette conique. En prenant $B_1 = A$, on trouve qu'elle passe par $A = (DB_1) \cap (QP_1)$, avec B_2 et B_3 les points tels que $AB_i = AC$, il y a symétrie de la figure, et en appelant i et e les bissectrices interne et externe de $\widehat{CAB}$, on trouve que ∞_i et ∞_e appartiennent à notre conique, qui est maintenant uniquement déterminée.

On va exhiber une transformation envoyant (DB_i) sur la tangente au cercle circonscrit à AP_iQ_i en A, notée t_i. Pour ce faire, on prolonge $\mathfrak{P}$ comme suit :

$$\mathfrak{P}' : (DB_i) \xrightarrow{\mathfrak{P}} (QP_i) \xrightarrow{\text{tangente par } A} t_i.$$

La dernière transformation conserve le birapport par angle tangent.

Ainsi, l'intersection de (DB_i) et t_i décrit une conique passant par A et D. On souhaite aussi mieux la déterminer : en choisissant $B_4 = \infty_{(AB)}$, l'intersection est P, en reprenant les même choix de B_2 et B_3, on retrouve que ∞_i et ∞_e appartiennent à notre conique. Or on voit que c'est la même que celle de $\mathfrak{P}$! Donc (DB_i), (QP_i) et t_i sont concourantes sur cette conique.

Solution de l'exercice 6

On regarde le faisceau de coniques passant par A, B, C et D. La droite (EF) le coupe en des points échangés par une involution d'après le troisième théorème de Desargues. Donc $E \leftrightarrow F, X \leftrightarrow X$ et $Y \leftrightarrow Z$. Or, la symétrie d'axe (OX) échange $X \leftrightarrow X$ et $E \leftrightarrow F$, donc c'est notre involution, et $XY = XZ$.

Solution de l'exercice 7

D'après le théorème des involutions des points sur une conique, il existe une involution I qui échange $A \leftrightarrow A, B \leftrightarrow B$ et $C \leftrightarrow D$, donc $b_{ABCD} = b_{I(A)I(B)I(C)I(D)} = b_{ABDC}$ et les points $ABCD$ sont harmoniques. Soit Q l'intersection des tangentes passant par C et D. La droite (QA) recoupe le cercle en A', et il existe une involution I' qui échange $A \leftrightarrow A', C \leftrightarrow C$ et $D \leftrightarrow D$ donc $b_{A'ACD} \overset{\text{par } I'}{=} b_{AA'CD}$ donc les points $AA'CD$ sont harmoniques aussi. Par unicité du birapport, $A' = B$.

Solution de l'exercice 8

Soient O_A, O_B et O_C les centres des triangles équilatéraux.

$$\widehat{BO_AC} + \widehat{CO_BA} + \widehat{AO_CB} = 3 \cdot \frac{2\pi}{3} = 0 \pmod{2\pi} \text{ et } \frac{AO_C}{BO_C} \cdot \frac{BO_A}{CO_A} \cdot \frac{CO_B}{AO_B} = 1.$$

Donc $b_{BAA'C'} = b_{B'A'AC}$ et il existe une involution projective complexe échangeant $A \leftrightarrow O_A, B \leftrightarrow O_B$ et $C \leftrightarrow O_C$. En appliquant le théorème du triangle fantôme, on trouve que les angles de $O_AO_BO_C$ valent tous $60°$.

Solution de l'exercice 9

On regarde l'involution dans le quadrilatère $(AB), (AC), (BC), (DE)$, de centre A qui échange $D \leftrightarrow C, B \leftrightarrow E, A \leftrightarrow \infty$. Après recherche, on se rend compte qu'elle échange aussi γ_1 et γ_2 L'axe de symétrie de notre involution est la bissectrice de $\widehat{BAC}$, elle échange (AO_1) avec (AO_2), et en appelant T et T' les points de tangence de γ_1 et γ_2 à (AB) et (AC), on a $AO_1T \sim AO_2T'$, d'où $\frac{TO_1}{T'O_2} = \frac{AO_1}{AO_2}$.

Ensuite, étudions l'homothétie négative envoyant γ_1 sur γ_2, de centre l'intersection P des tangentes internes : on a $\frac{TO_1}{T'O_2} = \frac{PO_1}{PO_2}$.

Donc $\frac{AO_1}{AO_2} = \frac{PO_1}{PO_2}$, et P appartient à la bissectrice interne de $\widehat{O_1AO_2} = \widehat{BAC}$.

Solution de l'exercice 10

On applique le dual du second théorème de Desargues dans le quadrilatère $(AC), (BD), (AD), (BC)$: il existe une involution projective qui échange $(XA) \leftrightarrow (XB)$, $(XC) \leftrightarrow (XD)$ et $(XY) \leftrightarrow (XZ)$. Or, le passage à l'orthogonal est une involution qui échange $(XA) \leftrightarrow (XB)$ ainsi que $(XC) \leftrightarrow (XD)$, donc c'est notre involution, et elle échange bien $(XY) \leftrightarrow (XZ)$, donc XYZ est rectangle en X.

Solution de l'exercice 11

Il faut avoir en tête l'exercice 3 : les équation du second degré peuvent se mettre sous la forme d'une homographie, qui est aussi une transformation projective. On transforme la première équation en $a = \frac{-c}{a+b-c}$ En posant $S = a+b+c$, on a $a = \frac{c}{c-S} = f(c)$ où f est une transformation projective. De même on trouve $b = f(a)$ et $c = f(b)$.

Étudions $f \circ f \circ f$: c'est une transformation projective qui a pour points fixes A, B et C. Or, une transformation projective n'a que deux points fixes distincts, donc $a = b$ sans perte de généralité. Ainsi, on peut résoudre notre équation et trouver les triplets $(0, 0, 0)$ et $(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2})$.

5 Pot-pourri

1 IMO 2019

– Jour 1 –

Exercice 1
Montrer que pour tout n strictement positif :

$$\frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{2n-1} \geqslant n(\sqrt[n]{2} - 1).$$

Exercice 2
Montrer qu'il existe une infinité de couples d'entiers (m, n) tels que :

$$\frac{m+1}{n} + \frac{n+1}{m}$$

soit un entier.

Exercice 3 (Problème C6, Liste courte OIM 2009)
Une tour boiteuse se déplace sur un échiquier 2019×2019. Elle se déplace toujours d'une seule case à la fois et alterne des mouvements le long des lignes et le long des colonnes (elle ne peut pas faire deux déplacements consécutifs dans la même direction). Elle parcourt un cycle qui la ramène à son point de départ sans jamais passer deux fois par la même case. Quel est le nombre maximal de cases que la tour peut visiter lors de son cycle ?

– Jour 2 –

Exercice 4 (Problème G4, Liste courte OIM 2009)
Soit $ABCD$ un quadrilatère cyclique. On note E l'intersection des droites (AC) et (BD), et F l'intersection des droites (AD) et (BC). Les milieux des segments $[AB]$ et $[CD]$ sont respectivement G et H. Montrer que la droite (EF) est tangente au cercle passant par E, G et H.

Exercice 5 (Problème 4, Tournoi des villes de printemps 2007, catégorie senior difficile)
Alice mélange un jeu de 52 cartes et les dispose en cercle en laissant un 53^{ieme} emplacement vide. Bob, qui ne voit pas l'ordre initial des cartes, donne à Alice une liste de noms de cartes (dans laquelle certaines cartes peuvent apparaitre plusieurs fois). Pour chaque carte listée, Alice regarde si cette carte est située à côté de l'emplacement vide. Si c'est le cas, elle la place sur l'emplacement vide (l'ancien emplacement de la carte devenant alors vide), sinon elle ne fait rien. Elle répète cette opération jusqu'à atteindre le bout de la liste.

(a) Existe t-il une stratégie pour Bob qui garantit qu'aucune carte ne finit à sa position initiale ?

(b) Existe t-il une stratégie pour Bob qui garantit que la dame de pique ne finira pas sur une case voisine de l'emplacement vide ?

Exercice 6 (Problème 5, APMO 2018)
Déterminer tous les polynômes P à coefficients entiers tels que pour tous réels s et t tels que $P(s)$ et $P(t)$ soient entiers, $P(st)$ soit entier.

– Solutions –

Solution de l'exercice 1
On utilise l'inégalité arithmético-géométrique :

$$\frac{1}{n}+\frac{1}{n+1}+\ldots+\frac{1}{2n-1} \geqslant \frac{n+1}{n}+\frac{n+2}{n+1}+\ldots+\frac{2n}{2n-1}-n \geqslant n(\sqrt[n]{2}-1).$$

Solution de l'exercice 2
On utilise le Vieta jumping pour prouver qu'il existe une infinité de couples (m,n) avec $m<n$ tels que $\frac{m+1}{n}+\frac{n+1}{m}=3$: en effet, il en existe au moins un (par exemple $(1,2)$), et si (m,n) est un tel couple, alors m est une racine de l'équation polynomiale de degré 2 $X^2+(3n-1)X+(n^2+n)=0$. La seconde racine r de ce polynôme vaut alors (d'après les formules de Viète) $3n-1-m$, donc elle est entière et supérieure à n. Par conséquent, (n,r) est aussi un couple qui respecte les conditions recherchées, avec $n>m$. En répétant cette méthode avec le nouveau couple, on peut générer une infinité de solutions de l'équation.

Solution des exercices 3 à 6
Corrigé disponible sur le site de la compétition, ou dans le forum *Contest collections* de l'inévitable site AoPS.

6 Exercices d'entraînement

1 Entraînement de mi-parcours

– Énoncés –

Exercice 1
Soit ABC un triangle et D un point dans le triangle. On note E et F les intersections respectives de (BD) et (CD) avec (AC) et (AB). Les droites (DK) et (FE) se coupent en un point K. On note enfin G et J les points d'intersection de la droite (CK) avec les droites (AB) et (BE) ainsi que H et I les points d'intersection de la droite (BK) avec les droites (CF) et (CA). Montrer que les droites (BC), (EF), (HG) et (IJ) sont concourantes.

Exercice 2
Soit S un ensemble fini de points du plan, trois quelconques non alignés. Chaque point de S est colorié soit en bleu soit en rouge. On suppose que tout triangle dont les trois sommets sont bleus contient au moins un point rouge, et tout triangle dont les trois sommets sont rouges contient au moins un point bleu.

Déterminer la plus grande valeur possible de $\mid S \mid$.

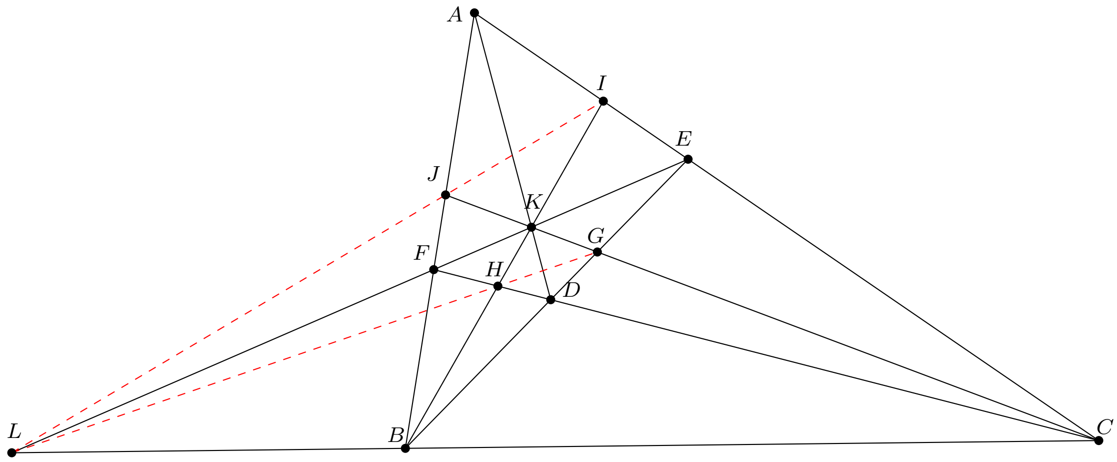
Exercice 3
Trouver tout les $P \in \mathbb{Z}[X]$, tel que $P(n)$ divise $n^{n-1} - 1$ pour tout $n \geqslant 2001$.

Exercice 4
Soit A, B, C et D quatre points. On note $(\ell_1) = (AB)$, $(\ell_1') = (CD)$, $(\ell_2) = (BC)$, $(\ell_2') = (DA)$, $(\ell_3) = (AC)$ et $(\ell_3') = (BD)$. On note M_3 le point de Miquel de (ℓ_1), (ℓ_1'), (ℓ_2) et (ℓ_2'), on définit de la même manière M_2 et M_1. On note ensuite X_3 l'intersection des droites (ℓ_3) et (ℓ_3'), on définit de la même manière X_2 et X_1. Pour tout i, on note (d_i) la droite (M_iX_i).

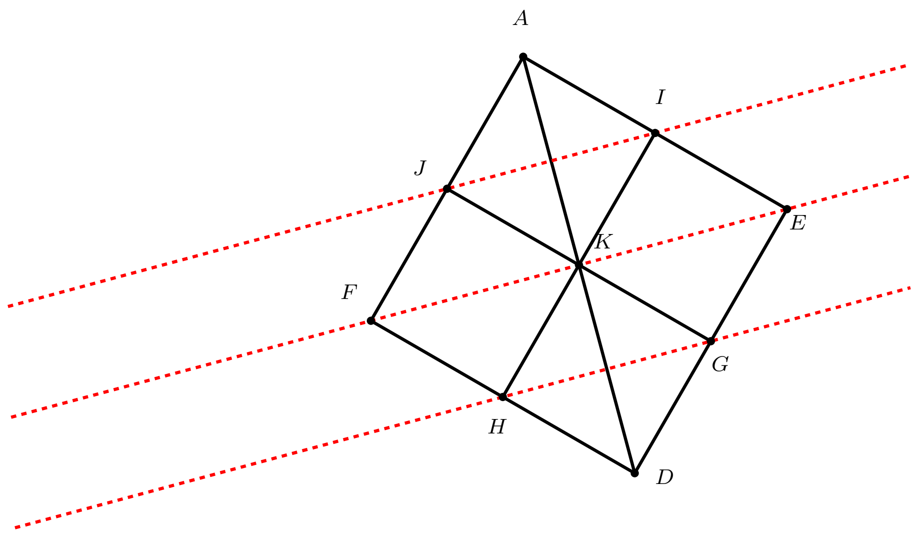
Montrer que (d_1), (d_2) et (d_3) sont concourantes.

– Solutions –

Solution de l'exercice 1



Première démonstration : l'ensemble de la configuration est projective c'est à dire que la figure est constituée uniquement de points et de droites sans obligation de rapport ou d'angle. On peut ainsi envoyer le quadrilatère $AFDE$ sur un carré. On obtient alors la figure suivante :



Les points B et C sont les points à l'infini des droites (AF) et (DE) respectivement, ainsi la droite (BC) devient la droite à l'infini après notre transformation. La droite (HI) est parallèle à (AF) et passe par K, donc H et I sont les milieux des segments $[FD]$ et $[AE]$. De la même manière les points G et J sont les milieux respectifs des segments $[DE]$ et $[AF]$. Ainsi, d'après

Thalès les droites (HG), (IJ) et (FE) sont parallèles, donc ce coupent sur la droite à l'infini. Cela conclut

Deuxième preuve :

On note X_1, X_2 et X_3 les intersections des droites (FE), (IJ) et (HG) respectivement et Y l'intersection de (AD) avec (CB). Dans le quadrilatère (AB), (BE), (AC) et (CF), d'après le théorème du quadrilatère complet on trouve que les points B, C, Y et X_1 sont harmoniques. Dans la quadrilatère (BK), (CK), (BA) et (AC) on trouve que les points B, C, Y et X_2 sont harmoniques. Dans la quadrilatère (BK), (CK), (BD) et (DC) on trouve que les points B, C, Y et X_3 sont harmoniques. Cela montre que $X_1 = X_2 = X_3$ et cela conclut l'exercice.

Solution de l'exercice 2

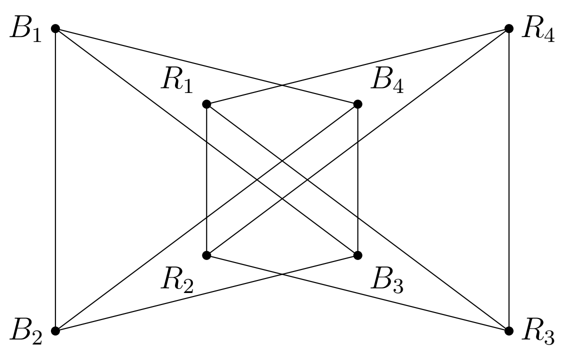
La réponse est 8. On va en fait montrer qu'il y a au plus 4 points bleus, et au plus 4 points rouges. Supposons qu'il y ait au moins 5 points bleus. Quitte à effectuer une rotation, on peut supposer que les points ont des abscisses deux à deux distinctes. On note $\mathcal{B}$ l'ensemble des 5 points bleus d'abscisse la plus petite.

Si l'enveloppe convexe de $\mathcal{B}$ est un pentagone, ce pentagone ne contient aucun point bleu. Le pentagone peut être divisé en 3 triangles, qui contiennent chacun un point rouge. Ces trois points rouges forment un triangle, qui ne contient aucun point bleu, ce qui est impossible.

Si l'enveloppe convexe de $\mathcal{B}$ est un quadrilatère $B_1B_2B_3B_4$, notons B_5 le dernier point de $\mathcal{B}$. Les triangles $B_5B_1B_2$, $B_5B_2B_3$, $B_5B_3B_4$ et $B_5B_4B_1$ contiennent chacun un point rouge, donc on a 4 points rouges R_1, R_2, R_3 et R_4 dans l'enveloppe convexe de $\mathcal{B}$, et un seul point bleu B_5. Ce point bleu doit donc être dans tous les triangles formés par R_1, R_2, R_3 et R_4, ce qui est impossible.

Enfin, si l'enveloppe convexe de $\mathcal{B}$ est un triangle $B_1B_2B_3$, on peut tracer des segments reliant entre eux les cinq points de $\mathcal{B}$ de manière à découper l'enveloppe convexe en 5 triangles, qui contiennent donc 5 points rouges. Par le principe des tiroirs, on peut en trouver 3 du même côté de (B_4B_5). Ces trois points forment un triangle rouge qui ne contient pas de sommet bleu, ce qui est aussi impossible.

Le nombre total de sommets ne peut donc dépasser 8. Enfin, $\mid S \mid = 8$ est réalisable, comme le montre la figure ci-dessous.



Solution de l'exercice 3

Réponse : $P(n) = \pm 1$, $P(n) = \pm(n-1)$ et $P(n) = \pm(n-1)^2$.

On sait que $a - b \mid P(a) - P(b)$ pour a et b deux entiers sachant que $P \in \mathbb{Z}[X]$. Donc $n + P(n) - n \mid P(n+P(n)) - P(n)$ ou encore, sachant que $P(n) \mid P(n)$, donc $P(n) \mid P(n+P(n))$.

