STAGE OLYMPIQUE DE MONTPELLIER 2012

Du 20 au 30 août 2012

Avant-propos

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

Son objet a été de rassembler les lauréats des diverses compétitions et de les faire travailler sur des exercices en vue de la formation de l'équipe qui représentera la France à l'Olympiade Internationale de Mathématiques à Santa Marta en Colombie en juillet 2013. Cette année une attention particulière a été apportée au recrutement de collégiens brillants en vue de les préparer aux Olympiades Internationales pendant plusieurs années.

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

Les Animatheux

Razvan Barbulescu	Pierre Bertin	Margaret Bilu
Damien Clementz	Noé de Rancourt	Theresia Eisenkoelbl
Vincent Jugé	Igor Kortchemski	Bodo Lass

Emmanuel Lecouturier François Lo Jacomo Irène Marcovici

Louis Nebout Simon Pépin-Lehalleur Antoine Taveneaux

Sadr Yassai Maxime Zavidovique

Les élèves

Yassir Akram	Julien Alamelle	Etienne Apers	Michael Ayoun-Compagnon	Augustin Bariant
Sébastien Baumert	Laurent Beaughon	Khalil Besrour	Moïse Blanchard	Arthur Blanc-Renaudie
Marine Bonora	Vincent Bouis	Félix Breton	Romain Caplier	Noémie Cartier
Raphaël Clisson	Alice Contat	Guillaume Couairon	Nathanaël Courant	Edwige Cyffers
Colin Davalo	Timothée Defourne	Matthieu Dolbeault	Etienne Duclos	Antoine Dupuis

Lucas Flammant	Léonard Fleutot	Marc Ganet	Charles Gassot	Quentin Gendre
Ewen Goisot	Solène Gomez	Cécile Gontier	Théo Guillaumot	Yassine Hamdi
Nicolas Heutte	Aymeric Jacquin	Paul Laubie	Adrien Lemercier	Jérémy Lengelé
Cyril Letrouit	Clément Lezane	Clémentine Linyer	Marc Michoux	Séginus Mowlavi
Arthur Nebout	Florent Noisette	Hizir Nuhoglu	Anatole Oraison	Tobias Parker

Pierre Pelletetier	Lucas Perotin	Auriane Perrin	Loïc Petitjeans	Titouan Poquillon
Loïc Pujet	Maxime Rémon	Timothée Schoen	Alexander Semenov	Antoine Séré
Maxence Seymat	Alexandre Thiault	Mehdi Trense	Malik Tuwebti	Lucie Wang

Yiren Wang Quentin Woinet

Table des matières

I. Déroulement du stage

Nous avons bénéficié cette année d'une subvention Cap' Maths qui nous a permis d'élargir le stage, tant dans sa durée (dix jours au lieu de sept, du lundi 20 août vers midi au jeudi 30 août en fin de matinée) que dans son recrutement (67 élèves au lieu de 43 en 2011). L'épreuve de sélection a été organisée dans 177 établissements pour 345 candidats (nous avions contacté quelque 700 élèves, et certains se sont portés candidats sans avoir été contactés), et nous avons admis davantage de collégiens, pour poursuivre notre effort de préparation sur plusieurs années. Merci à l'Internat d'Excellence de Montpellier de nous avoir accueillis dans ses locaux tout neufs, équipés de tableaux blancs interactifs dans chaque classe...

Le stage lui-même se divisait en trois périodes de trois jours. Dans chacune des périodes, les deux premiers jours (21 et 22, 24 et 25, 27 et 28) étaient des journées de cours et exercices (de 9 h à 12 h et de 14 h à théoriquement 17 h) ; le troisième jour, il y avait un test le matin, de 9 h à 12 h ou 12 h 30, et une après-midi "récréative" : visite guidée de Montpellier le jeudi 23 (15 h - 17 h), après-midi libre le dimanche 26, planétarium "Le temps des galaxies" le mercredi 29 (16 h - 17 h). Les corrections des tests étaient présentées généralement le soir même.

Trois soirées étaient libres, les autres consacrées à une conférence sur Turing le mardi 28, un film "Dimensions" le mercredi 22, des présentations : Animath et la préparation olympique le lundi 20, et les Olympiades en Roumanie, Autriche, Allemagne le vendredi 24. Les soirées commençaient à 20 h 30 (les horaires des repas étaient : petit-déjeuner 8 h, déjeuner 12 h 30, dîner 19 h), et les élèves devaient être couchés à 23 h 30.

Pour les cours et exercices (travaux dirigés), les élèves étaient répartis en quatre groupes, pas nécessairement les mêmes d'une période à l'autre. Ceux qui n'étaient pas encore familiarisés avec les techniques olympiques travaillaient les chapitres "incontournables" : géométrie les 21 et 22 (test le 23), stratégies de base les 24 et 25 (test le 26), arithmétique les 27 et 28 (test le 29). Pour ces trois chapitres incontournables, ils étaient répartis en deux groupes, a priori les collégiens (en salle B) et les lycéens (en salle A, la plus grande : ce groupe représentait la moitié de l'effectif global). Pour ceux qui avaient déjà une certaine expérience olympique, un choix s'offrait entre : salle C, géométrie projective (en première période), combinatoire (en seconde période) et arithmétique avancée (en troisième période), ou, salle D, des chapitres franchement différents : inégalités en première période, équations fonctionnelles en seconde période, algèbre en troisième période. C'est l'après-midi du premier jour, lundi 20, après la présentation du stage à 14 h 30, que des entretiens individuels ont eu lieu pour orienter les élèves dans les différents groupes. La constitution des groupes pour chaque période n'a été annoncée qu'après délibération.

Quelques liens utiles pour poursuivre le travail réalisé pendant ce stage :

- Le site d'Animath : http ://www.animath.fr
- Le site MathLinks : http ://www.mathlinks.ro
- Les polycopiés de stages olympiques précédents :
  http ://www.animath.fr/spip.php ?article260
- Les cours de l'Olympiade Française de Mathématiques :
  http ://www.animath.fr/spip.php ?article255

		Débutants collège	Débutants lycée	Intermédiaires	Avancés
Lundi 20/08		Arrivé, accueil des élèves et première évaluation			
Mardi	9h - 12h	Cours de Géométrie (François)	Cours de Géométrie (Pierre)	Géométrie (Bodo)	Cours d'inégalités (Theresia)
	14h - 17h+ϵ	TD de Géométrie (Simon)	TD de Géométrie (Igor)	Géométrie (Bodo)	TD d'inégalités (Razvan)
	20h30 -22h	Présentation des OIM			
Mercredi	9h - 12h	Cours de Géométrie (Theresia)	Cours de Géométrie (François)	Géométrie (Bodo)	Cours d'inégalités (Emmanuel)
	14h - 17h+ϵ	TD de Géométrie (Pierre)	TD de Géométrie (Razvan)	Géométrie (Bodo)	TD d'inégalités (Simon)
	20h30 -22h30	Projection du film *Dimensions*			
Jeudi	9h - 12h	Test			
	Après-midi	Visite de Montpellier			
	20h30 - 21h 30	Correction du Test			
Vendredi	9h - 12h	Stratégies de base (Theresia)	Stratégies de base (Emmanuel)	Équations fonctionnelles (Razvan)	Combinatoire avancée (Simon)
	14h - 17h+ϵ	Stratégies de base (Irène)	Stratégies de base (Pierre)	Équations fonctionnelles (Emmanuel)	Combinatoire avancée (Louis)
	20h30 - 21h 30	Présentation d'olympiades nationales de mathématiques de différents pays			
Samedi	9h - 12h	Stratégies de base (François)	Stratégies de base (Igor)	Équations fonctionnelles (Theresia)	Combinatoire avancée (Bodo)
	14h - 17h+ϵ	Stratégies de base (Louis)	Stratégies de base (Noé)	Équations fonctionnelles (Irène)	Combinatoire avancée (Razvan)
	20h30 - 21h 30	Soirée libre			Correction du test de géométrie projective
Dimanche	9h - 12h	Test			
	Après-midi	Libre			
	20h30 - 21h 30	Correction du Test			
Lundi 27/08	9h - 12h	Arithmétique (Maxime)	Arithmétique (Margaret)	Algèbre (Pierre)	Arithmétique (Louis)
	14h - 17h+ϵ	Arithmétique (Igor)	Arithmétique (Irène)	Algèbre (François)	Arithmétique (Noé)
	20h30 - 21h 30	Soirée libre			
Mardi	9h - 12h	Arithmétique (Bodo)	Arithmétique (Vincent)	Algèbre (Razvan)	Arithmétique (Margaret)
	14h - 17h+ϵ	Arithmétique (Antoine)	Arithmétique (Maxime)	Algèbre (Noé)	Arithmétique (François)
	20h30 - 21h 30	Soirée Turing			
Mercredi	9h - 12h	Test			
	Après-midi	Sortie au planétarium			
	20h30 - 21h 30	Correction du Test			
Jeudi	Matinée	Brunch puis départ			

II. Première période

Contenu de cette partie

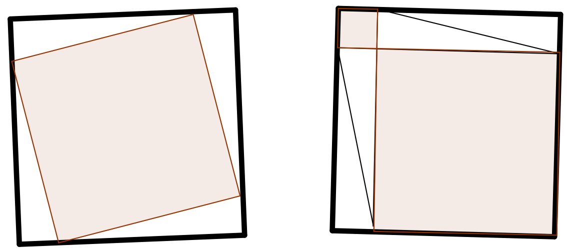
1 Incontournables (4èmes-3èmes) : Géométrie

Nous renvoyons aux différents cours de géométrie disponibles sur le site d'Animath pour des compléments de cours (voir les liens en haut de la page 14).

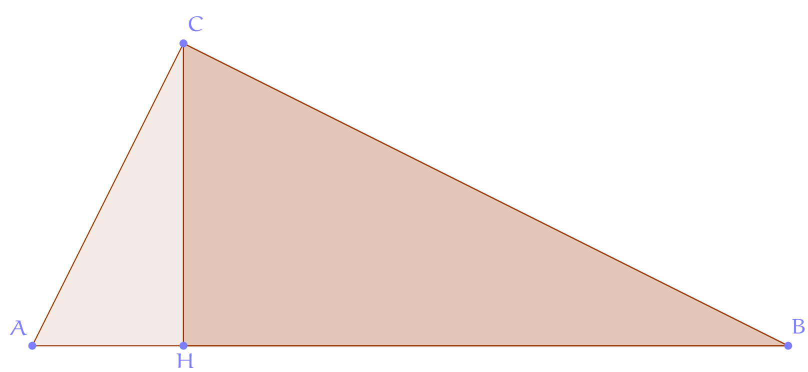
1 Premier cours

- Angle droit -

L'une des premières propriétés de l'angle droit est le théorème de Pythagore : le carré de l'hypoténuse est égal à la somme des carrés des côtés de l'angle droit. On en connaît de nombreuses démonstrations, par exemple la figure ci-dessous : en disposant différemment les quatre triangles rectangles dans le même carré, on libère soit un carré de côté l'hypoténuse, soit deux carrés de côtés les côtés de l'angle droit.



On peut aussi tracer la hauteur CH du triangle ABC rectangle en C. Posons $a = BC, b = CA, c = AB$. Le triangle rectangle ACH a les mêmes angles que le (est semblable au) triangle rectangle ABC, mais son hypoténuse vaut b et non c, chacune des longueurs sera donc la longueur homologue multipliée par $\frac{b}{c}$, par exemple $CH = \frac{ab}{c}$, $AH = \frac{b^2}{c}$. De même pour le triangle BCH, $\frac{a}{c}$ fois plus grand que BAC, donc $HB = \frac{a^2}{c}$. Dès lors, on peut soit écrire $AH + HB = AB$, donc : $\frac{b^2}{c} + \frac{a^2}{c} = c$, soit dire que la somme des aires des triangles ACH et BCH, respectivement $\frac{b^2}{c^2}$ et $\frac{a^2}{c^2}$ fois plus grandes que l'aire de ABC, est égale à l'aire de ABC : d'une manière ou d'une autre, on trouve $a^2 + b^2 = c^2$.



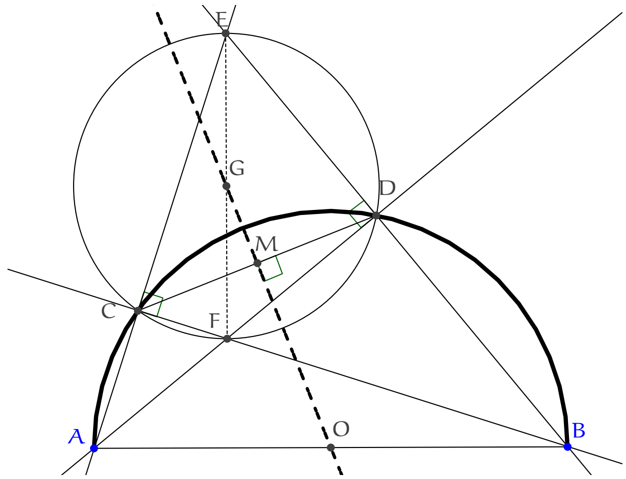
Le triangle rectangle ABC, rectangle en C, permet de définir le sinus et le cosinus : appelons α l'angle en A du triangle. $\sin\alpha = \frac{BC}{AB}$ et $\cos\alpha = \frac{AC}{AB}$. Comme les angles en A et en B sont complémentaires, $\sin(90° - \alpha) = \cos\alpha$. Par ailleurs, d'après le théorème de Pythagore, $\sin^2\alpha + \cos^2\alpha = 1$.

Enfin, l'angle droit est l'angle sous lequel un point d'un cercle voit un diamètre de ce cercle. Ce résultat important s'utilise dans les deux sens : si AB est un diamètre d'un cercle contenant C, l'angle $\widehat{ACB} = 90°$. Si $\widehat{ACB}$ est un angle droit, nécessairement C appartient au demi-cercle de diamètre AB.

Exercice 1

Soient C et D deux points sur un demi-cercle de diamètre AB. Les droites (AC) et (BD) se coupent en E, les droites (AD) et (BC) se coupent en F. Montrer que les milieux de [AB], [CD] et [EF] sont alignés.

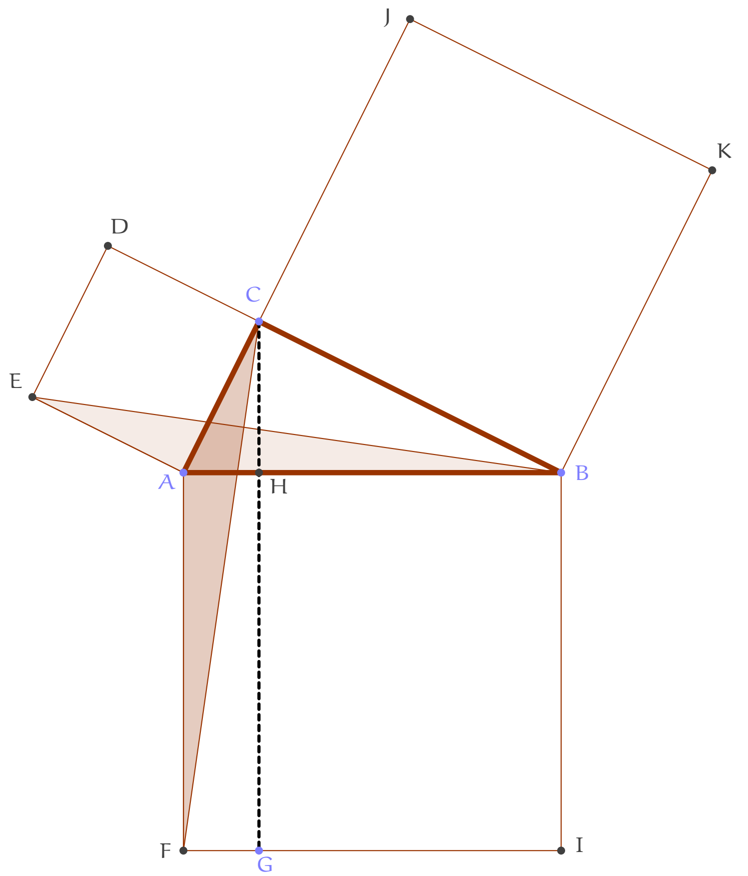
<u>*Solution de l'exercice 1*</u>



Le milieu du diamètre AB est le centre O du cercle contenant C et D, donc OC = OD : O est sur la médiatrice de [CD]. Si l'on appelle M le milieu de [CD], (OM) est donc précisément la médiatrice de [CD], et il reste à prouver que le milieu G de [EF] est lui aussi sur cette médiatrice de [CD], donc que GC = GD. Or C et D étant sur le cercle de diamètre [AB], $\widehat{ACB} = \widehat{ADB} = 90°$. Il en résulte que $\widehat{FCE}$ et $\widehat{FDE}$ sont eux aussi droits, donc que C et D appartiennent aussi au cercle de diamètre [EF] et de centre G, d'où GC = GD, ce qui achève la démonstration.

- Aire du triangle -

L'aire d'un triangle peut se calculer de plusieurs manières. La principale, c'est : aire = $\frac{1}{2}$Base×Hauteur, compte tenu qu'un triangle a trois bases et trois hauteurs. C'est d'ailleurs là-dessus que repose la démonstration du théorème de Pythagore figurant dans les Eléments d'Euclide. Les deux triangles grisés sont isométriques : il suffit de pivoter de 90° autour de A le triangle AEB pour obtenir le triangle ACF. Ils ont donc même aire. Mais pour AEB, on choisit comme base AE, la hauteur correspondante est égale à CA vu que CB est parallèle à la base EA, donc l'aire vaut la moitié de l'aire du carré $ACDE$. Pour ACF, on choisit AF comme base, la hauteur correspondante est égale à HA si CH est perpendiculaire à AB, donc parallèle à la base AF, et l'aire est égale à la moitié du rectangle $AFGH$. De même (mais Euclide refait une deuxième fois la démonstration) la moitié de l'aire du carré $BCJK$ est égale à la moitié de l'aire du rectangle $BIGH$. Donc la somme des aires des deux carrés est égale à la somme des aires des deux rectangles, c'est-à-dire à l'aire du carré de l'hypoténuse.



Si l'on note a, b, c les trois longueurs BC, CA, AB, et $\widehat{A}, \widehat{B}, \widehat{C}$ les trois angles $\widehat{BAC}, \widehat{CBA}, \widehat{ACB}$, l'aire S peut aussi s'écrire : $S = \frac{1}{2}ab\sin\widehat{C} = \frac{1}{2}bc\sin\widehat{A} = \frac{1}{2}ca\sin\widehat{B}$. Il suffit pour le prouver de remarquer, par exemple, que la hauteur opposée à $BC = a$ a pour longueur : $AC.\sin\widehat{C} = b\sin\widehat{C} = AB.\sin\widehat{B} = c\sin\widehat{B}$.

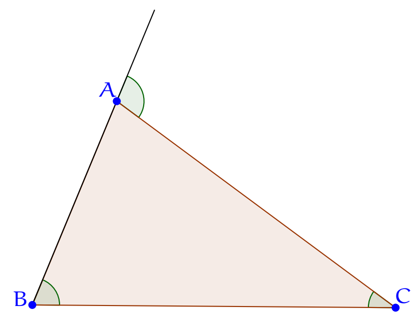
Une autre formule permet de calculer l'aire d'un triangle à partir des seules longueurs a, b, c des côtés BC, CA, AB. C'est la formule de Héron :

$$S = \frac{1}{4}\sqrt{(a+b+c)(a+b-c)(a-b+c)(-a+b+c)}.$$

On remarquera tout d'abord que l'aire du triangle est nulle si et seulement si les trois sommets sont alignés, donc l'un des côtés est somme des deux autres, donc si et seulement si $(a+b-c)(a-b+c)(-a+b+c)$ est nul. Mais la démonstration nécessite de regrouper les termes deux par deux : $(a+b+c)(a+b-c) = (a+b)^2-c^2 = (a^2+b^2-c^2)+2ab$, $(a-b+c)(-a+b+c) = c^2-(a-b)^2 = (c^2-a^2-b^2)+2ab$. Il reste à utiliser la formule d'Al Kashi : $c^2 = a^2+b^2-2ab\cos\widehat{C}$: $(a+b+c)(a+b-c) = 2ab(1+\cos\widehat{C})$ et $(a-b+c)(-a+b+c) = 2ab(1-\cos\widehat{C})$ ont pour produit : $4a^2b^2\left(1-\cos^2\widehat{C}\right) = 4a^2b^2\sin^2\widehat{C}$ dont la racine carrée : $2ab\sin\widehat{C}$ est bien le quadruple de l'aire. Une autre manière de noter cette même formule de Héron est d'appeler p le demi-périmètre : $p = \frac{a+b+c}{2}$. On a alors : $S = \sqrt{p(p-a)(p-b)(p-c)}$.

- **Angles** -

On rappelle que la somme des angles d'un triangle vaut 180°. Une manière souvent utile d'écrire cela : si l'on prolonge un côté, AB par exemple, au delà de A, l'angle extérieur, supplémentaire de $\widehat{A}$, est la somme des deux angles à la base : $\widehat{B} + \widehat{C}$.

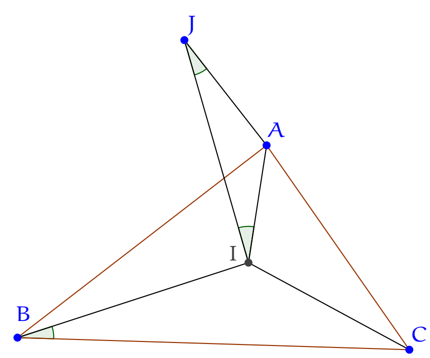


Rappelons également qu'un triangle isocèle est un triangle ayant deux côtés égaux et deux angles égaux : s'il a deux côtés égaux, il a deux angles égaux, et réciproquement. Enfin, la bissectrice coupe un angle en deux angles égaux. Les points de la bissectrice sont à égale distance des côtés de l'angle. On en déduit que les trois bissectrices d'un triangle se coupent en un point I : si l'on appelle I l'intersection des deux bissectrices de $\widehat{B}$ et $\widehat{C}$, I est à la même distance de AB et BC, de BC et AC, donc de AC et AB, ce qui implique qu'il est sur la bissectrice de $\widehat{A}$. Si l'on appelle r la distance de I aux trois côtés, le cercle de centre I et de rayon r est tangent aux trois côtés : on l'appelle cercle inscrit dans le triangle, et I est souvent désigné comme centre du cercle inscrit dans le triangle.

Exercice 2

Soit ABC un triangle, I le centre du cercle inscrit. On suppose que : $CA + AI = BC$. Déterminer le rapport des angles : $\frac{\widehat{BAC}}{\widehat{CBA}}$

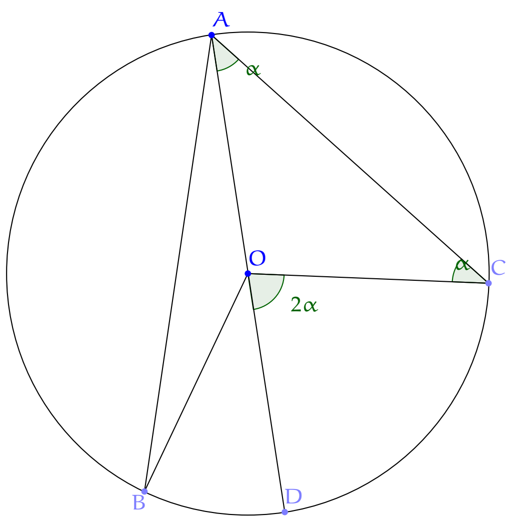
<u>*Solution de l'exercice 2*</u>

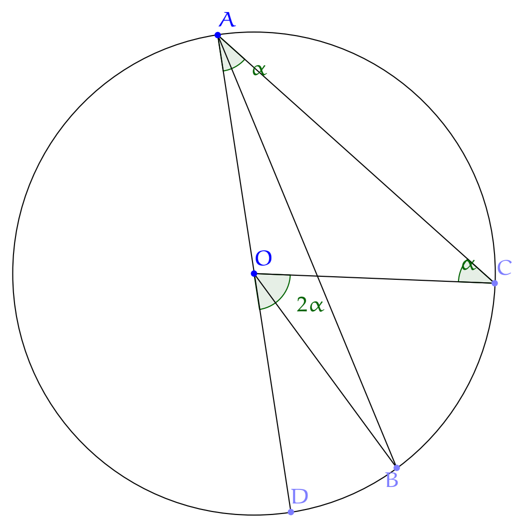


Pour tirer profit de la relation de l'hypothèse avec une somme de longueurs, il faudrait que les trois points soient alignés. On va donc considérer un point J sur (CA) tel que $AI = AJ$, A étant entre C et J, de sorte que $CJ = CB$. Appelons alors α l'angle $\widehat{AJI}$. Comme le triangle AJI est isocèle, $\widehat{AIJ} = \alpha$, donc $\widehat{IAC} = 2\alpha$, ce qui entraîne $\widehat{BAC} = 4\alpha$, puisque (AI) est bissectrice de $\widehat{BAC}$. Par ailleurs, $CJ = CA + AJ = CA + AI = BC$, donc les triangles JCI et BCI sont isométriques : deux côtés égaux et les angles entre ces deux côtés égaux, puisque (CI) est bissectrice de $\widehat{BCA}$. Donc $\widehat{IBC} = \widehat{IJC} = \alpha$, et comme (BI) est bissectrice de $\widehat{CBA}$, $\widehat{CBA} = 2\alpha$, ce qui entraîne : $\frac{\widehat{BAC}}{\widehat{CBA}} = 2$.

- Angle inscrit -

La notion d'angle inscrit est un cas particulièrement important d'utilisation des angles. Soit A, B, C trois points d'un cercle de centre O. L'angle inscrit $\widehat{BAC}$, qui intercepte l'arc BC, vaut la moitié de l'angle au centre associé $\widehat{BOC}$. En effet, prolongeons (AO), qui recoupe le cercle en D. Dans le triangle AOC, l'angle extérieur $\widehat{DOC}$ vaut la somme des angles à la base, $\widehat{OAC}+\widehat{ACO}$, mais ces angles sont égaux car le triangle AOC est isocèle. Donc $\widehat{DOC} = 2\times\widehat{OAC}$, et de même $\widehat{BOD} = 2 \times \widehat{BAD}$. Selon le cas de figure, l'angle au centre $\widehat{BOC}$ est la somme ou la différence des angles au centre $\widehat{DOC}$ et $\widehat{BOD}$, mais dans les deux cas il vaut le double de l'angle inscrit $\widehat{BAC}$.