On a donc $P(n) \mid P(n+P(n)) \mid n^{n+P(n)-1}-1$. On a également $P(n) \mid (n^{n-1}-1)n^{P(n)}$ et donc en soustrayant les deux derniers choses à droite on trouve enfin que $P(n) \mid n^{P(n)}-1$

On utilise maintenant le lemme suivant : $\text{PGCD}(a^m-1, a^n-1) = a^{\text{PGCD}(m,n)}-1$ (lemme connu dont la démonstration est laissée au lecteur). Ainsi, $P(n)$ divise $\text{PGCD}(n^{n-1}-1, n^{P(n)}-1) = n^{\text{PGCD}(P(n),(n-1))}-1$, on prend maintenant $n \geqslant 2001$ tel que $n-1$ est premier, si $P(n)$ n'est pas divisible par $n-1$, alors on obtient que $P(n)$ divise $n^{\text{PGCD}(P(n),(n-1))}-1 = n-1$, alors soit $P(n) = \pm 1$ pour une infinité de n soit $P(n) = \pm 1$ pour tout n, ou bien $P(n)$ est divisible par une nombre infini de $n-1$ premier ce qui est une contradiction avec l'hypothèse que $n-1$ ne divise pas $P(n)$ (on a utilisé le principe de tiroirs). Donc, $n-1 \mid P(n)$ pour tout $n-1$ premier plus grand que 2000 soit une infinité de nombre, on en déduit que $n-1$ divise $P(n)$ pour tout n entier, En écrivant $P(n) = Q(n)(n-1)+r$ donc r est divisible pour une infinité de premier donc $r=0$ et $P(n)$ est divisible par $n-1$. On prend maintenant $R(n) = \dfrac{P(n)}{n-1}$, alors $R(n)$ est aussi une solution de l'exercice. Donc $P(n) = a(n-1)^k$ pour un certain k entier.

On montre tout d'abord que $a = \pm 1$. En effet, en posant $n = am$ avec m suffisamment grand pour que $am \geqslant 2001$, on trouve $a \mid P(ak) \mid (ak)^{ak-1}-1$ ce qui est une contradiction si a est différent de 1 et -1. Donc $a = \pm 1$.

On en déduit que $P(n)$ est de la forme $\pm(n-1)^k$. On va en fait montrer que k vaut 0, 1 et 2.

Si $k=0$, on a clairement que $P(n) \mid n^{n-1}-1$ pour tout entier $n \geqslant 2001$. $P(n) = \pm 1$ est bien une solution.

Si $k=1$, on a $n^{n-1}-1 = (n-1)(n^{n-2}+n^{n-3}+\ldots+n+1)$, donc bien divisible par $\pm n-1$. $P(n) = \pm(n-1)$ est bien une solution.

Si $k=2$, on a $n^{n-2}+n^{n-3}+\ldots+n+1 \equiv 1+1+\ldots+1+1 \equiv n-1 \equiv 0 \pmod{n-1}$. Donc $n^{n-1}-1 = (n-1)(n^{n-2}+n^{n-3}+\ldots+n+1)$ est bien divisible par $(n-1)^2$.

On va maintenant montrer que $(n-1)^3$ ne divise pas tout le temps $n^{n-1}-1$ et ainsi $P(n) = \pm(n-1)^k$ n'est pas une solution si $k \geqslant 3$. Après translation on veut montrer que a^3 ne divise pas tout le temps $(a+1)^a-1$. Or $(a+1)^a-1 = a^a + a\cdot a^{a-1} + \binom{a}{2}\cdot a^{a-2} + \ldots + \binom{a}{2}\cdot a^2 + a\cdot a + 1 - 1 = (\cdots)a^3 + \binom{a}{2}\cdot a^2 + a^2$. On veut donc démontrer que a^3 ne divise pas tout le temps $\binom{a}{2}\cdot a^2 + a^2$, ou encore que a ne divise pas tout le temps $\left(\dfrac{a(a-1)}{2}+1\right)$. Or en prenant a impair, $2 \mid a-1$ et ainsi $a \nmid \dfrac{a(a-1)}{2}+1$, ce qui conclut la preuve.

Solution de l'exercice 4

On note $\sigma_1 = I_{M_3}$ l'involution projective complexe de centre M_3 qui échange A et C mais également B et D.

Ainsi elle échange $X_1 = (DC) \cap (AB)$ avec l'intersection des cercles ABM_3 et DCM_3 soit X_2.

On montre également que M_1 et M_2 sont échangés dans cette même involution.

On définit également $\sigma_2 = I_{M_1}$ et $\sigma_3 = I_{M_2}$.

Lemme 6.1.1.

$$\sigma_1 \circ \sigma_2 \circ \sigma_3 = \text{id}$$

Démonstration. On regarde ce qu'il advient des points de Miquel dans les involutions, en appliquant la composition des involutions sur les points de Miquel, le résultat est à chaque fois l'identité, le résultat de la transformation est une transformation projective car elle conserve le birrapport (vrai dans après chaque transformation, donc vrai à la fin). Cette transformation est uniquement déterminée après l'image de trois points, ici la transformation est l'identité pour trois points donc la transformation projective finale est confondue avec l'identité, ce qui conclut la preuve du lemme. □

Lemme 6.1.2.
Soit τ_1 et τ_2 deux involutions tel que $\tau_3 = \tau_1 \circ \tau_2$ est une involution alors : $\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$.

Démonstration. $\tau_3 \circ \tau_2 \circ \tau_1 = \tau_1 \circ \tau_2 \circ \tau_2 \circ \tau_1 = id$.

Donc $\tau_3 \circ \tau_3 \circ \tau_2 \circ \tau_1 = \tau_3$

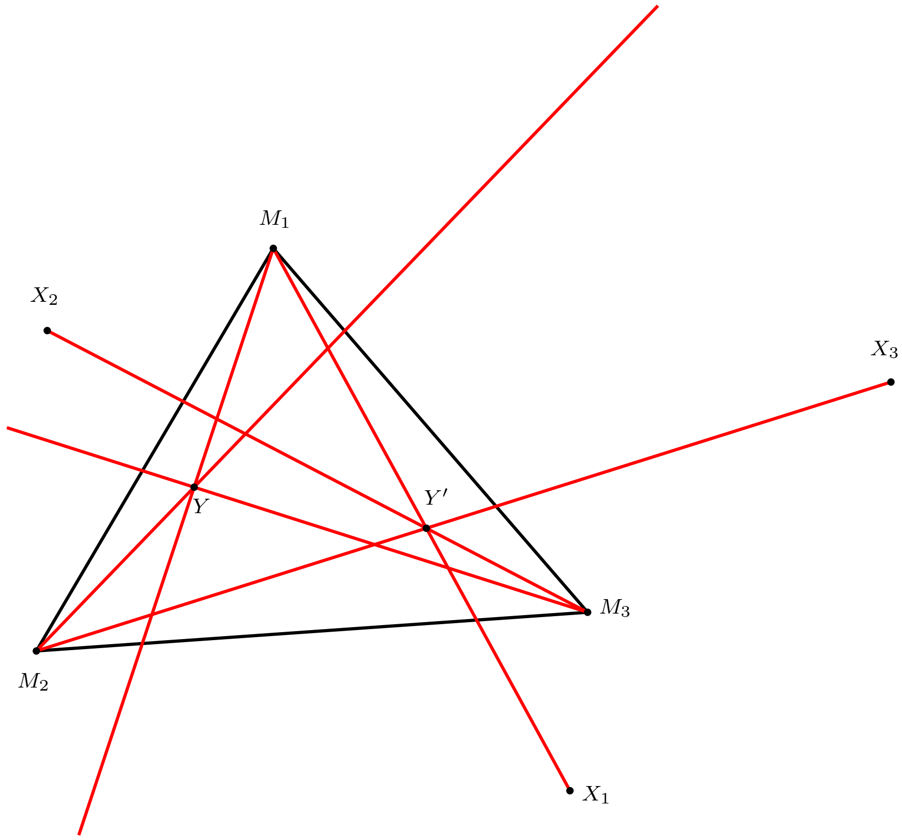
Donc $\tau_2 \circ \tau_1 = \tau_3 = \tau_1 \circ \tau_2$.

Ce qui finit.

□

En combinant les deux lemmes on montre donc que σ_1, σ_2 et σ_3 commutent deux à deux.
$\sigma_1 \circ \sigma_2(X_3) = X_1$
Donc $\sigma_1(X_3) = \sigma_2(X_1)$

On trouve donc $I_{M_3}(X_3) = I_{M_1}(X_1) = I_{M_2}(X_2)$
On pose Y ce point.
On a la figure suivante :



Comme les points M_1 et M_2 sont également échangés dans l'inversion de centre M_3, les droites M_3X_3 et M_3Y sont conjugués isogonales dans le triangle $M_1M_2M_3$. Les droites M_3Y, M_2Y et M_1Y sont concourantes, donc d'après Céva les droites d_1, d_2 et d_3 sont concourantes.

Cela conclut.

2 Entraînement final

– Énoncés –

Exercice 1
Soit g une fonction définie sur $\mathbb{R}$ telle que, pour tout entier relatif n, $g(n) = (-1)^n$, et g soit affine sur le segment $[n, n+1]$. Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que, pour tous réels x, y :

$$f(x + f(y)) = f(x) + g(y).$$

Exercice 2
Trouver tous les triplets (m, n, p) d'entiers positifs avec p premier tels que $(m^3 + n)(n^3 + m) = p^3$.

Exercice 3
Soit G un graphe non-orienté. On considère une coloration des sommets de G en un minimum

χ de couleurs telle que deux sommets voisins n'aient jamais la même couleur. Montrer qu'il existe un chemin à χ sommets tel que chaque sommet ait une couleur différente.

Exercice 4
Soit $a_n = \lfloor \sqrt{n^2 + (n+1)^2} \rfloor$ pour tout $n \geqslant 1$. Prouver qu'il existe une infinité d'entiers n tels que $a_n - a_{n-1} > 1$ et $a_{n+1} - a_n = 1$.

– Solutions –

Solution de l'exercice 1
Supposons qu'il existe une fonction solution du problème. Fixons $x_1 = 0$ et faisons varier y : $f(x + f(y))$ prend toutes les valeurs dans $[f(0) - 1, f(0) + 1]$. Pour $n \geqslant 2$, on prend x_n tel que $f(x_n) = f(x_{n-1}) + 1$, et on prouve par récurrence que f prend toutes les valeurs possibles dans $[f(0), f(0) + n]$. On prouve de même qu'on peut atteindre toutes les valeurs dans $[f(0) - n, f(0)]$. Ainsi, f est surjective sur $\mathbb{R}$.

Maintenant, fixons x. Alors lorsque y décrit $\mathbb{R}$, $x + f(y)$ aussi par surjectivité de f, donc $f(x + f(y))$ aussi. Or $f(x + f(y)) = f(x) + g(y)$ et le membre de droite ne peut prendre ses valeurs que dans $[f(x) - 1, f(x) + 1]$. Cette contradiction montre que f n'existe en fait pas.

Solution de l'exercice 2
Si $m = n$, on a $p^3 = (m^3 + m)^2$, donc p est un carré parfait, ce qui est impossible. On peut donc supposer que $m > n$. Si $n = 0$, on a $m^4 = p^3$, ce qui est également impossible.

Cela signifie que $m^3 + n = p^2$ et $n^3 + m = p$. On en tire $m = p - n^3$ puis $(p - n^3)^3 + n = p^2$. On développe et on obtient $p \mid n^9 - n = n(n-1)(n+1)(n^2+1)(n^4+1)$. Comme $p > n^3$, on a soit $n^9 - n = 0$, et alors $n = 1$, soit $p \mid n^4 + 1$.

1. Si $n = 1$, alors $m = p - 1$, donc $(p-1)^3 + 1 = p^2$. On en déduit que $p = 3$ et $m = 2$.
2. Si $n > 1$ et $p \mid n^4+1$, alors $p|n(n^3+m)-(n^4+1) = mn-1$. Or, $p^2 = m^3+n \geqslant 2\sqrt{m^3 n} \geqslant 2mn$, ce qui constitue une contradiction.

Ainsi, les triplets solutions sont $(m, n, p) = (2, 1, 3), (1, 2, 3)$.

Solution de l'exercice 3
L'on identifie les couleurs aux entiers compris entre 1 et χ. Orientons les arêtes de G par couleur croissante : soit $\overrightarrow{G}$ le graphe orienté acyclique ainsi obtenu. Il est alors suffisant de trouver un chemin de longueur χ dans $\overrightarrow{G}$.

À chaque sommet s, on associe $L(s)$, le nombre maximal de sommets d'un chemin terminant par s. Pour $k \geqslant 1$, l'ensemble $E(k)$ défini comme $E(k) = \{s \in S : L(s) = k\}$ est une partie indépendante dans G, ce qui signifie que les sommets de l'ensemble ne sont pas reliés. En effet, si u et v sont reliés dans G, alors (u, v) ou (v, u) est une arête de $\overrightarrow{G}$, donc $L(u) < L(v)$ ou $L(v) < L(u)$.

Ainsi, en notant ℓ le nombre maximal de sommets dans un chemin de $\overrightarrow{G}$, les ensembles $E(1), \ldots, E(\ell)$ fournissent une coloration de G en ℓ couleurs. Cela montre que $\ell \geqslant \chi$. Il existe donc un chemin à χ sommets dans $\overrightarrow{G}$, qui constitue en particulier un chemin à χ sommets de couleurs différentes dans G.

Solution de l'exercice 4
Tentons de voir si $\sqrt{n^2 + (n+1)^2}$ peut être entier : il faudrait un entier y tel que $n^2+(n+1)^2 =$

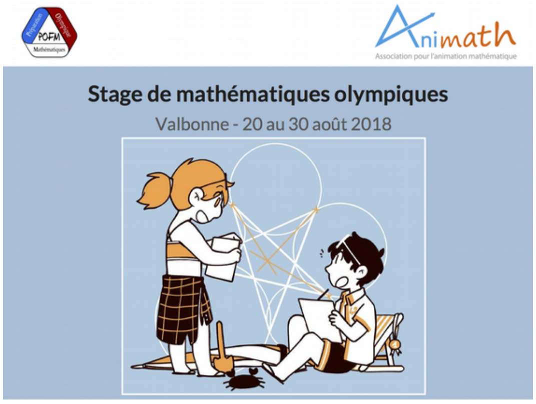
y^2, soit $2(n+1/2)^2 - 1/2 - y^2 = 0$, ou encore $(2n+1)^2 - 2y^2 = -1$ L'équation de Pell négative $x^2 - 2y^2 = -1$ admet une infinité de solutions strictement positives, car $x = y = 1$ en est une. Comme x doit être impair, on en déduit qu'il existe une infinité de n tels qu'il existe y vérifiant $(2n+1)^2 - 2y^2 = -1$.

Posons $a_n = y$, de sorte que $a_n \in \mathbb{N}$. On a $a_{n-1} = \lfloor \sqrt{y^2 - 4n} \rfloor$. On vérifie que $y^2 - 4n < (y-1)^2$ pour n assez grand, donc que $a_{n-1} < a_n$. Et $a_{n+1} = \lfloor \sqrt{y^2 + 4n + 4} \rfloor$. Comme $n < y < 2n+1$, on trouve rapidement que $\sqrt{y^2 + 4n + 4} \in [y+1, y+2[$, donc que $a_{n+1} - a_n = 1$.

VII. Les soirées

Contenu de cette partie

1 Présentation du stage, de la POFM et des Olympiades



Ce soir, on a souhaité la bienvenue aux élèves, à qui l'on a ensuite présenté le programme du stage, les consignes (concernant en particulier les chambres, les repas et la piscine), la muraille, et la répartition des élèves en groupes.

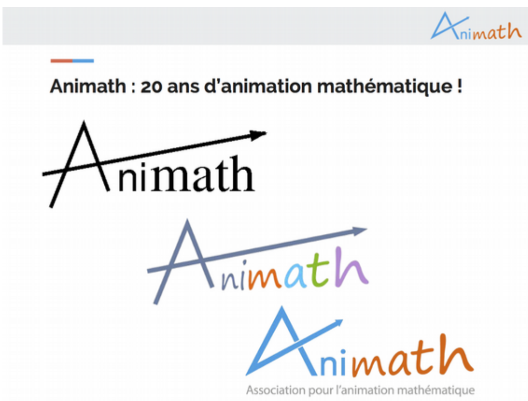
– Qu'est-ce qu'Animath ? –

Animath est l'association qui organise ce stage.

Animath est une association créée en 1998, dont le but est de favoriser le goût et la pratique des mathématiques chez les jeunes. Animath fédère les différentes entités qui partagent ces objectifs et déploie elle-même des actions dans ce sens.

Animath permet chaque année à des milliers de collégien·ne·s et lycéen·ne·s intéressé·e·s par les mathématiques de participer à des activités complémentaires du cadre scolaire : stages, compétitions nationales et internationales prestigieuses, rencontres avec des chercheurs, etc. Ces activités existent à différentes échelles : locale, nationale ou internationale. Une attention particulière est apportée à celles et ceux qui, pour des raisons d'origine sociale ou géographique, ou parce qu'il s'agit de filles, ont tendance à moins s'engager vers les mathématiques, ainsi qu'aux plus jeunes.

Les actions d'Animath reposent sur un fort engagement bénévole pour organiser les événements et surtout pour encadrer des projets scientifiques. Professeur·e·s, chercheur·e·s, ingénieur·e·s, ou encore étudiant·e·s, ancien·ne·s bénéficiaires des actions de l'association ou non, les nombreux·ses bénévoles de l'association sont uni·e·s par la volonté de partager leur passion avec un large public.



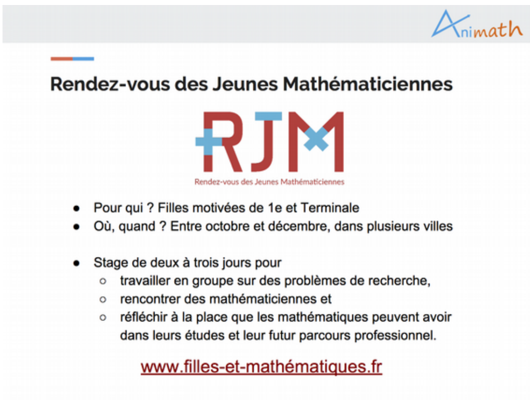
– Les actions d'Animath –

En vingt ans d'existence, l'association s'est beaucoup diversifiée. Animath organise la participation d'équipes françaises aux compétitions de mathématiques olympiques, à travers la Préparation Olympique Française de Mathématique, qui est l'objet de ce stage. Mais de nombreuses autres actions sont organisées par l'association.

Vous pouvez retrouver la liste complète des actions d'Animath sur le site www.animath.fr, mais en voici une sélection qui peut vous intéresser particulièrement.

Les Rendez-vous des Jeunes Mathématiciennes

Pendant deux à trois jours, des lycéennes intéressées par les mathématiques participent à un stage pour travailler en groupe sur des problèmes de recherche, rencontrer des mathématiciennes et réfléchir à la place que les mathématiques peuvent avoir dans leurs études et leur futur parcours professionnel. L'objectif est d'encourager les jeunes filles motivées à affirmer leur intérêt pour les mathématiques et à formuler un projet ambitieux d'études scientifiques.



filles-et-maths.fr

Le Concours Alkindi

Le concours Alkindi est une compétition de cryptanalyse : l'art de déchiffrer les codes secrets. L'objectif est de faire découvrir aux élèves cette application des mathématiques et de l'informatique en s'amusant et de les sensibiliser à la question importante de la sécurité de l'information. Aucune connaissance préalable en cryptanalyse n'est requise.

concours-alkindi.fr

Les Correspondances des Jeunes Mathématicien·ne·s – Nouvelle action !

Les Correspondances de Jeunes Mathématicien·ne·s proposent d'échanger par vidéo sur des problèmes de mathématiques. Une liste de problèmes ouverts est proposée. Chaque équipe choisit celui qui l'intéresse et dispose de plusieurs semaines pour réfléchir au problème et réaliser une courte vidéo pour exposer ses résultats. Ensuite, les élèves reçoivent une vidéo réalisée par une autre équipe sur le même problème et échangent avec cette équipe. Enfin, les élèves réalisent une seconde vidéo pour présenter la synthèse de leurs échanges. Les meilleures vidéos sont primées et diffusées.

correspondances-maths.fr

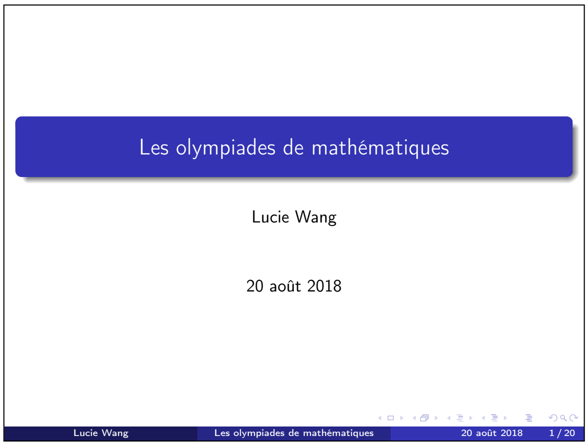
Le Tournoi Français des Jeunes Mathématiciennes et Mathématiciens ($\mathbb{TFJM}^2$)

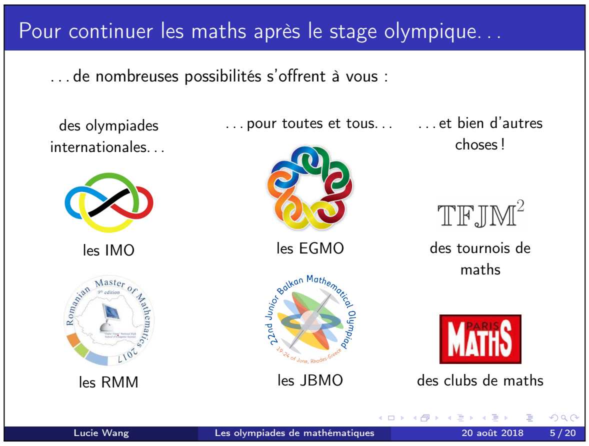
Le Tournoi Français des Jeunes Mathématiciennes et Mathématiciens ($\mathbb{TFJM}^2$) est une compétition qui s'inspire de la recherche en mathématiques. Les élèves ont plusieurs mois pour réfléchir en équipe à une dizaine de problèmes sans solution connue. Pendant le tournoi, les équipes de chaque région se rencontrent lors d'un weekend. Elles présentent leurs résultats à un jury et critiquent les solutions des autres équipes lors d'un débat oral. Les meilleures équipes de chaque région sont sélectionnées pour la finale nationale.

tfjm.org

– La Préparation Olympique Française de Mathématiques (POFM) –

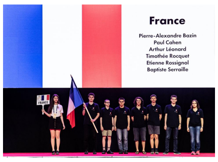
Lucie a ensuite présenté les olympiades de mathématiques et la POFM : voici un fac-simile des transparents qu'elle a montrés aux élèves.





Les IMO : quésaco ?

- Depuis 1959, tous les ans en été, une dizaine de jours
- Une centaine de pays, soit autour de 600 participants
- Une délégation, c'est :
  - 6 participants, élèves dans le secondaire
  - 1 team leader
  - 1 deputy leader



Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 7 / 20

Des maths...

- 6 problèmes en 2 matinées consécutives de 4h30 chacune
- 4 domaines des mathématiques :
  - algèbre
  - combinatoire
  - géométrie
  - arithmétique

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 8 / 20

... mais pas que !

- Des activités et des sorties pour profiter pleinement du séjour

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 9 / 20

... mais pas que !

- Des activités et des sorties pour profiter pleinement du séjour

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 10 / 20

... mais pas que !

- Des rencontres et des échanges marquants

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 11 / 20

... mais pas que !

- Des récompenses au terme des épreuves

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 12 / 20

Cap sur les IMO

Cette année : la France est repartie avec 6 médailles
À suivre : Royaume-Uni, Russie, États-Unis, ...

IMO 2019
60TH INTERNATIONAL MATHEMATICAL OLYMPIAD

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 13 / 20

L'ensemble des compétitions

En maths, il y en a pour tout le monde...

- Le Romanian Master of Mathematics (RMM)
- Les Olympiades Européennes Féminines de Mathématiques (EGMO)
- Les Olympiades de Mathématiques du Benelux (BxMO)
- Les Olympiades Balkaniques Junior de Mathématiques (JBMO)
- Les Olympiades Internationales de Mathématiques (IMO)

... en olympiades comme ailleurs :

- Le Mediterranean Youth Mathematical Championship (MYMC)

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 15 / 20

POFM, mode d'emploi

- Un test d'entrée début octobre
- Un envoi par correspondance tous les mois
- Des tests de sélection au fil de l'année
- Un stage pendant les vacances de février

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 17 / 20

Les clubs et les stages

Des clubs aux quatre coins de la France...

- Parimaths
- Club de mathématiques de Lyon
- Cercle mathématique de Strasbourg
- Cercle Sofia Kovalevskaïa à Toulouse
- Club mathématique de Nancy

...et désormais en ligne aussi :

- Mathmosphère

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 18 / 20

Et pour en savoir plus ?

Après le stage...

- L'adresse à retenir :

`maths-olympiques.fr`

Lucie Wang — Les olympiades de mathématiques — 20 août 2018 — 20 / 20

2 Présentation du $\mathbb{TFJM}^2$

Cette conférence de présentation du $\mathbb{TFJM}^2$ (Tournoi français des jeunes mathématiciennes et mathématicens) était destinée à proposer aux stagiaires une approche assez différente des mathématiques : plus axée sur la recherche.

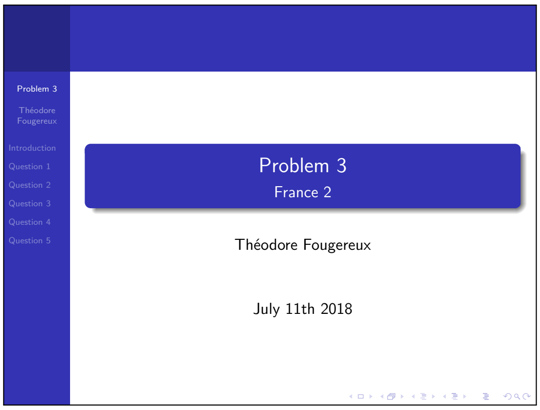
Le tournoi existe depuis 2011, il a débuté à l'Université Paris-Sud, organisé par Animath. Il était alors conçu comme la branche française de la compétition internationale « International Tournament of Young Mathematicians » (ITYM), crée pour sa part en 2009, et dont l'édition 2018 s'est déroulée à Paris. Le $\mathbb{TFJM}^2$ s'est développé en 7 ans et compte aujourd'hui une phase de sélection régionale organisée à Lille, Lyon, Paris, Rennes, Strasbourg et Toulouse suivie d'une finale organisée à Palaiseau suur le campus de l'École polytechnique. Il s'agit d'une compétition destinée aux élèves de lycée mais la présence d'un collégien motivé dans une équipe n'est en aucun cas un problème.

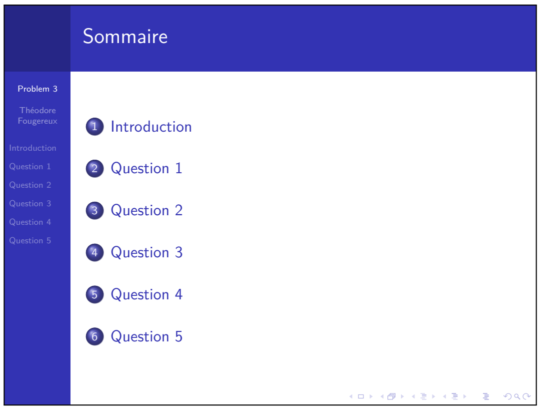
Le $\mathbb{TFJM}^2$ de distingue des autres compétitions mathématiques en proposant des problèmes ouverts qui n'admettent pas, à la connaissance du jury, de solution complète, et qui sont cherchés en équipes. Ces dernières possèdent des encadrants qui sont destinés à éviter les sorties de piste, coordonner les recherches et fournir aux participants les connaissances théoriques dont ils poourraient avoir besoin. Le tournoi en lui-même compte une phase en temps libre dédiée à la recherche et à la rédaction : elle commence en décembre-janvier pour s'achever une semaine avant les tournois régionaux, en avril. Et ensuite, une phase de présentation des résultats qui a lieu pendant deux jours lors du tournoi (régional comme national). Les tournois régionaux et la finale utilisent la même liste de problèmes.

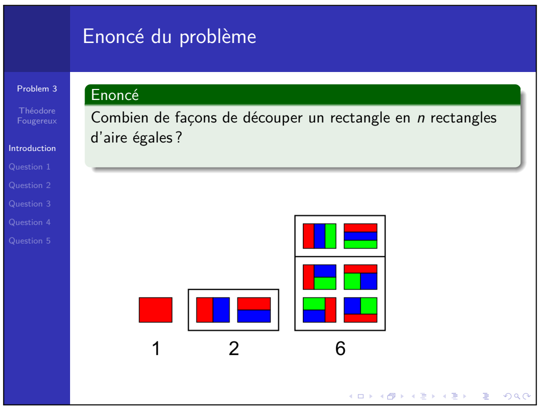
Ces problèmes sont innhabituels pour les élèves et leur donnent une première approche de la recherche : traiter les petits cas, faire des essais, conjecturer, faire preuve d'esprit critique, etc. Les questions abordées recoupent les domaines de théorie des nombres, algèbre, analyse, combinatoire et géométrie.

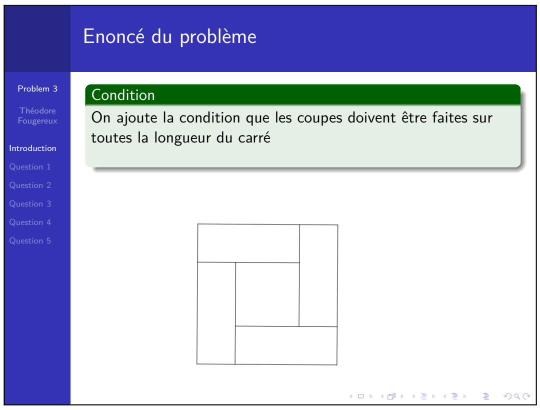
Pour illustrer le déroulement du $\mathbb{TFJM}^2$, les élèves ont eu droit à un tour blanc fait par d'anciens participants. Ils ont même pu poser leurs questions aux différents acteurs pour se mettre dans la peau du jury. Pour plus d'informations, on pourra bien sûr se rendre sur le site officiel de la compétition : tfjm.org.

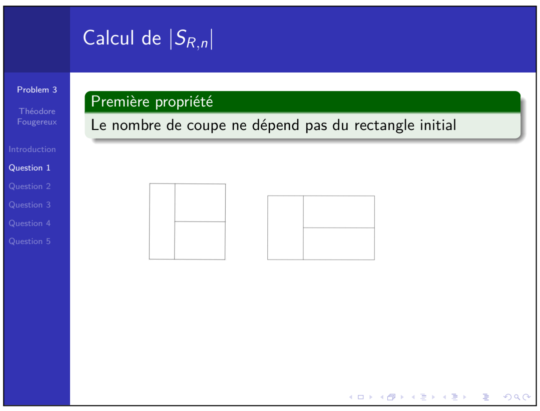
Voici les planches qu'a présentées Théodore Fougereux, participant au stage ayant également pris part aux finales du $\mathbb{TFJM}^2$ et de l'ITYM en 2018.

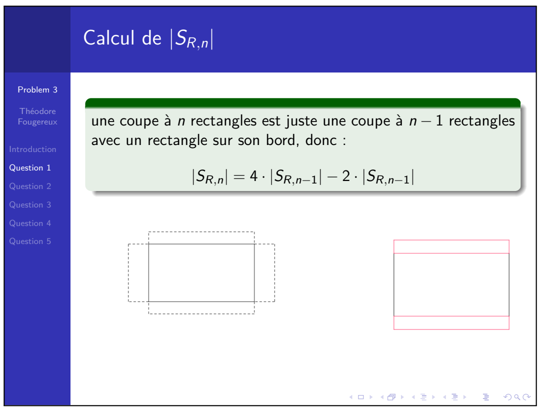












Calcul de $|S_{R,n}|$

Il existe une formule pour calculer ce le terme général de ces suites, on trouve alors :

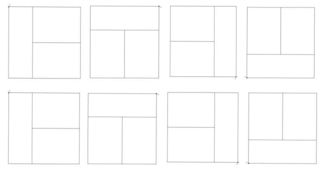
$$= \frac{1}{2}((2+\sqrt{2})^{n-1} + (2-\sqrt{2})^{n-1})$$

Nombre de coupes à symétrie près

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

Comment compter le nombre de coupes ?

- Il existe 8 symétrie du rectangle.
- On compte une pièce comme son nombre de symétrie divisé par 8 :

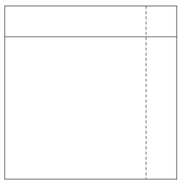


Nombre de coupes à symétrie près

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

première remarque

On commence par remarquer qu'une coupe ne peut pas être envoyée sur elle même par une rotation à ± 90 degrés

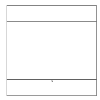


Nombre de coupes à symétrie près

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

Rotation à 180 degrés

- On commence par compter le nombre de pièces envoyées sur elle-mêmes par une rotation à 180 degrés :



Relation de récurrence

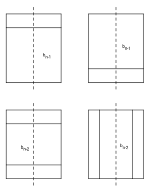
On peut alors montrer par récurrence que le nombre de pièces envoyées sur elles même par rotation à 180 degrés est $2^{\lfloor \frac{n}{2} \rfloor}$

Nombre de coupes à symétrie près

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

symétrie

On compte maintenant le nombre de pièces envoyées sur elles mêmes par une symétrie horizontale :



Nombre de coupes à symétrie

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

Relation de récurrence

On déduit que $b_{n+1} = 2b_n - b_{n-1} + b_{n-1}$, so $b_n = 2^{n-1}$ as $b_1 = 1$

Nombre de coupes à symétrie près

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

Rotation à 180 degrés composée avec une symétrie

Une symétrie à 180 degrés composée avec une symétrie reste une symétrie.

Nombre de coupes à symétrie près

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

Formule

On en déduit la formule suivante :

$$s_n = \frac{2^{n-1} + 2^{n-1} + 2^{\lfloor \frac{n}{2} \rfloor} + 1/2((2+\sqrt{2})^{n-1} + (2-\sqrt{2})^{n-1})}{8}$$

what is $|C_{R,n}|$

upper bound

We use a result from R. Haggkvist, P.-O. Lindberg, and B. Bindstrom to prove that :

$$C_{R,n} \leq 8c_n \leq \cdot \frac{16 \cdot (2n)! \cdot 3^n}{n!(n+2)!}$$

Where c_n is the number of cuts up to symmetry.

Idea of the proof

The main idea of that proof is to show that two cuts can't be homeomorph. More intuitively, if two cuts are different, then the disposition of the rectangles will be different.

what is $|C_{R,n}|$

lower bound

We clealy have $S \subseteq C$, so we have :

$$\frac{1}{2}((2+\sqrt{2})^{n-1} + (2-\sqrt{2})^{n-1}) \leq |C_{R,n}|$$

what is $|C_{R,n}|$

Equivalent for the lower bound

$$\frac{1}{2}((2+\sqrt{2})^{n-1} + (2-\sqrt{2})^{n-1}) \sim \frac{(2+\sqrt{2})^n}{4+2\sqrt{2}}$$

Equivalent for the upper bound

Using stirling formula, which yields that :

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

We deduce the following equivalent for the upper bound :

$$\frac{16 \cdot (2n)! \cdot 3^n}{n!(n+2)!} \sim \frac{16 \cdot 12^n}{n^2\sqrt{\pi n}}$$

(There was a typo in our written materials)

what is c_n (The number of cuts up to symmetry)

Formula

Using the fact that $c_n \leq |C_{R,n}| \leq 8c_n$ as the group of the symmetries of the square has only 8 elements, we can deduce the formula :

$$\frac{1}{16}((2+\sqrt{2})^{n-1} + (2-\sqrt{2})^{n-1}) \leq |c_n| \leq \frac{2 \cdot (2n)! \cdot 3^n}{4n!(n+2)!}$$

k-dimensional generalization

Cuts in S

Using the same idea as the 2-dimensional case, we can easily find a recursive formula :

$$|S_{R,n}| = 2k \cdot |S_{R,(n-1)}| - k \cdot |S_{R,(n-2)}|$$

Its characteristic polynomial is :

$$x^2 - 2kx + k = 0$$

Therefore $|S_{R,n}|$ should of the form :

$$C_1(k+\sqrt{k^2-k})^n + C_2(k-\sqrt{k^2-k})^n$$

k-dimensional generalization

Final formula

Using the fact that $|S_{R,1}| = 1$ and $|S_{R,2}| = k$, we find :

$$|S_{R,n}| = \frac{1}{2}\left((k+\sqrt{k^2-k})^{n-1} + (k-\sqrt{k^2-k})^{n-1}\right)$$

k-dimensional generalization

lower bound in C

In order to find a lower bound we first use that $S \subseteq C$, so we clearly have :

$$|C_{R,n}| \leq \frac{1}{2}\left((k+\sqrt{k^2-k})^{n-1} + (k-\sqrt{k^2-k})^{n-1}\right)$$

k-dimensional generalization

upper bound in C

We consider the following transformation :

$$\mathcal{H}_1 \ : \ (x_1, x_2, ..., x_k) \to (f_1(x_1), f_2(x_2), ..., f_k(x_k))$$

Where $f_i(x)$ is an increasing bijective function from $[0;1]$ to $[0;1]$. We suppose that there are two distinct cuts in C such that we can map the first one on the second one with the transformation $\mathcal{H}$.

k-dimensional generalization

Coordinates

For an hyperparallelepiped H_m in the cut, we consider the two opposite points A and B such that :

$$A_m = (x_{m,1}, x_{m,2}, ..., x_{m,k})$$

$$B_m = (y_{m,1}, y_{m,2}, ..., y_{m,k})$$

$$x_{m,i} < y_{m,i} \quad \forall 1 \leq i \leq n$$

k-dimensional generalization

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

Volume

The volume of an hyperparallelepiped H_m will be :

$$\frac{1}{n} = V_{H_m} = \prod_{i=1}^{k} (x_{m,i} - y_{m,i})$$

And the image of this hyperparallelepiped H'_m wil be :

$$\frac{1}{n} = V_{H'_m} = \prod_{i=1}^{k} (f_i(x_{m,i}) - f_i(y_{m,i}))$$

k-dimensional generalization

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

Property

Now we consider the transformation $g_i(x_i) = \dfrac{x_i + f_i(x_i)}{2}$. It maps hyperparallelepiped on hyperparallelepiped, so :

$$V_{C_1} = 1 = \sum_{m=1}^{n} \prod_{i=1}^{k} \left(\frac{f_i(x_{m,i}) + x_{m,i}}{2} - \frac{f_i(y_{m,i}) + y_{m,i}}{2} \right)$$

$$\geq \sum_{m=1}^{n} \prod_{i=1}^{k} \sqrt{(f_i(y_{m,i}) - f_i(x_{m,i}))(y_{m,i} - x_{m,i})} \quad \text{AM-GM inequality}$$

$$= 1$$

Then we have $x_{m,i} - y_{m,i} = (f_i(y_{m,i}) - f_i(x_{m,i}))$, so our transformation conserves the length

k-dimensional generalization

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

upper bound

We just need to compute the number of ways to order our coordinates over one coordinate x_i, we can show that there are at most $(2^n \cdot k)^{2n}$ ways to do that, so :

$$|C_{R,n}| \leq 4^{nk^2} \cdot n^{2nk}$$

k-dimensional generalization

Problem 3
Théodore Fougereux
Introduction
Question 1
Question 2
Question 3
Question 4
Question 5

bounds for c_n

Knowing that there are $2^k \cdot k!$ automorphism of the hypercube, we find :

$$\frac{2}{2^k \cdot k!} \left((k + \sqrt{k^2 - k})^{n-1} + (k - \sqrt{k^2 - k})^{n-1} \right) \leq c_n \leq 4^{nk^2} \cdot n^{2nk}$$

3 Conférence : Des cercles, des lampes et $\pi^2/6$

But de l'exposé Le but est de montrer la formule suivante :

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots=\frac{\pi^2}{6}\;(\approx 1,6449340668482264).$$

Un peu d'histoire :

— Problème posé pour la première fois en 1644 par Mengoli.