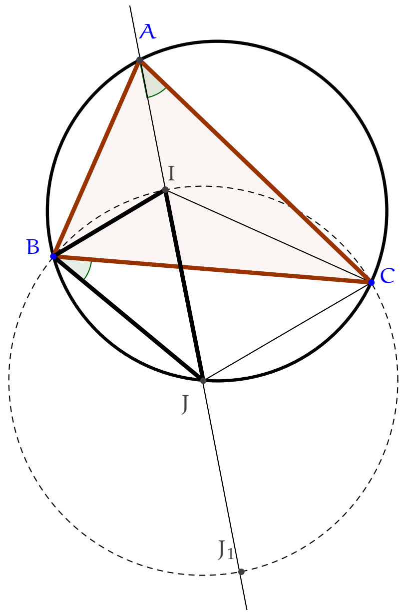


Il en résulte essentiellement que si l'on fixe les points B et C, quel que soit le point A, l'angle inscrit $\widehat{BAC}$ aura toujours même mesure. Sous réserve que lorsque A traverse la corde BC, l'angle inscrit est transformé en son supplémentaire, l'angle au centre devenant l'angle rentrant égal au double du supplémentaire. Cette égalité des angles inscrits s'utilise dans les deux sens : d'une part, si A, B, C, D sont sur un même cercle, A et D du même côté de (BC), les angles $\widehat{BAC}$ et $\widehat{BDC}$ sont égaux, d'autre part, réciproquement, si A, B, C, D sont quatre points (A et D du même côté de (BC)) vérifiant : $\widehat{BAC} = \widehat{BDC}$, alors les quatre points A, B, C, D sont cocycliques, c'est-à-dire sur un même cercle. Il est fréquent qu'on utilise le théorème dans les deux sens, d'une part pour prouver que quatre points sont cocycliques, d'autre part pour en conclure que des angles autres que ceux connus initialement sont égaux.

Exercice 3

Soit ABC un triangle, I le centre de son cercle inscrit. La droite (AI) recoupe en J le cercle circonscrit au triangle (ABC). Montrer que $JB = JC = JI$.

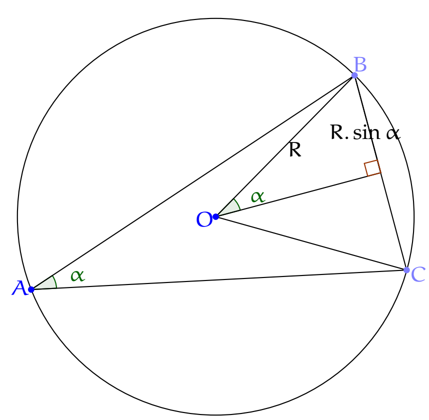
Solution de l'exercice 3



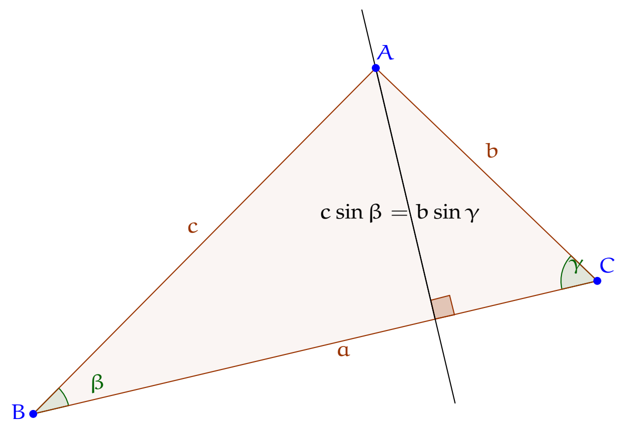
Les angles inscrits $\widehat{JAC}$ et $\widehat{JBC}$ sont égaux, tout comme les angles inscrits $\widehat{BAJ}$ et $\widehat{BCJ}$. Mais comme $(AI) = (AJ)$ est bissectrice de $\widehat{BAC}$, $\widehat{JAC} = \widehat{BAJ}$ donc $\widehat{JBC} = \widehat{BCJ}$, d'où l'on déduit que le triangle BCJ est isocèle : $JB = JC$. Par ailleurs, dans le triangle IBA, l'angle extérieur $\widehat{BIJ}$ est la somme des angles à la base $\widehat{IAB} + \widehat{IBA}$. Mais, nous l'avons vu, $\widehat{IAB} = \widehat{JAC} = \widehat{JBC}$, et, comme (BI) est bissectrice de $\widehat{CBA}$, $\widehat{IBA} = \widehat{CBI}$. Donc en définitive, $\widehat{BIJ} = \widehat{JBI}$, ce qui prouve que le triangle JBI est lui aussi isocèle, donc que $JB = JI$.

- Loi des sinus -

Une dernière propriété importante : la loi des sinus. Dans un triangle, la longueur des côtés est proportionnelle aux sinus des angles opposés. Cela peut se démontrer de deux manières au moins : d'une part, la bissectrice de l'angle au centre est médiatrice du côté opposé, or si l'on note $\widehat{A}$ la mesure de l'angle inscrit $\widehat{BAC}$, la moitié de l'angle au centre vaut également $\widehat{A}$ donc la moitié de la corde BC vaut $R.\sin\widehat{A}$ si l'on appelle R le rayon du cercle. Le côté opposé à l'angle $\widehat{A}$ ayant pour longueur : $2R.\sin\widehat{A}$, si l'on note $a = BC, b = CA, c = AB$, $\frac{a}{\sin\widehat{A}} = \frac{b}{\sin\widehat{B}} = \frac{c}{\sin\widehat{C}} = 2R$.



Une autre démonstration possible est de considérer par exemple la hauteur issue de A. Sa longueur peut se calculer de deux manières : c'est soit $AB. \sin \widehat{B}$ soit $AC. \sin \widehat{C}$, d'où $\frac{AB}{\sin \widehat{C}} = \frac{AC}{\sin \widehat{B}}$. Le même raisonnement avec les deux autres hauteurs donne la loi des sinus.



2 Deuxième cours

- Énoncés des exercices vus en cours -

Exercice 1 Un internat et un lycée sont situés de deux cotés d'une rue droite.

On veut construire un chemin de l'internat jusqu'à la rue, un passage pieton qui traverse la rue de manière perpendiculaire, et un chemin de l'autre bout de passage jusqu'au lycée.

Quel est le chemin le plus cours sous ces conditions ?

Exercice 2 Tu veux aller à la rivière (une ligne droite), remplir un seau et après courir pour donner de l'eau à tes lièvres assoiffés qui se trouvent sur la même rive de la rivière que toi. Quel est le chemin le plus court ?

Exercice 3 Soient $\Delta_1, \Delta_2, \Delta_3$ trois droites. Existe-t-il un triangle équilateral tel que $A \in \Delta_1$, $B \in \Delta_2$ et $C \in \Delta_3$?

Exercice 4 Montrer que les médianes se coupent dans la proportion 1 : 2.

Exercice 5 (Droite d'Euler) Soit ABC un triangle, G sont centre de gravité, O son centre du cercle circonscrit et H son orthocentre.

Montrer que G,O et H sont alignés.

Exercice 6 (Théorème de Napoléon) Sur les trois cotés d'un triangle donné on construit vers l'extérieur des triangles équilatéraux. Montrer que les centres de ces triangles forment un triangle équilatéral.

Exercice 7 Sur les trois cotés d'un triangle donné on construit vers l'extérieur des triangles isocèles rectangles BAR avec l'angle droit à R, ACQ avec l'angle droit à Q et CBP avec l'angle droit à P.

Monter que $QR \perp AP$ et $\overline{QR} = \overline{AP}$.

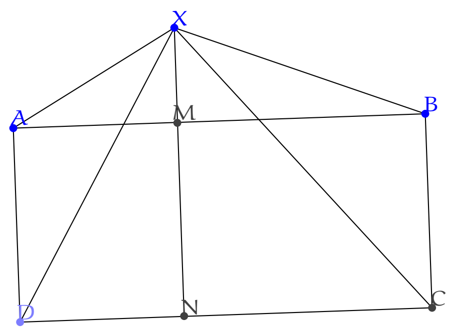
Exercice 8 (Point de Fermat) Soit ABC un triangle, et soit F le point à l'intérieur tel que $\overline{AF} + \overline{BF} + \overline{CF}$ minimal. Montrer que $\measuredangle AFB = \measuredangle BFC = \measuredangle CFA = 120°$.

3 Premier TD

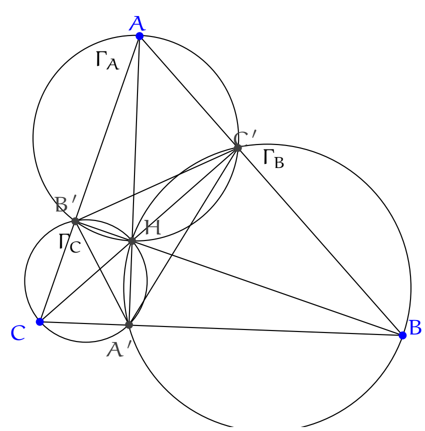
- Énoncés -

Exercice 1 Soient A, B, C, D quatre points du plan. Prouver l'équivalence des deux conditions suivantes :

1. $ABCD$ est un rectangle.
2. Pour tout point X du plan, $AX^2 + CX^2 = BX^2 + DX^2$

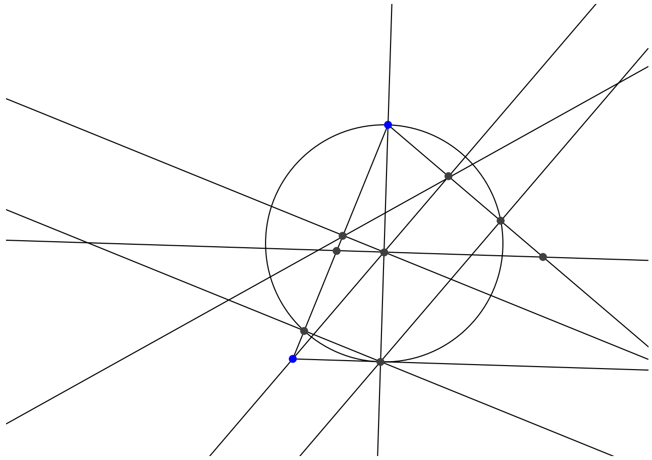


Exercice 2



Soit ABC un triangle aigu. On note A' le pied de la hauteur issue de A, et de même pour B' et C'. Calculer les angles du triangle $A'B'C'$ en fonction de ceux de ABC. Montrer que le plus grand angle de $A'B'C'$ est supérieur ou égal au plus grand angle de ABC. Quand y a-t-il égalité ?

Exercice 3

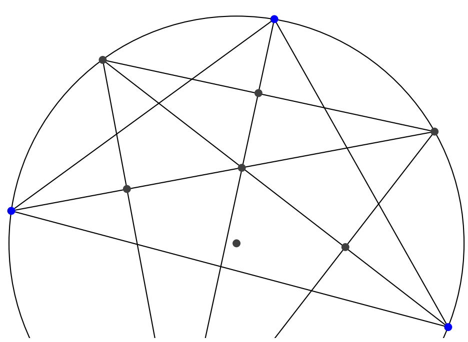


Soit ABC un triangle, H_A le point d'intersection de la hauteur issue de A avec la droite (BC), H_B le point d'intersection de la hauteur issue de B avec la droite (AC) et H_C le point d'intersection de la hauteur issue de C avec la droite (AB). On projette orthogonalement H_A sur les droites (AB), (BC) ce qui donne deux points D et E. Prouver que $(DE) \parallel (H_B H_C)$.

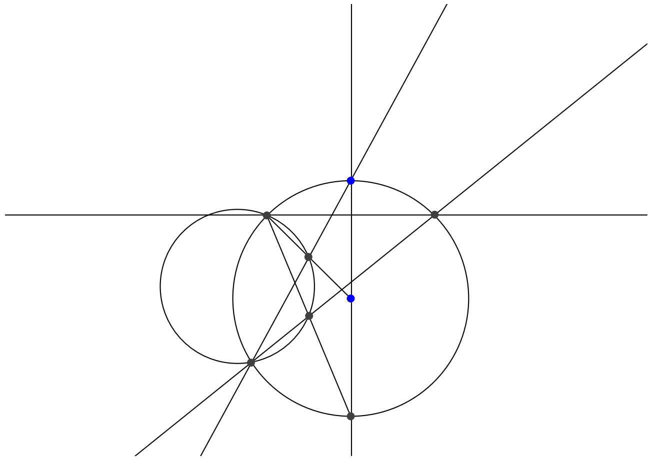
Exercice 4 Soit ABC un triangle, G son centre de gravité. Prouver que

$$AG \perp BG \Leftrightarrow BC^2 + AC^2 = 5AB^2$$

Exercice 5



Soient six points A, C_1, B, A_1, C, B_1 pris sur un cercle dans cet ordre. Prouver que les droites (AA_1), (BB_1), (CC_1) sont les hauteurs du triangle ABC si et seulement si ce sont les bissectrices du triangle $A_1B_1C_1$.



Exercice 6 Soit Γ un cercle de centre O et de diamètre AB, CD une corde de Γ avec $(AB)\perp(CD)$. Soit AE la corde passant par A et le milieu M de OC. Prouver que DE passe par le milieu de BC.

Exercice 7 Soit ABC un triangle. On note $a = BC$, $b = AC$, $c = AB$, $p = 1/2(a+b+c)$, r le rayon du cercle inscrit et R le rayon du cercle circonscrit. Montrer que :

$$abc = 4prR$$
$$ab + bc + ca = r^2 + p^2 + 4rR$$

- Corrigé -

Solution de l'exercice 1 "$ABCD$ est un rectangle" est équivalent à "$ABCD$ est un parallélogramme" et "$AB\perp AD$", ou encore en termes vectoriels à "$\overrightarrow{AB} = \overrightarrow{DC}$" et "$\overrightarrow{AB} \cdot \overrightarrow{AD} = 0$".

Solution avec le théorème de Pythagore : Preuve de $(1) \Rightarrow (2)$: on introduit les projetés orthogonaux M et N de X sur (AB) et (CD) respectivement. Par le théorème de Pythagore :

$$AX^2 + CX^2 = AM^2 + MX^2 + CN^2 + NX^2$$
$$BX^2 + DX^2 = BM^2 + MX^2 + DN^2 + NX^2$$

Comme $ABCD$ est un rectangle, les points X, M, N sont alignés (sur la perpendiculaire commune à (AB) et (CD) passant par X), et l'on a :

$$AM^2 = DN^2$$
$$BM^2 = CN^2$$

En mettant tout ensemble, on obtient (2).

Preuve de $(2) \Rightarrow (1)$: on spécialise l'hypothèse (2) aux points particuliers du problème, à savoir les sommets A, B, C, D, ce qui donne :

$$AC^2 = AB^2 + AD^2$$
$$AB^2 + BC^2 = BD^2$$
$$AC^2 = BC^2 + CD^2$$
$$AD^2 + CD^2 = BD^2$$

En sommant deux à deux, cela entraîne $2AC^2 = AB^2 + BC^2 + CD^2 + AD^2 = 2BD^2$, d'où $AC = BD$. En réinjectant dans le système, on obtient tout de suite $AB = CD$ et $AD = BC$. Mais alors on a par exemple $BD^2 = AB^2 + AD^2$, donc d'après la réciproque du théorème de Pythagore, on a $(AB)\perp(AD)$, et de même pour tous les autres angles. Donc $ABCD$ est un rectangle.

Solution vectorielle : On manipule l'expression intervenant dans (2) pour isoler la dépendance en X :

$$\begin{aligned} AX^2 + CX^2 - BX^2 - DX^2 &= (\overrightarrow{AB} + \overrightarrow{BX})^2 + (\overrightarrow{CD} + \overrightarrow{DX})^2 - BX^2 - DX^2 \\ &= AB^2 + 2\overrightarrow{AB} \cdot \overrightarrow{BX} + CD^2 + 2\overrightarrow{CD} \cdot \overrightarrow{DX} \\ &= AB^2 + 2\overrightarrow{AB} \cdot (\overrightarrow{BD} + \overrightarrow{DX}) + CD^2 + 2\overrightarrow{CD} \cdot \overrightarrow{DX} \\ &= AB^2 + 2\overrightarrow{AB} \cdot \overrightarrow{BD} + CD^2 + 2\overrightarrow{DX} \cdot (\overrightarrow{AB} + \overrightarrow{CD}) \end{aligned}$$

Preuve de $(2) \Rightarrow (1)$: l'hypothèse (2) entraine en particulier que $AX^2 + CX^2 - BX^2 - DX^2$ est indépendant de X, donc d'après le calcul précédent que le vecteur en facteur $\overrightarrow{AB} + \overrightarrow{CD}$ est nul. Donc (2) entraine que $ABCD$ est un parallélogramme. On a en particulier $AB = CD$. On réinjecte ces informations dans le calcul :

$$\begin{aligned} AX^2 + CX^2 - BX^2 - DX^2 &= 2AB^2 + 2\overrightarrow{BD} \cdot \overrightarrow{AB} \\ &= 2\overrightarrow{AB} \cdot \overrightarrow{AD} \end{aligned}$$

Donc (2) entraine que $AB \perp AD$. On a montré que $ABCD$ est un rectangle.

Preuve de $(1) \Rightarrow (2)$: il suffit de reprendre le raisonnement précédent à l'envers.

Solution de l'exercice 2 Le fait que ABC est aigu implique que H est à l'intérieur du triangle ABC, ce qui assure que l'ordre des points sur les cercles considérés est celui qu'on utilise dans la preuve. Que se passe-t-il si ABC n'est pas aigu ?

Notons α, β, γ les angles de ABC en A, B, C, et la même chose pour $A'B'C'$. On introduit l'orthocentre H de ABC, et les cercles Γ_A, Γ_B, Γ_C de diamêtre HA, HB et HC. On a $A' \in \Gamma_B \cap \Gamma_C$, $B' \in \Gamma_A \cap \Gamma_C$, $C' \in \Gamma_A \cap \Gamma_B$. D'après la propriété des angles inscrits, on a $\widehat{B'C'H} = \widehat{B'AH}$. D'autre part le triangle ACA' est rectangle donc $\widehat{B'AH} = 90^\circ - \gamma$. On montre de même que $\widehat{CC'A'} = 90^\circ - \gamma$, d'où

$$\gamma' = \widehat{B'C'A'} = 180^\circ - 2\gamma$$

On montre de même que $\alpha' = 180^\circ - 2\alpha$, $\beta' = 180^\circ - 2\beta$.

Par symétrie, on peut supposer que $\alpha \geqslant \beta \geqslant \gamma$. Alors $\gamma' \geqslant \beta' \geqslant \alpha'$ et $\gamma' - \alpha = 180^\circ - 2\gamma - -\alpha = \beta - \gamma \geqslant 0$. On a égalité si et seulement si $\beta = \gamma$, i.e si ABC est isocèle en A et $\alpha \geqslant \beta = \gamma$.

Solution de l'exercice 3 On va montrer qu'en fait les triangles AH_CH_B et ADE sont directement semblables car chacun est inversement semblable au triangle ABC. La réciproque du théorème de Thalès montre alors que $(DE) \parallel (H_BH_C)$.

ADE et ABC inversement semblables : On introduit le cercle Γ de diamêtre AH_A. On a $\widehat{H_ADA} = \widehat{AEH_A} = 90^\circ$, donc les points D et E lui appartiennent. La propriété des angles inscrits implique que $\widehat{EDA} = \widehat{EH_AA}$. Or $\widehat{EH_AA} = 90^\circ - \widehat{CH_AE}$ car $(AH_A)\perp(BC)$ et $\widehat{CH_AE} = 90^\circ - \widehat{ACB}$ car $(H_AE)\perp(AC)$. Donc $\widehat{EDA} = \widehat{ACB}$. De même $\widehat{AED} = \widehat{CBA}$. Comme on a bien sûr $\widehat{DAE} = \widehat{BAC}$, on en conclut que ADE et ABC sont inversement semblables.

AH_CH_B et ABC inversement semblables : Soit H l'orthocentre du triangle (qui est le point de concours des trois hauteurs). On introduit la parallèle à (BC) passant par H, qui coupe (AB) en B' et (AC) en C'. Par le théorème de Thalès, les triangles ABC et $AB'C'$ sont directement semblables. Mais par ailleurs, le point H joue le même rôle dans le triangle $AB'C'$ que le point D dans le triangle ABC ! (et les points H_B, H_C jouent le rôle des points E et D.) Donc par la première partie de la preuve, AH_CH_B et $AB'C'$ sont inversement semblables, et on a terminé.

Solution de l'exercice 4 Le théorème de Pythagore et sa réciproque montrent que $AG \perp BG \Leftrightarrow AB^2 = AG^2 + BG^2$. Pour exploiter cette condition, on donne deux rédactions : une utilisant seulement la formule d'Al Kashi, l'autre avec du calcul vectoriel. Les deux sont équivalentes, mais cela illustre comment le produit scalaire "automatise" ce type de raisonnement.
Solution avec Al Kashi : Soient M_A, M_B les milieux de BC et de AC. Comme G est le centre de gravité de ABC, on $AG = 2/3AM_A$ et $2/3BM_B$. D'autre part, en appliquant la formule d'Al Kashi dans les triangles ABM_B et ABM_A, on obtient :

$$BM_B^2 = AB^2 + AC^2/4 - AB \cdot AC \cdot \cos(\alpha)$$

$$AM_A^2 = AB^2 + BC^2/4 - AB \cdot BC \cdot \cos(\beta)$$

D'où $AG^2 + BG^2 = AB^2 + AC^2 - 4AB(BC \cdot \cos(\alpha) + AC \cdot \cos(\beta))$. Pour conclure, il suffit de remarquer que

$$AB = BC \cdot \cos(\alpha) + AC \cdot \cos(\beta)$$

formule qui vient en découpant AB au niveau du pied de la hauteur issue de C.

Solution vectorielle : Comme G est le centre de gravité de ABC, on a $\overrightarrow{AG} = 1/3(\overrightarrow{AB} + \overrightarrow{AC})$ et $\overrightarrow{BG} = 1/3(\overrightarrow{AB} + \overrightarrow{BC})$.

$$\begin{aligned}
AB^2 &= AG^2 + BG^2 + 2\overrightarrow{AG} \cdot \overrightarrow{BG} \\
AB^2 &= 1/9(AB^2 + AC^2 + 2\overrightarrow{AB} \cdot \overrightarrow{AC} + AB^2 + BC^2 + 2\overrightarrow{AB} \cdot \overrightarrow{BC}) + 2\overrightarrow{AG} \cdot \overrightarrow{BG} \\
5AB^2 &= AC^2 + BC^2 + 18\overrightarrow{AG} \cdot \overrightarrow{BG}
\end{aligned}$$

L'équivalence à démontrer est maintenant claire.

Solution de l'exercice 5 Implication directe : on suppose que (AA_1), (BB_1), (CC_1) sont les hauteurs de ABC. Montrons par exemple que (AA_1) es la bissectrice de $A_1B_1C_1$ en A_1, c'est-à-dire que $\widehat{B_1A_1A} = \widehat{AA_1C_1}$ (les deux autres se traitent de la même manière). Soit $D = (AC) \cap (BB_1)$ et $E = (AB) \cap (CC_1)$. Alors les deux triangles rectangles ABD et AEC ont un angle commun, d'où $\widehat{B_1BA} = \widehat{ACC_1}$. Or par la propriété des angles inscrits, $\widehat{B_1BA} = \widehat{B_1A_1A}$ et $\widehat{ACC_1} = \widehat{AA_1C_1}$, ce qui conclut.

Implication inverse : on suppose que (AA_1), (BB_1) et (CC_1) sont les bissectrices de $A_1B_1C_1$. Montrons par exemple que (AA_1) est la hauteur de ABC en A, c'est-à-dire que $(AA_1) \perp (BC)$. On écrit :

$$\widehat{CFA} = 180^\circ - \widehat{ACF} - \widehat{CAF}$$

D'une part, par la propriété des angles inscrits et l'hypothèse :

$$\widehat{CAF} = \widehat{CC_1A_1} = 1/2\widehat{B_1C_1A_1}$$

D'autre part, en appliquant deux fois la propriété des angles inscrits, puis l'hypothèse :

$$\widehat{ACF} = \widehat{AA_1B} = \widehat{AA_1C_1} + \widehat{C_1A_1B} = \widehat{AA_1C_1} + \widehat{C_1A_1B} = 1/2(\widehat{B_1A_1C_1} + \widehat{C_1B_1A_1})$$

D'où finalement :

$$\widehat{CFA} = 180° - 1/2(\widehat{B_1C_1A_1} + \widehat{B_1A_1C_1} + \widehat{C_1B_1A_1}) = 90°$$

<u>*Solution de l'exercice 6*</u> Notons $N = (DE) \cap (BC)$. La réciproque du théorème de Thalès dans le triangle OCB montre que N est le milieu de BC si et seulement si (MN) est parallèle à (BC), ou encore si et seulement si $\widehat{MNC} = \widehat{OBC}$. C'est cette égalité d'angle que l'on va démontrer. Par la propriété des angles inscrits, on a $\widehat{OBC} = \widehat{AEC} = \widehat{MEC}$, donc l'égalité à démontrer se réécrit $\widehat{MEC} = \widehat{MNC}$, ce qui est équivalent à montrer que M, N, E, C sont cocycliques. On va démontrer cette cocyclicité.

Les arcs AC et AD de Γ sont de même longueur par symétrie. Comme $E \in \Gamma$, ceci entraîne $\widehat{DEA} = \widehat{AEC}$. Par la propriété des angles inscrits, $\widehat{AEC} = \widehat{ABC}$. Comme le triangle OCB est isocèle, $\widehat{ABC} = \widehat{BCO}$. Donc $\widehat{DEA} = \widehat{BCO}$, c'est-à-dire $\widehat{NEM} = \widehat{NCM}$, ce qui montre que M, N, E, C sont cocycliques.