— Euler trouve la valeur $\frac{\pi^2}{6}$ en 1735 avec un argument non-rigoureux, puis donne une preuve rigoureuse en 1741.

— Une preuve élementaire (mais pas très amusante) a été donnée par Cauchy en 1821.

— La preuve qu'on va présenter est beaucoup plus récente (et amusante !), et est due à Wästlund.

Sommes infinies Premier problème : le membre de gauche est une somme infinie. Qu'est-ce-que ça veut dire ? Supposons qu'on veuille sommer une infinité de nombres positifs $a_1, a_2, a_3, \ldots$. On les ajoute un par un, obtenant des sommes finies de plus en plus grandes. Deux cas sont possibles :

— Si on attend assez longtemps, on finit par dépasser n'importe quel nombre. On dit alors que la somme *diverge*, ou qu'elle est *infinie*, et on note

$$a_1+a_2+a_3+\cdots=+\infty.$$

— Il existe un nombre qu'on n'arrivera jamais à dépasser. Dans ce cas, les sommes finies se rapprochent d'une certaine valeur S. On note

$$a_1+a_2+a_3+\cdots=S<+\infty.$$

Quelques exemples

— Si tous les nombres valent 1 :

$$1+1+1+\cdots=+\infty.$$

— Si tous les nombres valent 0 sauf un nombre fini :

$$18+7+17+0+0+0+\cdots<+\infty.$$

— Si $a_n=\frac{1}{2^n}$, alors

$$\begin{aligned}&\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}\\ =\;&\left(\frac{1}{1}-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{4}\right)+\left(\frac{1}{4}-\frac{1}{8}\right)+\cdots+\left(\frac{1}{2^{n-1}}-\frac{1}{2^n}\right)\\ =\;&1-\frac{1}{2^n},\end{aligned}$$

donc

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots=1.$$

— Si $a_n = \frac{1}{n}$, on fait des paquets séparés par les puissances de 2 :

$$\begin{aligned} & \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots \\ = \quad & \frac{1}{1} + \left(\frac{1}{2} + \frac{1}{3}\right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7}\right) + \left(\frac{1}{8} + \dots + \frac{1}{15}\right) + \dots \end{aligned}$$

On estime la somme de chaque paquet :

$$\frac{1}{2^k} + \dots + \frac{1}{2^{k+1}-1} \geqslant \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}} + \dots + \frac{1}{2^{k+1}} = 2^k \times \frac{1}{2^{k+1}} = \frac{1}{2}.$$

On a une infinité de paquets de somme au moins $\frac{1}{2}$, donc la somme est infinie.

— Si $a_n = \frac{1}{n^2}$, on peut écrire (pour $n \geqslant 2$) :

$$\frac{1}{n^2} \leqslant \frac{1}{n(n-1)} = \frac{n-(n-1)}{n(n-1)} = \frac{1}{n-1} - \frac{1}{n},$$

donc

$$\begin{aligned} & \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} \\ \leqslant \quad & 1 + \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \dots + \left(\frac{1}{n-1} - \frac{1}{n}\right) \\ = \quad & 2 - \frac{1}{n} \leqslant 2, \end{aligned}$$

donc finalement

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots < +\infty.$$

Une preuve pas vraiment élémentaire On veut maintenant calculer cette dernière somme. On considère la fonction identité $f(x) = x$ sur $[-\pi, \pi[$, étendue à $\mathbb{R}$ de manière 2π-périodique. On calcule ses coefficients de Fourier (par intégration par partie) :

$$c_n(f) = \frac{(-1)^n}{n} i.$$

D'après la formule de Parseval, on a

$$2 \sum_{n=1}^{+\infty} \frac{1}{n^2} = \sum_{n=-\infty}^{+\infty} |c_n|^2 = \frac{1}{2\pi} \int_0^{2\pi} f(x)^2 \mathrm{d}x,$$

donc

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots = \frac{1}{4\pi} \int_0^{2\pi} x^2 \, \mathrm{d}x = \frac{\pi^2}{6}.$$

Problème : on n'a rien compris ! But de l'exposé : donner une preuve **élémentaire**.

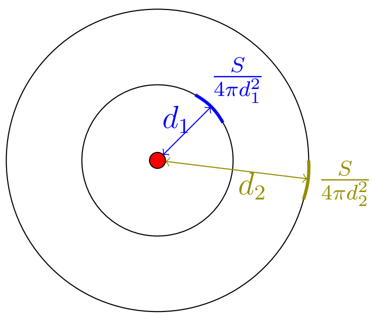


FIGURE 1 – L'observateur couvre une surface S. La sphère de rayon d_1 a pour aire $4\pi d_1^2$, donc l'observateur à distance d_1 capte une proportion $\frac{S}{4\pi d_1^2}$ de l'énergie émise par la lampe.

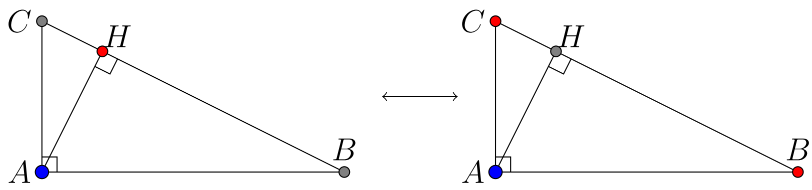


FIGURE 2 – Illustration du lemme permettant de remplacer une lampe (en rouge à gauche) par deux lampes (en rouge à droite).

Un petit détour par la physique... Si une lampe émet de la lumière dans toutes les directions, un observateur à distance d reçoit une énergie proportionnelle à $\frac{1}{d^2}$ (voir Figure 1).

On supposera dans la suite que l'énergie reçue est exactement $\frac{1}{d^2}$ (en maths, toutes les constantes physiques valent 1).

On ne considère que des lampes ayant toutes la même puissance. On veut calculer l'énergie reçue par un observateur placé en 0 sur une droite si chaque entier strictement positif est occupé par une lampe.

Un lemme de géométrie (voir aussi Figure 2)

Lemme 3.0.1.
Soit ABC un triangle rectangle en A, et H le pied de la hauteur issue de A. L'observateur est placé en A. Alors une lampe en H équivaut à deux lampes placées en B et C.

Démonstration. On veut montrer que $\frac{1}{AB^2} + \frac{1}{AC^2} = \frac{1}{AH^2}$.

Or, on a $\frac{1}{AB^2} + \frac{1}{AC^2} = \frac{AB^2+AC^2}{AB^2 \times AC^2} = \left(\frac{BC}{AB \times AC}\right)^2$ d'après Pythagore. Il suffit donc de montrer $\frac{BC}{AB \times AC} = \frac{1}{AH}$, soit $AB \times AC = BC \times AH$, ce qui est vrai car

$$\mathcal{A}(ABC) = \frac{1}{2} AB \times AC = \frac{1}{2} BC \times AH.$$

□

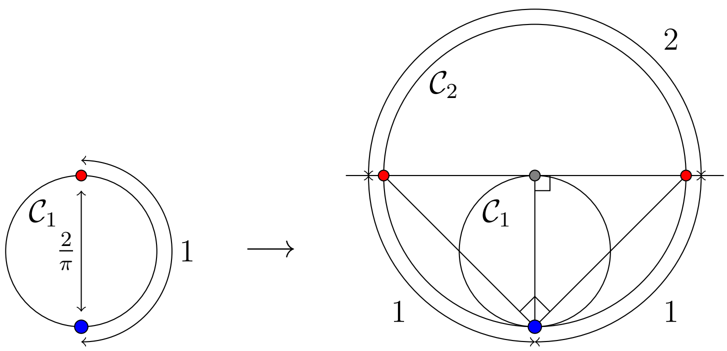


FIGURE 3 – Remplacement d'une lampe sur $\mathcal{C}_1$ par deux lampes sur $\mathcal{C}_2$, en utilisant le lemme du triangle rectangle.

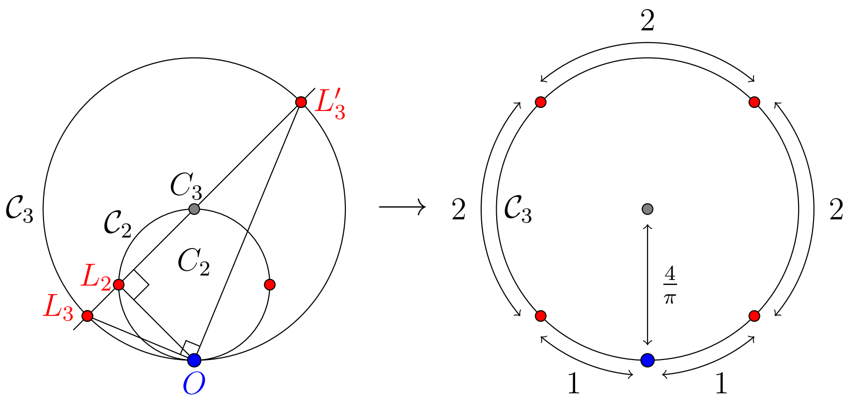


FIGURE 4 – Remplacement des deux lampes sur $\mathcal{C}_2$ par quatre lampes sur $\mathcal{C}_3$. À gauche, la construction des 2 lampes qui vont remplacer l'une des lampes sur $\mathcal{C}_2$. À droite, les 4 lampes sur $\mathcal{C}_3$.

Quelques cercles... On part d'un cercle $\mathcal{C}_1$ de rayon $\frac{1}{\pi}$, avec l'observateur au pôle Sud, et une lampe au pôle Nord. L'énergie reçue vaut alors $\frac{1}{(2/\pi)^2} = \frac{\pi^2}{4}$.

On trace ensuite un cercle $\mathcal{C}_2$, deux fois plus grand, centré au pôle Nord de $\mathcal{C}_1$, et passant par l'observateur. On remplace notre lampe sur $\mathcal{C}_1$ par deux lampes sur $\mathcal{C}_2$ en utilisant notre lemme, comme sur la Figure 3.

On recommence ! On trace maintenant un cercle $\mathcal{C}_3$, dont le centre est le pôle Nord de $\mathcal{C}_2$, deux fois plus grand que $\mathcal{C}_2$ et qui passe par l'observateur. On remplace les deux lampes sur $\mathcal{C}_2$ par quatre lampes sur $\mathcal{C}_3$, comme indiqué sur la Figure 4.

On a $\widehat{OC_3L_3} = \widehat{OC_3L_2} = \frac{1}{2}\widehat{OC_2L_2}$ d'après le théorème de l'angle inscrit, donc $\widehat{OC_3L_3} = 45°$, et $\widehat{OC_3L_3'} = 135°$. Cela montre que deux lampes consécutives sur $\mathcal{C}_3$ forment un angle au centre de $90°$. Comme la circonférence de $\mathcal{C}_3$ est de 8, la distance le long du cercle entre deux lampes consécutives vaut 2, et celle entre l'observateur et les lampes les plus proches vaut 1.

Et on continue...

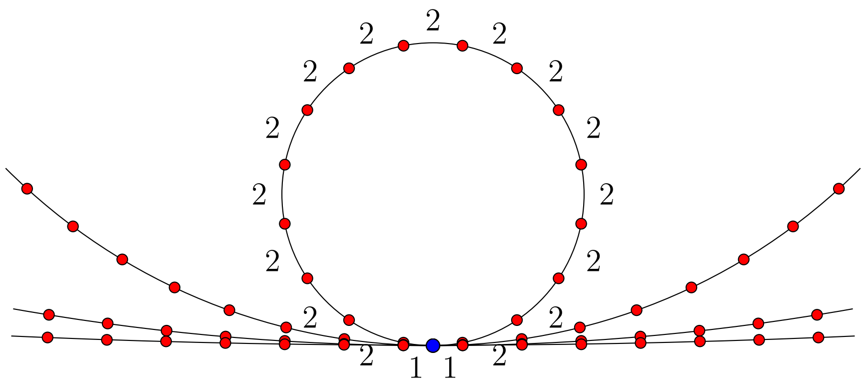


FIGURE 5 – Chacun des cercles représentés ci-dessus donne un ensemble de lampe qui fournit à l'observateur une énergie $\frac{\pi^2}{4}$. Quand le rayon du cercle tend vers l'infini, l'ensemble de lampes se rapproche des entiers impairs sur une droite.

— À chaque étape, le rayon du cercle double, donc le rayon de $\mathcal{C}_i$ vaut $\frac{1}{\pi} \times 2^{i-1}$, et sa circonférence 2^i.

— En passant de $\mathcal{C}_i$ à $\mathcal{C}_{i+1}$, chaque lampe de $\mathcal{C}_i$ est remplacée par deux lampes de $\mathcal{C}_{i+1}$. De plus, si la lampe faisait un angle au centre α dans $\mathcal{C}_i$, les deux nouvelles lampes font des angles au centre $\frac{\alpha}{2}$ et $180° - \frac{\alpha}{2}$ dans $\mathcal{C}_{i+1}$.

— On en déduit (par récurrence) que les lampes sur $\mathcal{C}_i$ sont régulièrement espacées (l'angle au centre entre deux lampes consécutives vaut $\frac{1}{2^{i-1}} \times 360°$).

— Comme la circonférence de $\mathcal{C}_i$ vaut 2×2^i, la distance le long du cercle entre deux lampes consécutives vaut 2, et la distance le long du cercle entre l'observateur et les deux lampes les plus proches vaut toujours 1.

— Enfin, notre lemme sur les triangles rectangles garantit qu'à chaque étape, l'énergie reçue par l'observateur ne change pas.

Passage à la limite Par conséquent, pour tout i, l'observateur reçoit une énergie $\frac{\pi^2}{4}$ pour chacun des ensembles de lampes représentés sur la Figure 5 (où il y a 2^i lampes). Quand i tend vers l'infini, le cercle se rapproche de la droite horizontale passant par l'observateur. Comme les distances le long du cercle valent toujours 1 (entre l'observateur et la lampe la plus proche) et 2 (entre deux lampes voisines), les lampes se rapprochent des entiers impairs sur la droite.

L'énergie de la configuration limite vaut donc

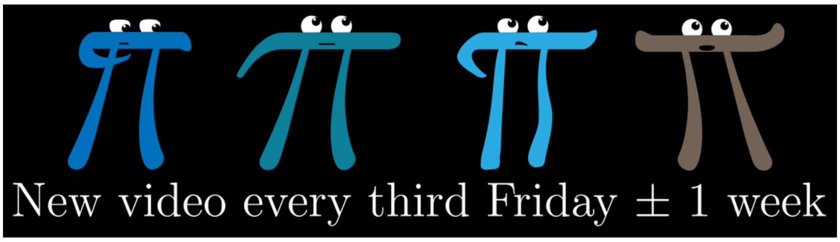
$$2 \times \left(\frac{1}{1^2} + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \dots \right) = \frac{\pi^2}{4}.$$

Fin de la preuve Notons S la somme que l'on cherche. Alors

$$\begin{aligned}
\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\dots &= S-\left(\frac{1}{2^2}+\frac{1}{4^2}+\frac{1}{6^2}+\dots\right)\\
&= S-\left(\frac{1}{4}\times\frac{1}{1^2}+\frac{1}{4}\times\frac{1}{2^2}+\frac{1}{4}\times\frac{1}{3^2}+\dots\right)\\
&= S-\frac{1}{4}S=\frac{3}{4}S.
\end{aligned}$$

On a finalement $\frac{3}{4}S=\frac{\pi^2}{8}$, donc $S=\frac{\pi^2}{6}$.

Un peu de pub Cette preuve est issue d'une vidéo postée sur la passionnante chaîne Youtube *3blue1brown* (« trois bleus un marron », en anglais).



Il existe aussi de nombreuses chaînes francophones de vulgarisation de qualité :

— en maths : Micmaths, Science4all, La statistique expliquée à mon chat...

— en sciences : e-penser, DirtyBiology, ScienceEtonnante...

4 Conférence : Être plus efficace grâce au hasard

Cette conférence portait sur la présentation de plusieurs cadres d'utilisation du hasard, que ce soit pour fêter son anniversaire entre amis, estimer une population, trier un tableau plus rapidement ou montrer que l'on connaît un secret sans divulguer ce secret.

Être plus efficace grâce au hasard

Vincent Jugé

Stage olympique de Valbonne

25/08/2018

Y a-t-il deux élèves avec la même date d'anniversaire ?

Oui ! Il y a même 9 paires d'élèves dans ce cas !

Paradoxe des anniversaires

Problème considéré

On a k boules numérotées de 1 à n. Quelle est la probabilité qu'au moins 2 boules aient le même numéro ?

Théorème

Si $k \gg \sqrt{n}$, c'est très probable !

Esquisse de preuve (avec arnaque)

1. On met $k/2$ boules dans le groupe A et $k/2$ boules dans le groupe B.
2. Chaque boule du groupe B a une probabilité $\mathbb{P} = k/(2n)$ d'avoir le même numéro qu'une boule du groupe A.
3. On a donc une probabilité $k\mathbb{P}/2 = k^2/(4n) \gg 1$ d'avoir deux boules des groupes A et B de même numéro.

Paradoxe des anniversaires

Esquisse de preuve (sans arnaque)

1. On répartit les boules en des groupes $G_1, G_2, \ldots, G_{2\ell}$ de taille $\sqrt{n}/2$, avec $\ell = k/\sqrt{n} \gg 1$.
2. La probabilité que deux boules des groupes G_{2i} et G_{2i+1} n'aient jamais le même numéro vaut $\mathbb{P} = (1 - 1/(2\sqrt{n}))^{\sqrt{n}/2}$.
3. Si $v > u$, alors on montre par récurrence sur v que :
   1. $(1 - 1/v)^u \geqslant 1 - u/v$;
   2. $(1 - 1/v)^u \leqslant 1 - u(1 - u/v)/v = 1 - u/v + (u/v)^2$.
4. Donc $\mathbb{P} \leqslant 1 - 1/4 + 1/16 = 13/16$, et la probabilité que nos k boules aient toutes des numéros distincts vaut au plus $(1 - \mathbb{P})^\ell \ll 1$.

Cas pratique

Pour $n \approx 400$ et $k \approx 80$, on a $\ell \approx 4$ et $(1 - \mathbb{P})^\ell \leqslant (13/16)^4 \approx 0.44$.

Combien cette chambre compte-t-elle de jouets ?

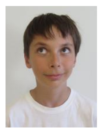
Combien cette chambre compte-t-elle de jouets ?

Méthode n°1 : Ranger la chambre. ☹
Temps nécessaire $\approx n$

Méthode n°2 : Tirer des jouets au hasard jusqu'à retomber sur le même.
Temps nécessaire $\approx \sqrt{n}\log(n)$ grâce au **paradoxe des anniversaires** !

Esquisse de preuve (sans arnaque)

1. Tirer k jouets revient à tirer k boules numérotées de 1 à n.
2. Après $k \approx \sqrt{n}$ tirages, on a tiré deux fois la même boule.
3. Félix B. sait tester en temps $\log(n)$ si une boule figure déjà parmi les k premières que l'on a tirées.



Trier efficacement des copies

Vincent Jugé — Être plus efficace grâce au hasard

Tri rapide

Un **algorithme** couramment utilisé pour trier un tableau est le **tri rapide**.
En moyenne, il utilise environ $n \log(n)$ opérations pour trier n entiers.

Petits entiers

Pivot

Grands entiers

Entiers inconnus

Vincent Jugé — Être plus efficace grâce au hasard

Tri rapide – Le bug de la copie oubliée

Un **algorithme** couramment utilisé pour trier un tableau est le **tri rapide**.
En moyenne, il utilise environ $n \log(n)$ opérations pour trier n entiers.

Complexité attendue $\approx n^2/4 \gg n \log(n)$

Petits entiers

Pivot

Grands entiers

Entiers inconnus

Ruses possibles pour contrer le bug

1. Choisir le pivot **au hasard** ! (facile)
2. **Mélanger** le tableau avant de le trier. (facile)
3. Choisir la **médiane** comme pivot. (très difficile à faire efficacement)

Vincent Jugé — Être plus efficace grâce au hasard

Preuve interactive de connaissance

Vincent Jugé — Être plus efficace grâce au hasard

Preuve interactive de connaissance – logarithme discret

Cadre de travail

1. Alice a choisi trois entiers p, g et k.
2. Elle divulgue p, g et l'entier $g^k \pmod p$ à Bob.
3. Bob doit vérifier qu'Alice connaît bien **un** entier ℓ tel que $g^\ell \equiv g^k \pmod p$ **sans découvrir de tel entier**.

Comment s'y prendre ?

Il suffit d'appliquer le protocole suivant :

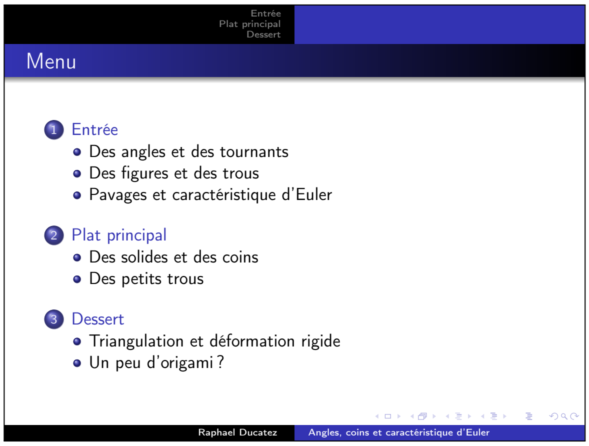
1. Alice choisit un entier m **au hasard** et divulgue $g^m \pmod p$ à Bob.
2. Bob choisit **au hasard** un entier $\epsilon \in \{0, 1\}$ et demande $m + k\epsilon$ à Alice.
3. Alice lui donne un entier n en guise de réponse.
4. Bob vérifie que $g^n \equiv (g^k)^\epsilon g^m \pmod p$.

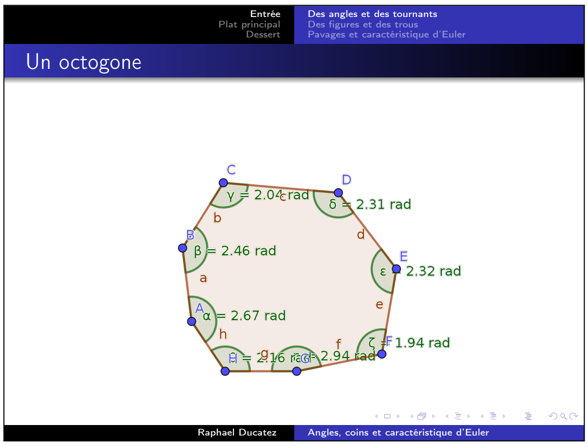
Théorème : Si Alice ne connaît pas ℓ, le protocole échoue 1 fois sur 2.

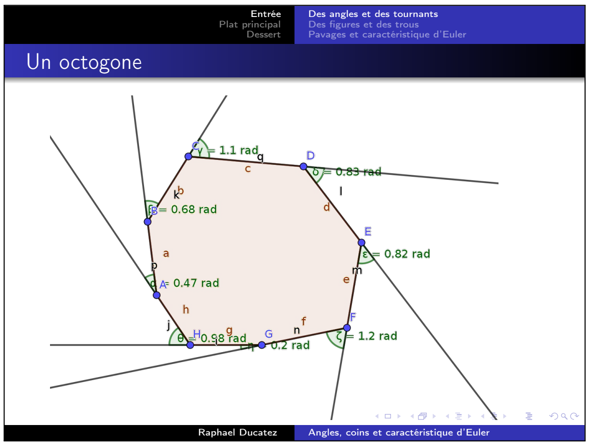
Vincent Jugé — Être plus efficace grâce au hasard

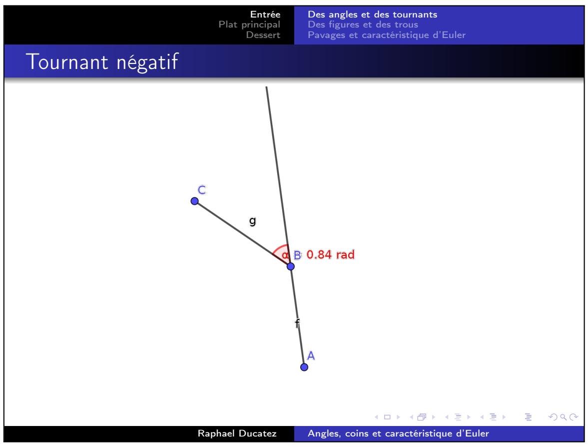
5 Conférence : Angles, coins et caractéristique d'Euler

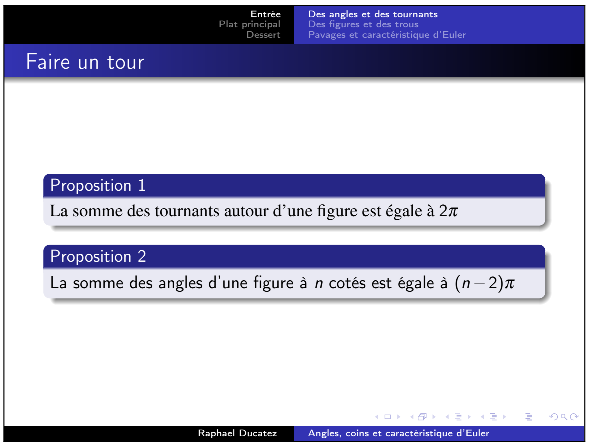
Lors de cette conférence ont été présentés aux élèves deux invariants très importants quand on étudie la géométrie des surfaces et des solides, en fonction de la présence de trous ou pas.

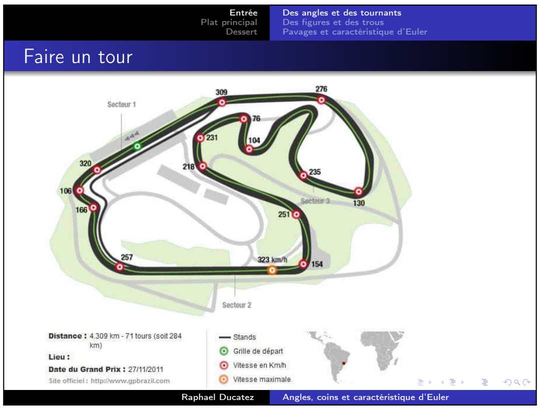


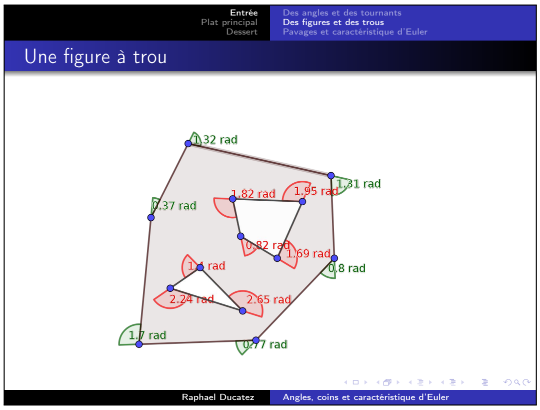


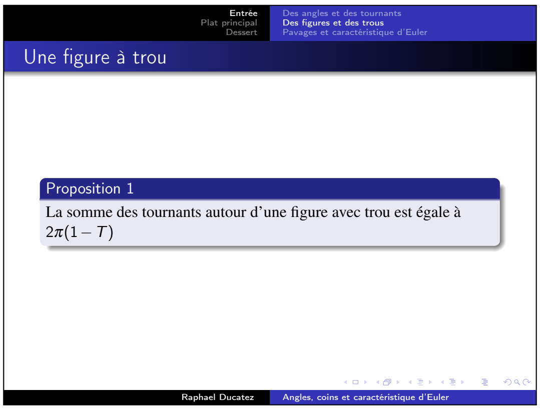


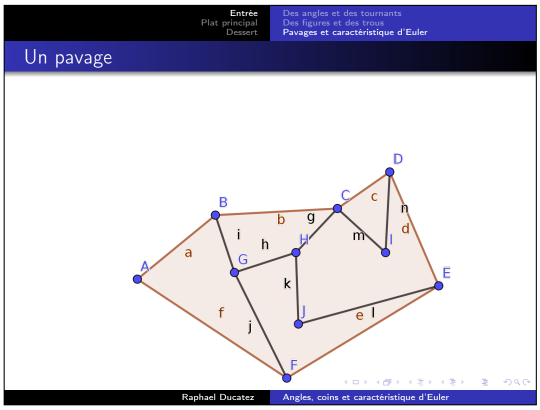


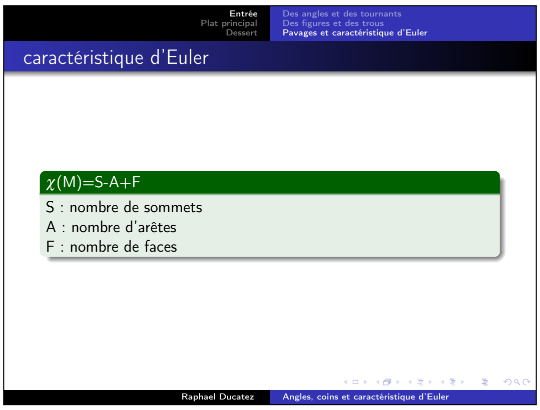


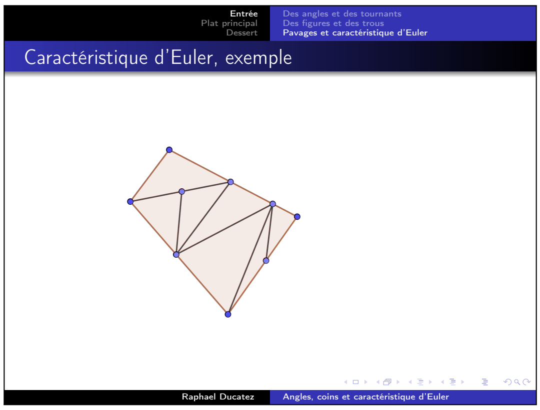

Entrée
Plat principal
Dessert
Des angles et des tournants
Des figures et des trous
Pavages et caractéristique d'Euler
Faire un tour
Secteur 1
Secteur 2
Distance : 4.309 km - 71 tours (soit 284 km)
Lieu :
Date du Grand Prix : 27/11/2011
Stands
Grille de départ
Vitesse en Km/h
Vitesse maximale
Raphael Ducatez
Angles, coins et caractéristique d'Euler

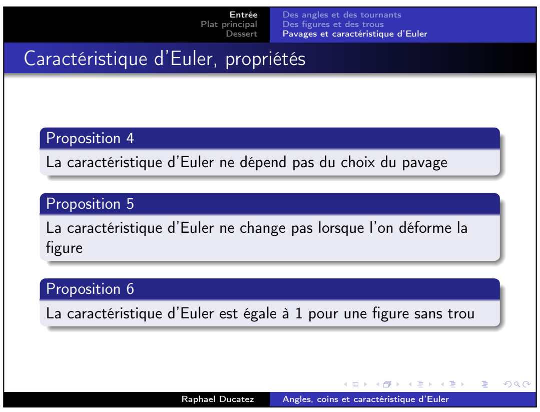

Entrée
Plat principal
Dessert
Des angles et des tournants
Des figures et des trous
Pavages et caractéristique d'Euler
Une figure à trou
1.82 rad
1.95 rad
1.31 rad
0.82 rad
1.69 rad
0.8 rad
2.24 rad
2.65 rad
0.77 rad
Raphael Ducatez
Angles, coins et caractéristique d'Euler

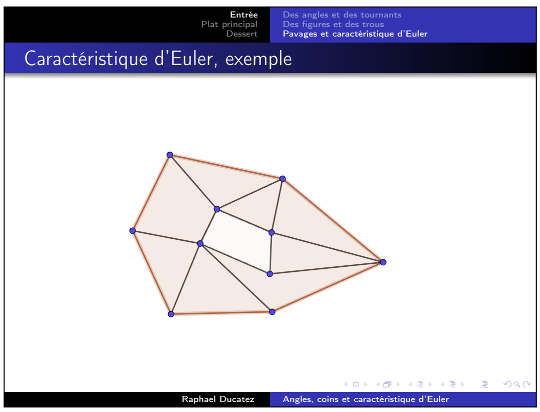

Entrée
Plat principal
Dessert
Des angles et des tournants
Des figures et des trous
Pavages et caractéristique d'Euler
Une figure à trou
Proposition 1
La somme des tournants autour d'une figure avec trou est égale à $2\pi(1-T)$
Raphael Ducatez
Angles, coins et caractéristique d'Euler


Entrée
Plat principal
Dessert
Des angles et des tournants
Des figures et des trous
Pavages et caractéristique d'Euler
Un pavage
A
B
C
D
E
F
G
H
I
J
a
b
c
d
e
f
g
h
i
j
k
l
m
n
Raphael Ducatez
Angles, coins et caractéristique d'Euler

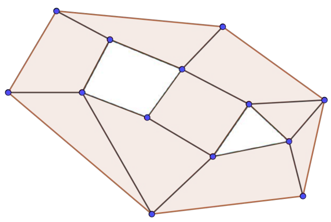

Entrée
Plat principal
Dessert
Des angles et des tournants
Des figures et des trous
Pavages et caractéristique d'Euler
caractéristique d'Euler
χ(M)=S-A+F
S : nombre de sommets
A : nombre d'arêtes
F : nombre de faces
Raphael Ducatez
Angles, coins et caractéristique d'Euler


Entrée
Plat principal
Dessert
Des angles et des tournants
Des figures et des trous
Pavages et caractéristique d'Euler
Caractéristique d'Euler, exemple
Raphael Ducatez
Angles, coins et caractéristique d'Euler


Entrée
Plat principal
Dessert
Des angles et des tournants
Des figures et des trous
Pavages et caractéristique d'Euler
Caractéristique d'Euler, propriétés
Proposition 4
La caractéristique d'Euler ne dépend pas du choix du pavage
Proposition 5
La caractéristique d'Euler ne change pas lorsque l'on déforme la figure
Proposition 6
La caractéristique d'Euler est égale à 1 pour une figure sans trou
Raphael Ducatez
Angles, coins et caractéristique d'Euler


Entrée
Plat principal
Dessert
Des angles et des tournants
Des figures et des trous
Pavages et caractéristique d'Euler
Caractéristique d'Euler, exemple
Raphael Ducatez
Angles, coins et caractéristique d'Euler

Caractéristique d'Euler, exemple



Caractéristique d'Euler, propriétés

Proposition 6(bis)

La caractéristique d'Euler est égale à 1 moins le nombre de trou de la figure

Petit résumé

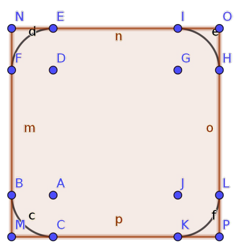
Théorème 1

La caractéristique d'Euler et la somme des tournants ne changent pas lorsque l'on déforme la figure

Théorème 2

La somme des tournants d'une figure
$= 2\pi$ fois $(1 -$ nombre de trou$)$
$= 2\pi$ fois la caractéristique d'Euler

Un cercle caché ?



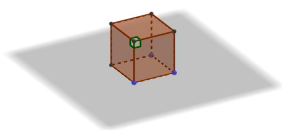
Coins et angles

Coins

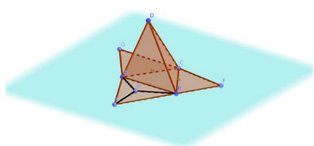
Un coin est égale à 2π moins la somme des angles qui le compose.

$$C = 2\pi - \sum_i \alpha_i$$

Coin, exemple



Tordons la figure



Tordons la figure

Proposition 5

La somme des coins ne change pas lorsque l'on déforme le solide où que l'on complexifie le pavage.

Coins et caractéristique d'Euler

Théorème 3
La somme des coins est égale à la 2π fois la caractéristique d'Euler.

Entrée / Plat principal / Dessert — Des solides et des coins / Des petits trous

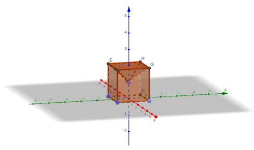
Coins et caractéristique d'Euler

$$\begin{aligned}\sum_{s\in S}\Big(2\pi-\sum_{\alpha\sim s}\alpha\Big) &= 2\pi S-\sum_{\alpha}\alpha\\ &= 2\pi S-\sum_{F}\sum_{\alpha\in F}\alpha\\ &= 2\pi S-\sum_{F}(\pi n_F-2\pi)\\ &= 2\pi S-\pi\sum_{F}n_F+2\pi F\\ &= 2\pi S-2\pi A+2\pi F\\ &= 2\pi\chi\end{aligned}$$

Raphael Ducatez — Angles, coins et caractéristique d'Euler

Entrée / Plat principal / Dessert — Des solides et des coins / Des petits trous

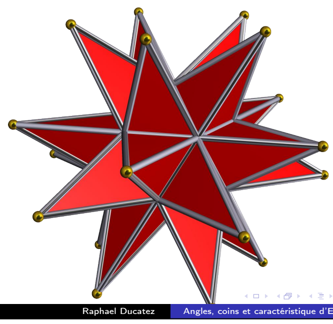
Un coin négatif ?



Raphael Ducatez — Angles, coins et caractéristique d'Euler

Entrée / Plat principal / Dessert — Des solides et des coins / Des petits trous

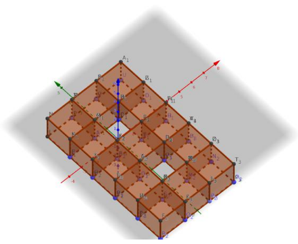
Un coin négatif ?