<u>*Solution de l'exercice 7*</u> Notons $\alpha = \widehat{BAC}$, $\beta = \widehat{CBA}$, $\gamma = \widehat{ACB}$ et S l'aire de ABC.

<u>Première formule :</u> On écrit la formule standard pour S et la loi des sinus en C :

$$S = \frac{1}{2}ab\sin(\gamma) = \frac{1}{4}abc/R$$

Donc on est ramené à démontrer $S = pr$, qui devient évidente si l'on découpe ABC en trois triangles le long des bissectrices et que l'on applique la formule "base*hauteur/2".

<u>Seconde formule :</u> On combine la formule de Héron avec la première formule démontrée et la formule $S = pr$:

$$\begin{aligned} p^2r^2 &= S^2 \\ &= p(p-a)(p-b)(p-c) \\ &= p^3 - (a+b+c)p^2 + (ab+bc+ac)p - abc \\ &= -p^3 + (ab+bc+ac)p - 4prR. \end{aligned}$$

On obtient ce qu'on cherche en divisant par p.

4 Deuxième TD

- Énoncés -

Exercice 1 Deux cercles sont tangents intérieurement en un point A. Soit B le point diamétralement opposé sur le grand cercle. On trace BC une corde du grand cercle qui est tangente au petit cercle au point D. AD est-elle la hauteur, la médiane ou la bissectrice du triangle ABC issue de A ?

Exercice 2 Montrer qu'un quadrilatère $ABCD$ est inscrit dans un cercle si et seulement si $\widehat{A}+\widehat{C}=\widehat{B}+\widehat{D}=180°$.

Exercice 3 Soit ABC un triangle et H son orthocentre. Montrer que les symétriques de H par rapport aux trois côtés sont sur le cercle circonscrit.

Exercice 4 (droite de Simpson) Soit ABC un triangle et P un point. Soient P_1, P_2 et P_3 les projections de P sur les trois côtés du triangle. Montrer que P_1, P_2, P_3 alignés si et seulement si P est sur le cercle circonscrit.

Exercice 5 Soit ABC un triangle, H son orthocentre et O le centre du cercle circonscrit. Montrer que $\widehat{BAO}=\widehat{CAH}$.

Exercice 6 Soit ABC un triangle tel que la médiane, la hauteur et la bissectrice issues de A coupent l'angle $\widehat{A}$ en quatre angles égaux α. Exprimer tous les angles de la figure en fonction de α et calculer α.

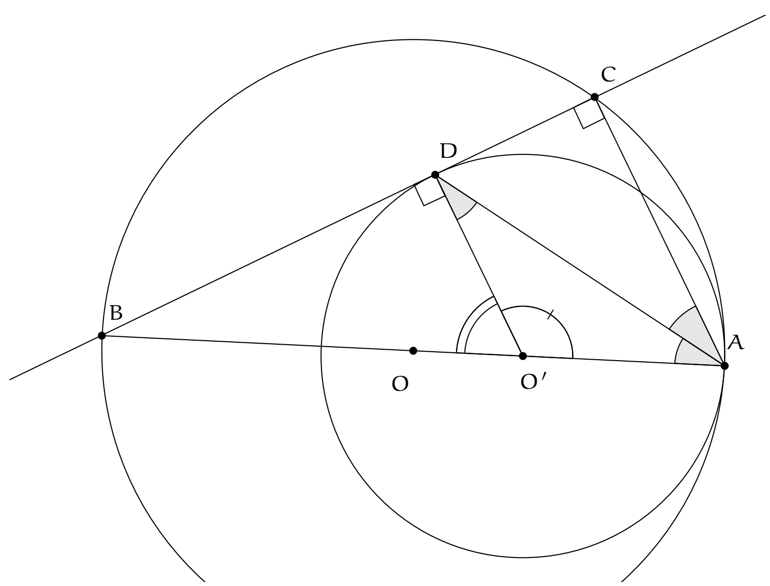
Exercice 7 Soit ABC un triangle et O le centre de son cercle circonscrit. Soit D l'intersection de la bissectrice de $\widehat{B}$ et du côté AC, et E un point du côté BC tel que $AB=BE$. Montrer que (BO) et (DE) sont perpendiculaires.

Exercice 8 Soit ABC un triangle dont la longueur des côtés est 3, 4, 5. Calculer le rayon du cercle inscrit.

Exercice 9 Soit Γ un cercle et BC une corde de Γ. Soit A le milieu de l'arc BC. Par A on mène deux cordes quelconques AD et AE qui coupent BC en F et G. Montrer que le quadrilatère $DFGE$ est inscriptible dans un cercle.

- Corrigé -

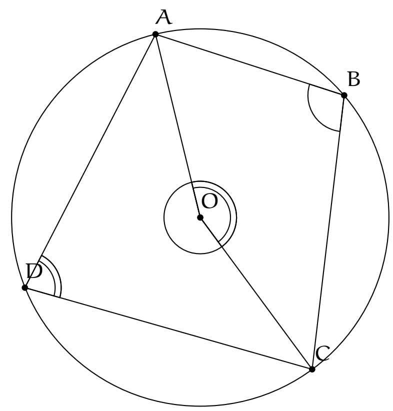
<u>*Solution de l'exercice 1*</u> Cet exercice est surtout la pour vous faire tracer une jolie figure :



Sur la figure on voit tout de suite que AD n'est ni une hauteur ni une médiane. Essayons donc de montrer que c'est la bissectrice de $\widehat{A}$. Soit ABC un triangle et H son orthocentre.

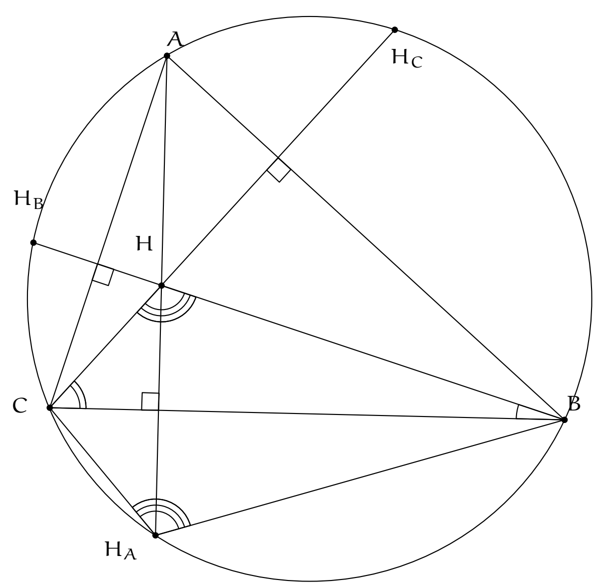
Montrer que les symétriques de H par rapport aux trois côtés sont sur le cercle circonscrit. Appelons $\alpha = \widehat{BAD}$. Comme le triangle $O'AD$ est isocèle, $\widehat{O'DA} = \alpha$, donc $\widehat{DO'A} = 180° - 2\alpha$ et $\widehat{BO'D} = 2\alpha$. Ensuite, comme AC et $O'D$ sont toutes deux perpendiculaires à BC, elles sont parallèles. Les angles $\widehat{BO'D}$ et $\widehat{BAC}$ sont égaux et valent 2α. La droite AD coupe bien l'angle $\widehat{A}$ en deux parties égales.

Solution de l'exercice 2 Prenons un quadrilatère $ABCD$ inscrit dans un cercle. Par le théorème de l'angle interne et de langle au centre, $\widehat{BOC} = 2 * \widehat{BAC}$ et $\widehat{COB} = 2 * \widehat{CDB}$. Mais comme $\widehat{BOC} + \widehat{COB} = 360°$, on a bien $\widehat{BAC} + \widehat{CDB} = 180°$.



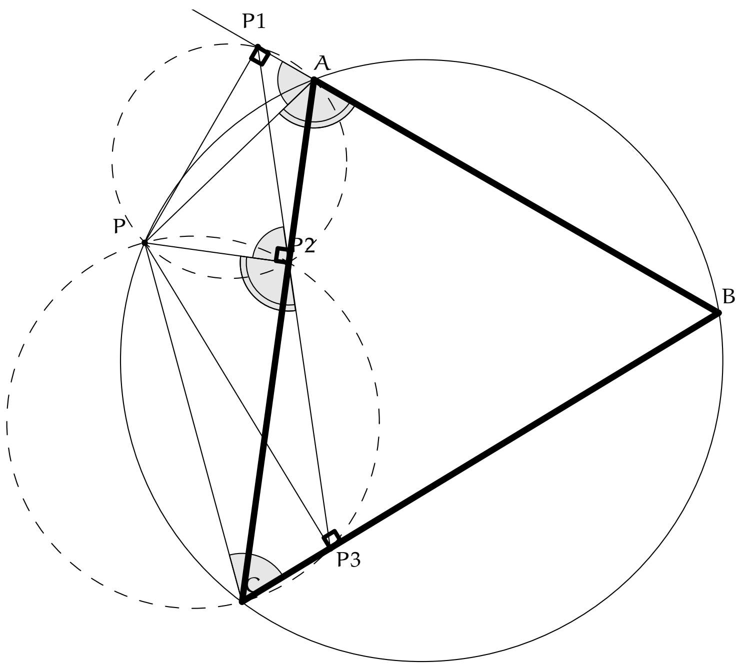
Il faut aussi montrer le sens inverse : supposons que $\widehat{A} + \widehat{C} = 180°$. Soit C' l'intersection du côté BC avec le cercle qui passe par A, B et D. Nous voulons montrer que $C = C'$. Par la question précédente, on sait que $\widehat{BC'D} = 180° - \widehat{BAD} = \widehat{BCD}$. Donc les droites (BC) et (BC') sont parallèles et comme elles passent par B toutes les deux elles sont confondues et on a bien $C = C'$.

Solution de l'exercice 3 Commençons par une jolie figure :



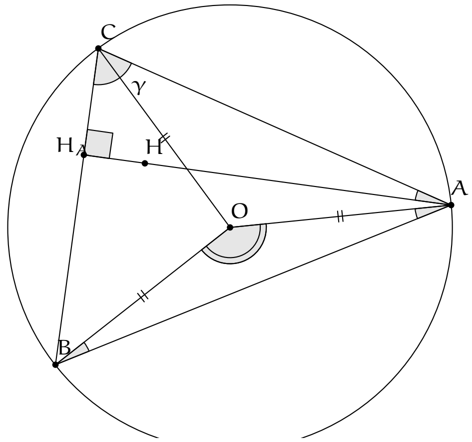
Nous allons juste montrer que H_A, le symétrique de H par rapport à BC, est sur le cercle circonscrit. Nous noterons α, β et γ les trois angles du triangle. Comme BH est une hauteur, l'angle $\widehat{CBH}$ vaut $90°-\gamma$. De même, $\widehat{BCH} = 9O°-\beta$ et donc $\widehat{BHC} = 180°-(90°-\beta)-(90°-\gamma) = \beta+\gamma$. Comme c'est l'angle symétrique, $\widehat{BH_AC} = \widehat{BHC}$ et $\widehat{BH_AC} + \widehat{BAC} = \alpha+\beta+\gamma = 180°$. Donc d'après le critère de l'exercice précédent, les points A, B, C et H_A sont cocycliques.

<u>*Solution de l'exercice 4*</u> Commençons par faire la figure :



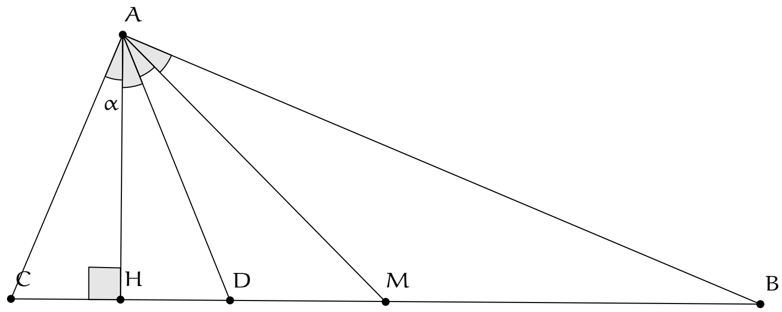
Comme il y a des angles droits en P_2 et P_1, le quadrilatère PP_1AP_2 est inscrit dans un cercle, donc $\widehat{P_1AP} = \widehat{P_1P_2P} = 180° - \widehat{PAB}$. Comme P est sur le cercle circonscrit de ABC, $\widehat{PCB} = 180° - \widehat{PAB} = \widehat{P_1P_2P}$. Enfin, comme P, P_2, P_3, C sont cocycliques, on a $\widehat{PP_2P_3} = 180° - \widehat{PCP_3} = 180° - \widehat{P_1P_2P}$. Donc $\widehat{P_1P_2P_3} = \widehat{P_1P_2P} + \widehat{PP_2P_3} = 180°$, les trois points sont alignés.

<u>*Solution de l'exercice 5*</u> Faisons la figure :



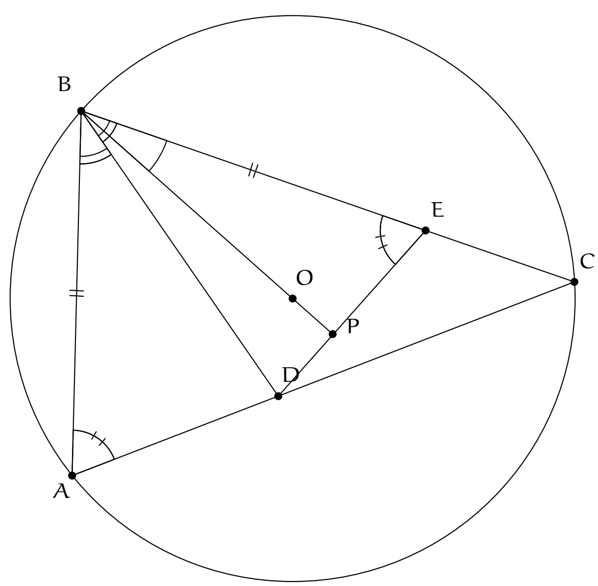
Nous allons calculer les angles en question en fonction de $\gamma = \widehat{BCA}$. Tout d'abord, le triangle CAH_A est rectangle en H_A, donc $\widehat{HAC} = 90° - \gamma$. Pour calculer l'autre angle, on commence par utiliser angle inscrit-angle au centre et on trouve $\widehat{BOA} = 2\gamma$. Ensuite, comme le triangle BOA est isocèle en O, il est facile de calculer $\widehat{OAB} = \frac{180°-\widehat{BOA}}{2} = 90° - \gamma = \widehat{CAH}$.

<u>*Solution de l'exercice 6*</u> Faisons le dessin :



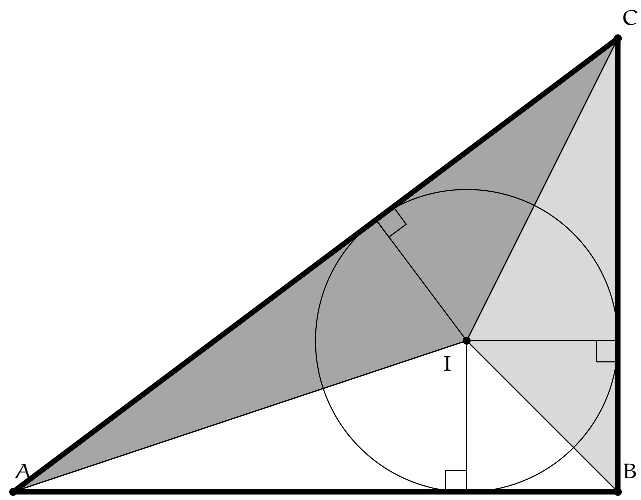
Il est facile de calculer tous les angles en fonction de α : $\widehat{BCA} = \widehat{HDA} = 90° - \alpha$, $\widehat{DMA} = 90° - 2\alpha$ et $\widehat{CBA} = 90° - 3\alpha$. Intéressons-nous maintenant au calcul de α. Appelons O le centre du cercle circonscrit de ABC. Nous savons grâce à l'exercice d'avant d'avant, que $\widehat{BAO} = \widehat{CAH} = \alpha$. Mais cela signifie que O est sur la médiane (AM). Comme O est également sur la médiatrice de $[BC]$, cela veut dire que $0 = M$. Le rayon du cercle circonscrit est sur le segment $[BC]$, donc le triangle est rectangle en A et $\alpha = \frac{90°}{4} = 22.5°$.

<u>*Solution de l'exercice 7*</u> Commençons par faire la figure :



Nous voulons montrer que l'angle $\widehat{BPE}$ est droit, nous allons donc chercher les valeurs des deux autres angles du triangle. Si on note $\alpha = \widehat{A}$, alors l'angle $\widehat{EBP} = 90° - \alpha$ d'après l'exercice précédent. Ensuite on remarque que le point E est le symétrique de A par rapport à la droite BD, donc les triangles BAD et BED sont le symétrique l'un de l'autre et $\widehat{BED} = \alpha$. Donc $\widehat{BPE} = 180° - (90° - \alpha + \alpha) = 90°$.

<u>*Solution de l'exercice 8*</u> Si vous ne le saviez pas déjà, en dessinant le triangle 3,4,5 vous vous rendrez compte qu'il est rectangle :

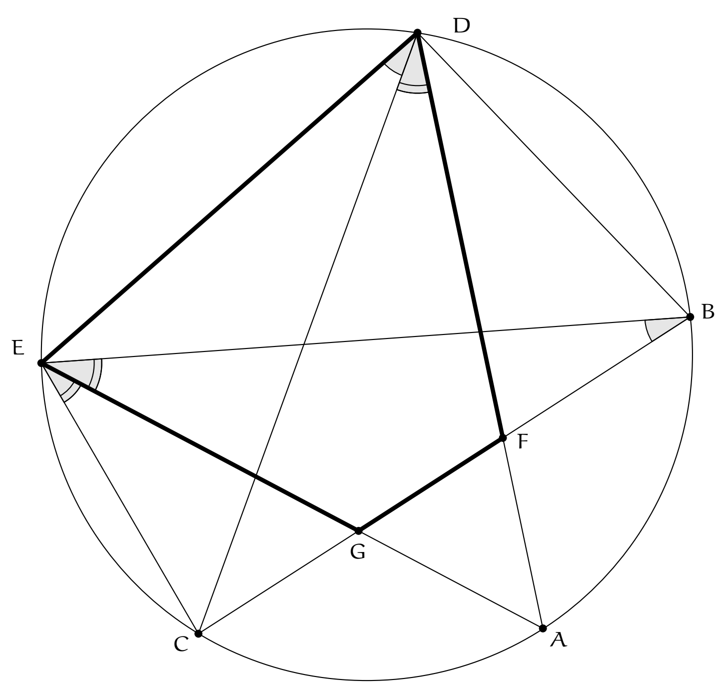


Pour calculer le rayon r du cercle inscrit, nous allons calculer l'aire $\mathcal{A}$ du triangle de deux façons différentes. Tout d'abord, $\mathcal{A} = \frac{3\times4}{2} = 6$. Ensuite, si on calcule séparément les aires des 3 triangles de couleurs différentes, on obtient :

$$\mathcal{A} = \frac{5\times r}{2} + \frac{4\times r}{2} + \frac{3\times r}{2} = 6r.$$

On en déduit que $r = 1$.

<u>*Solution de l'exercice 9*</u> Comme d'habitude, on commence par une figure :



Nous voulons montrer que le quadrilatère EDFG est inscriptible dans un cercle, essayons de montrer que $\widehat{EDF} + \widehat{FGE} = 180°$. Par les angles inscrits, on a que $\widehat{EDC} = \widehat{EBC}$ et $\widehat{CDA} = \widehat{CEA}$. Comme de plus les arcs CA et AB sont de même longueur, $\widehat{CEA} = \widehat{EAB}$. Maintenant, en faisant la somme des angles dans le triangle EBG on trouve que $\widehat{BGE} = 180° - \widehat{GEB} - \widehat{EBG}$ et en utilisant toutes les égalités obtenues précédemment on a le résultat souhaité.

5 Test

- Énoncés (durée : 3h) -

Exercice 1 Soient Γ_1 et Γ_2 deux cercles s'intersectant en P et Q. On trace le segment $[PQ]$. On considère une droite d qui le coupe en un point intérieur au segment. On note A, B, C, D dans cet ordre ses 4 points d'intersection de d avec Γ_1 (pour A et C) et Γ_2 (pour B et D).

Prouver que $\widehat{APB} = \widehat{CQD}$.

Exercice 2 Soient ABC un triangle et M le milieu de BC. Montrer que :

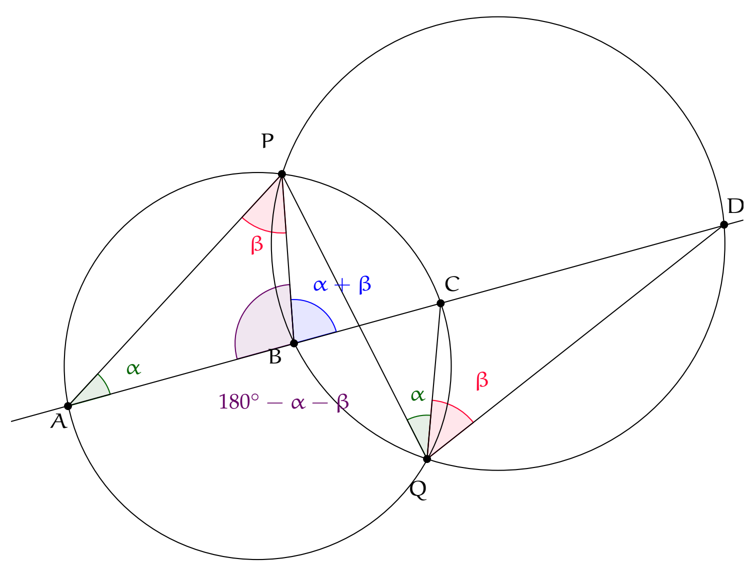
$$AM^2 = \frac{2AB^2 + 2AC^2 - BC^2}{4}$$

Exercice 3 Soit ABC un triangle. On construit vers l'extérieur un triangle équilatéral AFB porté par le côté AB, vers l'extérieur un triangle équilatéral ACE porté par le côté AC et vers l'intérieur un triangle isocèle CBD avec $\widehat{CDB} = 120°$. Montrer que $DE = DF$.

Exercice 4 Soit ABC un triangle. On note A', B', C' les pieds des hauteurs issues de A, B et C, H l'orthocentre de ABC et O le centre du cercle circonscrit de ABC. Montrer que $(OA) \perp (B'C')$.

- Corrigé -

<u>*Solution de l'exercice 1*</u> On commence par tracer une figure :



La présence de nombreux points cocycliques nous invite à chasser les angles : posons $\alpha = \widehat{PQC}$ et $\beta = \widehat{CQD}$. Les points P, B, Q, D sont cocycliques. Les angles $\widehat{PBD}$ et $\widehat{PQD}$ interceptent le même arc et sont donc égaux. Ainsi, $PBD = \alpha + \beta$, et donc $\widehat{ABP} = 180^\circ - \alpha - \beta$.

D'autre part, les points P, A, Q, C sont cocycliques. Les angles $\widehat{PAC}$ et $\widehat{PQC}$ interceptent le même arc et sont donc égaux. Ainsi, $\widehat{PAB} = \alpha$.

Nous avons de cette manière réussi à trouver deux des trois angles du triangle ABP. L'angle $\widehat{APB}$ vaut donc $180^\circ - (\alpha + 180^\circ - \alpha - \beta) = \beta$. On a bien $\widehat{CQD} = \widehat{APB}$, ce qu'il fallait démontrer.

Solution de l'exercice 2 On applique la formule d'Al Kashi aux triangles ABM et AMC en leurs sommets B et C :

$$AM^2 = BM^2 + AB^2 - 2BM \cdot AB\cos(\widehat{MBA}) = \frac{BC^2}{4} + AB^2 - BC \cdot AB\cos(\widehat{MBA})$$
$$AM^2 = CM^2 + AC^2 - 2CM \cdot AC\cos(\widehat{ACM}) = \frac{BC^2}{4} + AC^2 - BC \cdot AC\cos(\widehat{ACM})$$

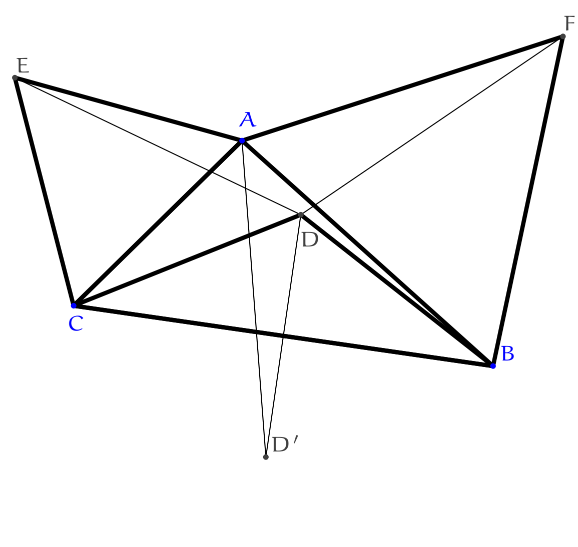
On fait la somme :

$$2AM^2 = AB^2 + AC^2 + \frac{BC^2}{2} - BC(AB\cos(\widehat{MBA}) + AC\cos(\widehat{ACM}))$$

Or $BC = AB\cos(\widehat{MBA}) + AC\cos(\widehat{ACM})$, comme on le voit en découpant suivant le pied de la hauteur issue de A. Donc :

$$AM^2 = \frac{2AB^2 + 2AC^2 - BC^2}{2}$$

Solution de l'exercice 3

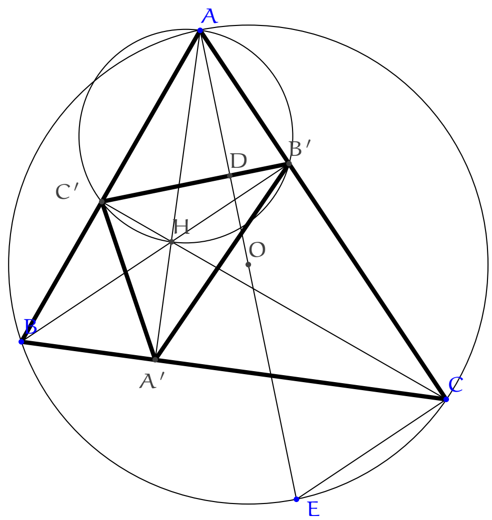


On introduit la rotation r_1 de centre C et d'angle 60°. On a $r_1(E) = A$ car ACE est équilatéral. D'autre part, $\widehat{BCD} = -30^\circ$, donc $\widehat{BCr_1(D)} = 60^\circ - 30^\circ = 30^\circ$. Donc $r_1(D)$ est le symétrique D'

de (AB) par rapport à la droite (BC). Si r_2 désigne la rotation de centre B et d'angle $-60°$, on vérifie de même que $r_2(F) = A$, $r_2(A) = D'$. Donc :

$$DE = r_1(D)r_1(E) = D'A = r_2(D)r_2(F) = DF$$

<u>*Solution de l'exercice 4*</u>



Notons D le point d'intersection de (OA) et de $B'C'$. On va montrer que $\widehat{DC'A} + \widehat{C'AD} = 90°$, ce qui conclut.