Raphael Ducatez — Angles, coins et caractéristique d'Euler

Entrée / Plat principal / Dessert — Des solides et des coins / Des petits trous

Un solide à trous



Raphael Ducatez — Angles, coins et caractéristique d'Euler

Entrée / Plat principal / Dessert — Des solides et des coins / Des petits trous

Petit résumé

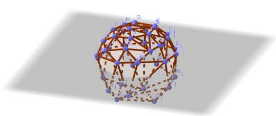
Théorème 3
La caractéristique d'Euler et la somme des coins ne changent pas lorsque l'on déforme la figure

Théorème 4
La somme des coins d'un solide
$= 2\pi$ fois $(2 - 2 *$ nombre de trou$)$
$= 2\pi$ fois la caractéristique d'Euler

Raphael Ducatez — Angles, coins et caractéristique d'Euler

Entrée / Plat principal / Dessert — Des solides et des coins / Des petits trous

Triangulation de la sphère



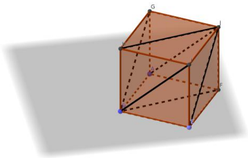
Raphael Ducatez — Angles, coins et caractéristique d'Euler

Entrée / Plat principal / Dessert — Des solides et des coins / Des petits trous

Petits objets

Raphael Ducatez — Angles, coins et caractéristique d'Euler

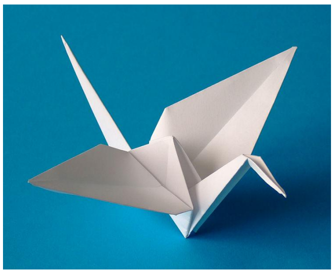
Une triangulation



Théorème remarquable

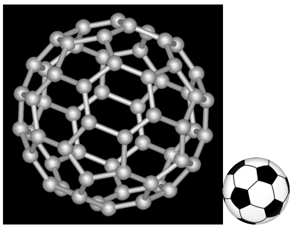
Théorème 5
Un coin dans une triangulation ne change pas lorsque l'on déforme la figure de manière rigide

De l'origami ?



Biosphère

Fullerène



Fullerène

Un coin (hexagone-hexagone-pentagone) : $2\pi - \frac{2\pi}{3} - \frac{2\pi}{3} - \frac{3\pi}{5} = \frac{\pi}{15}$
Il y a donc 60 coins (h-h-p) : 12 pentagones.

Fullerène

A retenir.

Théorème 3
La caractéristique d'Euler et la somme des coins ne changent pas lorsque l'on déforme la figure

Théorème 4
La somme des coins d'un solide
$= 2\pi$ fois $(2 - 2 *$ nombre de trou$)$
$= 2\pi$ fois la caractéristique d'Euler

Théorème 5
Un coin dans une triangulation ne change pas lorsque l'on déforme la figure de manière rigide

VIII. La Muraille

Une muraille de 142 exercices était affichée dans la salle commune. Les exercices 1 à 42 sont dits de NIVEAU 1. Les exercices 43 à 96 sont dits de NIVEAU 2. Les exercices 97 à 142 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 (étoilés ou non) de tous niveaux. Les élèves du groupe B cherchent les exercices (étoilés ou non) de NIVEAU 2 ou 3 et les exercices étoilés de NIVEAU 1. Les élèves du groupe C cherchent les exercices (étoilés ou non) de NIVEAU 3 et les exercices étoilés de NIVEAU 2. Les élèves du groupe D cherchent les exercices (étoilés ou non) de NIVEAU 3.

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).

Énoncés

– Exercices de niveau 1 –

Exercice 1*
Trouver tous les entiers n strictement positifs tels que $2^n + n$ divise $8^n + n$.

Exercice 2** (résolu par Nelly Cerf)
Soient a et b deux entiers relatifs non nuls tels que les fractions $\frac{a}{600}$ et $\frac{b}{700}$ soient deux fractions irréductibles. Quel est le plus petit dénominateur possible de la fraction $\frac{7a+6b}{4200}$?

Exercice 3***
Soit ABC un triangle équilatéral et P un point à l'intérieur de ce triangle. Soient D, E et F les pieds des perpendiculaires de P sur $[BC]$, $[CA]$ et $[AB]$ respectivement. Montrer que :

1. $AF + BD + CE = AE + BF + CD$ et que
2. $|APF| + |BPD| + |CPE| = |APE| + |BPF| + |CPD|$,

où $|XYZ|$ désigne l'aire du triangle XYZ.

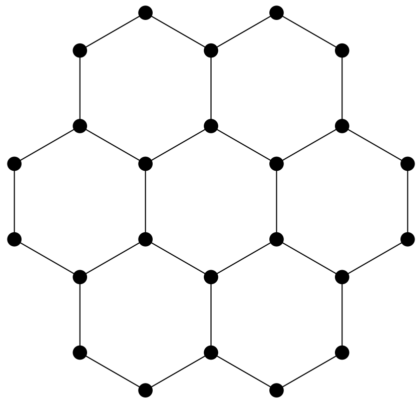
Exercice 4**
Soient x, y deux entiers relatifs et p un nombre premier. Montrer que si l'on a $x \equiv y\ [p]$, alors on a $x^p \equiv y^p\ [p^2]$.

Exercice 5*
Trouver tous les quadruplets d'entiers positifs (w, x, y, z) tels que

$$w^x + w^y = w^z.$$

Exercice 6** (résolu par Nelly Cerf)
On se donne 7 entiers, deux à deux distincts, strictement positifs, dont la somme vaut 100. Montrer que l'on peut en trouver trois dont la somme est au moins 50.

Exercice 7** (résolu par Alexandre Barbu et Mithil Krishnan)
La figure représente la section d'une ruche. A chacun des 24 sommets, il y a de 1 à 6 abeilles. Aux 6 sommets d'un même hexagone, les nombres d'abeilles doivent être tous différents les uns des autres. Quel est le nombre total d'abeilles de la ruche, au maximum ?



Exercice 8***
Trouver tous les entiers relatifs x et y tels que

$$x^2y + 7x = x^2 + 3xy + 3y + 4.$$

Exercice 9**
Les nombres de 1 à n sont écrits au tableau. À chaque étape, on choisit deux nombres a et b distincts du tableau, on les efface puis on les remplace par $ab+a+b$, et on réitère ce processus. Quel sera le dernier nombre écrit au tableau ?

Exercice 10*****
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 11**
Soient a et b deux nombres réels et f la fonction de $\mathbb{R}$ dans $\mathbb{R}$ qui à x associe $x^2 + ax + b$. On suppose qu'il existe un réel t tel que $f(t) = f(f(f(t))) = 0$. Montrer que $f(0) \times f(1) = 0$.

Exercice 12**
Combien y a-t-il d'entiers positifs n tels que

$$\frac{n^{2016}}{n - 2016}$$

soit un nombre entier ?

Exercice 13* (résolu par Matthieu Vogel)
Soit n un entier naturel. Montrer que si n et $8n^2+1$ sont premiers, alors $8n^2-1$ l'est également.

Exercice 14**** (résolu par Gaspard Delabre)
Montrer que $\sqrt{2}+\sqrt{5}+\sqrt{13}$ est irrationnel.

Exercice 15***
Montrer que tous les termes de la suite (a_n) définie par

$$\begin{cases} a_1 = a_2 = a_3 = 1 \\ a_{n+1} = \dfrac{1 + a_{n-1}a_n}{a_{n-2}} \end{cases}$$

sont des entiers.

Exercice 16**
On considère 101 points, placés à l'intérieur d'un carré 10×10. Montrer qu'il existe un triangle parmi les 101 points avec une aire inférieure ou égale à 1.

Exercice 17***
Existe-t-il une suite $(u_n)_{n \geqslant 1}$ d'entiers naturels non nuls telle que pour tous entiers $m, n \geqslant 1$ u_n et u_m sont premiers entre eux si et seulement si $|n-m| = 1$?

Exercice 18**
Soit ABC un triangle isocèle en A et D le pied de la bissectrice intérieure issue de B. On suppose que $BC = AD + DB$. Combien vaut $\widehat{BAC}$?

Exercice 19**
20 enfants sont attendus par leurs grands-pères à la sortie de l'école primaire. On suppose que deux enfants quelconques choisis parmi les 20 ont au moins un grand-père en commun. Montrer qu'il y a au moins un grand-père qui attend au moins 14 de ses petits-enfants.

Exercice 20**** (résolu par Gaspard Delabre)
Trouver les entiers naturels n tels que $n^4 + 4^n$ soit premier.

Exercice 21** (résolu par Nelly Cerf)
Athalie et Bérénice jouent à un jeu. Elles prennent un cube, et tour à tour, elles en choisissent trois arêtes qu'elles colorient (Athalie en rouge, Bérénice en bleu). Le but de chaque joueuse est de colorier avant l'autre quatre arêtes d'une même face.

Athalie commence. A-t-elle une stratégie gagnante ?

Exercice 22*
On inscrit 100 entiers sur un cercle. Leur somme vaut 1. On appelle séquence positive une suite de nombres consécutifs sur le cercle telle que leur somme soit strictement positive. Combien y a-t-il de séquences positives sur le cercle ?

Exercice 23** (résolu par Matthieu Vogel)
Matthieu fabrique des puzzles de forme carrée. Malheureusement, il ne sait découper que des pièces carrées. Pour chaque puzzle, il prépare une boîte contenant les pièces nécessaires à la reconstitution du puzzle, et sur chaque boîte, il indique le nombre de pièces qu'elle contient.

Quel est l'ensemble des nombres qu'on peut lire sur les boîtes ?

Exercice 24* (résolu par Elio Audusse, Gaspard Delabre et Caleb Ott)
L'espiègle princesse Turandot pense secrètement à trois entiers à deux chiffres, x, y et z. Le prince de Perse doit choisir trois entiers a, b et c, et Turandot lui donne la somme $ax + by + cz$. Pour sauver sa tête, le prince doit alors en déduire x, y et z. Quelle stratégie lui conseillez-vous ?

Exercice 25**
Soit $ABCD, ECGF$ deux carrés tels que B, C, G sont alignés et A, D, E, F sont du même côté de la droite (BC). Soit M l'autre point d'intersection des cercles circonscrits à $ABCD$ et à $ECGF$.

Donner une autre construction du point M, n'utilisant qu'une règle non graduée.

Exercice 26**
Un naturel n est *hydraté* si il a exactement deux diviseurs premiers. Existe-t-il une suite de 18 naturels consécutifs hydratés ?

Exercice 27**
Alice et Bob jouent au jeu suivant : Alice part du nombre 2 et les joueurs jouent chacun leur tour. A chaque tour, en notant n le nombre atteint par le joueur précédent, on ajoute un nombre m tel que m divise n, $m \neq n$, et $m + n \leqslant 2016$. Le premier joueur à ne plus pouvoir jouer a perdu. Quel joueur peut s'assurer la victoire ?

Exercice 28* (résolu par Baptiste Vibert)
Peut-on remplir les cases d'un tableau 10×10 avec des $1, -1$ ou 0 de sorte que les sommes de chaque ligne et de chaque colonne soient toutes différentes ?

Exercice 29*
Rusalka observe par un beau soir d'été 50 étoiles. Avec son matériel d'astronomie, elle calcule la somme des distances mutuelles entre elles, qui vaut S. Soudain, un nuage surgit et cache 25 étoiles. Montrer que la somme des distances mutuelles entre les 25 étoiles restantes ne dépasse pas $S/2$.

Exercice 30**
Soit $f : \mathbb{R} \mapsto \mathbb{R}$ une fonction telle que $f(x + y) \geqslant f(xy)$ pour tous les réels x, y. Montrer que f est constante.

Exercice 31**
Soit ABC un triangle isocèle en B, puis F un point sur la bissectrice de $\widehat{ABC}$ tel que (AF) soit parallèle à (BC). Enfin, soit E le milieu de $[BC]$, et soit D le symétrique de A par rapport à F. Calculer le rapport des distances EF/BD.

Exercice 32******
Soit $\mathcal{P} = A_1 \ldots A_{2n}$ 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 33**
Montrer que pour x, y des réels positifs on a toujours :

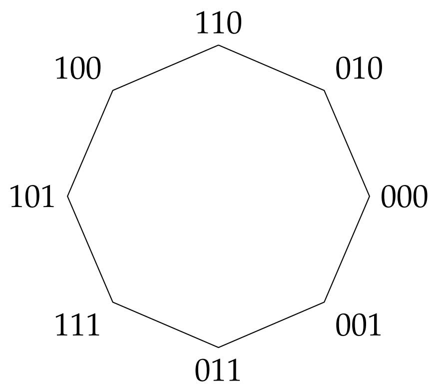
$$\frac{x}{x^4+y^2}+\frac{y}{y^4+x^2}\leqslant\frac{1}{xy}.$$

Exercice 34*
Si tous les points du plan sont colorés soit en rouge, soit en orange soit en violet, peut-on toujours trouver deux points de même couleur éloignés d'un centimètre exactement ?

Exercice 35** (résolu par Gaspard Delabre)
Il y a 17 tours sur un échiquier ordinaire. Montrer qu'on peut toujours en trouver 3 qui ne se menacent pas entre elles.

Exercice 36**
Soit ABC un triangle, I le centre du cercle inscrit dans ABC, D le pied de la hauteur de ABI issue de B, et E le pied de la hauteur de BCI issue de B. Montrer que $AB = BC$ si et seulement si $BD = BE$.

Exercice 37**
Pour quels naturels $n \geqslant 2$ peut-on assigner à chaque sommet d'un 2^n-gone une suite de n chiffres 0 et 1 de telle sorte que chaque suite soit utilisée une et une seule fois et que deux suites sur deux sommets adjacents diffèrent par exactement un chiffre ? Ci-dessous, un exemple d'une telle configuration pour $n = 3$.



Exercice 38****** (résolu par Nelly Cerf)
Trouver tous les entiers positifs a, b, c tels que

$$2^a3^b+9=c^2.$$

Exercice 39**
Soit ABC un triangle actuangle. La bissectrice de $\widehat{BAC}$ coupe BC en D et le cercle circonscrit à ABC en E. La tangente au cercle circonscrit à ABC en B coupe AD en F. On suppose que $AD^2 = 2CD^2$. Montrer que E est le milieu de $[AF]$.

Exercice 40**
On donne un nombre n plus grand que 10^{2018}. Quel est le premier chiffre après la virgule dans l'écriture décimale de la racine carré de $(n^2 + n + 200)$?

Exercice 41**
Mathieu joue au billard sur un billard rectangulaire de 2,03 m sur 3,03 m. Sa boule, de 6 cm de diamètre, est placée au milieu d'un grand côté du billard et Mathieu la fait rouler, sans effet, selon un angle de 45 degré par rapport au côté du billard. En supposant que Mathieu lui ait donné suffisamment de force, à quelle distance du point de départ le centre de la boule sera-t-il au moment du 59e rebond ?

Exercice 42*
Eva et Victor disposent d'une tablette de chocolat rectangulaire de n carrés de longueur et 2 carrés de hauteur pour un certain entier $n > 0$ et jouent au jeu suivant : chacun leur tour, en commençant par Eva, ils choisissent un carré de la tablette et le croquent ainsi que tous les carrés situés en haut ou à droite de celui-ci. Le dernier carré, en bas à gauche, étant fourré au piment, le joueur qui se trouve obligé de le manger a perdu. Est-ce que Victor ou Eva possède une stratégie gagnante ? Si oui, quelle est-elle ?

– Exercices de niveau 2 –

Exercice 43**
Savinien et Martin jouent à un jeu. Les cases d'un échiquier $n \times n$ sont toutes vides et blanches, sauf celle en bas à gauche qui est noire et sur laquelle se trouve une tour. Tour à tour, Savinien et Martin la déplacent sur une case blanche et colorient cette case en noir. Le premier qui ne peut plus jouer a perdu. Sur quelle case Savinien peut-il jouer son premier coup et avoir une stratégie gagnante ?

Exercice 44*** (résolu par Clément Chapot)
Soit $\mathcal{P}$ la parabole d'équation $y = x^2$. Trouver une condition nécessaire et suffisante pour que des points de $\mathcal{P}$ d'abscisse a, b, c et d soient cocycliques.

Exercice 45****
Pour quels entiers $n \geqslant 1$ existe-t-il une bijection

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\},$$

de sorte que $|\sigma(i) - i| \neq |\sigma(j) - j|$ si $i \neq j$?

Exercice 46**
Martin et Savinien jouent à un jeu : une droite est tracée dans le plan. Martin choisit une caractéristique pour cette droite parmi "médiatrice", "médiane", "hauteur", "bissectrice intérieure". Savinien trace ensuite une deuxième droite coupant la première en un point P. Martin trace alors une troisième droite sécante aux deux autres en P. Si Savinien parvient à dessiner un triangle dont ce sont les trois droites remarquables à la caractéristique choisie, il gagne. Sinon c'est Martin. Qui a une stratégie gagnante ?

Exercice 47**
Quel est l'entier n minimal tel que, si on place n points sur le réseau hexagonal, il existe forcément deux de ces points dont le milieu est sur le réseau hexagonal ?

Exercice 48***** (résolu par Clément Chapot)
On considère un triangle acutangle ABC avec $\widehat{A} = 60°$. Déterminer les points $M \in (AB)$ et $N \in (AC)$ qui minimisent la somme

$$|CM| + |MN| + |BN|.$$

Exercice 49***
Soit P un point de l'espace et $r > 0$. Montrer qu'il existe 8 sphères disjointes de même rayon r qui cachent le point P, c'est-à-dire que toute demi-droite issue de P rencontre au moins l'une des sphères. On supposera que les centres des sphères sont tous à des distances $> r$ de P.

Exercice 50***
Parmi les quadrilatères de côtés a,b,c,d caractériser géométriquement celui qui a la plus grande aire.

Exercice 51**
Achille et Briséis ont un tas de $2n + 1$ jetons. Tour à tour, ils peuvent en retirer un nombre au choix entre 1 et $2k + 1$, et ce jusqu'à épuisement du tas. Le but de chaque joueur est de finir en ayant retiré, en tout, un nombre pair de jetons.

Achille commence. A-t-il une stratégie gagnante ?

Exercice 52***
Soit P un point à l'intérieur d'un cercle de rayon R, d une droite passant par P et d' la perpendiculaire à d en P. On fait tourner les droites d et d' d'un angle ϕ autour de P. Montrer que quelle que soit la position du point P, l'aire balayée par d et d' à l'intérieur du cercle (qui a la forme d'une croix) vaudra $\pi R^2 \dfrac{4\phi}{360}$.

Exercice 53*
Prouver qu'il existe une infinité de triplets d'entiers positifs (m, n, p) tels que $4mn - m - n = p^2 - 1$, mais aucun tel que $4mn - m - n = p^2$.

Exercice 54***** (résolu par Timothé Ringeard)
Soit ABC un triangle, D le milieu de $[AB]$, M le milieu de $[CD]$. 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 55** (résolu par Victor Chen)
Sophie choisit au hasard un polynôme P dont tous les coefficients sont des entiers naturels. Thomas a le droit de demander à Sophie la valeur prise par P en un nombre a donné, puis, en tenant éventuellement compte de la première réponse de Sophie, en un autre nombre b. Thomas doit ensuite deviner le polynôme P. Comment faire ?

Exercice 56** (résolu par Sylvain Chabredier, Rémi Guenet et Louis Vassaux)
Peut-on trouver deux rationnels a et b tels qu'un carré de côté a ait même aire qu'un triangle équilatéral de côté b ?

Exercice 57** (résolu par Joseph Lenormand)
Au stage de maths, il y a $2n$ stagiaires. Chaque semaine, n stagiaires partent en voyage. Après un certain nombre de voyages (le stage dure longtemps), chaque paire de stagiaires a déjà été ensemble au cours d'au moins un voyage. Au minimum, combien y a-t-il eu de voyages ?

Exercice 58**** (résolu par Timothé Ringeard)
Soit ABC un triangle rectangle isocèle en C, D et E des points de $[AC]$ et $[BC]$ tels que $CE = CD$. Les perpendiculaires à (AE) passant par D et C coupent (AB) respectivement en K et L. Montrer que $KL = LB$.

Exercice 59*
Déterminer les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que pour tous m, n entiers naturels,

$$f(f(m) + f(n)) = m + n.$$

Exercice 60***
On considère n entiers $a_1, \dots a_n$ dans $\{1, \dots 2015\}$ tels que le ppcm de deux d'entre eux est toujours > 2015. Montrer que

$$\frac{1}{a_1} + \cdots + \frac{1}{a_n} < 2.$$

Exercice 61****
Déterminer tous les couples de polynômes non constants P et Q unitaires, de degré n et admettant n racines positives ou nulles (non nécessairement distinctes) tels que

$$P(x) - Q(x) = 1.$$

Exercice 62* (résolu par Michaël Chen, Rémi Guenet et Évelyne Le Bezvoët)
Déterminer les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que pour tout n entier positif,

$$f(f(f(n))) + f(f(n)) + f(n) = 3n.$$

Exercice 63** (résolu par Benoît Fanton, Joseph Lenormand et Louis Vassaux)
On construit un triangle de la manière suivante : Les nombres de 1 à n sont sur la première ligne. Sur les autres lignes, chaque nombre est la somme du nombre au-dessus de lui et de celui au-dessus à droite de lui. Le coin supérieur gauche du triangle est représenté ci-dessous. Quel nombre y a-t-il sur la dernière ligne ? En donner une formule sans symbole sommatoire.

$$\begin{array}{cccc} 1 & 2 & 3 & \dots \\ 3 & 5 & & \\ 8 & & & \\ \vdots & & & \end{array}$$

Exercice 64*
Les tangentes au cercle circonscrit d'un triangle ABC en A et C se coupent en un point P. Les droites (AB) et (CP) se coupent en un point Q. Montrer que si les triangles ABC, ACP et BCQ ont même aire, alors ABC est rectangle.

Exercice 65****
Soit $a_1, a_2, \dots$ une suite infinie strictement croissante d'entiers naturels telle que pour tout n, le terme a_n soit égal soit à la moyenne arithmétique, soit à la moyenne géométrique des deux termes a_{n-1} et a_{n+1}. Cette suite est-elle nécessairement toujours arithmétique ou toujours géométrique à partir d'un certain rang ?

Exercice 66*
Aujourd'hui, Léo l'escargot a avancé le long du chemin de huit heures du matin à six heures du soir. Plusieurs personnes l'ont observé dans son trajet : chacune est restée une heure exactement, et a pu observer que Léo avait avancé d'un mètre exactement. À tout moment de la journée, il y avait au moins un observateur. Quelle est la plus grande distance que Léo a pu parcourir ?

Exercice 67* (résolu par Noémie Cerrina et Émilie Zheng)
La reine d'Angleterre a décidé d'investir massivement dans l'euro : elle dispose d'une réserve illimitée de pièces de $1, 2, 5, 10, 20, 50$ centimes et de 1 euro (elle en a une infinité de chaque sorte). Pour certains entiers U et K, elle sait qu'elle peut obtenir U centimes avec K pièces. Prouver qu'elle peut obtenir K euros avec U pièces.

Exercice 68***
Soit $x_0, x_1, x_2, \dots$ une suite de nombres réels. On dit que la suite $x_0, x_1, \dots$ est convexe si :

$$\frac{x_{n-1} + x_{n+1}}{2} \geqslant x_n \quad \text{pour tout entier } n \geqslant 0$$

et qu'elle est log-convexe si :

$$x_{n+1}x_{n-1} \geqslant x_n^2 \quad \text{pour tout entier } n \geqslant 0$$

On suppose que pour tout nombre réel $a > 0$, la suite $x_0, ax_1, a^2x_2^2, a^3x_3^3, \dots$ est convexe. Prouver que la suite $x_0, x_1, \dots$ est log-convexe.

Exercice 69*
Quels sont les cinquante premiers chiffres après la virgule de $(10+\sqrt{101})^{40}$?

Exercice 70***
Soit ABC un triangle équilatéral de côté a et P un point à l'intérieur de ce triangle. On construit un triangle XYZ de côtés de longueur PA, PB et PC et on note F son point de Fermat. Montrer que $FX+FY+FZ=a$.

Exercice 71*****
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 $\dfrac{AP}{PC}=2\dfrac{AB}{BC}$

Exercice 72****
Trouver toutes les fonctions f de $\mathbb{N}$ dans $\mathbb{N}$ telles que pour tous entiers $m,n\geqslant 0$ on ait

$$f(m+f(n))=f(f(m))+f(n).$$

Exercice 73*
Trouver tous les couples d'entiers strictement positifs (a,b) tels que a^2+3b et b^2+3a soient des carrés parfaits.

Exercice 74*****
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) parallèles. 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 75* (résolu par Noémie Cerrina, Luc Dauge, Adrien Patoz, Clément Rougeron et Émilie Zheng)
Rémi donne à Martin deux sacs contenant respectivement n et m chouquettes. Il lui autorise les deux opérations suivantes : retirer le même nombre de chouquettes de chaque sac, et doubler le nombre de chouquettes du sac de son choix (Rémi ayant travaillé dur aux fourneaux, il y en a une infinité en réserve). Si Martin arrive à vider les deux sacs après un nombre fini d'opérations, il aura le droit de manger toutes les chouquettes. Peut-il arriver à ses fins, quels que soient les entiers naturels n et m ? Que se passe-t-il si on remplace "doubler" par "tripler" ?

Exercice 76**
On trace un grand triangle ABC, et on le pave avec des triangles. On étiquette ensuite les sommets créés de la façon suivante : à chaque sommet appartenant au côté $[AB]$ du grand triangle est attribuée une lettre, A ou B ; à chaque sommet appartenant au côté $[BC]$ du grand triangle est attribué un B ou un C ; à chaque sommet appartenant au côté $[CA]$ du grand triangle est attribué un C ou un A. On étiquette les sommets situés strictement à l'intérieur du grand triangle avec un A, un B ou un C au choix.

Montrer qu'on peut trouver un triangle (hormis le grand triangle) étiqueté ABC.

Exercice 77***** (résolu par Clément Chapot)
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 78* (résolu par Alexandre Barbu, Mithil Krishnan et Katherine Ellison)
On dispose d'un échiquier de taille 8×8 dont une case a été enlevée. Peut-on le paver avec des rectangles de taille 1×3 ?

Exercice 79*
Soit $A = \{a_1, a_2, \ldots, a_n\}$ un ensemble fini de réels. La k-ème fonction symétrique élémentaire de A, notée σ_k, est la somme des produits k par k des éléments de A. Ainsi, $\sigma_1 = a_1 + a_2 + \ldots + a_n$, $\sigma_2 = a_1a_2 + a_1a_3 + a_2a_3 + \ldots$ et, plus généralement, $\sigma_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} a_{i_1}a_{i_2} \ldots a_{i_k}$. On suppose que toutes les fonctions symétriques élémentaires de A sont strictement positives. Les éléments a_i sont-ils également strictement positifs ?

Exercice 80*
Existe-t-il deux nombres réels distincts a et b et deux polynômes réels unitaires distincts non constants P et Q tels que P et Q prennent la valeur a simultanément (i.e. sur le même ensemble de valeurs, supposé non vide) et de même la valeur b simultanément ?

Exercice 81***
Trouver tous les polynômes P à coefficients réels tels que, pour tout $n \in \mathbb{N}$, il existe un rationnel r tel que $P(r) = n$.

Exercice 82*
Soit ABC un triangle rectangle en C et M le milieu de $[AB]$. Soit G un point de $[MC]$. Soit P sur la demi-droite $[AG)$ tel que $\widehat{CPA} = \widehat{BAC}$ et Q sur la demi-droite $[BG)$ tel que $\widehat{BQC} = \widehat{CBA}$. Montrer que les cercles circonscrits aux triangles AQG et BPG se coupent sur (AB).

Exercice 83*
On construit la suite (u_n) de la façon suivante : on pose $u_0 = 0$, et pour tout $n \in \mathbb{N}^*$, on choisit u_n de sorte que $|u_n| = |u_{n-1} + 1|$. Quelle est la plus petite valeur que puisse prendre

$$|u_1 + u_2 + \ldots + u_{2017}| \text{ ?}$$

Exercice 84**
Soit $f(x) = x^{2016} + a_{2015}x^{2015} + \cdots + a_1x + a_0$ un polynôme. Llawgad et Aelwyd jouent au jeu suivant : chacun leur tour, ils fixent la valeur (réelle) d'un des coefficients $a_0, \ldots, a_{2015}$. Une fois qu'une valeur a été fixée par l'un d'entre eux, l'autre ne peut plus la changer. Le jeu se termine lorsque tous les coefficients ont reçu une valeur.

Llawgad commence. Son objectif est qu'à la fin du jeu, $f(x)$ soit divisible par un certain polynôme $m(x)$. Aelwyd tente de l'en empêcher.

1. Qui a une stratégie gagnante si $m(x) = x - 2018$?
2. Qui a une stratégie gagnante si $m(x) = x^2 + 1$?

Exercice 85****
On définit une suite u_n ainsi : u_1 et u_2 sont des entiers entre 1 et 10000 (au sens large), et u_{k+1} est la plus petite valeur absolue des différences deux à deux des termes précédents. Montrer que $u_{21} = 0$.

Exercice 86***
Soit ABC un triangle acutangle, avec $AC > BC$. On note H son orthocentre, O le centre de son cercle circonscrit et M le milieu de $[AC]$. Soit F le pied de la hauteur issue de C, et P le symétrique de A par rapport à F. On note X l'intersection de (PH) avec (BC), Y l'intersection de (FX) avec (OM), et Z l'intersection de (OF) avec (AC). Montrer que F, M, Y et Z sont cocycliques.

Exercice 87**
Deux amis A et B s'envoient des messages chiffrés de la façon suivante :

— Ils fixent ensemble un grand nombre premier $p > 2$.

— Chacun de leur côté, A choisit un nombre a, $1 < a < p - 1$ premier à $p - 1$, tandis que B choisit nombre b, $1 < b < p - 1$ premier à $p - 1$.

— A calcule l'inverse $\widehat{a}$ de a modulo $p - 1$ et B calcule l'inverse $\widehat{b}$ de b modulo $p - 1$.

— A choisit un message m (un nombre modulo p) à envoyer à B.

— A calcule $m_1 = m^a$ et l'envoie à B.

— B calcule $m_2 = (m_1)^b$ et l'envoie en retour à A.

— A calcule $m_3 = (m_2)^{\widehat{a}}$ et l'envoie encore une fois à B.

— B calcule $m_4 = (m_3)^{\widehat{b}}$.

Montrer que le nombre m_4 obtenu par B correspond bien au message m envoyé par A et expliquer pourquoi un observateur extérieur, même s'il arrive à intercepter les messages, aura du mal à retrouver m.

Exercice 88**
Soient p et q des entiers premiers entre eux. Montrer que l'entier

$$\sum_{k=0}^{pq-1} (-1)^{\lfloor k/p \rfloor + \lfloor k/q \rfloor}$$

est égal à 0 si pq est pair, et à 1 si pq est impair.

Exercice 89***** (résolu par Timothé Ringeard)
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_1. Le cercle $\mathcal{C}_2$ est tangent à l'axe des abscisse 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 abscisses. 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 $\sum\limits_{n=1}^{N} S_n$?

Exercice 90**
Déterminer toutes les applications $f : \mathbb{N} \to \mathbb{N}$ telles que $f(1) > 0$ et pour tout $(m,n) \in \mathbb{N}^2$, on ait

$$f(m^2 + n^2) = f(m)^2 + f(n)^2$$

Exercice 91**
Pour un entier n, soit $f(n)$ le nombre obtenu en inversant les 0 et les 1 de l'écriture binaire de n. Par exemple, l'écriture binaire de 23 est 10111. En inversant les 0 et les 1, on obtient 01000, ce qui correspond au nombre 8. Ainsi $f(23) = 8$. Montrer que

$$\sum_{k=1}^{n} f(k) \leqslant \frac{n^2}{4}.$$

Pour quelles valeurs de n y a-t-il égalité ?

Exercice 92**
On se donne un certain nombre de polynômes unitaires de degré 2 de même discriminant. On suppose que la somme de deux quelconques de ces polynômes a toujours deux racines réelles distinctes. Montrer qu'il en est de même de la somme de tous les polynômes considérés.

Exercice 93****
Soit $n \geqslant 4$ un entier. On considère des entiers strictement positifs $a_1, \ldots, a_n$ placés sur un cercle. On suppose que chaque terme a_i ($1 \leqslant i \leqslant n$) divise la somme de ses deux voisins, c'est-à-dire qu'il existe un entier k_i tel que

$$\frac{a_{i-1} + a_{i+1}}{a_i} = k_i,$$

avec la convention $a_0 = a_n$ et $a_{n+1} = a_1$. Montrer que

$$2n \leqslant k_1 + k_2 + \cdots k_n < 3n.$$

Exercice 94***
Soit $n \in \mathbb{N}$. Montrer que si $2 + 2\sqrt{28n^2 + 1}$ est un entier, alors c'est un carré parfait.

Exercice 95***
On écrit un nombre premier $p = a_k a_{k-1} ... a_0$ en base 10 et on pose

$$Q_p(x) = a_k x^k + a_{k-1} x^{k-1} + ... + a_1 x + a_0$$

Montrer que Q_p n'a pas de racines entières sauf pour 4 valeurs de p que l'on déterminera.

Exercice 96**
Soient a et b des entiers positifs. Montrer que

$$\sum_{i=0}^{a} \frac{1}{2^{b+i}} \binom{b+i}{i} + \sum_{i=0}^{b} \frac{1}{2^{a+i}} \binom{a+i}{i} = 2.$$

– Exercices de niveau 3 –

Exercice 97** (résolu par Marie Peeters)
Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ satisfaisant pour tout $x, y \in \mathbb{R}$:

$$x^2 + 2f(xy) + y^2 = f(x^2) + 2xy + f(y^2).$$

Exercice 98*** (résolu par Jean Zablocki)
Soit ABC un triangle d'orthocentre H. On prend un point P sur $[BC]$ et on appelle D le projeté orthogonal de H sur $[AP]$. On trace la parallèle à (BC) passant par D : elle recoupe (AB) en E, (AC) en F, le cercle circonscrit à ADB en X et le cercle circonscrit à ADC en Y. Enfin, soit Z l'intersection de (XB) et (YC). Montrer que $ZE = ZF$ si et seulement si P est le milieu de $[BC]$.

Exercice 99** (résolu par Clément Chapot, Michaël Chen et Lucien Hua)
Soit $a_1, a_2, \dots$ une suite d'entiers strictement croissante tel que pour chaque sous suite $a_{2k-1}, a_{2k}, a_{2k+1}$ soit géométrique et que chaque sous suite $a_{2k}, a_{2k+1}, a_{2k+2}$ soit arithmétique. Avec $a_{13} = 2016$, que vaut a_1 ?

Exercice 100** (résolu par Théodore Fougereux)
Soient $a_1, a_2, \dots, a_n$ et $b_1, b_2, \dots, b_n$ des réels tels que $a_i + b_i > 0$ pour $i = 1, 2, \dots, n$. Montrer que

$$\sum_{i=1}^{n} \frac{a_i b_i - b_i^2}{a_i + b_i} \leq \frac{\displaystyle\sum_{i=1}^{n} a_i \cdot \sum_{i=1}^{n} b_i - \left(\sum_{i=1}^{n} b_i\right)^2}{\displaystyle\sum_{i=1}^{n}(a_i + b_i)}$$

Exercice 101**** (résolu par Théodore Fougereux)
Soit u_n le nombre de résidus différents, modulo n, des entiers de la forme $k(k+1)/2$ avec $k \geqslant 0$. Calculer u_n.

Exercice 102*
On fixe un entier $n \geqslant 2$. On dit que deux polynômes $P, Q \in \mathbb{R}[X]$ sont *semblables par blocs* lorsque pour tout entier $i \in \{1, \dots, n\}$, la suite $P(2017i), P(2017i-1), \dots, P(2017i-2016)$ est une permutation de la suite $Q(2017i), Q(2017i-1), \dots, Q(2017i-2016)$.

1. Prouver qu'il existe des polynômes semblables par blocs distincts de degré $n+1$.
2. Prouver qu'il n'existe pas de polynômes semblables par blocs distincts de degré n.

Exercice 103***** (résolu par Timothée Rocquet)
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 $\widehat{BC}$ 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 104** (résolu par Théodore Fougereux)
Soit $f : \mathbb{N} \mapsto \mathbb{N}$ ayant les propriétés suivantes :

(i) $f(0) = 0$

(ii) $f(3n) = f(n) \quad \forall n \in \mathbb{N}$

(iii) $f(3n+1) = -3/2 f(n)^2 + 5/2 f(n) + 1 \quad \forall n \in \mathbb{N}$

(iiii) $f(3n+2) = 3/2 f(n)^2 - 7/2 f(n) + 2 \quad \forall n \in \mathbb{N}$

Posons $u_0 = 1$, $u_1 = 3$ et $u_n = 3^{u_{n-1}}$. Calculer $f(\sum_{k=0}^{n} u_k)$

Exercice 105** (résolu par Julien Cahuzac, Roméo Nazaret et Jean Zablocki)
Dans une ville de n habitants, on suppose que chaque habitant a exactement 1000 amis (l'amitié est une relation réciproque). Montrer qu'on peut trouver une sous-ville S telle qu'au moins $\lfloor \frac{n}{2017} \rfloor$ habitants de S ont exactement deux amis dans S.

Exercice 106*** (résolu par Julien Cahuzac, Roméo Nazaret et Jean Zablocki)
Soit ABC un triangle et N son point de Nagel. Soit Δ une droite qui passe par N. La droite Δ recoupe (BC), (CA) et (AB) en D, E et F respectivement. Soit X le symétrique de D par rapport au milieu de $[BC]$. On définit de même Y et Z.

(i) Montrer que X, Y et Z sont alignés.

(ii) Montrer que la droite passant par XYZ est tangente au cercle inscrit de ABC.

Exercice 107** (résolu par Daniel Cortild, Théodore Fougereux et Timothée Rocquet)
Dans un pays, des mathématiciens ont choisi $\alpha > 2$ et ont produit des pièces de 1 rouble et des pièces de α^k roubles pour tout k naturel non nul. De plus, α a été choisi de telle sorte que la valeur de chaque pièce, sauf celle de 1 rouble, soit irrationnelle. Est-il possible que l'on puisse régler chaque montant naturel de roubles avec au plus 6 pièces de chaque dénomination ?

Exercice 108*** (résolu par Daniel Cortild et Théodore Fougereux)
On place quatre points dans le plan, et on suppose que les six distances qui les relient entre eux sont toutes entières. Montrer qu'alors au moins une d'entre elles est divisible par 3.

Exercice 109***** (résolu par Timothée Rocquet)
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 $\widehat{SP}$ (ne contenant pas B) et $\widehat{TP}$ (ne contenant pas C). Prouver que les droites (MN) et (O_1O_2) sont parallèles.