D'une part, on remarque que les points A, C', H, B' sont cocycliques car $\widehat{HC'A} = \widehat{AB'H} = 90°$. On a donc par la propriété des angles inscrits :

$$\widehat{DC'A} = \widehat{B'C'A} = \widehat{B'HA}$$

Comme les triangles $B'AH$ et CAA' sont rectangles, on a :

$$\widehat{B'HA} = 90° - \widehat{HAB'} = \widehat{ACA'}$$

D'autre part, on introduit le diamètre AE du cercle circonscrit. Alors par la propriété des angles inscrits et le fait que AE est un diamètre :

$$\widehat{BAO} = \widehat{BAE} = \widehat{BCE} = 90 - \widehat{ACA'}$$

On a donc bien $\widehat{DC'A} + \widehat{C'AD} = 90°$.

2 Incontournables (2ndes-1ères) : géométrie

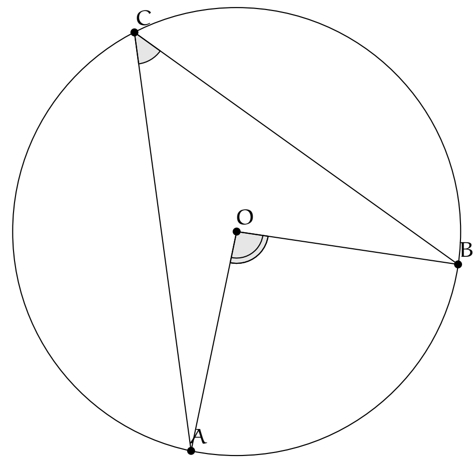
Nous renvoyons aux différents cours de géométrie disponibles sur le site d'Animath pour des compléments de cours (voir les liens en haut de la page 14).

1 Premier cours

- La chasse aux angles -

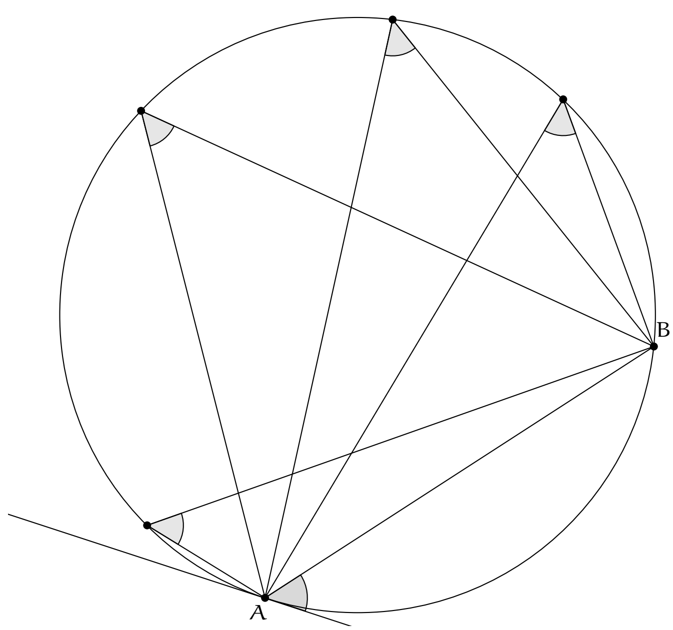
Il est bien souvent très pratique dans un problème de géométrie de savoir quels sont les angles égaux dans les figures, ou quelles sont les relations entre différents angles. Voici quelques techniques pour chasser les angles d'une figure.

Angle au centre - angle inscrit



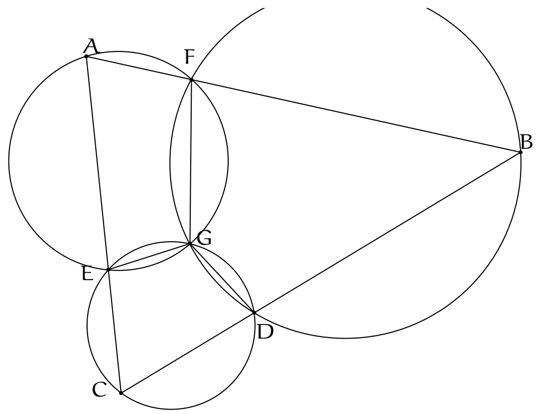
Théorème 1. $\widehat{ACB} = \frac{1}{2}\widehat{AOB}$, l'angle inscrit est la moitié de l'angle au centre.

Le corollaire très pratique est le suivant :



Corollaire 2. Tous les angles inscrits sont égaux, y compris l'angle inscrit "limite" : l'angle formé par la tangente.

Exercice 1 Montrer qu'un quadrilatère $ABCD$ est inscrit dans un cercle si et seulement si $\widehat{A} + \widehat{C} = \widehat{B} + \widehat{D} = 180°$.



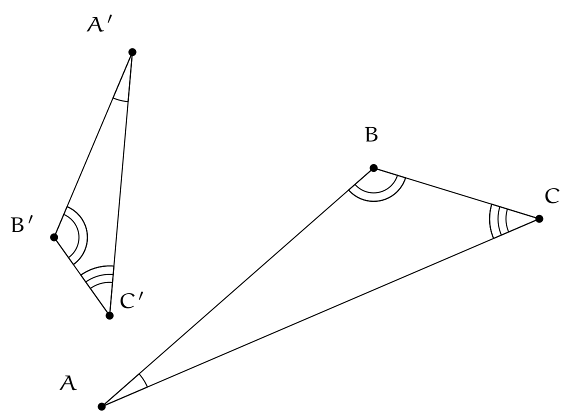
Exercice 2 (Théorème de Miquel) Soit ABC un triangle et D, E, F trois points sur les trois côtés du triangles. Montrer que les cercles circonscrits à AEF, BDF et CDE se coupent en un même point.

Exercice 3 Soit ABC un triangle, H son orthocentre et O le centre du cercle circonscrit. Montrer que $\widehat{BAO} = \widehat{CAH}$.

Exercice 4 (droite de Simpson) Soit ABC un triangle et P un point. Soient P_1, P_2 et P_3 les projections de P sur les trois côtés du triangle. Montrer que P_1, P_2, P_3 alignés si et seulement si P est sur le cercle circonscrit.

Triangles semblables

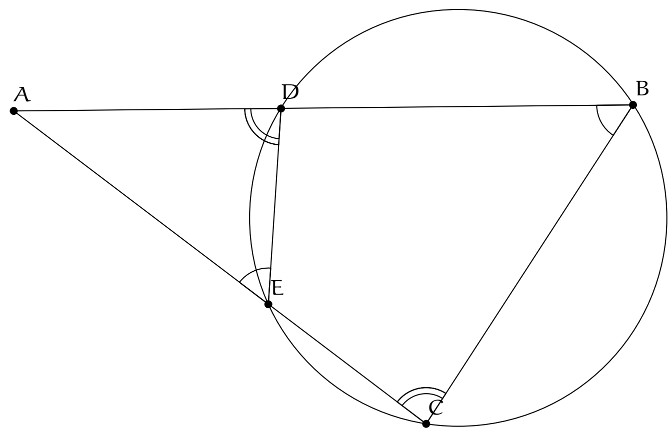
On dit que deux triangles sont semblables lorsqu'ils ont la même forme.



Proposition 3. Les quatres propositions suivantes sont équivalentes :

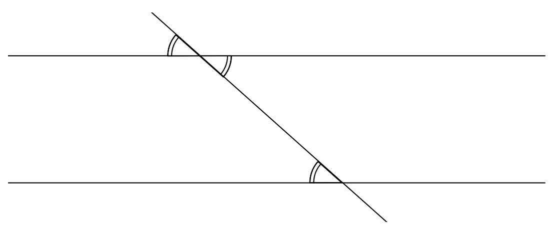
1. les triangles ABC et $A'B'C'$ sont semblables
2. $\widehat{A} = \widehat{A'}$, $\widehat{B} = \widehat{B'}$ et $\widehat{C} = \widehat{C'}$
3. $\frac{AB}{A'B'} = \frac{BC}{B'C'} = \frac{AC}{A'C'}$
4. $\widehat{A} = \widehat{A'}$ et $\frac{AB}{A'B'} = \frac{AC}{A'C'}$

Remarque 4. Dans la dernière propriété, les quotients concernent les deux côtés de l'angle $\widehat{A}$, et pas n'importe quels côtés.



Proposition 5. Les triangles ABC et AED ci-dessus sont semblables.

Droites parallèles



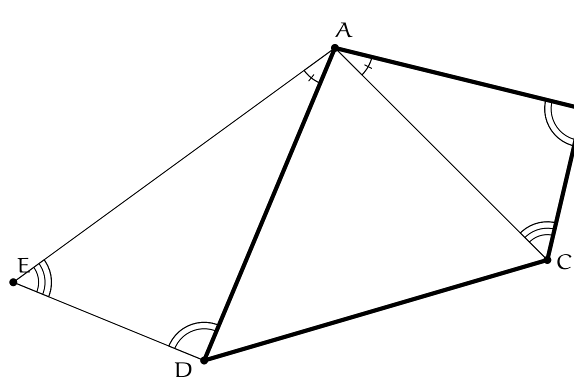
Lorsque deux droites sont parallèles, les angles alternes-internes et les angles correspondants sont égaux. Pour trouver des droites parallèles, n'oubliez pas que vous pouvez utiliser le théorème de Thalès.

- La géométrie du cercle -

Théorème de Ptolémée

Théorème 6. Soit $ABCD$ un quadrilatère. Alors $AC \cdot BD \leqslant AB \cdot BD + AD \cdot BC$, avec égalité ssi A, B, C, D cocycliques dans cet ordre.

Démonstration On commence la démonstration en construisant le point E tel que le triangle ADE soit semblable au triangle ABC.



Les triangles ABC et ADE sont semblables, donc

$$\frac{AC}{AE} = \frac{AB}{AD} = \frac{BC}{DE}.$$

En prenant la seconde égalité on peut exprimer

$$DE = \frac{AD \cdot BC}{AB}.$$

Ensuite intéressons-nous aux triangles ABD et ACE. On se rend compte facilement que $\widehat{BAD} = \widehat{CAE}$, et en regardant la première égalité au-dessus on voit que $\frac{AB}{AC} = \frac{AD}{AE}$, donc les deux triangles sont semblables.

$$\frac{AB}{AC} = \frac{BD}{CE} \implies CE = \frac{AC \cdot BD}{AB}.$$

Ensuite on utilise simplement l'inégalité triangulaire :

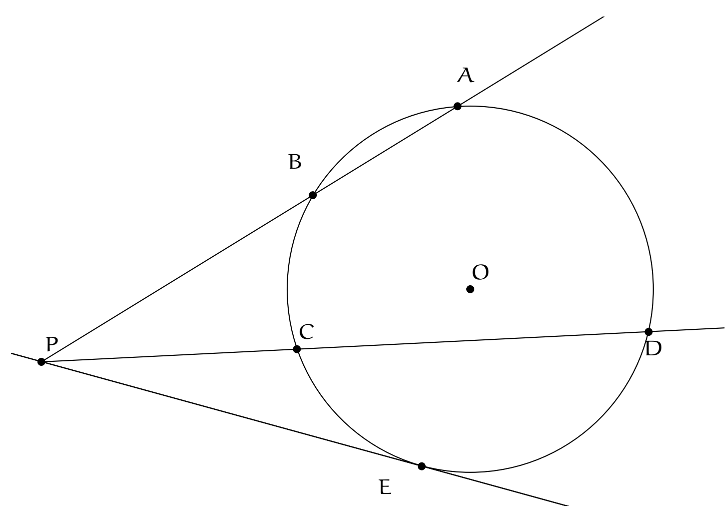
$$CE \leqslant CD + DE \implies AC \cdot BD \leqslant AB \cdot BD + AD \cdot BC.$$

Ensuite regardons le cas d'égalité. L'inégalité triangulaire est une égalité ssi les points C, D, E sont alignés, ie ssi

$$\widehat{CDA} = 180° - \widehat{ADE} = 180° - \widehat{ABC} \iff A, B, C, D \text{ cocycliques}.$$

Puissance d'un point par rapport à un cercle

Considérons un cercle Γ et un point P quelconque comme dans la figure suivante :



Proposition 7. $PA \cdot PB = PC \cdot PD = PE^2 = PO^2 - r^2$.

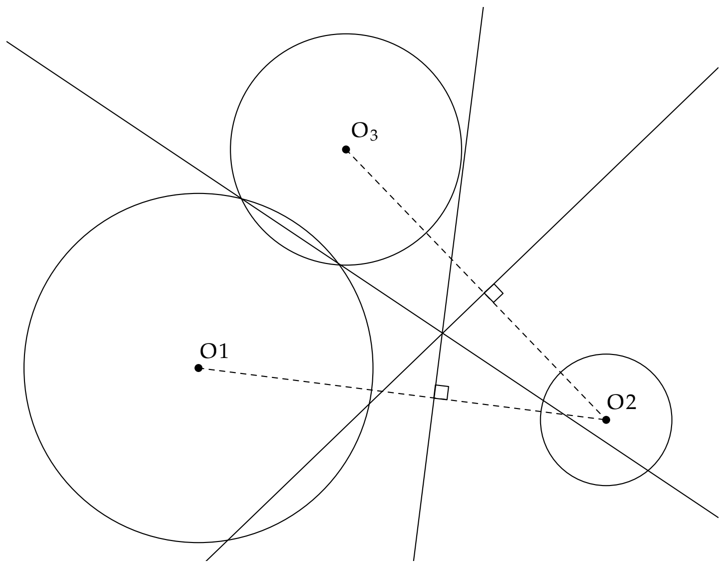
Démonstration Rappelez-vous que les triangles PAD et PCB sont semblables, donc $\frac{PA}{PC} = \frac{PD}{PB}$, ou encore $PA \cdot PB = PC \cdot PD$. Cette quantité ne dépend pas de quelle droite passant par P on utilise, si on utilise la tangente on trouve PE^2, si on utilise la droite passant par O on trouve $(PO - r)(PO + r) = PO^2 - r^2$.

Cette quantité est appelée la puissance du point P par rapport au cercle Γ, on la note $\mathcal{P}_\Gamma(P)$. Lorsqu'on calcule la puissance d'un point on considère des longueurs algébriques : $PA \cdot PB$

est positif si PA et PB sont dans le même sens (si P est à l'extérieur du cercle) et négatif s'ils sont dans des sens opposés (si P à l'intérieur).

Axe radical de deux cercles

Il est intéressant de savoir, si on se donne deux cercles Γ_1 et Γ_2, quel est le lieu des point squi ont la même puissance par rapport à Γ_1 et à Γ_2. Je laisse au lecteur le soin de vérifiér que ces points forment une droite Δ perpendiculaire à O_1O_2 appelée l'*axe radical* de Γ_1 et Γ_2.



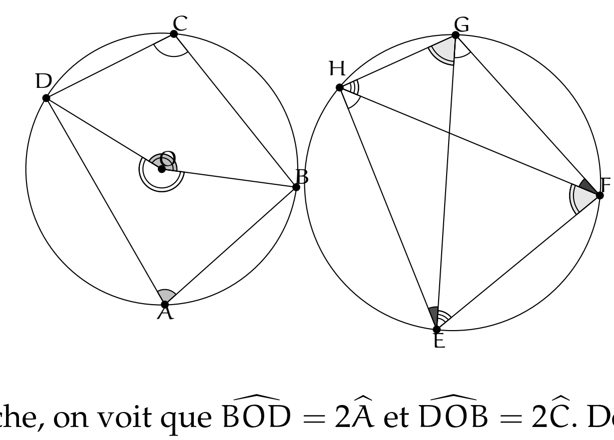
Proposition 8. Soient Γ_1, Γ_2 et Γ_3 trois cercles. Les axes radicaux Δ_{12}, Δ_{13} et Δ_{23} sont concourants.

Démonstration : Soit P le point d'intersection de Δ_{12} et Δ_{13}. Par définition, $\mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_2}(P)$ et $\mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_3}(P)$, donc $\mathcal{P}_{\Gamma_2}(P) = \mathcal{P}_{\Gamma_3}(P)$.

Exercice 5 Soient Γ_1 et Γ_2 deux cercles qui se coupent en A et B. On trace une tangente commune qui rencontre les cercles en C et D. Montrer que (AB) coupe $[CD]$ en son milieu.

Solutions des exercices

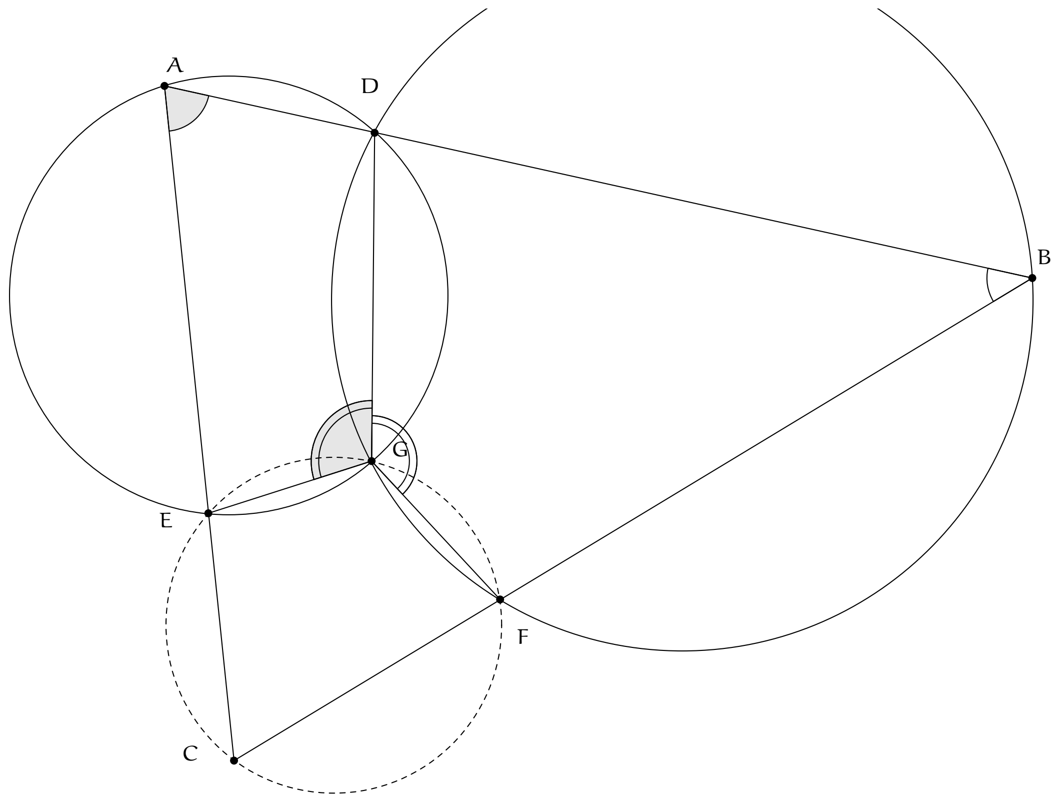
Solution de l'exercice 1 Nous allons exposer deux façons de résoudre ce problème.



Sur la figure de gauche, on voit que $\widehat{BOD} = 2\widehat{A}$ et $\widehat{DOB} = 2\widehat{C}$. Donc $\widehat{A} + \widehat{C} = \frac{\widehat{BOD}+\widehat{DOB}}{2} = 180°$.

Sur la figure de droite, on peut trouver quatre couples d'angles inscrits. Donc $\widehat{F} + \widehat{H} = \widehat{GHF} + \widehat{HFG} + \widehat{FGE} + \widehat{EGH} = 180°$ puisque ce sont tous les angles du triangle FGH.

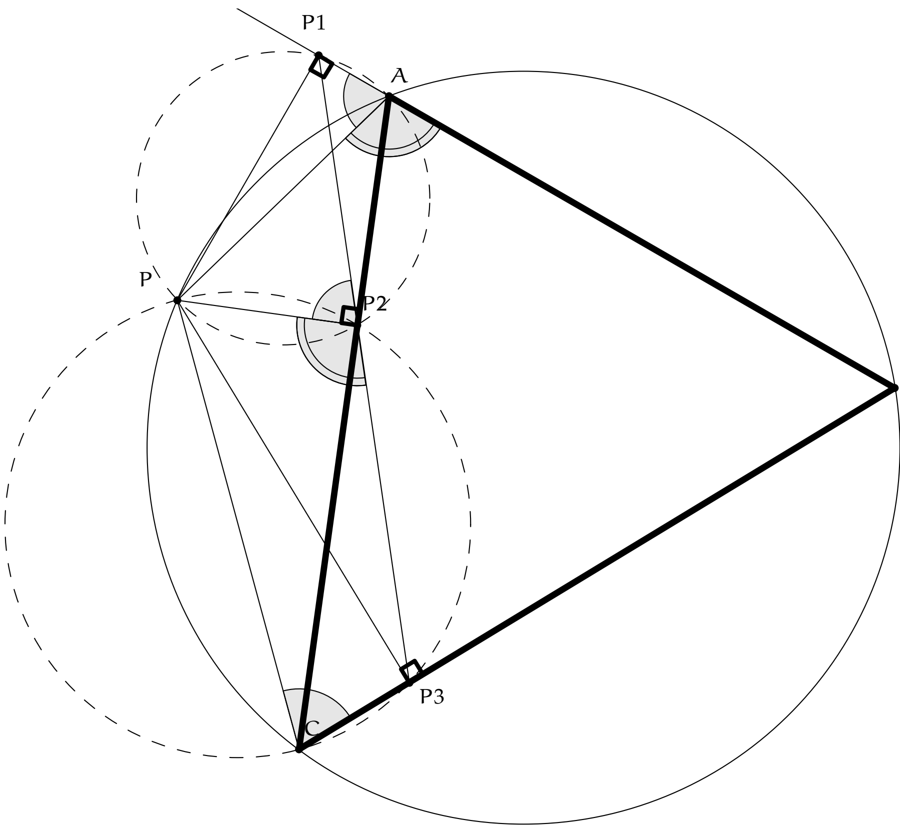
<u>*Solution de l'exercice 2*</u> Faisons la figure :



Définissons G l'intersection des cercles circonscrits à ADE et à BDF, et nous montrerons que G est sur le cercle circonscrit de CEF. Soient α, β et γ les trois angles de ABC. Comme A, D, G, E cocycliques, $\widehat{DGE} = 180° - \alpha$. De même, $\widehat{EGF} = 180° - \beta$. Donc $\widehat{FGD} = 360° - (180° - \alpha) - 180° - \beta)$ et donc $\widehat{FGD} + \gamma = 180°$. Les points C, D, G, F sont donc cocycliques.

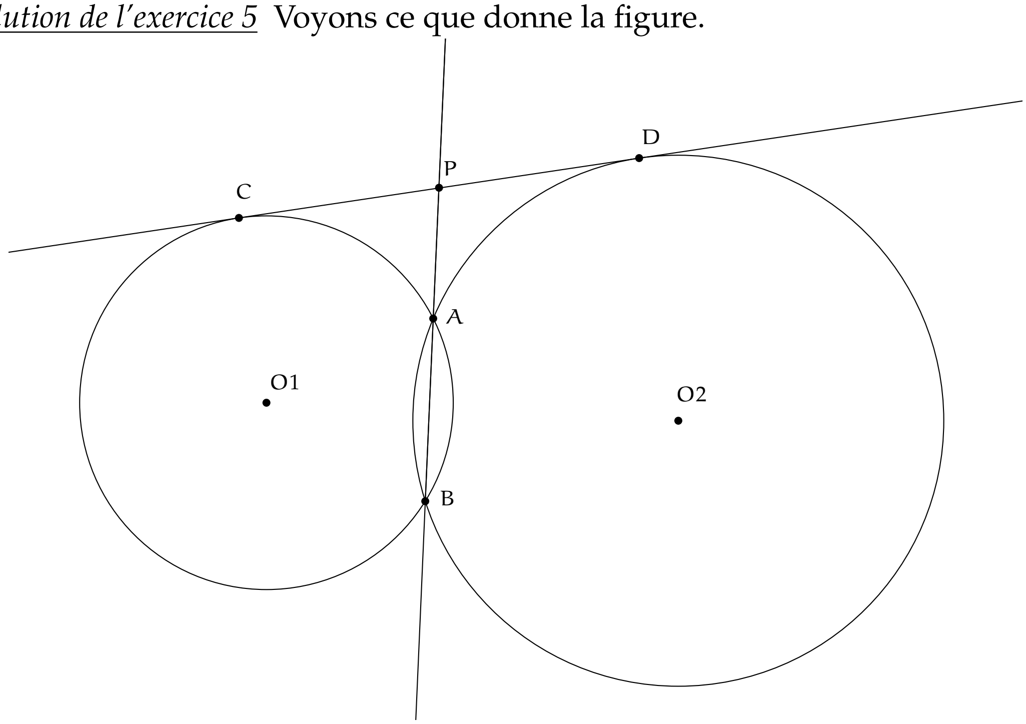
<u>*Solution de l'exercice 3*</u> Définissons G l'intersection des cercles circonscrits à ADE et à BDF, et nous montrerons que G est sur le cercle circonscrit de CEF. PSoient α, β et γ les trois angles de ABC. Comme A, D, G, E cocycliques, $\widehat{DGE} = 180° - \alpha$. De même, $\widehat{EGF} = 180° - \beta$. Donc $\widehat{FGD} = 360° - (180° - \alpha) - 180° - \beta)$ et donc $\widehat{FGD} + \gamma = 180\circ$. Les points C, D, G, F sont donc cocycliques.

<u>*Solution de l'exercice 4*</u> Commençons par faire la figure :



Comme il y a des angles droits en P_2 et P_1, le quadrilatère PP_1AP_2 est inscrit dans un cercle, donc $\widehat{P_1AP} = \widehat{P_1P_2P} = 180° - \widehat{PAB}$. Comme P est sur le cercle circonscrit de ABC, $\widehat{PCB} = 180° - \widehat{PAB} = \widehat{P_1P_2P}$. Enfin, comme P, P_2, P_3, C sont cocycliques, on a $\widehat{PP_2P_3} = 180° - \widehat{PCP_3} = 180° - \widehat{P_1P_2P}$. Donc $\widehat{P_1P_2P_3} = \widehat{P_1P_2P} + \widehat{PP_2P_3} = 180°$, les trois points sont alignés.

Solution de l'exercice 5 Voyons ce que donne la figure.



Comme A est sur l'intersection des deux cercles, il a une puissance nulle par rapport aux deux cercles, il est donc sur l'axe radical. De même pour B, donc AB est l'axe radical des deux cercles. Soit P le point d'intersection de (AB) avec $[CD]$.

$$PC^2 = \mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_1}(P) = PD^2.$$

2 Deuxième cours

- Énoncé des exercices vus en cours -

Exercice 1

Soit $ABCD$ un parallélogramme, O un point intérieur tel que $\widehat{AOB} + \widehat{COD} = 180°$. Montrer que $\widehat{OBC} = \widehat{ODC}$.

Exercice 2 (problème 2 de l'Olympiade Internationale 1997)

L'angle $\widehat{A}$ est le plus petit dans un triangle ABC. Les points B et C divisent le cercle circonscrit au triangle en deux arcs. Soit U un point intérieur à l'arc délimité par B et C qui ne contient pas A.

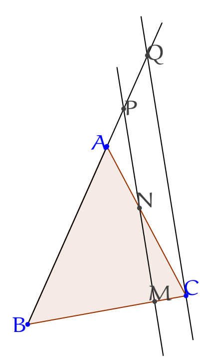
Les médiatrices des segments $[AB]$ et $[AC]$ rencontrent la droite (AU) respectivement en V et W. Les droites (BV) et (CW) se coupent au point T. Montrer que $AU = TB + TC$.

- Théorème de Ménélaüs -

Soit ABC un triangle, M, N, P trois points sur les côtés du triangle : $M \in (BC), N \in (CA), P \in (AB)$. M, N, P sont alignés si et seulement si : $\frac{\overline{MB}}{\overline{MC}} \times \frac{\overline{NC}}{\overline{NA}} \times \frac{\overline{PA}}{\overline{PB}} = 1$.

Remarquons d'abord que chacun des sommets du triangle doit apparaître une fois au numérateur et une fois au dénominateur. Comme M, B, C sont alignés, on peut faire le quotient des mesures algébriques, et ce quotient est indépendant du sens positif choisi sur la droite : $\frac{\overline{MC}}{\overline{MB}} < 0$ si M est entre B et C, > 0 sinon.

La démonstration peut se faire à l'aide du théorème de Thalès. Supposons les trois points alignés, et menons par C une parallèle à cette droite, qui coupe (AB) en Q. D'après Thalès, $\frac{\overline{MB}}{\overline{MC}} = \frac{\overline{PB}}{\overline{PQ}}$, et $\frac{\overline{NC}}{\overline{NA}} = \frac{\overline{PQ}}{\overline{PA}}$, donc : $\frac{\overline{MB}}{\overline{MC}} \times \frac{\overline{NC}}{\overline{NA}} \times \frac{\overline{PA}}{\overline{PB}} = \frac{\overline{PB}}{\overline{PQ}} \times \frac{\overline{PQ}}{\overline{PA}} \times \frac{\overline{PA}}{\overline{PB}} = 1$.



Pour prouver la réciproque, à savoir que si le produit vaut 1, les trois points sont alignés, supposons que le produit vaut 1 et considérons le point P', intersection de (MN) et (AB). D'après le théorème direct, $\frac{\overline{MB}}{\overline{MC}} \times \frac{\overline{NC}}{\overline{NA}} \times \frac{\overline{P'A}}{\overline{P'B}} = 1$ et d'après l'hypothèse, $\frac{\overline{MB}}{\overline{MC}} \times \frac{\overline{NC}}{\overline{NA}} \times \frac{\overline{PA}}{\overline{PB}} = 1$. On en déduit que $\frac{\overline{PA}}{\overline{PB}} = \frac{\overline{P'A}}{\overline{P'B}}$, ce qui n'est possible que si $P = P'$, donc si M, N, P sont alignés, car la fonction qui à un point P de la droite (AB) associe $\frac{\overline{PA}}{\overline{PB}}$ est monotone et bijective lorsque P parcourt la droite.

- Théorème de Céva -

L'énoncé du théorème de Céva ressemble au théorème de Ménélaüs, mais la démonstration est moins immédiate.

Soient M, N, P trois points des côtés $(BC), (CA), (AB)$ d'un triangle ABC. Les trois droites $(AM), (BN), (CP)$ sont concourantes si et seulement si $\frac{\overline{MB}}{\overline{MC}} \times \frac{\overline{NC}}{\overline{NA}} \times \frac{\overline{PA}}{\overline{PB}} = -1$.

Il s'agit du même produit que dans le théorème de Ménélaüs, chacun des points A, B, C apparaissant une fois au numérateur et une fois au dénominateur, mais ce produit est égal à -1 et non 1. Notamment, si les droites se coupent à l'intérieur du triangle, chacun des rapports $\frac{\overline{MB}}{\overline{MC}}, \frac{\overline{NC}}{\overline{NA}}, \frac{\overline{PA}}{\overline{PB}}$ est négatif, car M est entre B et C, N entre C et A et P entre A et B.

La démonstration la plus naturelle de ce théorème utilise la notion de "barycentre". Rappelons que sur une droite (AB), un point P est barycentre de A et B affectés de coefficients α et β si et seulement si : $\alpha.\vec{PA} + \beta.\vec{PB} = \vec{0}$, ce qui équivaut à $\frac{\overline{PA}}{\overline{PB}} = -\frac{\beta}{\alpha}$. Les coefficients sont donc définis à proportionnalité près.

Dans le plan, Q est barycentre de A, B, C affectés de coefficients α, β, γ si et seulement si : $\alpha.\vec{QA} + \beta.\vec{QB} + \gamma.\vec{QC} = \vec{0}$. Tout point Q du plan peut être défini comme barycentre de A, B et C affectés de bons coefficients (de somme non nulle) - qu'on appelle coordonnées barycentriques de Q -, et trois coefficients (de somme non nulle) définissent le point Q de manière unique car pour un point quelconque fixé O du plan, $\vec{OQ} = \frac{\alpha}{\alpha+\beta+\gamma}.\vec{OA} + \frac{\beta}{\alpha+\beta+\gamma}.\vec{OB} + \frac{\gamma}{\alpha+\beta+\gamma}.\vec{OC}$. L'étape importante, c'est la composition des barycentres : si P est barycentre de A et B affectés de coefficients α et β et Q barycentre de P et C affectés de coefficients λ et μ, Q est barycentre de A, B, C affectés de coefficients $\lambda\alpha, \lambda\beta, \mu(\alpha+\beta)$. Il en résulte notamment que si Q est barycentre de A, B, C affectés de coefficients α, β, γ et si les droites $(AQ), (BQ), (CQ)$ coupent respectivement $(BC), (CA), (AB)$ en M, N, P, M est barycentre de B, C affectés des coefficients β, γ, N de C, A affectés de γ, α et P de A, B affectés de α, β. Il est clair que ce résultat équivaut au théorème de Céva, dans le sens direct : soit Q de coordonnées barycentriques α, β, γ et M, N, P les intersections de $(AQ), (BQ), (CQ)$ avec $(BC), (CA), (AB)$ respectivement. Alors $\frac{\overline{MB}}{\overline{MC}} \times \frac{\overline{NC}}{\overline{NA}} \times \frac{\overline{PA}}{\overline{PB}} = \left(-\frac{\gamma}{\beta}\right)\left(-\frac{\alpha}{\gamma}\right)\left(-\frac{\beta}{\alpha}\right) = -1$. Réciproquement, si pour M, N, P le produit vaut -1, appelons Q l'intersection de (AM) et (BN), et P' l'intersection de (CQ) et (AB). P' vérifie, d'après le théorème direct, la même relation que P. Donc $\frac{\overline{P'A}}{\overline{P'B}} = \frac{\overline{PA}}{\overline{PB}}$ ce qui entraîne que $P' = P$, soit en définitive que $(AM), (BN)$ et (CP) sont concourantes.

Exercice 3

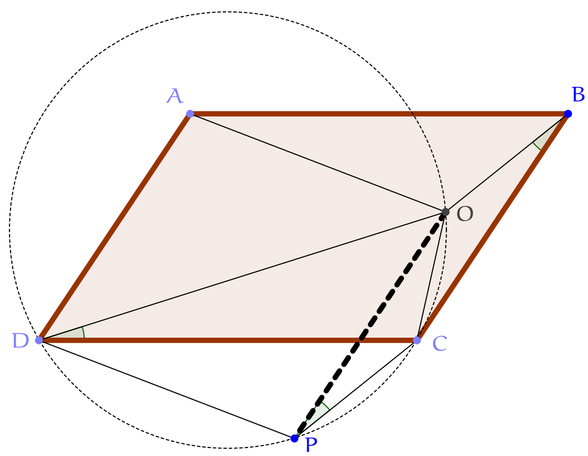
a) Soit ABC un triangle équilatéral, et M un point quelconque du plan. Montrer que $MA \leqslant MB + MC$. A quelle condition a-t-on l'égalité ?

b) Soit ABC un triangle quelconque, et M un point quelconque du plan. Montrer que $MA.BC \leqslant MB.CA + MC.AB$. A quelle condition a-t-on l'égalité ?

- Solution des exercices -

Solution de l'exercice 1

Pour bien utiliser la relation de l'énoncé, il faut y voir deux angles inscrits de part et d'autre de (CD). Mais pour ce faire, il faut translater le point O d'un vecteur $\vec{BC}$: considérons donc le point P tel que $OPCB$ soit un parallélogramme. Le triangle PDC est translaté, donc isométrique, du triangle OAB. Les angles $\widehat{DPC}$ et $\widehat{COD}$ sont supplémentaires, de part et d'autre de (CD), donc les quatre points C, D, O, P sont cocycliques. On en déduit que les angles inscrits $\widehat{ODC}$ et $\widehat{OPC}$ sont égaux. Or dans le parallélogramme $OPCD$, $\widehat{OPC} = \widehat{OBC}$, d'où le résultat.

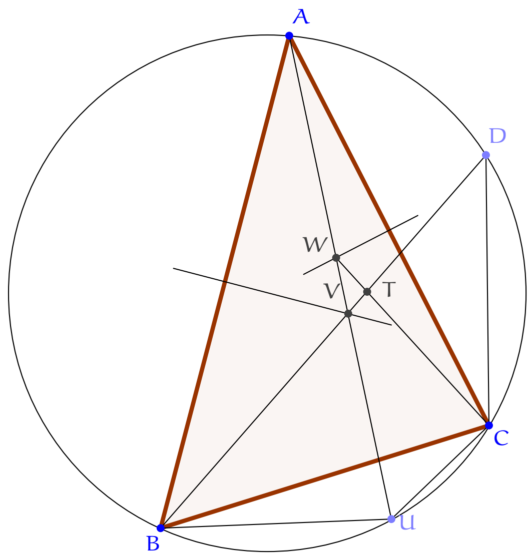


On notera qu'il est difficile de faire une figure juste en se basant sur la seule hypothèse, car peu de points O vérifient cette hypothèse. Mais on peut s'aider de la conclusion, donc tracer des angles $\widehat{ODC}$ et $\widehat{OBC}$ égaux pour construire une figure juste.

Solution de l'exercice 2

Comme dans beaucoup de problèmes, il faut faire apparaître sur la figure un élément supplémentaire, en l'occurrence un point, qui permette de mieux tirer profit de la relation $AU = TB + TC$. Il faudrait un point D sur (TB) tel que $TD = TC$ (T étant entre C et D) et $AD = AU$. Il se trouve que ce point D est sur le cercle circonscrit à ABC.

La droite (BT) recoupe le cercle en D. La symétrie par rapport à la médiatrice de $[AB]$ transforme A en B, V en lui-même, donc (AU) en (BD), et elle transforme le cercle en lui-même car la médiatrice d'une corde $[AB]$ passe nécessairement par le centre du cercle. Donc elle transforme U en D, ce qui entraîne : $AU = BD$. Reste à prouver que $TD = TC$. L'angle inscrit $\widehat{BDC} = \widehat{BAC}$. Or W étant sur la médiatrice de $[AC]$, le triangle WAC est isocèle : $\widehat{TCA} = \widehat{WAC}$. Et $\widehat{ACD} = \widehat{ABD} = \widehat{BAV}$ car le triangle VAB est lui aussi isocèle. Donc en additionnant, $\widehat{TCD} = \widehat{BAC} = \widehat{TDC}$: le triangle TCD est isocèle, ce qui entraîne $TD = TC$. D'où $TB + TC = BD = AU$.



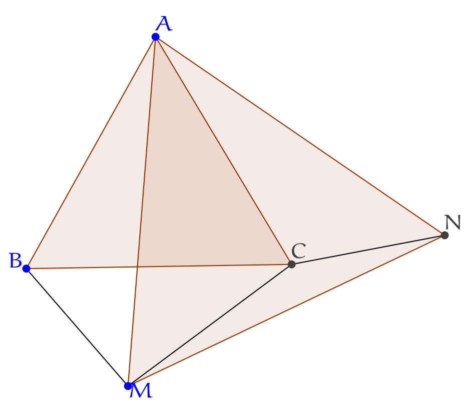
On pouvait s'en sortir sans faire apparaître ce point D, en étudiant soigneusement les angles et les côtés du triangle TBC. Appelons ϕ l'angle $\widehat{ABU}$, donc $\pi - \phi$ l'angle $\widehat{ACU}$, et α l'angle $\widehat{BAC}$. $\widehat{ABV} = \widehat{BAV}$ et $\widehat{UBC} = \widehat{UAC}$, donc $\widehat{TBC} = \phi - \alpha$. De même, $\widehat{WCA} = \widehat{WAC}$, $\widehat{UCB} = \widehat{UAB}$ donc $\widehat{TCB} = \pi - \phi - \alpha$. Il en résulte que $\widehat{BTC} = 2\alpha$. D'où $\frac{TB}{\sin(\pi-\phi-\alpha)} = \frac{TC}{\sin(\phi-\alpha)} = \frac{BC}{\sin 2\alpha} = \frac{R}{\cos\alpha}$ car si l'on appelle R le rayon du cercle circonscrit, dans le triangle ABC, $BC = 2R\sin\alpha$. D'où :

$$TB + TC = \frac{R}{\cos\alpha}\left(\sin(\phi+\alpha) + \sin(\phi-\alpha)\right) = 2R\sin\phi$$

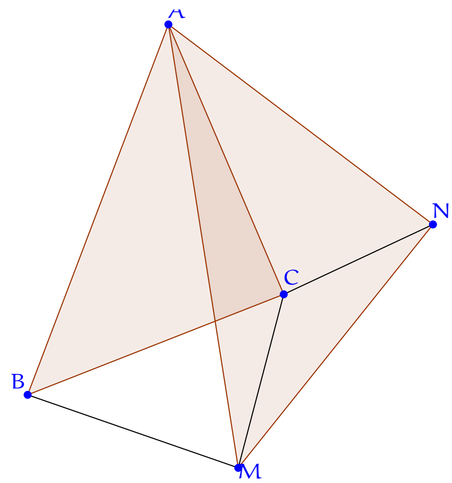
ce qui est bien égal à AU.

<u>*Solution de l'exercice 3*</u>

Dans le cas du triangle équilatéral : la rotation de centre A et d'angle 60° qui envoie B en C envoie M en un point N tel que le triangle AMN soit équilatéral. On a donc $MB = NC$ et $AM = NM$: l'inégalité à démontrer équivaut donc à l'inégalité triangulaire $NM \leqslant NC + CM$. Il y a égalité lorsque M, N, C sont alignés (C entre M et N), donc lorsque l'angle $\widehat{ACM}$ et l'angle $\widehat{ACN} = \widehat{ABM}$ sont supplémentaires, ce qui équivaut à : A, B, M, C sur un même cercle, avec B et C de part et d'autre de (AM), donc M appartient au cercle circonscrit à ABC, et plus précisément à l'arc BC ne contenant pas le point A.



Dans le cas du triangle quelconque, la démonstration est similaire. Ce n'est plus une rotation de centre A qui transforme B en C, mais une similitude, composée d'une rotation et d'une homothétie. Soit N le transformé de M par cette similitude. L'important est que les triangles ABM et ACN sont semblables, donc $\frac{MB}{AB} = \frac{NC}{AC}$, et les triangles ABC et AMN sont eux aussi semblables, donc $\frac{MA}{MN} = \frac{AB}{BC}$. L'inégalité triangulaire $NM \leqslant NC + CM$ s'écrit donc : $\frac{MA.BC}{AB} \leqslant \frac{MB.AC}{AB} + MC$, ce qui équivaut à la relation de l'énoncé. Une fois encore, l'égalité a lieu lorsque les points sont alignés dans le bon ordre, donc $\widehat{ACM}$ et $\widehat{ACN} = \widehat{ABM}$ supplémentaires, c'est-à-dire lorsque M est sur le cercle circonscrit à ABC, plus précisément sur l'arc BC ne contenant pas le point A. C'est le théorème de Ptolémée : dans un quadrilatère convexe inscriptible, la produit des diagonales est égal à la somme des produits des côtés opposés.



3 Premier TD

- Énoncés-

Exercice 1 Soit ABC un triangle. Montrer que l'intersection de la bissectrice issue de $\widehat{B}$ et de la médiatrice de $[AC]$ appartient au cercle circonscrit de ABC.

Exercice 2 Soit ABC un triangle aux angles aigus d'orthocentre H. Montrer que les symétriques de H par rapport aux côtés du triangle appartiennent à son cercle circonscrit.

Exercice 3 On considère deux cercles tangents intérieurement en un point C et une corde $[AB]$ du grand cercle tangente au petit cercle en E. Montrer que la droite (CE) est la bissectrice de l'angle $\widehat{ACB}$.

Exercice 4 (Olympiades Balkaniques de Mathématiques 2012, exercice 1) Soient A, B, C trois points d'un cercle Γ de centre O. On suppose que $\widehat{ABC} > 90°$. Soit D l'intersection de la droite (AB) avec la perpendiculaire à (AC) passant par C. Soit l la droite passant par D perpendiculaire à (AO). Soit E l'intersection de la droite l avec (AC), et soit F l'intersection de Γ et de de l qui se situe entre D et E.

Prouver que les cercles circonscrits des triangles BFE et CFD sont tangents en F.

Exercice 5 Soient Γ_1, Γ_2 deux cercles qui se coupent en A et en B. Soit Δ une droite tangente aux deux cercles en M et en N. Montrer que (AB) coupe le segment $[MN]$ en son milieu.

Exercice 6 Soient $ABCD$ et $CDEF$ deux quadrilatères inscrits dans deux cercles Γ_1, Γ_2. On suppose que parmi les droites (AB), (CD) et (EF) il n'y en a pas deux qui soient parallèles. Alors les droites (AB), (CD) et (EF) sont concourantes si, et seulement si, les points A, B, E et F sont cocycliques.

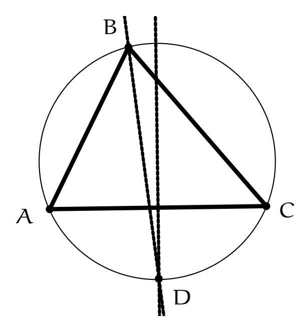
Exercice 7 Soit ABC un triangle, H son orthocentre. Soient M un point de $[AB]$ et N un point de $[AC]$. Les cercles de diamètre BN et CM se coupent en P et Q. Montrer que P, Q et H sont alignés.

Exercice 8 (Olympiades internationales de Mathématiques 2000, Exercice 1) Soient Ω_1 et Ω_2 deux cercles qui se coupent en M et en N. Soit Δ la tangente commune aux deux cercles, qui est plus proche de M que de N. Δ est tangente à Ω_1 en A et à Ω_2 en B. La droite passant par M et parallèle à Δ rencontre Ω_1 en C et Ω_2 en D. Soient E l'intersection des droites (CA) et (BD), P le point d'intersection de droites (AN) et (CD) et Q le point d'intersection des droites (BN) et (CD). Montrer que $EP = EQ$.

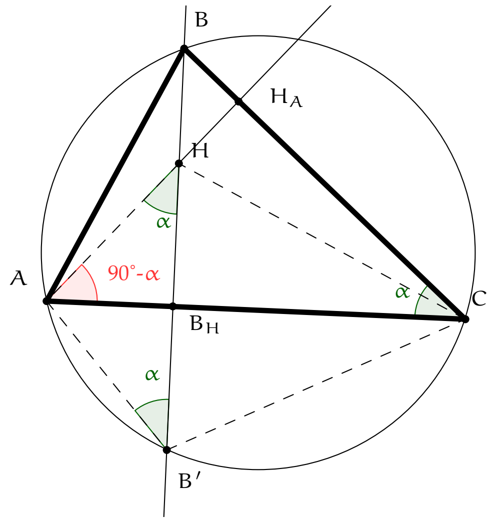
Exercice 9 Soit ABC un triangle acutangle. On note respectivement D, E, F les pieds des hauteurs sur les côtés $[BC], [CA], [AB]$. Soit P un point d'intersection de (EF) avec le cercle circonscrit à ABC. Soit Q le point d'intersection des droites (BP) et (DF). Montrer que $AP = AQ$.

- Corrigé-

<u>*Solution de l'exercice 1*</u> Notons D l'intersection de la bissectrice issue de l'angle $\widehat{B}$ et du cercle circonscrit de ABC. Il faut et il suffit de montrer que D appartient à la médiatrice de $[AC]$. Comme les angles $\widehat{ABD}$ et $\widehat{DBC}$ sont égaux, ceci implique que les longueurs des arcs AD et DC sont égales, et donc que D appartient à la médiatrice de $[AC]$.



<u>*Solution de l'exercice 2*</u> Notons B_H le pied de la hauteur issue de B, B' son intersection avec le cercle circonscrit à ABC et A_H le pied de la hauteur issue de A (voir figure).



Il suffit de montrer que les angles $\widehat{AB'B_H}$ et $\widehat{AHB_H}$ sont égaux. En effet, dans ce cas, les triangles rectangles HAB_H et B_HAB' auraient trois angles identiques et un angle en commun et seraient donc alors égaux. Ceci implique $B'B_H = B_HH$ et donc que B' est le symétrique de H par rapport au côté (AC).

Montrons donc que $\widehat{AB'B_H} = \widehat{AHB_H}$. Notons $\alpha = \widehat{AB'B_H}$. Comme les angles $\widehat{AB'B_H}$ et $\widehat{ACB}$ interceptent le même arc, ils sont égaux. On en déduit que $\widehat{ACB} = \alpha$, puis $\widehat{H_AAC} = 90° - \alpha$ car AH_AC est rectangle en H_A. Mais alors, puisque AHB_H est rectangle en B_H, $\widehat{AHB_H} = 90° - \widehat{HAB_H} = \alpha$, ce qu'on voulait montrer.

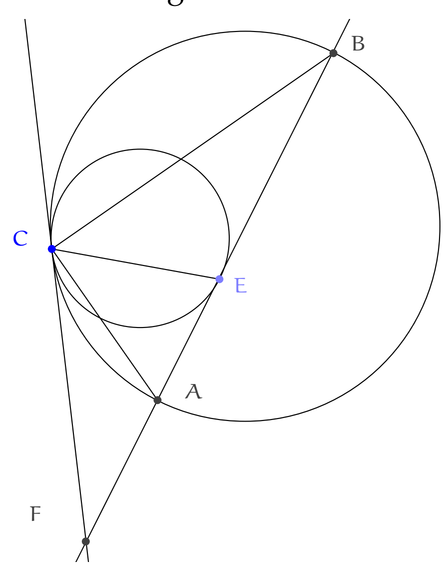
On démontre de même que les symétriques de H par rapport aux autres côtés appartiennent au cercle circonscrit.