Exercice 110** (résolu par Yaël Dilliès, Aurélien Fourré, Léonie Kittel et Suzanne Mairesse)
Raphaël la grenouille est la recherche d'une rivière. Celle ci se trouve sur la ligne horizontale $y = 24$. Une clôture est localisé sur la ligne horizontale $y = 0$. Raphaël saute de coordonnées entières à coordonnées entières en choisissant de manière complètement aléatoire l'une des quatre directions et fait un saut de longueur 1. Mais si il est au bord la barrière, il ne peut la traverser et choisit alors aléatoirement son nouveau saut dans l'une des 3 directions restantes. Il part du point $(0, 21)$ et s'arrête une fois arrivé à la rivière. En moyenne combien de sauts faudra-t-il à Raphaël pour atteindre la rivière ?

Exercice 111****** (résolu par Justien Cahuzac, Roméo Nazaret et Jean Zablocki)
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 112** (résolu par Théodore Fougereux)
Soit $f : \mathbb{R} \to \mathbb{R}$ telle que

$$f(x) = \begin{cases} \lim\limits_{n \to +\infty} \tan(n!\pi x) & \text{si cette limite existe} \\ 0 & \text{sinon} \end{cases}$$

Montrer que f est surjective sur tout intervalle de $\mathbb{R}$ non réduit à un point.

Exercice 113* (résolu par Daniel Cortild, Théodore Fougereux et Marie Peeters)
Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y, on ait

$$(f(x) + xy)f(x - 3y) + (f(y) + yx)f(3x - y) = f(x + y)^2.$$

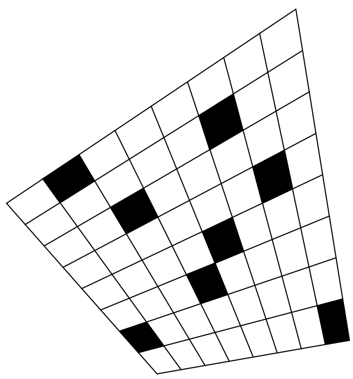
Exercice 114**** (résolu par Daniel Cortild, Théodore Fougereux et Timothée Rocquet)
Soit m et n deux entiers naturels non nuls. On note $\phi(m, n)$ le cardinal de l'ensemble $\{k : 1 \leqslant k \leqslant n, \mathrm{PGCD}(k, m) = 1\}$. Trouver tous les entiers $m \geqslant 1$ tels que $n\phi(m, m) \leqslant m\phi(m, n)$ pour tout $n \in \mathbb{N}^*$.

Exercice 115***** (résolu par Daniel Cortild, Théodore Fougereux et Timothée Rocquet)
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 116** (résolu par Daniel Cortild, Théodore Fougereux et Timothée Rocquet)
Dans une feuille de format A5 (14,8 cm x 21 cm), Mathilde a découpé deux rectangles dont les côtés mesurent tous des nombres entiers de centimètres. Ces deux rectangles ont le même périmètre, mais l'aire du second est double de celle du premier. Combien mesure le périmètre de ces rectangles ?

Exercice 117****** (résolu par Daniel Cortild)
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 118****** (résolu par Théodore Fougereux)
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 119* (résolu par Théodore Fougereux)
Soit P un polynôme à coefficients réels de degré 2016, et $a_0, a_1, \dots, a_{2016}$ des réels tels que pour tout $x \in \mathbb{R}$,

$$P(x) = a_{2016}x^{2016} + a_{2015}x^{2015} + \ldots + a_1 x + a_0.$$

Montrer que si

$$|a_1 + a_3 + \ldots + a_{2015}| > |a_2 + a_4 + \ldots + a_{2016}|,$$

alors le nombre de racines de P dans $[-1, 1]$ (comptées avec multiplicité) est impair.

Exercice 120**
Soit ABC un triangle, G le centre de gravite, H le pied de la hauteur issue de A, A' le point d'intersection du cercle ABC avec la droite HG sur l'arc BC contenant A. Montrer que AA'est parallele a BC

Exercice 121****
Soit $k \geqslant 6$ un entier et P un polynôme à coefficients entiers tel qu'il existe k entiers distincts $x_1, \dots, x_k$ tels que pour tout $i \in \{1, \dots, k\}$, $P(x_i) \in \{1, \dots, k-1\}$. Montrer que $P(x_1) = \ldots = P(x_k)$.

Exercice 122**** (résolu par Théodore Fougereux)
Soient $k \geqslant 2$ un entier et $a \geqslant k-1$ un nombre réel. Montrer que pour tout n-uplet de nombres réels strictement positifs $(x_1, \dots, x_n)$ on a

$$\frac{x_1 + \cdots + x_n}{1+a} \leqslant \frac{x_1^{k+1}}{x_1^k + a x_2^k} + \cdots + \frac{x_n^{k+1}}{x_n^k + a x_1^k}.$$

Exercice 123****
On considère une ligne de n carrés. On note $S(n)$ le nombre minimal de carrés à colorier en bleu tels que chacun des $n-1$ traits séparant deux cases voisines soit à égale distance de deux cases bleues. Montrer que

$$\lceil 2\sqrt{n-1} \rceil \leqslant S(n) \leqslant \lceil 2\sqrt{n} \rceil + 1.$$

Exercice 124*** (résolu par Daniel Cortild, Théodore Fougereux et Timothée Rocquet)
Soit $n \geqslant 3$ un nombre entier et $x_1, \dots, x_n$ des nombres réels strictement positifs. Montrer que

$$\frac{x_1}{x_2 + x_3} + \frac{x_2}{x_3 + x_4} + \ldots + \frac{x_n}{x_1 + x_2} \geqslant \frac{5n}{12}.$$

Exercice 125****
Soit $k \geqslant 1$ un entier. Trouver tous les polynômes P à coefficients entiers tels que $P(n)$ divise $(n!)^k$ pour tout entier $n \geqslant 1$.

Exercice 126** (résolu par Timothé Ringeard)
Cédric et Damien jouent à un jeu. Il y a $n \geqslant 3$ points sur le plan. Cédric commence, et tour à tour ils doivent relier deux points distincts (par une ligne droite ou non), sans faire passer la ligne par un autre point et sans intersecter une ligne déjà tracée. Deux points ne peuvent être reliés par plus d'une ligne. Celui qui ne sait plus jouer a perdu. Qui a une stratégie gagnante ?

Exercice 127******
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 peuvent ainsi être formés.

Exercice 128*****
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 129*** (résolu par Timothée Rocquet)
Soit X un point à l'intérieur du triangle ABC tel que

$$XA \cdot BC = XB \cdot CA = XC \cdot AB.$$

Soient I_1, I_2, I_3 les centre des cercles inscrits respectifs de BXC, AXC et AXB. Montrer que les droites AI_1, BI_2 et CI_3 sont concourantes.

Exercice 130** (résolu par Théodore Fougereux)
Soit p un nombre premier et $a_1, a_2, \ldots, a_p$ des entiers. Montrer qu'il existe un entier k tel que les nombres

$$a_1 + k, a_2 + 2k, \ldots, a_p + pk$$

donnent au moins $\dfrac{p}{2}$ restes distincts modulo p.

Exercice 131**** (résolu par Théodore Fougereux)
Soient a, b, c des nombres réels strictement positifs tels que $a+b+c=3$. Prouver que

$$\frac{a}{1+(b+c)^2} + \frac{b}{1+(a+c)^2} + \frac{c}{1+(a+b)^2} \leq \frac{3(a^2+b^2+c^2)}{a^2+b^2+c^2+12abc}.$$

Exercice 132**** (résolu par Daniel Cortild, Théodore Fougereux et Timothée Rocquet)
Soit ABC un triangle non isocèle. Son cercle inscrit, de centre I, touche le côté $[BC]$ en D. Soit X un point de l'arc $\widehat{BC}$ du cercle circonscrit de ABC tel que si E, F sont respectivement les projetés orthogonaux de X sur (BI) et (CI) et M le milieu de $[EF]$, alors $MB = MC$. Prouver que $\widehat{BAD} = \widehat{CAX}$.

Exercice 133*
Existe-t-il des entiers positifs a, b, c tels que

$$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4\ ?$$

Exercice 134**
Soit F_n la suite de Fibonacci : $F_0 = 0$, $F_1 = 1$ et pour tout entier positif n $F_{n+2} = F_{n+1} + F_n$. On définit le polynôme P_n de degré n dont les coefficients sont les termes de la suite de Fibonacci :

$$P_n(X) = F_1X^n + F_2X^{n-1} + \ldots + F_nX + F_{n+1} = \sum_{k=0}^{n} F_{k+1}X^{n-k}$$

Déterminer en fonction de n le nombre de racines réelles de P_n.

Exercice 135******
Soient $a, b, c > 0$ des nombres réels tels que $a + b + c = 3$. Prouver que :

$$\frac{ab}{b^3+1}+\frac{bc}{c^3+1}+\frac{ca}{a^3+1}\leq\frac{3}{2}.$$

Exercice 136******
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 137***
Soit ABC un triangle, I son centre du cercle inscrit. Soient D, E et F ses projetés sur les côtés de ABC. Soient P et Q les intersections de la droite (EF) avec le cercle circonscrit de ABC. Soient O_1 et O_2 les centres des cercles circonscrits de AIB et de AIC. Montrer que le centre du cercle circonscrit de DPQ est sur la droite (O_1O_2).

Exercice 138*****
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 rationnelle.

Exercice 139** (résolu par Timothée Rocquet)
Raphaël vient de faire naufrage. Il est assis sur un tonneau et attend d'être secouru. Il voit apparaître à l'horizon l'avion Paris-Miami et 15 minutes plus tard, il le voit disparaître sans avoir pu se faire repérer. Le segment joignant le point d'aparition et celui de disparition est vu par Raphaël sous un angle de 120 degrés. L'avion vole en ligne directe à une altitude constante de 5000 m. Quelle est la vitesse de l'avion en km/h, arrondie à la dizaine la plus proche ?

Exercice 140** (résolu par Daniel Cortild et Timothée Rocquet)
Soit ABCD un quadrilatere convexe cyclique X, l'intersection des diaguonales K, L et M sont les milieux de XD, XC et DC. Les droites AK et BL se coupent en Y. La droite YM recoupe les droites AC et BD en E et F. Montrer que la droite XY est tangente au cercle XEF

Exercice 141**** (résolu par Théodore Fougereux)
Soit Γ le cercle circonscrit d'un triangle acutangle ABC. Le point D est le centre de l'arc $\widehat{BC}$ contenant A, et I est le centre du cercle inscrit de ABC. La droite (DI) coupe (BC) en E et recoupe Γ en F. Soit P un point de la droite (AF) tel que (PE) et (AI) soient parallèles. Prouver que (PE) est la bissectrice de l'angle $\widehat{BPC}$.

Exercice 142*** (résolu par Daniel Cortild et Timothée Rocquet)
Soit ABC un triangle. On note D, E, F les points de tangence du cercle inscrit de centre I de ABC avec les côtés de ABC. Soit X le point de $[AB]$ tel que (XD) et (EF) soient perpendiculaires. Soit Y le second point d'intersection des cercles AEF et ABC. Montrer que le triangle XYF est rectangle.

Exercice 143** (résolu par Daniel Cortild et Théodore Fougereux)
Soit $a \in]2, +\infty[$.

$$a_0 = 1, a_1 = a \text{ et } \forall n \in \mathbb{N}^*, a_{n+1} = \left(\frac{a_n^2}{a_{n-1}^2} - 2\right) a_n$$

Montrer que, $\forall n \in \mathbb{N}^*, \sum_{k=0}^{n} \frac{1}{a_k} < \frac{2 + a - \sqrt{a^2 - 4}}{2}$.

IX. Citations mémorables

Mathieu B. : « Je pensais être l'homme de la soirée ; c'est raté. »

Théodore : « C'est de la géométrie, sans étoile. Comment tu veux que ça m'intéresse ? »

Anonyme Gachet : « Le truc c'est que même quand il lève la main, on le voit pas. »

Daniel : « Dans la vie, il y a les nombres hydratés et les nombres lyophillisés ! »

Employé du CIV : « Quand tu connais la logique du bâtiment, tu arrives à t'y retrouver. Seulement, dans le bâtiment il n'y a aucune logique. »

Pierre-Marie : « -1, c'est 1, mais pas exactement. »

Pierre-Marie : « $\frac{1}{-1} = -1$, un élève de CP comprend. »
La classe : « Non. »
Pierre-Marie : « Bon. . . Un CP de Louis-le-Grand. »

Martin R., à deux élèves coincés dehors : « Ah mais c'est pas parce qu'on vous a sauvé la vie que vous pouvez vous asseoir à notre table ! »
Baptiste S. : « Les mecs tu leur donnes ça ils te prennent ça. »

Lucie : « Y a un Jeanbert dans le groupe B ? »
Martin R. : « Non ! »
Lucie : « Ah ouf ! »

Thomas : « Elles ouvrent tout, les clés qui ouvrent tout ? »

Pierre-Marie, en parlant des quadrilatères complets : « Faites attention à cette figure. Elle est partout. Elle vous regarde. Elle sait tout. Elle sait ce que vous avez mangé à midi. Elle sait ce que vous mangerez ce soir. »

Pierre-Marie : « Je dois préparer le vidéo-projecteur. »
« Oooh ! » enthousisaste de la classe.
« Mais on ne va pas voir un film, je vous préviens direct. »
« Oooh ! » décu.

Baptiste C. : « Ce livre, il est à Lucie ? »
Héloïse : « Nan »

Martin R. : « On laisse Lucie faire »

Pierre-Marie : « J'ai l'impression de vous arnaquer. Mais je le fait avec mon cœur. »

Martin R. à Lucie : « Nan mais tu sais que 90, c'est égal à 90, mais aussi à 180-90 ? »

Thomas : « Après avoir testé les petites valeurs de 2018, vous raisonnez par récurrence sur 2018. »

Madison : « Moi je voulais faire par récurration. »

Martin R. (à propos de son prof de prépa) : « Moi je le respecte, Pierre ! »

Andrei : « Dans le plan projectif complexe, il y a un point à l'infini, c'est 42. »

Andrei : « $\frac{42}{\infty} = 0$. Du coup, $\frac{42}{-\infty}$, ça fait -0. »

Yakob : « J'aime pas la plage, sauf les plages de galets, mais ça fait mal... donc j'aime pas. »

Yakob : « Je crois que c'est une parodie d'IKEA... mais je sais pas à quoi ça ressemble un catalogue IKEA. »

Théodore, regardant les racines complexes d'un polynôme sur Wolfram : « Ooooh, c'est un joli soleil ! »
Timothée : « Mais elles sont toutes sur le cercle unité, c'est vachement important ! »

Pierre-Marie : « Je peux utiliser le rétroprojecteur ? »
Matthieu L. : « C'est pour projeter le DVD Dimensions ? »

Xavier : « Tu fais quel exo ? »
Yaël : « J'ai fait le 7. »
Xavier : « Mais il ne fallait pas le chercher ! »
Yaël : « Je ne l'ai pas cherché, je l'ai trouvé ! »

Running gag sur les Barbu : « Y a un jeu qui s'appelle le Roi des barbus... Il faut qu'on les fasse jouer ! »

Léonie, à propos du Set : « La meilleure stratégie, c'est le talent. »

Lucie : « Moi, je m'intersecte avec moi-même. »

Pierre-Marie, en trébuchant sur l'unité centrale d'un ordi : « Si je me prends la tour, je vais pêter un câble ! »

Pierre : « Baptiste, tu vas te choquer toi-même ! »

Vincent : « Je confonds ma droite et ma gauche ; du coup, je vote Macron. »

Lucie, à propos des synesthètes : « Moi mon 5 il est bleu. »
Pierre : « Moi mon 5 c'est une chèvre. »

Vincent : « En géométrie, la mort survient en général au bout de 10 minutes. »

Yakob : « À quoi elle sert la pissotière de Marcel Duchamp ? »
Pierre : « On trouve jamais les toilettes dans les musées… »

Vincent : « Quand vous voyez plein de a_k, au début, c'est comme les All Blacks, ça vous fait peur. »

Quelqu'un : « Savinien il a peu dormi la nuit dernière… »
Martin : « Et alors, c'est pas une excuse, nous on s'est dormi tard. »

Pierre-Marie : « Rechercher 3 points fixes, ça peut être un but dans votre vie. »

Pierre-Marie : « Vous connaissez le point de Miquel ? C'est mon point préféré ! Certains ont des passions, moi j'ai un point préféré. »

Lucie : « On peut applaudir Théo. »
"Théo" : « En fait je m'appelle Rémi… »
Lucie : « On peut applaudir Rémi. »

Baptiste S., au tableau : « Baptiste Vuibert est en fait Théo Goix. »

Jean, après que Pierre-Marie a volé des craies au groupe D en adoptant une démarche moonwalk-grenouille : « Un exemple des ravages de la géométrie projective sur l'âme d'un homme ! »

Collectif : « Invectif, c'est quand c'est bivectif mais pas survectif. »

Vincent : « Là il nous manque $2n$ mais il n'y a qu'à regarder les infos pour voir qu'il y en a plein partout ! »

Martin R. : « La partie est un peu lente… »
Savinien : « Si tu la trouves lente t'as qu'à jouer. »

Pierre-Marie : « À condition d'être intelligent, une involution projective complexe est toujours de la forme $x \mapsto \dfrac{1}{x}$! »

Vincent : « Dans la vie, il n'y a pas que les maths… il y a aussi l'informatique ! »

Anonyme : « C'est beaucoup plus drôle de faire du bowling avec des bouteilles et des pommes ! »

Vincent : « Ça pue le produit chimique mais je vais en prendre quand même. »

Xavier : « Ma figure est fausse. Pourtant, il n'y a pas de raison. »
Yaël : « Ben c'est toi qui l'as tracée. C'est une condition suffisante, non ? »

Baptiste C. : « Ce matin j'ai failli pas me réveiller pour mon cours de l'après-midi. »

Yakob, au moins dix fois par jour : « J'ai faim ! »

Félix : « Avec cette égalité d'angles, tout bon géomètre trouve que la droite est tangente au cercle. Sur ma figure, elle est même tangente en deux points ! »

Mathieu B. : « Vous faites des shortlists ? »
Martin R. : « Même pas. »

Vladimir, pendant le jeu du passager clandestin : « La production appartient à la classe des travailleurs. Collaborez, vous n'avez rien à perdre à part cos champs ! »

Guillaume : « Ton score est congru à zéro modulo pi. »

Vladimir : « Mais la géométrie, c'est pas comme l'algèbre ou la théorie des nombres, il n'y a pas besoin de réfléchir. »

Mathieu B. à Guillaume : « Tu connais pas l'autre Phillipe, toi ? Ah nan, l'autre Philippe c'est Jean-Marc… »

Poète anonyme : « La vie c'est comme les maths, ça commence par un Bézout dans Lagrange et ça se finit par un Gauss. »

Vincent : « Je suis content de m'être fait piquer par un moustique, mon biceps à doublé de taille. »
Yakob : « 2 fois 0 ça fait 0… »

Alexandre, après le cours sur la récurrence : « Si le premier domino ne tombe pas, alors le $(k+1)^{\text{ème}}$ domino ne tombera pas non plus. »

Félix : « D'année en année je trouve les élèves de plus en plus jeunes. »

Vincent : « La récurrence forte, c'est comme la récurrence normale, mais en plus fort. »

Martin A. : « Dans cinq minutes, on va faire quelque chose d'horrible et qui va nous prendre trop de temps. »
Yaël : « Une pause ? »