Solution de l'exercice 3

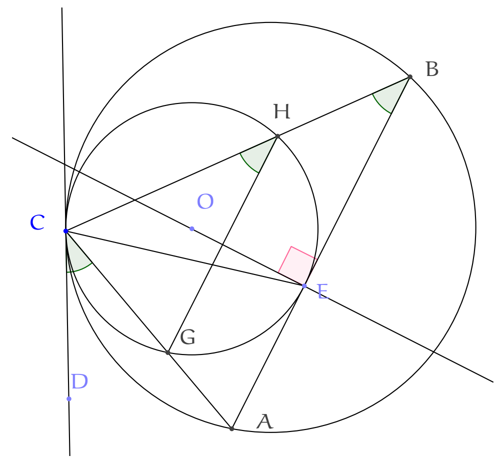
- (Première solution) Soit F le point d'intersection de la corde (AB) avec la tangente commune. Les triangles FAC et FCB sont semblables et $FC = FE$. Par suite :

$$\frac{CA}{CB} = \frac{FE}{FB} = \frac{FA}{FE} = \frac{FE - FA}{FB - FE} = \frac{AE}{EB},$$

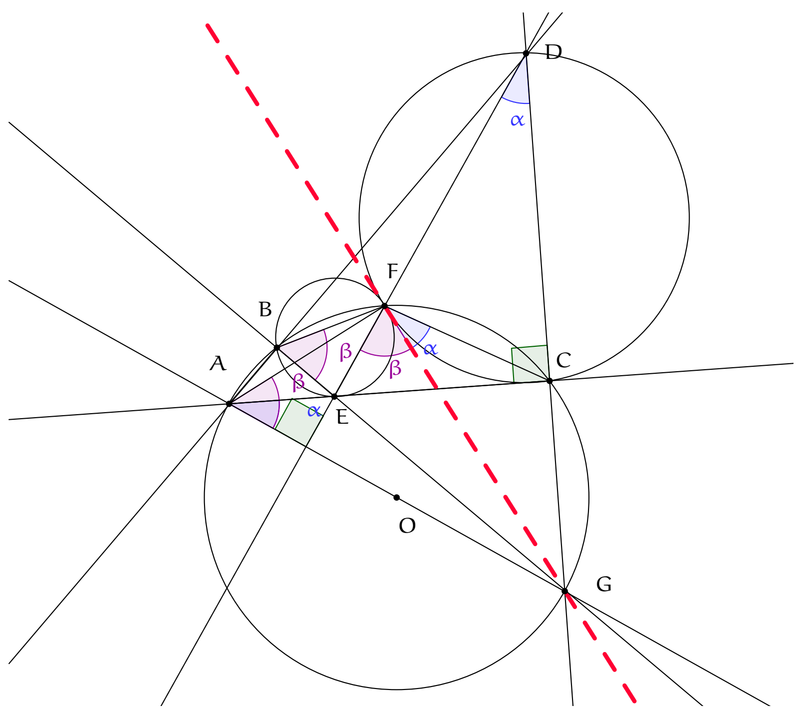
  et la droite (CE) est la bissectrice de l'angle $\widehat{ACB}$.



- (Deuxième solution) Notons O le centre du petit cercle et soient G, H les points d'intersection de respectivement (CB) et (CA) avec le petit cercle. On introduit le point D comme sur la figure. On commence par faire une petite chasse aux angles pour montrer que (AB) et (GH) sont parallèles. On a $\widehat{ABC} = \widehat{ACD} = \widehat{GHC}$. Donc (AB) et (GH) sont parallèles. Or (OE) et (AB) sont perpendiculaires. Donc (OE) et (GH) sont perpendiculaires. Donc (OE) est la médiatrice de $[GH]$. Donc, d'après le premier exercice, (CE) est la bissectrice de $\widehat{ACB}$.



<u>*Solution de l'exercice 4*</u> On commence par faire une figure soignée :



Cette figure suggère que les les droites (AO), (BE), la tangente commune cherchée et (DC) vont être concourantes. Notons ainsi G le point diamétralement opposé à A sur Γ.

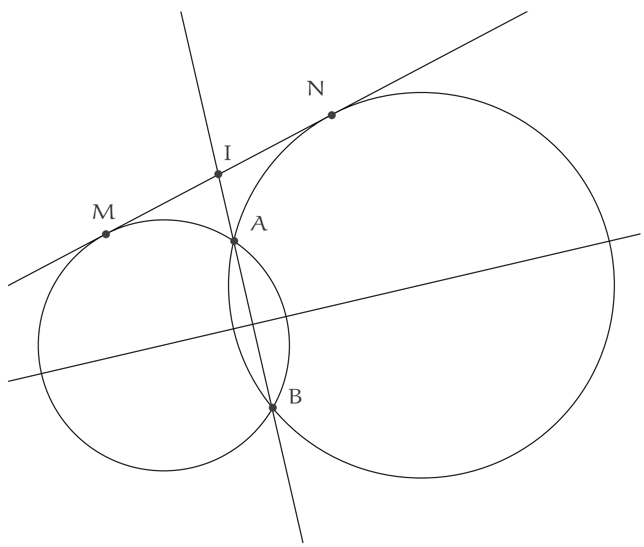
Première étape : (DC) passe par G. En effet, $[AG]$ étant un diamètre de Γ, ACG est rectangle en C, ce qui implique que les droites (DC) et (CG) sont les mêmes.

Deuxième étape : prouvons que (BE) passe par G. Pour cela, on remarque que E est l'orthocentre de ADG car E est l'intersection des deux hauteurs (AC) et (DE). Or ABG est rectangle en B, car $[AG]$ est un diamètre de Γ, ce qui implique que (BG) et (AD) sont perpendiculaires. Donc (BG) est la hauteur issue de G dans ADG, et donc l'orthocentre E appartient à (BG).

Troisième étape : posons $\alpha = \widehat{EDG}$. Pour montrer que (FG) est tangente au cercle circonscrit de FDC, montrons que $\widehat{GFC} = \alpha$. On a $\widehat{DEC} = 90° - \alpha$. Les droites (DE) et (AG) étant perpendiculaires, on en déduit que $\widehat{EAG} = \alpha$. Finalement, par cocyclicité de A,F,C,G, on en déduit que $\widehat{GFC} = \alpha$.

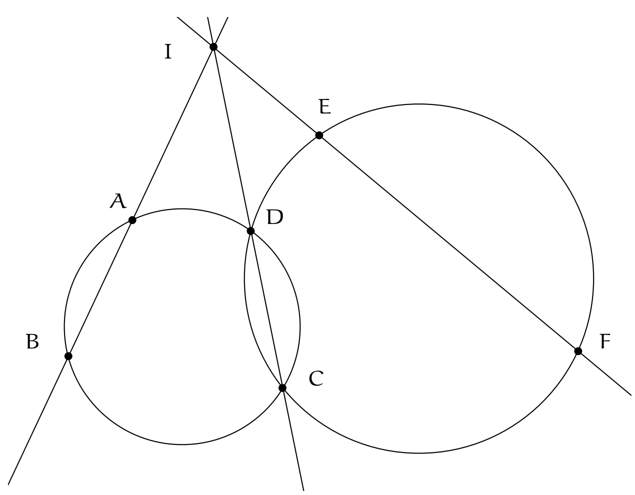
Posons $\beta = \widehat{EBF}$. Pour montrer que (FG) est tangente au cercle circonscrit de BEF, montrons que $\widehat{EFG} = \beta$. Par cocyclicité de A, B, F, G, on a $\widehat{FAG} = \beta$. Puis, en utilisant deux triangles rectangles, il vient $\widehat{AFE} = 90 - \beta$, puis $\widehat{EFG} = \beta$, ce qui conclut l'exercice.

Solution de l'exercice 5



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

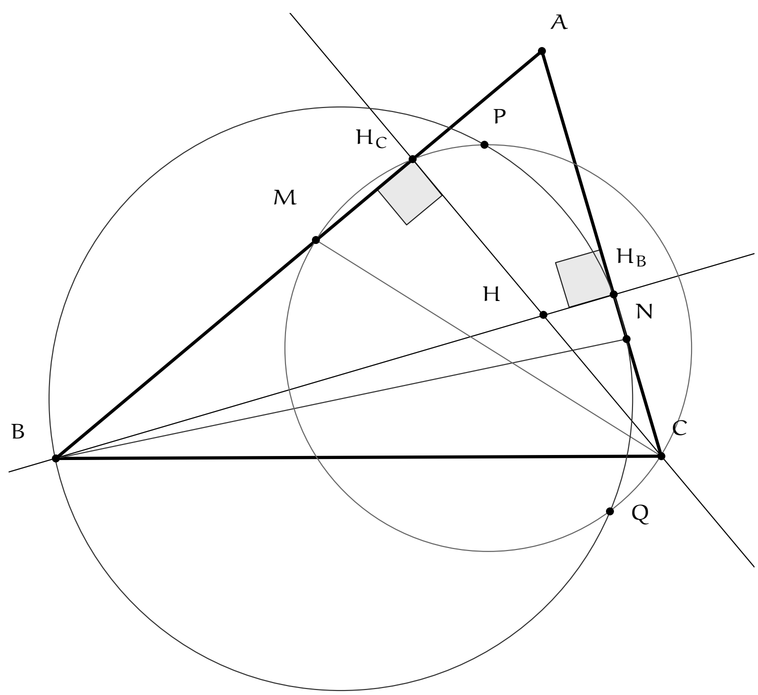
Solution de l'exercice 6



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

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

Solution de l'exercice 7

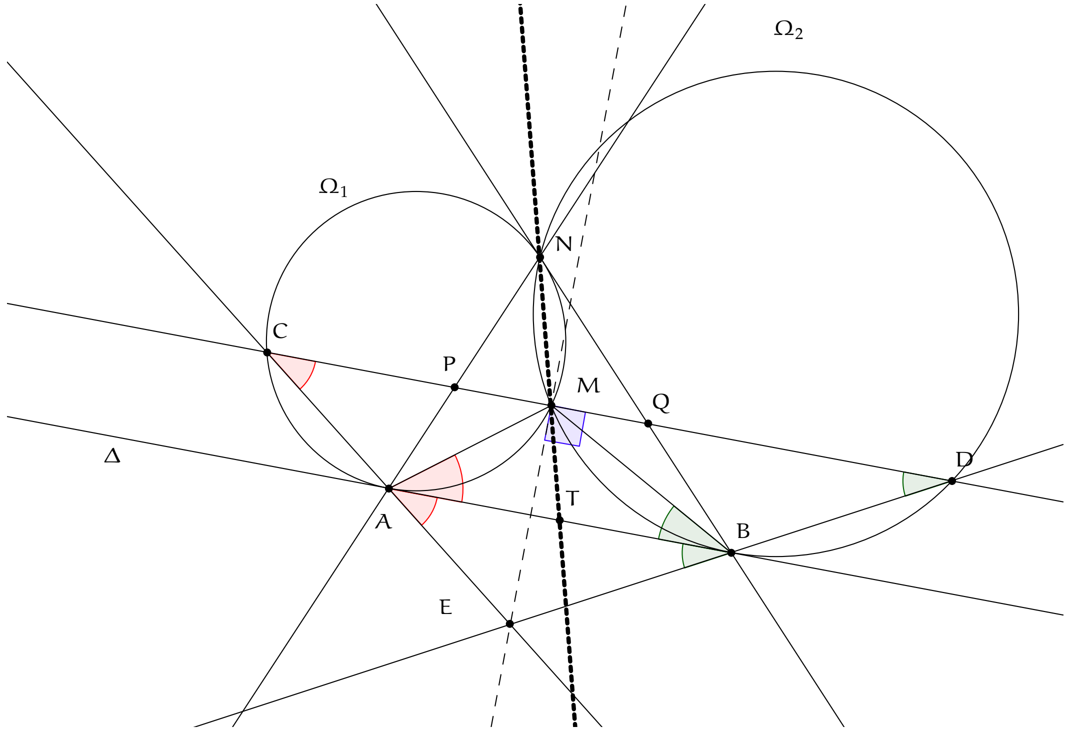


Nous allons montrer que H a la même puissance par rapport aux deux cercles de la figure, ce qui impliquera que H est sur leur axe radical, qui est (PQ).

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

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

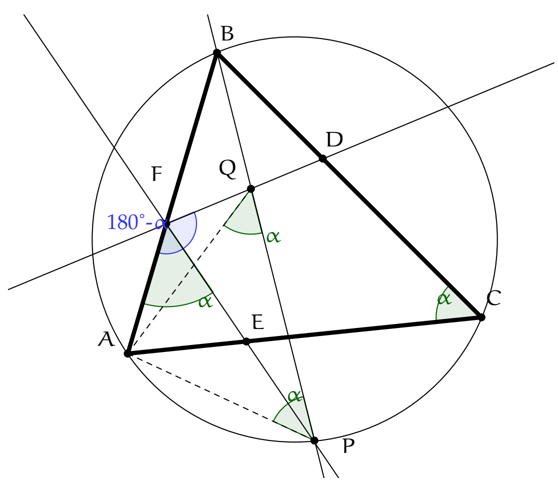
Solution de l'exercice 8



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

Il faut également savoir reconnaître les situations classiques : ici, en notant T l'intersection des droites (MN) et (AB), il faut savoir que $TA = TB$ (voir exercice 5). Le théorème de Thalès montre alors que M est le milieu de $[PQ]$. En somme, (ME) est la médiatrice de $[PQ]$. E est donc bien équidistant de P et de Q.

Solution de l'exercice 9



Posons $\alpha = \widehat{APB}$. Par cocyclicité des points A, B, C, P, on a $\widehat{BCA} = \alpha$. Comme (AD) et (CF) sont des hauteurs, les points A, C, D, F sont cocycliques et donc $\widehat{AFD} = 180° - \alpha$. Donc $\widehat{AFD} + \widehat{APQ} = 180°$, ce qui implique que les points A, P, Q, F sont cocycliques.

On continue la chasse aux angles : $\widehat{AFE} = \widehat{BFD} = \widehat{BCA} = \alpha$ (pourquoi ?), et donc $\widehat{AQP} = \widehat{AFP} = \widehat{BCA}$. Le triangle APQ est donc isocèle, ce qui implique $AP = AQ$.

4 Deuxième TD

- Énoncés -

Exercice 1 Démontrer que le centre du cercle circonscrit 0, le centre de gravité G et l'orthocentre H d'un triangle ABC quelconque sont colinéaires et que $OG = \frac{1}{2}GH$.

Exercice 2 Étant donnés le point A, le centre du cercle circonscrit O et l'orthocentre H d'un triangle ABC, contruire à la règle et au compas les points Bet C.

Exercice 3 Soient A, B et C trois points sur le cercle Γ de centre O. On suppose $\widehat{ABC} > 90$. Soit D le point d'intersection de la droite AB avec la perpendiculaire en C à AC. Soit ℓ la droite passant par D perpendiculaire à AO. Soit E le point d'intersection de ℓ avec la droite AC, et soit F le point d'intersection de Γ avec ℓ, situé entre D et E. Montrer que les cercles circonscrits à BFE et CFD sont tangents en F.

Exercice 4 Les cercles k_1 et k_2 se rencontrent en A et B. La droite t est tengente à k_1 et k_2 en M et respectivement N. Sachant que $t \perp AM$ et $MN = 2AM$, calculer la mesure de $\widehat{NMB}$.

Exercice 5 Soient B, D et C trois points fixes situés sur une droite de façon que $D \in [BC]$. Soient A un point mobile en dehors de la droite BC et P un point mobile sur $[AD]$. On note E, F et D' les trois points tels que $\{E\} = AC \bigcap BP$, $\{F\} = AB \bigcap CP$ et $\{D'\} = FE \bigcap BC$. Montrer que D' est fixe.

Exercice 6 Soit $ABCD$ un trapèse avec $AB \parallel DC$. On note Y l'intersection de AD et BC. On appelle X l'intersection des diagonales, N le milieu de $[AB]$ et M celui de $[DC]$. Montrer que M, N, X et Y sont colinéaires.

Exercice 7 Les diagonales d'un trapèse $ABCD$, avec $BC \parallel AD$, s'intersectent en P. Soit Q tel que $\widehat{AQD} = \widehat{CQB}$ et la droite CD sépare P et Q. Montrer que $\widehat{BQP} = \widehat{DAQ}$.

Exercice 8 Soient BD et CE les hauteurs du triangle ABC. Montrer que si $AB \geqslant AC$ alors $AB + CE \geqslant AC + BD$.

Exercice 9 Soient ABC un triangle et P un point intérieur et D, E, F les pieds des perpendiculaires de P sur BC, CA et AB. On suppose que $PA^2 + PD^2 = PB^2 + PE^2 = PC^2 + PF^2$. Montrer que P est le centre du cercle circonscrit au triangle $I_aI_bI_c$, où I_a, I_b et I_c sont les centres des cercles exinscrits au triangle ABC.

Exercice 10 Les points O et H sont le centre du cercle circonscrit et l'orthocentre du triangle ABC. Montrer qu'un des triangles OHA, OHB et OHC a l'aire égale à la somme des deux autres.

Exercice 11 On note O, H et R le centre du cercle circonscrit, l'orthocentre et le rayon du cercle circonscrit du triangle ABC. On note D, E et F les symétriques de A,B et C par rapport au droites BC, CA et respectivement AB. On suppose que D, E et F sont colinéaires. Montrer que $OH = 2R$.

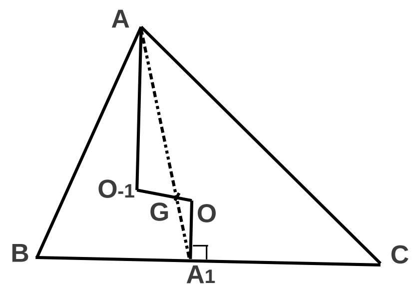


FIGURE 1 – Droite d'Euler.

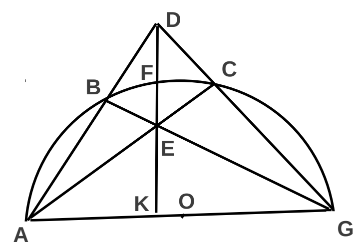


FIGURE 2 – Figure de l'exercice 3

- Corrigé -

Solution de l'exercice 1

On appelle A_1, B_1 et C_1 les pieds des médianes partant de A, B et respectivement C. On appelle h l'homothétie de centre G et de rapport $-\frac{1}{2}$. On appelle O_{-1} le point $h^{-1}(O)$, comme dans la figure 1, et on voit qu'il suffit de montrer $O_{-1} = H$. Une des propriétés des homothéties montre que

$$h(A)h(O_{-1}) \parallel AO_{-1}. \tag{II.1}$$

Or, il est connu que G est situé à un tiers de longueur de A_1 et 2 de A, donc $A_1 = h(A)$. Ainsi, on a :

$$A_1O \parallel AO_{-1}. \tag{II.2}$$

Comme A_1O est la médiatrice du segment BC, $A_10 \perp BC$ et, par conséquent, $AO_{-1} \perp BC$. De manière analogue, $BO_{-1} \perp AC$, donc O_{-1} appartient à deux hauteurs du triangles. Ainsi $O_{-1} = H$.

Solution de l'exercice 2 On s'inspire de la Figure 1. On commence par trouver G à deux tiers de H et un de O. Ensuite on construit A_1 comme image de A par l'homothétie de centre G et rapport $\frac{1}{2}$. La droite passant par A_1 et perpendiculaire à OA_1 est la droite BC. On obtient les deux points à l'intersection de cette droite avec le cercle de centre O et rayon OA.

Solution de l'exercice 3 On note G l'intersection de AO avec Γ et K l'intersection de ℓ avec AO. L'idée est de montrer $\widehat{GFC} = \widehat{FDC}$, ce qui montrera que FG est la tangente en F au cercle circonscrit au triangle CFD, puis de faire de même pour le triangle BFE.

Comme $\widehat{ACG} = 90°$, D, C et G sont colinéaires. Ainsi, E est l'orthocentre du triangle ADG, donc $GE \perp AB$. Comme le quadrilatère $AGCB$ est inscrit dans un cercle, $\widehat{ABG} = \widehat{ACG}$, donc $EB \perp AB$. Ainsi, B, E et G sont colinéaires.

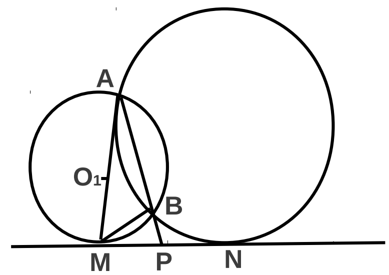


FIGURE 3 – Figure de l'exercice 4.

Puisque $\widehat{CDF} = \widehat{GDK} = \widehat{GAC} = \widehat{GFC}$, FG est tangent en F au cercle circonscrit au triangle CFD. Puisque $\widehat{FBE} = \widehat{FBG} = \widehat{FAG} = \widehat{GFE}$, FG est tangente en F au triangle BFE.

Solution de l'exercice 4 On appelle P le milieu de $[MN]$. Puisque P a des puissances égales par rapport aux cercles k_1 et k_2, il appartient à la droite radicale, donc à AB. Comme t est tangente à k_1, $\widehat{NMB} = \widehat{MAB}$, qui vaut $\widehat{MAP}$ car A, B et P sont colinéaires. Comme le triangle MAP est rectangle isocèle, on a $\widehat{MAP} = 45°$.

Solution de l'exercice 5 Il suffit d'appliquer le Théorème de Ceva dans $\triangle ABC$ et le Théorème de Ménélaüs à $\triangle ABC$ avec la sécante EF.

Solution de l'exercice 6 Si on note N' l'intersection de YM avec AB, alors le Théorème de Thalès implique que $N = N'$. Ensuite de Théorème de Ceva montre que Y, X et M sont alignés.

Solution de l'exercice 7 On trace la parallèle passant par D à BQ et on note D' son intersection avec PQ. Comme $Q'D$ est parallèle à BQ et comme AD est parallèle à BC, $\widehat{CBQ} = \widehat{D'DA}$. Puisque $D'D \parallel QB$, $\triangle PD'D \simeq \triangle PBQ$, d'où $\frac{AD}{BC} = \frac{DD'}{BQ}$. Ainsi on a $\triangle CBQ \simeq \triangle ADD'$ par similarité de type côté-angle-côté.

Cela implique que $\widehat{CQB} = \widehat{DD'A}$, et comme $\widehat{CQB} = \widehat{AQD}$, $\widehat{DD'A} = \widehat{AQD}$, impliquant que $D'ADQ$ est cyclique. Cela implique $\widehat{QAD} = \widehat{QD'D}$, et $\widehat{QD'D} = \widehat{BQD'}$ car $BQ \parallel D'D$, d'où $\widehat{QAD} = \widehat{BQD'} = \widehat{BQP}$.

Solution de l'exercice 8 On note S l'aire du triangle ABC. On a $BD = \frac{2S}{AC}$ et $CE = \frac{2S}{AB}$. Ainsi $(AB+CE)-(AC+BD) = (AB+\frac{2S}{AB})-(AC+\frac{2S}{AC})$. Ensuite, cela vaut $(AB-AC) = (1-\frac{2S}{AB\cdot AC}) = (AB-AC)(1-\sin\widehat{A}) \geqslant 0$.

Solution de l'exercice 9 Comme le problème fait intervenir les cercles exinscrits il faut se souvenir de leurs propriétés. La plus importante est que si on note D' le pied de la perpendiculaire de I_a sur BC, alors $BD' = \frac{a+b-c}{2}$ et les égalités analogues, où a, b, c désignent les longueurs des côtés du triangle ABC. Pour montrer cela, on note D_b et D_c les pieds des perpendiculaires de I_a sur AC et AB. Comme BI_a est bissectrice, $BD = BD_b$. Similairement, $CD = CD_c$. Or, $\triangle AD_bI_a \equiv \triangle AD_cI_a$, donc $BD_b + AB = CF_c + AB$. Ainsi $BD + AB = DC + AC$. Comme $BD + DC = BC$ on trouve $BD = \frac{a+b-c}{2}$.

Revenons au problème. On a $(AE^2+PE^2)+PD^2 = PA^2+PE^2 = PB^2+PE^2 = (BD^2+PD^2)+PE^2$. Donc $AE = BD$ et les égalités analogues. Si on note $AE = u$, $BF = v$ et $CD = w$, alors on a : $a = u+w$, $b = v+w$ et $c = u+v$. En résolvant le système on a $BD = \frac{a+b-c}{2}$, donc D est égal à D', le pied de la perpendiculaire de I_a sur BC. De manière analogue E et F sont les pieds des perpendiculaires de I_b et I_c sur les côtés de ABC. On conclut que les perpendiculaires de I_a, I_b et I_c sur les côtés correspondantes de ABC sont concourantes.

On a $m((\widehat{BI_aP}) = m(\widehat{BI_aD}) = 90 - m(\widehat{I_aBC}) = \frac{1}{2}m(\widehat{B})$. De même $m(\widehat{CI_cP}) = \frac{m(\widehat{C}}{2}$, donc $\triangle I_aPI_c$ est isocèle et $I_aP = I_cP$. de manière analogue, $I_aP = I_bP$, donc P est le centre du cercle circonscrit au triangle $I_aI_bI_c$.

<u>*Solution de l'exercice 10*</u> On appelle h l'homothétie de centre G et de rapport $-\frac{1}{2}$, où G est le centre de gravité. On sait que h envoie O sur H et A, B et C sur les milieux des segments $[BC]$, $[AC]$ et AB, que l'on appelle A_1, B_1 et C_1. La doite OH doit rencontrer au moins deux côtés du triangle ABC, disons $[AB]$ et $[AC]$.

Comme A_1 est le milieu de $[BC]$, on a $d(A_1, OH) = \frac{d(B,0H)+d(C,OH)}{2}$.Comme h est une homothétie, $OH = h(OH)$ et $A_1 = h(A)$, on a $d(A_1, OH) = \frac{d(A,OH)}{2}$. Donc $d(A, OH) = d(B, OH) + d(C, OH)$, ce qui donne $S[OHA] = S[OHB] + S[OHC]$.

<u>*Solution de l'exercice 11*</u> On considère l'homothétie h de centre G et rapport $-\frac{1}{2}$, où G est le centre de gravité. On se rappelle que $h(H) = O$ et que les points $A_1 := h(A)$, $B_1 := h(B)$ et $C_1 := h(C)$ sont les milieux des côtés du triangle ABC. On note $A_{-1} = h^{-1}(A)$, $B_{-1} = h^{-1}(B)$, $C_{-1} = h^{-1}(C)$, $D_1 = h(D)$, $E_1 = h(E)$ et $F_1 = h(F)$. Comme D, E, F sont colinéaires on a D_1, E_1, F_1 colinéaires.

Comme AD est perpendiculaire sur BC, A_1D_1 est perpendiculaire sur B_1C_1. Comme, $B_1C_1 \parallel BC \parallel B_{-1}C_{-1}$, A_1D_1 est perpendiculaire sur $B_{-1}C_{-1}$. Comme $A_1D_1 = \frac{1}{2}AD = \frac{1}{2}(2d(A, BC))$, $A_1D_1 = d(A, BC)$.
Or $d(A, BC) = \frac{1}{2}d(A_{-1}, B_{-1}C_{-1}) = d(BC, B_{-1}C_{-1})$ car BC est la médiane de $A_{-1}B_{-1}C_{-1}$. On conclut que $D_1 \in B_{-1}C_{-1}$. Finalement $H \in AD$, donc $O = h(H) \in A_1D_1$. Ainsi D_1 est le pied de la perpendiculaire de O sur $B_{-1}C_{-1}$. De manière analogue, les points D_1, E_1, F_1 sont les pieds des perpendiculaires de O sur les côtés de $A_1B_1C_1$. Il est connu que les projections d'un point sur les côtés d'un triangle sont colinéaires si et seulement si le point appartient au cercle circonscrit. Ainsi D_1, E_1, F_1 sont colinéaires si et seulement si $O \in (A_{-1}B_{-1}V_{-1})$. Puisque H est de centre de $(A_{-1}B_{-1}C_{-1})$, cela équivaut à $OH = 2R$.

5 Test

- Énoncés (durée : 3h) -

Exercice 1 Soient Γ_1 et Γ_2 deux cercles s'intersectant en P et Q. On trace le segment $[PQ]$. On considère une droite d qui le coupe en un point intérieur au segment. On note A, B, C, D dans cet ordre ses 4 points d'intersection de d avec Γ_1 (pour A et C) et Γ_2 (pour B et D).

Prouver que $\widehat{APB} = \widehat{CQD}$.

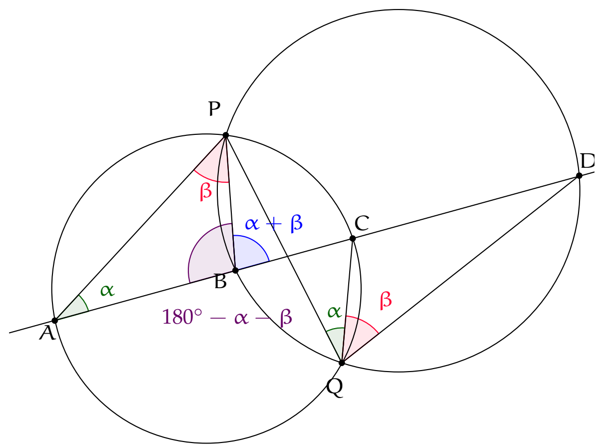
Exercice 2 Soit ABC un triangle d'orthocentre H. Soit F un point d'intersection des deux cercles de diamètre $[AH]$ et de diamètre $[BC]$. Montrer que les tangentes en F à ces deux cercles sont perpendiculaires.

Exercice 3 Soit P un point à l'intérieur d'un triangle ABC. On note P_A l'intersection de la droite (AP) avec $[BC]$, P_B l'intersection de la droite (BP) avec $[AC]$ et P_C l'intersection de la droite (CP) avec $[AB]$. Prouver que :

$$\frac{P_BP}{P_BB} + \frac{P_AP}{P_AA} + \frac{P_CP}{P_CC} = 1.$$

- Corrigé -

<u>*Solution de l'exercice 1*</u> On commence par tracer une figure :

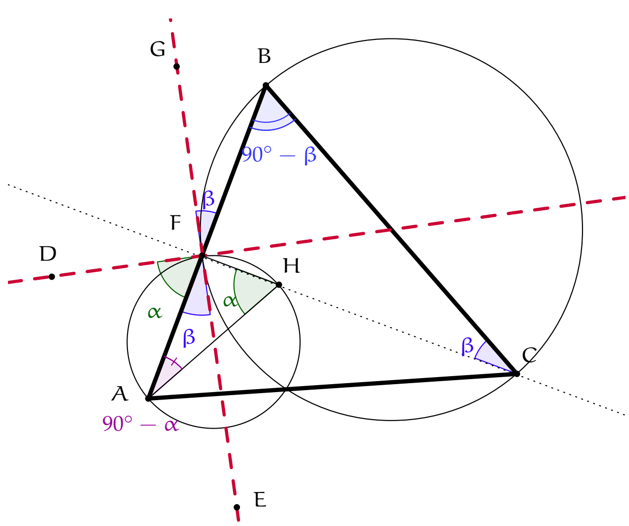


La présence de nombreux points cocycliques nous invite à chasser les angles : posons $\alpha = \widehat{PQC}$ et $\beta = \widehat{CQD}$. Les points P, B, Q, D sont cocycliques. Les angles $\widehat{PBD}$ et $\widehat{PQD}$ interceptent le même arc et sont donc égaux. Ainsi, $PBD = \alpha + \beta$, et donc $\widehat{ABP} = 180° - \alpha - \beta$.

D'autre part, les points P, A, Q, C sont cocycliques. Les angles $\widehat{PAC}$ et $\widehat{PQC}$ interceptent le même arc et sont donc égaux. Ainsi, $\widehat{PAB} = \alpha$.

Nous avons de cette manière réussi à trouver deux des trois angles du triangle ABP. L'angle $\widehat{APB}$ vaut donc $180° - (\alpha + 180° - \alpha - \beta) = \beta$. On a bien $\widehat{CQD} = \widehat{APB}$, ce qu'il fallait démontrer.

<u>*Solution de l'exercice 2*</u> Commençons par tracer une figure :



Cette jolie figure semble nous suggérer que F est sur le segment $[BC]$. Qu'à cela ne tienne, démontrons-le ! $[AH]$ et $[BC]$ étant deux diamètres, on a $\widehat{AFH} = 90°$ et $\widehat{BFC} = 90°$. Donc $AFB = \widehat{AFC} + \widehat{CFB} = 90° + 90°$, ce qui prouve que A, F, B sont alignés.

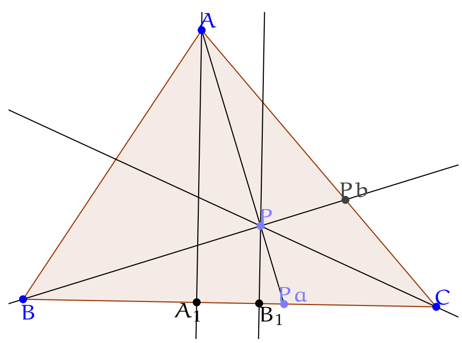
Cette jolie figure semble également nous suggérer que F, H, C sont alignés. Qu'à cela ne tienne, démontrons-le ! Nous avons déjà vu que $\widehat{AFH} = 90°$. Comme H est l'orthocentre de ABC, cela implique que (FH) est la hauteur issue de C dans ABC. Les points F, H, C sont donc bien alignés.

Plaçons des points D, E, G sur les deux tangentes comme sur la figure, et montrons que $\widehat{DFE} = 90°$. Pour cela, posons $\alpha = \widehat{DFA}$ et $\beta = \widehat{AFE}$, et montrons que $\alpha + \beta = 90°$. La présence de tangentes et de points cocycliques nous invite à faire une chasse aux angles en utilisant la forme limite du théorème de l'angle inscrit.

D'après la forme limite du théorème de l'angle inscrit, on a $\widehat{FHA} = \alpha$ et donc $\widehat{BAH} = 90° - \alpha$. Toujours d'après la forme limite du théorème de l'angle inscrit, on a $\beta = \widehat{GFB} = \widehat{FCB}$, et donc $\widehat{ABC} = 90° - \beta$.

Or $\widehat{BAH} + \widehat{ABC} = 90°$, car la droite (AH) est perpendiculaire à (BC). Donc $90° - \alpha + 90° - \beta = 90°$, ce qui implique $\alpha + \beta = 90°$ et conclut l'exercice.

Solution de l'exercice 3 On appelle A_1 et B_1 les pieds des perpendiculaires de A respectivement P sur BC.



D'après le théorème de Thalès on a : $\frac{PP_1}{AA_1} = \frac{A_PP}{A_PA}$. La formule de l'aire dans $\triangle ABC$ donne $S[ABC] = \frac{AA_1 \cdot BC}{2}$. La même formule dans $\triangle BPC$ donne $S[PBC] = \frac{PP_1 \cdot BC}{2}$. Ainsi $\frac{PA_P}{AA_P} = \frac{S[BPC]}{S[ABC]}$. De manière analogue, $\frac{B_PP}{B_PB} = \frac{S[APC]}{S[ABC]}$ et $\frac{C_PP}{C_PC} = \frac{S[ABP]}{S[ABC]}$. Or, l'additivité des aires donne $S[ABC] = S[APC] + S[ABP] + S[PBC]$. D'où le résultat.

3 Intermédiaires : inégalités

Nous renvoyons au cours d'inégalités disponible sur le site d'Animath pour des compléments de cours (voir les liens en haut de la page 14).

1 Premier cours/TD

- Énoncés -

Exercice 1 (Moyenne arithmétique - moyenne géométrique, 2 variables) Soient $x, y \geqslant 0$.

Montrer que

$$\frac{x+y}{2} \geqslant \sqrt{xy}.$$

Exercice 2 Soit $x > 0$. Montrer que

$$x + \frac{1}{x} \geqslant 2.$$

Pour quels x a-t-on égalité ?

Exercice 3 Déterminer les x réels tels que

$$x^2 + 2x + 2 > 0.$$

Exercice 4 Déterminer les x réels tels que

$$x^2 + 3x + 2 > 0.$$

Exercice 5 (Inégalité moyenne arithmétique - moyenne harmonique) Soient $x_1, x_2, \dots, x_n > 0$? Montrer que

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geqslant \frac{n}{\frac{1}{x_1} + \dots \frac{1}{x_n}}.$$

Exercice 6 (Cauchy-Schwarz) Soient $x_i, y_i \in \mathbb{R}$. Montrer que

$$x_1y_1 + \cdots + x_ny_n \leqslant \sqrt{x_1^2 + \cdots + x_n^2}\sqrt{y_1^2 + \dots y_n^2}.$$

Exercice 7 Déterminer tous les $n \in \mathbb{N}$ tels que :

$$3^n > n^2 - 2n + 91$$

Exercice 8 Montrer que

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2.$$

Exercice 9 (Inégalité moyenne arithmetique - moyenne géométrique) Soient $x_1, x_2, \dots, x_n > 0$. Montrer que

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geqslant \sqrt[n]{x_1 \dots x_n}.$$

Exercice 10 (Inégalité de Nesbitt) Soient $a, b, c \geqslant 0$. Montrer que

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

Exercice 11 Trouver $x_1, x_2, \dots, x_n \geqslant 0$ tq $x_1 + \dots x_n = 1$ et $x_1^1 x_2^2 x_3^3 \dots x_n^n$ est maximal.

- Corrigé -

<u>*Solution de l'exercice 1*</u> Cette inégalité est équivalente à

$$x + y - 2\sqrt{xy} = (\sqrt{x} - \sqrt{y})^2 \geqslant 0.$$

Or, un carré est toujours positif. Le cas d'égalité est obtenu exactement pour $\sqrt{x} - \sqrt{y} = 0$, c.à.d. pour les valeurs $x = y$.

<u>*Solution de l'exercice 2*</u> Cette inégalité est équivalente à $\left(\sqrt{x} - \frac{1}{\sqrt{x}}\right)^2 \geqslant 0$.

Donc, l'égalité est obtenue pour $x = \frac{1}{x}$, c.à.d. pour $x = 1$.

<u>*Solution de l'exercice 3*</u> $x^2 + 2x + 2 = (x+1)^2 + 1 \geqslant 1 > 0$.

<u>*Solution de l'exercice 4*</u> $x^2 + 3x + 2 = (x+1)(x+2)$.

Ce produit est strictement positif si et seulement si les deux facteurs ont le même signe, c.à.d., pour $x < -2$ et pour $x > -1$.

<u>*Solution de l'exercice 5*</u> En utilisant l'inégalité de Exercice 2, on trouve :

$$\begin{aligned}
&(x_1 + x_2 + \dots + x_n)\left(\frac{1}{x_1} + \dots \frac{1}{x_n}\right)\\
&\quad = \frac{x_1}{x_1} + \frac{x_2}{x_2} + \dots + \frac{x_n}{x_n}\\
&\quad + \left(\frac{x_1}{x_2} + \frac{x_2}{x_1}\right) + \left(\frac{x_1}{x_3} + \frac{x_3}{x_1}\right) + \dots + \left(\frac{x_2}{x_3} + \frac{x_3}{x_2}\right) + \dots + \left(\frac{x_{n-1}}{x_n} + \frac{x_n}{x_{n-1}}\right)\\
&\quad \geqslant 1 + 1 + \dots + 1 + 2 + 2 + \dots + 2\\
&\quad = 1 \cdot n + 2 \cdot \frac{n(n-1)}{2} = n + n^2 - n = n^2
\end{aligned}$$

Cas d'égalité : $\frac{x_i}{x_j} = 1, \forall i, j$, donc $x_1 = x_2 = \dots = x_n$.

<u>*Solution de l'exercice 6*</u>

$$(x_1^2 + \dots + x_n^2)(y_1^2 + \dots y_n^2) - (x_1 y_1 + \dots + x_n y_n)^2 = \sum_{1 \leqslant i < j \leqslant n} (x_i y_j - x_j y_i)^2 \geqslant 0.$$

Cas d' égalité : Les vecteurs $(x_1, x_2, \dots, x_n)$ et $(y_1, y_2, \dots y_n)$ sont proportionnels.

<u>*Solution de l'exercice 7*</u> Si l'inégalité est vraie, on a $3^n > (n-1)^2 + 90 \geqslant 90 > 81 = 3^4$, donc $n > 4$.

On peut montrer cette inégalité à partir de $n = 5$ par récurrence.

<u>*Solution de l'exercice 8*</u> On peut montrer par recurrence que

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leqslant 2 - \frac{1}{n}.$$

<u>*Solution de l'exercice 9*</u> *Si l'inégalité est vraie pour n, elle est vraie pour $2n$*

On applique le cas n deux fois aux variables $x_1, x_2, \ldots, x_n$ et aux variables $x_{n+1}, x_{n+2}, \ldots, x_{2n}$. Après, on applique le cas $n = 2$, qu'on a deja montré dans l'exercice 1

On obtient

$$\begin{aligned}
\frac{(x_1 + x_2 + \cdots + x_n) + (x_{n+1} + \ldots x_{2n})}{2n} &= \frac{\frac{x_1 + x_2 + \cdots + x_n}{n} + \frac{x_{n+1} + x_{n+2} + \cdots + x_{2n}}{n}}{2} \\
&\geqslant \frac{\sqrt[n]{x_1 x_2 \ldots x_n} + \sqrt[n]{x_{n+1} x_{n+2} \ldots x_{2n}}}{2} \\
&\geqslant \sqrt{\sqrt[n]{x_1 x_2 \ldots x_n}\,\sqrt[n]{x_{n+1} x_{n+2} \ldots x_{2n}}} \\
&= \sqrt[2n]{x_1 x_2 \ldots x_n x_{n+1} x_{n+2} \ldots x_{2n}}
\end{aligned}$$

Si l'inégalité est vraie pour $n \geqslant 2$, elle est vraie pour $n - 1$

Conclusion

<u>*Solution de l'exercice 10*</u> Cette inégalité est équivalente à

$$x + y - 2\sqrt{xy} = (\sqrt{x} - \sqrt{y})^2 \geqslant 0.$$

Or, un carré est toujours positif. Le cas d'égalité est obtenu exactement pour $\sqrt{x} - \sqrt{y} = 0$, c.à.d. lorsque $x = y$.

2 Deuxième cours/TD : convexité

- La Théorie -

Définition 9. Soit X un sous-ensemble de $\mathbb{R}^n$. On dit que X est convexe si pour tous points A, B de X on a $[A, B] \subset X$.

Exemple 10. En dimension 1, les ensembles convexes sont les intervalles de $\mathbb{R}$.

Définition 11. Soit $X \subset \mathbb{R}^n$ un ensemble convexe. Soit $f : X \to \mathbb{R}$. On dit que f est convexe si pour tous $x, y \in X$ et tout $\lambda \in [0, 1]$, $f(\lambda \cdot x + (1 - \lambda) \cdot y) \leqslant \lambda f(x) + (1 - \lambda) f(y)$.

Autrement dit l'image du barycentre de deux points est plus petite que le barycentre des images de ces deux points.

En fait si on suppose la fonction continue, on a la proposition suivante.

Proposition 12. Si $f : X \to \mathbb{R}^n$ est continue et vérifie $f(\frac{x+y}{2}) \leqslant \frac{f(x)+f(y)}{2}$ pour tous $x, y \in X$, alors f est convexe.

Démonstration. On peut supposer qu'on est en dimension 1 et que (pour simplifier) $X = [0, 1]$ car la convexité se vérifie sur tous les segments de X. Soit E l'ensemble des $\lambda \in [0, 1]$ tels que pour tous $x, y \in X$, $f(\lambda \cdot x + (1-\lambda) \cdot y) \leqslant \lambda f(x) + (1-\lambda) f(y)$. On sait que 0,1 $\in E$. De plus si $\lambda, \mu \in E$ alors $\frac{\lambda+\mu}{2} \in E$ (cela découle de l'hypothèse sur les milieux). Donc E contient les rationnels de la forme $\frac{k}{2^n}$ où $k, n \in \mathbb{N}$. Comme ces rationnels sont denses dans $[0, 1]$, on conclut par continuité de f. Les détails sont laissés au lecteur. □

On peut automatiquement renforcer l'inégalité de convexité.

Proposition 13. Soit $f :]a, b[\to \mathbb{R}$ une fonction convexe. Alors si x_1, ..., x_n sont dans $]a, b[$ et que $\lambda_1 + ... + \lambda_n = 1$ où $\lambda_i > 0$, alors $f(\lambda_1 x_1 + ... + \lambda_n x_n) \leqslant \lambda_1 f(x_1) + ... + \lambda_n f(x_n)$

Proposition 14. Si f et g sont deux fonctions convexes sur X, alors $f + g$ est convexe et λf est convexe pour $\lambda \geqslant 0$.

Le moyen le plus efficace (admis) pour voir si une fonction est convexe est le théorème suivant.

Théorème 15. Soit f une fonction deux fois dérivable sur un intervalle ouvert $I =]a, b[$. Alors f est convexe ssi $f'' \geqslant 0$ sur I.

Exemples : Les fonction $x \to x^\alpha$ sont convexes sur $\mathbb{R}_+^*$ pour $\alpha \geqslant 1$ ou $\alpha \leqslant 0$. En effet la dérivée seconde est $\alpha(\alpha-1)x^{\alpha-2}$.

Proposition 16. Sur un intervalle fermé $I = [a, b]$, une fonction convexe atteint son maximum aux bornes de l'intervalle.

Attention, comme nous le verrons en exercice, une fonction de plusieurs variables peut être convexe en chaque variable séparément, mais pas convexe en tant que fonction de trois variables. Cependant on peut quand même essayer d'appliquer la proposition précédente à chaque variable.

- Applications aux inégalités classiques -

Les inégalités entre moyennes découlent de la convexité/concavité de certaines fonctions.

Théorème 17. Comparaison des moyennes quadratique/arithmétique/géométrique/harmonique Soient $0 < x_1 \leqslant ... \leqslant x_n$. Alors

$$\left(\frac{x_1^2 + ... + x_n^2}{n}\right)^{1/2} \geqslant \frac{x_1 + ... + x_n}{n} \geqslant (x_1 \cdots x_n)^{1/n} \geqslant \frac{n}{\frac{1}{x_1} + ... + \frac{1}{x_n}}$$

Démonstration. La première inégalité découle de la convexité de la fonction $f : x \to x^2$. La deuxième découle de la concavité de la fonction logarithme. La dernière est une conséquence directe de la deuxième (I.A.G). Pour une preuve détaillée, cf. le poly de Pierre Bornsztein inégalités théorème 8. □

Théorème 18 (Inégalité de Holder)**.** Soit $p, q > 1$ tels que $\frac{1}{p} + \frac{1}{q} = 1$. Alors si $x_1, ..., x_n > 0$ et $y_1, ..., y_n > 0$, on a

$$a_1 b_1 + ... + a_n b_n \leqslant (a_1^p + ... + a_n^p)^{\frac{1}{p}} \times (b_1^q + ... + b_n^q)^{\frac{1}{q}}$$

Démonstration. On peut supposer $b_1^q + ... + b_n^q = 1$ car l'inégalité est homogène en les b_i. On sait que la fonction $x \to x^p$ est convexe sur $\mathbb{R}_+^*$. On pose $x_i = \frac{a_i}{b_i^{q-1}}$ et $\lambda_i = b_i^q$. Alors l'inégalité de Holder découle de l'inégalité de convexité appliqué aux x_i avec les rapports λ_i. □

- Exercices -

Exercice 1 Soient $a, b > 0$ tels que $a + b = 1$. Montrer que $(a + \frac{1}{a})^2 + (b + \frac{1}{b})^2 \geqslant \frac{25}{2}$.

Exercice 2 Soient $0 < a < b$ et $x_i \in [a, b]$. Prouver que $(x_1 + ... + x_n)(\frac{1}{x_1} + ... + \frac{1}{x_n}) \leqslant \frac{(a+b)^2}{4ab} n^2$.

Exercice 3 Soient $0 \leqslant a, b, c \leqslant 1$. Montrer que $\frac{a}{bc+1} + \frac{b}{ac+1} + \frac{c}{ab+1} \leqslant 2$.

Exercice 4 Soient $0 \leqslant a, b, c \leqslant 1$. Montrer que $\frac{a}{b+c+1} + \frac{b}{a+c+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c) \leqslant 1$.

Exercice 5 Soit $ABCD$ un tétraèdre et $KLMN$ un autre tétraèdre dont les sommets sont sur les faces de $ABCD$. Montrer que le périmètre de $KLMN$ est $\leqslant \frac{4}{3}$ fois le périmètre de $ABCD$.

Exercice 6 Soient a, b, c et d tels que $a^2 + b^2 + c^2 + d^2 = 1$. Montrer que $\sum_{\text{cyc}} \sqrt{1 - ab} \leqslant 2\sqrt{3}$.

Exercice 7 (IMO 2001) Soient a, b, c positifs. Montrer que $\frac{a}{\sqrt{a^2+8bc}} + \frac{b}{\sqrt{b^2+8ca}} + \frac{c}{\sqrt{c^2+8ab}} \geqslant 1$.

- Solutions -

Solution de l'exercice 1 La fonction $f(x) = (x + \frac{1}{x})^2$ est convexe sur $\mathbb{R}_+^*$ car $f(x) = x^2 + \frac{1}{x^2} + 2$ est somme de fonctions convexes. Donc $f(a) + f(b) \geqslant 2f(\frac{a+b}{2}) = 2f(\frac{1}{2}) = \frac{25}{2}$.

Solution de l'exercice 2 La fonction $f(x_1, ..., x_n) = (x_1 + ... + x_n)(\frac{1}{x_1} + ... + \frac{1}{x_n})$ est convexe en chaque variable (attention cela ne veut pas dire que f est une fonction convexe). En effet en développant l'expression on obtient une somme de fonctions convexes en chaque variable. Le maximum est donc atteint aux points extrémaux de $[a, b]$, c'est à dire qu'il y a p x_i égaux à a et $n - p$ x_i égaux à b ($0 \leqslant p \leqslant n$). On cherche à minimiser le terme de gauche de l'inégalité en fonction de p. Ce terme est $(pa + (n-p)b)(\frac{p}{a} + \frac{n-p}{b}) = p^2 + (n-p)^2 + (n-p)p(\frac{a}{b} + \frac{b}{a})$. Le coefficient en p est $n(\frac{a}{b} + \frac{b}{a} - 2)$ et celui en p^2 est $2 - \frac{a}{b} + \frac{b}{a}$. Donc $p^2 + (n-p)^2 + (n-p)p(\frac{a}{b} + \frac{b}{a})$ atteint son minimum pour $p = \frac{n}{2}$ (si on ne considère plus p entier). Et le minimum est alors $\frac{n^2}{4}(2 + \frac{a}{b} + \frac{b}{a}) = \frac{(a+b)^2}{4ab} n^2$.

Solution de l'exercice 3 La fonction $f(a, b, c)$ du membre de gauche est convexe en chaque variable, donc elle atteint son maximum sur un des 8 points $(\epsilon_1, \epsilon_2, \epsilon_3)$ avec $\epsilon_i \in \{0, 1\}$ (en effet on utilise le fait que si une fonction $g : [u, v] \to \mathbb{R}$ est convexe alors g atteint son maximum en u ou en v). On vérifie que le maximum correspond à $(1, 1, 0)$ et vaut 2.

Solution de l'exercice 4 La fonction $f(a, b, c)$ du membre de gauche est convexe en chaque variable, donc elle atteint son maximum sur un des 8 points $(\epsilon_1, \epsilon_2, \epsilon_3)$ avec $\epsilon_i \in \{0, 1\}$. On vérifie que le maximum vaut 1.

<u>*Solution de l'exercice 5*</u> La fonction distance à un point est convexe (le vérifier pour les milieux, en utilisant la formule de la médiane par exemple) donc si le périmètre de KLMN est maximal, alors K, L, M et N sont dans $\{A, B, C, D\}$. Il y a un nombre fini de cas à tester.

<u>*Solution de l'exercice 6*</u> On utilise la concavité de $\sqrt{1-x}$ et le fait que $ab+ac+ad+bc+bd+cd = \frac{(a+b+c+d)^2-a^2-b^2-c^2-d^2}{2}$.

3 Premier TD

- Énoncés-

Exercice 1 Prouver que, si $n \geqslant 2$ est un nombre naturel et $x_1, x_2, \dots, x_n$ sont des réels positifs, alors

$$4\left(\frac{x_1^3-x_2^3}{x_1+x_2}+(\frac{x_2^3-x_3^3}{x_2+x_3}+\cdots+\frac{x_1^3-x_2^3}{x_1+x_2}+\frac{x_1^3-x_2^3}{x_1+x_2}\right)\leqslant$$
$$(x_1-x_2)^2+(x_2-x_3)^2\cdots+(x_{n-1}-x_n)^2+(x_n-x_1)^2.$$

Exercice 2 (Roumanie 2012, 10è classe) Soient a et b deux nombres réels tels que $0 < a < b$. Prouver :

1. Pour tous x,y et $z \in [a, b]$, $2\sqrt{ab} \leqslant \frac{x+y+z}{3} + \frac{ab}{\sqrt[3]{xyz}} \leqslant a + b$.
2. $\left\{\frac{x+y+z}{3} + \frac{ab}{\sqrt[3]{xyz}}\right\} = [2\sqrt{ab}, \frac{a+b}{2}]$.

Exercice 3 On note a,b et c let trois côtés d'un triangle.

1. Montrer qu'il existe un triangle de côtés $\sqrt{q}$, $\sqrt{b}$ et $\sqrt{c}$.
2. Prouver que $\sqrt{ab}+\sqrt{bc}+\sqrt{ca} \leqslant a+b+c \leqslant 2\sqrt{ab}+2\sqrt{bc}+2\sqrt{ca}$.

Exercice 4 (BMO 2012) Prouver que, pour tous nombres réels positifs x, y, z, on a :

$$\sum_{\text{cyc}}(x+y)\sqrt{(y+z)(z+x)} \geqslant 4(xy+yz+zx). \tag{II.3}$$

Exercice 5 Étant donnés trois nombres positifs a, b et c tels que $a+b+c=1$, montrer que :

$$\frac{a}{b}+\frac{b}{c}+\frac{c}{a}+\frac{b}{a}+\frac{a}{c}+\frac{c}{b}+6 \geqslant 2\sqrt{2}\left(\sqrt{\frac{1-a}{a}}+\sqrt{\frac{1-b}{b}}+\sqrt{\frac{1-c}{c}}\right).$$

Exercice 6 (Inégalité arithmético-géométrique) Soient $x_1, x_2, \dots, x_n > 0$. Montrer :

$$\frac{x_1+\cdots+x_n}{n} \geqslant (x_1x_2\cdots x_n)^{\frac{1}{n}}.$$

Exercice 7 Montrer que pour tous $x, y, z > 0$ on :

$$\sum_{\text{cyc}} x^3 \geqslant \sum_{\text{cyc}} x^2\sqrt{yz}.$$

Exercice 8 Pour tout triplet de nombres non négatifs a, b, c, tels que a^2, b^2, c^2 sont les côtés d'un triangle, montrer l'inégalité :

$$(a+b+c)(a^2+b^2+c^2)(a^3+b^3+c^3) \geqslant 4(a^6+b^6+c^6).$$

- Corrigé-

<u>*Solution de l'exercice 1*</u> En posant $x_{n+1} = x_1$, on a

$$\sum_{i=1}^{n} \frac{x_i^3 - x_{i+1}^3}{x_i + x_{i+1}} = \sum_{i=1}^{n} \left(x_i^2 - x_{i+1}^2 + \frac{x_i x_{i+1}(x_{i+1} - x_i)}{x_i + x_{i+1}} \right) = \sum_{i=1}^{n} \frac{x_i x_{i+1}(x_{i+1} - x_i)}{x_{i+1} + x_i}.$$

D'autre part, pour tout i, $\frac{x_i x_{i+1}(x_{i+1}-x_i)}{x_{i+1}+x_i} \leqslant \frac{1}{2} x_{i+1}(x_{i+1} - x_i)$. En sommant ces inégalités pour $i = 1, 2, \ldots, n$, on obtient la conclusion.

<u>*Solution de l'exercice 2*</u>

1. Par l'inégalité des moyennes géométrique et arithmétique on a :

$$\frac{x+y+z}{3} + \frac{ab}{\sqrt[3]{xyz}} \geqslant \sqrt[3]{xyz} + \frac{ab}{\sqrt[3]{xyz}} \geqslant 2\sqrt{ab}.$$

   De nouveau, l'inegalité des moyennes donne :

$$\frac{x+y+z}{3} + \frac{ab}{\sqrt[3]{xyz}} \leqslant \frac{x+y+z}{3} + \frac{ab(\frac{1}{x} + \frac{1}{y} + \frac{1}{y})}{3} = \frac{1}{3}\left(f(x) + f(y) + f(z)\right),$$

   où $f :]0, \infty[\to]0, \infty[$, $f(t) = t + \frac{ab}{t}$. Pour tout $t \in [a, b]$, on a :

$$t(a + b + f(t)) = (b - t)(t - a) \geqslant 0,$$

   d'où résulte $f(t) \leqslant a + b$ pour tout $t \in [a, b]$. En sommant, on obtient l'inégalité demandée.

2. D'après la première partie de l'exercice, il suffit de montrer que l'intervalle $[2\sqrt{ab}, \frac{a+b}{2}]$ est contenu dans l'ensemble du membre gauche. On montrera $[2\sqrt{ab}, \frac{a+b}{2}] \subset f([a, b])$. Pour cela, soit $s \in [2\sqrt{ab}, \frac{a+b}{2}]$. L'équation $f(t) = s$ équivaut à $t^2 - st + ab = 0$. Puisque $s \geqslant 2\sqrt{ab}$, le discriminant de l'équation est positif, donc on a deux racines réelles, qui appartiennent à $[a, b]$. En choisissant, $x = y = z = \frac{s \pm \sqrt{s^2 - 4ab}}{2}$, on obtient $\frac{x+y+z}{3} + \frac{ab}{\sqrt[3]{xyz}} = s$. Cqfd.

<u>*Solution de l'exercice 3*</u>

1. Comme a,b et c sont les côtés d'un triangle, on sait qu'il existe u, v et $w > 0$ tels que $a = v + w$, $b = u + w$ et $c = u + v$. Alors l'inégalité $\sqrt{a} \leqslant \sqrt{b} + \sqrt{c}$ équivaut à $\sqrt{v+w} \leqslant \sqrt{u+w} + \sqrt{u+v}$, ce qu'on montre vrai en élevant au carré. De manière analogue on montre les deux autres inégalités satisfaites par les côtés d'un triangle.
2. La partie gauche s'obtient par $a + b \geqslant \sqrt{ab}$ et les analogues. Pour la partie droite, $\sqrt{a} \leqslant \sqrt{b} + \sqrt{c}$ implique $a \leqslant \sqrt{ab} + \sqrt{ac}$. De manière analogue, on trouve deux autres inégalités et par sommation, on a le résultat.

<u>*Solution de l'exercice 4*</u> On pose $a = \sqrt{y+z}$, $b = \sqrt{x+z}$ et $c = \sqrt{x+y}$. On a :

$$xy = \frac{b+c-a}{2} \cdot \frac{a+c-b}{2} = \frac{1}{4}\left((c^2 - (a-b)^2\right) = \frac{1}{4}\left(2a^2b^2 + (c^2 - a^2 - b^2)\right)$$

et les deux autres relations obtenues par permutations cycliques. En sommant les trois égalités, on obtient :

$$xy + yz + zx = \sum_{\text{cyc}} 2a^2b^2 - \sum_{\text{cyc}} a^4.$$

Or, l'identité suivante est connue :

$$\sum_{\text{cyc}} 2a^2b^2 - \sum_{\text{cyc}} a^4 = (a+b+c)\Pi_{\text{cyc}}(a+b-c).$$

Ainsi, l'ínégalité (II.3) n'est autre que :

$$abc(a+b+c) \geqslant (a+b+c)\Pi_{\text{cyc}}(a+b-c). \tag{II.4}$$

Comme, x, y et z sont positifs, a^2, b^2 et c^2 sont les côtés d'un triangle. Alors, a, b et c sont également les côtés d'un triangle. Ainsi, on peut poser $u = b + c - a$, $v = a + c - b$ et $w = a + b - c$ et obtenir des nombres positifs. Par l'inégalité des moyennes on a $\frac{u+v}{2} \geqslant \sqrt{uv}$ et les analogues. En multipliant on a :

$$\Pi_{\text{cyc}}(\frac{u+v}{2}) \geqslant uvw,$$

ce qui prouve (II.4), donc (II.3).

<u>*Solution de l'exercice 5*</u> Par l'inégalité des moyennes, on a :

$$(\frac{b}{a} + \frac{c}{a}) + 2 \geqslant 2\sqrt{2 \cdot \frac{b+c}{a}} = 2\sqrt{2}\sqrt{\frac{1-a}{a}}.$$

De manière analogue on trouve deux autres inégalités qui s'obtiennent par permutations cycliques. En sommant, on obtient le résultat.

<u>*Solution de l'exercice 6*</u> On montre d'abord l'inégalité pour les n de la forme $n = 2^k$. Pour cela on fait une récurrence sur k. Le cas $n = 2^1$ est bien connu. Supposons le résultat vrai pour $k-1$. Soient $x_1, \ldots, x_{2^k} > 0$. Par l'hypothèse de récurrence, appliquée aux 2^{k-1}-uplets $(x_1, \ldots, x_{2^{k-1}})$ et $(x_{(2^{k-1}+1)}, \ldots, x_{2^k})$, on obtient :

$$\frac{x_1 + \cdots + x_{2^{k-1}}}{2^{k-1}} \geqslant (x_1x_2\cdots x_{2^{k-1}})^{\frac{1}{2^{k-1}}}.$$
$$\frac{x_{2^{k-1}+1} + \cdots + x_{2^k}}{2^{k-1}} \geqslant (x_{1+2^{k-1}}\cdots x_{2^k})^{\frac{1}{2^{k-1}}}.$$

Les deux inégalités sommées donnent : $\frac{x_1+\cdots+x_{2^k}}{2^k} =$

$$= \frac{\frac{x_1+\cdots+x_{2^{k-1}}}{2^{k-1}} + \frac{x_{2^{k-1}+1}+\cdots+x_{2^k}}{2^{k-1}}}{2} \geqslant \frac{(x_1x_2\cdots x_2^{k-1})^{\frac{1}{2^{k-1}}} + (x_{1+2^{k-1}}\cdots x_{2^k})^{\frac{1}{2^{k-1}}}}{2}.$$

Le cas $n = 2$ pour $(x_1x_2\cdots x_{2^{k-1}})^{\frac{1}{2^{k-1}}}$ et $(x_{1+2^{k-1}}\cdots x_{2^k})^{\frac{1}{2^{k-1}}}$ donne :

$$\frac{x_1+\cdots+x_{2^k}}{2^k} \geqslant \sqrt{(x_1x_2\cdots x_{2^{k-1}})^{\frac{1}{2^{k-1}}}(x_{1+2^{k-1}}\cdots x_{2^k})^{\frac{1}{2^{k-1}}}} = (x_1\cdots x_{2^k})^{\frac{1}{2^k}}.$$

Ceci prouve l'inégalité pour les puissances de 2. Passons maintenant au cas général. Soit n un nombre naturel et $(x_1,\ldots,x_n)$ un n-uplet pour lequel on veut montrer l'inégalité. Soit k tel que $2^k \geqslant n$. On pose $y_i = x_i$ pour $i = 1,2,\ldots,n$ et $y_i = (x_1\cdots + x_n)^{\frac{1}{n}}$ pour $i = n+1,\ldots,2^k$. On applique le cas 2^k à $(y_1,\ldots,y_{2^k})$ et on trouve :

$$\frac{x_1+\cdots+x_n+(2^k-n)(x_1\cdots x_n)^{\frac{1}{n}}}{2^k} \geqslant (x_1\cdots x_n(x_1\cdots x_n)^{\frac{2^k-n}{n}})^{\frac{1}{2^k}} = (x_1x_2\cdots x_n)^{\frac{1}{n}}.$$

Solution de l'exercice 7 On a :

$$\sum_{cyc} x^3 = \sum_{cyc}\left(4\cdot\frac{x^3}{6}+\frac{y^3}{6}+\frac{z^3}{6}\right)$$

En appliquant l'inégalité arithmético-géométrique à $(x^3,x^3,x^3,x^3,y^3,z^6)$ on obtient que le membre droit est supérieur à $\sum_{cyc}\sqrt[6]{x^{12}y^3z^3} = \sum_{cyc} x^2\sqrt{yz}$.

Solution de l'exercice 8 Méthode 1. Par l'inégalité de Cauchy on a $(\sum a)(\sum a^3) \geqslant (\sum a^2)$. Il reste à montrer que pour tout triplet x,y,z de côtés de triangle vérifient $(x+y+z)^3 \geqslant 4(x^3+y^3+z^3)$. Pour cela on pose $z = \alpha+\beta$, $y = \alpha+\gamma$ et $x = \beta+\gamma$ avec $\alpha,\beta,\gamma \geqslant 0$. En remplaçant, on doit montrer $2(\sum\alpha)^3 \geqslant \sum(\alpha+\beta)^3$, soit $2(\alpha^3+\beta^3+\gamma^3)+6(\sum\alpha^2\beta+\beta^2\alpha)+12\alpha\beta\gamma \geqslant 2(\sum\alpha^2)+3\sum\alpha^2\beta+3\sum\alpha\beta^2$. Cela est évident car $\alpha,\beta,\gamma \geqslant 0$.

Méthode 2. Sans perte de généralité on peut supposer que $a \geqslant \max\{b,c\}$. Ainsi $a \geqslant b$, $a \geqslant c$ et $b^2+c^2 \geqslant a^2$. On a $(\sum a)(\sum a^2)(\sum a^3) \geqslant (a^2+b^2+c^2)\left(a^2+(b^2+c^2)\right)^2 \geqslant 4a^4(a^2+b^2+c^2) \geqslant 4a^6+4b^6+4c^6$.

4 Deuxième TD

- Énoncés -

Exercice 1 Soient $a,b > 0$ tels que $a+b = 1$. Montrer que :

$$\frac{a^2}{a+1}+\frac{b^2}{b+1} \geqslant \frac{1}{3}$$

Exercice 2 Soient $x_1,\ldots,x_n > 0$ avec $x_1\ldots x_n = 1$. Montrer que

$$x_1^{n-1}+x_2^{n-1}+\ldots+x_n^{n-1} \geqslant \frac{1}{x_1}+\ldots\frac{1}{x_n}$$

Exercice 3 Soient $a, b, c > 0$ tels que $abc = 1$. Montrer que $\frac{1}{a+b+1} + \frac{1}{b+c+1} + \frac{1}{a+c+1} \leqslant 1$

Exercice 4 Soient a, b, c les côtés d'un triangle.

$$2(a^2b^2 + b^2c^2 + a^2c^2) > (a^4 + b^4 + c^4)$$

(Suggestion : penser à la formule de Héron pour l'aire d'un triangle)

Exercice 5 Soit $ABCDEF$ un hexagone convexe. On suppose que tous les côtés sont de longueur $\leqslant 1$. Montrer qu'il existe une grande diagonale de longueur $\leqslant 2$.

Exercice 6 Soit $\mathcal{P}$, $\mathcal{P}'$ deux quadrilatères convexes avec P' à l'intérieur de $\mathcal{P}$, d (resp. d') la somme des longueurs des diagonales de $\mathcal{P}$ (resp. $\mathcal{P}'$). Montrer que :

$$d' < 2d$$

Exercice 7 Soit ABC un triangle de côtés a, b, c et d'aire A. Montrer :

$$a^2 + b^2 + c^2 \geqslant 4\sqrt{3}A$$

- Corrigé -

<u>*Solution de l'exercice 1*</u> Il y a beaucoup de solutions possibles, notamment par convexité.

<u>Solution directe :</u> On écrit $b = 1 - a$, on met au même dénominateur. L'inégalité est équivalente à :

$$3[(1-a)^2(a+1) + a^2(2-a)] \geqslant (2-a)(a+1)$$

On développe et on obtient

$$4a^2 - 4a + 1 = 4(a - 1/2)^2 \geqslant 0$$

<u>Solution par homogénéisation :</u> On commence par faire la simplification (la méthode marche aussi si on ne l'a pas vue !) :

$$\frac{a^2}{a+1} = \frac{a^2-1}{a+1} + \frac{1}{a+1} = a - 1 + \frac{1}{a+1}$$

L'inégalité se réecrit :

$$\frac{1}{a+1} + \frac{1}{b+1} \geqslant 4/3$$

On réduit au même

$$\frac{a^2}{(a+b)(2b+a)} + \frac{b^2}{(a+b)(2a+b)} \geqslant 1/3$$

On met au même dénominateur, on développe et on obtient

$$a^2 + b^2 \geqslant 2ab$$

et on a gagné.

<u>*Solution de l'exercice 2*</u> On multiplie à droite par $x_1 \dots x_n$:

$$x_1^{n-1} + \dots x_n^{n-1} \geqslant \sum_i x_1 \dots \hat{x_i} \dots x_n$$

On reconnait des sommes symétriques :

$$\frac{1}{(n-1)!} \sum_{sym} x^{n-1} \geqslant \frac{1}{(n-1)!} \sum_{sym} x_1 x_2 \dots x_{n-1}$$

et on conclut par Muirhead.

<u>*Solution de l'exercice 3*</u> On fait un changement de variable $a = x^3$, $b = y^3$, $c = z^3$, ce qui permet ensuite d'homogénéiser :

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

On met au même dénominateur, on simplifie :

$$x^6y^3 + y^6x^3 + x^6z^3 + x^3z^6 + y^6z^3 + y^3z^6 \geqslant 2(x^5y^2z^2 + x^2y^5z^2 + x^2y^2z^5)$$

soit

$$\sum_{sym} x^6y^3 = \sum_{sym} x^5y^2z^2$$

qui est un cas de l'inégalité de Muirhead.

<u>*Solution de l'exercice 4*</u> Il est possible de résoudre cet exercice "simplement" en faisant une transformation de Ravi et en développant le tout : on se ramène à l'inégalité évidente :

$$x^2yz + xy^2z + xyz^2 > 0$$

Mais la formule de Héron donne une preuve élégante. L'inégalité triangulaire implique :

$$(a+b+c)(a+b-c)(a+c-b)(b+c-a) > 0$$

Or ceci se réecrit :

$$\begin{aligned}
(a+b+c)(a+b-c)(a+c-b)(b+c-a) &= [(a+b)^2 - c^2][c^2 - (a-b)^2] \\
&= (a^2 + b^2 - c^2 + 2ab)(c^2 - a^2 - b^2 + 2ab) \\
&= 4a^2b^2 - (a^2 + b^2 - c^2)^2 \\
&= (a^2 + b^2 + c^2)^2 - 2(a^4 + b^4 + c^4)
\end{aligned}$$

<u>*Solution de l'exercice 5*</u> On ordonne les côtés du triangle ACE, disons $AC \leqslant AE \leqslant CE$. On écrit alors l'inégalité de Ptolémée dans le quadrilatère $ACDE$:

$$AD \cdot CE \leqslant CD \cdot AE + DE \cdot AC \leqslant AE + AC \leqslant 2CE$$

donc $AD < 2$.

Solution de l'exercice 6 Notons A, B, C, D (resp. A', B', C', D') les sommets de $\mathcal{P}$ (resp. $\mathcal{P}'$) et P (resp. P') la somme des longueurs des côtés de $\mathcal{P}$ (resp. $\mathcal{P}'$).

Solution pédestre : On va montrer qu'en fait :

$$\frac{P'}{2} < d' < P' < P < 2d < 2P$$

On a par inégalité triangulaire :

$$\begin{aligned} AC &< AB + BC \\ AC &< CD + AD \\ BD &< AB + AD \\ BD &< BC + CD \end{aligned}$$

En les additionnant, on obtient $2d < 2P$. D'autre part, si O est le point de concours des diagonales, on a par inégalité triangulaire :

$$\begin{aligned} AB &< AO + OB \\ BC &< BO + OC \\ CD &< OC + OD \\ AD &< OA + OD \end{aligned}$$

En les additionnant, on obtient $P < 2d$.

Les inégalités $\frac{P'}{2} < d' < P'$ sont exactement les mêmes appliquées à $\mathcal{P}'$. Il reste donc à démontrer que $P' < P$.

Soit M un point quelconque à l'intérieur de $\mathcal{P}'$. On trace les droites (MA'), (MB'), (MC'), (MD'). Par convexité de $\mathcal{P}'$, elles rencontrent le bord de $\mathcal{P}'$ en A', B', C',D'. On note A'', B'', C'', D'' les premiers points d'intersection avec le bord de $\mathcal{P}$. Alors par inégalité triangulaire : $P' = A'B' + B'C' + C'D' + D'A' < A''B'' + B''C'' + C''D'' < P$.

Solution astucieuse (due à Clément Lézane) : On remarque le fait suivant : tout segment contenu dans le polygone P est de longueur inférieure à sa plus grande diagonale. Ceci se voit en utilisant la convexité de la fonction "distance à un point". On l'applique ensuite aux deux diagonales de P', ce qui conclut.

Solution de l'exercice 7 Il existe beaucoup de preuves de cette inégalité (dite de Weitzenböck). On renvoie au livre de Engel, Problem solving strategies, chap.7 pour un florilège. Voici celle proposée par Clément Lézane et Lucas Flammant :

On fixe le périmètre $p = a + b + c$. Dans ce cas, le membre de gauche de l'inégalité est minimal quand $a = b = c$, alors que l'aire d'un triangle de périmètre fixé est maximal pour un triangle équilatéral. Ceci conclut.

5 Test

- Énoncés (durée : 3h) -

Exercice 1 Soient $x, y > 0$. Montrer que

$$\frac{4x+y}{6} \geqslant \left(\frac{x^2y}{2}\right)^{\frac{1}{3}}.$$

Exercice 2 Soit $a_1, \ldots, a_n$ des entiers strictement positifs distincts. Montrer que

$$\sum_{k=1}^{n} \frac{a_k}{k^2} \geqslant \sum_{k=1}^{n} \frac{1}{k}.$$

Exercice 3 Soient $0 < a < b$ et des réels $x_1, \ldots, x_n$ tous appartenant à $[a, b]$. Prouver que

$$(x_1 + \ldots + x_n)\left(\frac{1}{x_1} + \ldots + \frac{1}{x_n}\right) \leqslant \frac{(a+b)^2}{4ab} n^2.$$

Exercice 4 Soit ABC un triangle de périmètre 2. On pose $a = BC$, $b = AC$ et $c = AB$. Montrer que :

$$a^2 + b^2 + c^2 < 2(1 - abc).$$

- Corrigé -

Solution de l'exercice 1 On écrit $4x + y = 2x + 2x + y$. On applique l'Inégalité Arithmético-Géométrique (IAG) : $4x + y \geqslant 3(4x^2y)^{\frac{1}{3}}$, ce qui est le résultat voulu en divisant par 6.

Solution de l'exercice 2 On applique l'inégalité du réordonnement : la somme est minimale quand les a_k sont classés par ordre croissant. Dans ce cas, $a_k \geqslant k$ par récurrence sur k car $1 \leqslant a_1 < a_2 < \cdots < a_n$. Donc la somme est supérieure ou égale à

$$\frac{1}{1} + \frac{2}{2^2} + \cdots + \frac{n}{n^2} = \sum_{k=1}^{n} \frac{1}{k},$$

ce qui est ce qu'on voulait démontrer.

Solution de l'exercice 3 La fonction

$$f(x_1, \ldots, x_n) = (x_1 + \cdots + x_n)\left(\frac{1}{x_1} + \cdots + \frac{1}{x_n}\right)$$

est convexe en chaque variable (attention cela ne veut pas dire que f est une fonction convexe). En effet en développant l'expression on obtient une somme de fonctions convexes en chaque variable. Le maximum est donc atteint aux points extrémaux de $[a, b]$, c'est à dire qu'il y a p des x_i égaux à a et $n - p$ des x_i égaux à b (pour un certain $0 \leqslant p \leqslant n$). On cherche donc à maximiser le terme de gauche de l'inégalité en fonction de p. Ce terme est

$$(pa + (n-p)b)\left(\frac{p}{a} + \frac{n-p}{b}\right) = p^2 + (n-p)^2 + (n-p)p\left(\frac{a}{b} + \frac{b}{a}\right).$$

Le coefficient en p est $n(\frac{a}{b}+\frac{b}{a}-2)$ et celui en p^2 est $2-\frac{a}{b}-\frac{b}{a}<0$ (par l'IAG, $x+\frac{1}{x}\geqslant 2$ avec égalité ssi $x=1$). Donc $p^2+(n-p)^2+(n-p)p(\frac{a}{b}+\frac{b}{a})$ atteint son maximum pour $p=\frac{n}{2}$ (si on ne considère plus p entier). Et le maximum est alors

$$\frac{n^2}{4}\left(2+\frac{a}{b}+\frac{b}{a}\right)=\frac{(a+b)^2}{4ab}n^2.$$

<u>*Solution de l'exercice 4*</u> On fait la transformation classique $a=x+y$, $b=y+z$ et $c=x+z$ avec x, y et $z>0$. On a $x+y+z=1$. On homogénéise l'inégalité : elle est équivalente à $(x+y+z)((x+y)^2+(y+z)^2+(z+x)^2)<2((x+y+z)^3-(x+y)(y+z)(z+x))$ (tout est de degré 3). En développant, c'est équivalent à $2xyz>0$ ce qui est clair.

4 Avancés : géométrie

1 Test

- Énoncés (durée : 3h30) -

Exercice 1 Soit $ABCD$ un quadrilatère convexe et M le milieu de sa diagonale AC. Supposons que $\widehat{BCD}=\widehat{BMA}=\widehat{AMD}$. Montrer que A, B, C et D sont cocycliques.

Exercice 2 On considère $ABCDEF$ un hexagone ayant un centre de symétrie. Sur chaque côté, on construit vers l'extérieur un triangle équilatéral et on regarde l'hexagone formé par les 6 sommets ainsi construits. Montrer que les milieux des côtés du nouvel hexagone forment un hexagone régulier.

Exercice 3 Soit $ABCDE$ un pentagone fixé qui est convexe et inscriptible. Une triangulation est une subdivision en trois triangles à l'aide de deux diagonales de $ABCDE$ ne s'intersectant pas (il y a 5 triangulations différentes). On associe à chaque triangulation la somme des rayons des cercles inscrits aux trois triangles. Montrer que cette somme ne dépend pas du choix de la triangulation.

Exercice 4 Soit $ABCD$ un quadrilatère convexe inscriptible. Les droites AB et CD s'intersectent au point P, et les droites BC et DA s'intersectent en Q. Montrer que la bissectrice de $\widehat{CQD}$ et la bissectrice de $\widehat{DPA}$ s'intersectent sur la droite joignant le milieu de AC avec le milieu de BD.

Exercice 5 Soit ABC un triangle, soit M et N des points appartenant respectivement aux segments $[AB]$ et $[AC]$ et tels que $MN \parallel BC$. Soit P l'intersection de BN et CM, et $Q\neq P$ l'autre point d'intersection des cercles circonscrits aux triangles BMP et CNP. Montrer que $\widehat{BAQ}=\widehat{CAP}$.

Exercice 6 Soit P un point à l'intérieur du triangle ABC tel que

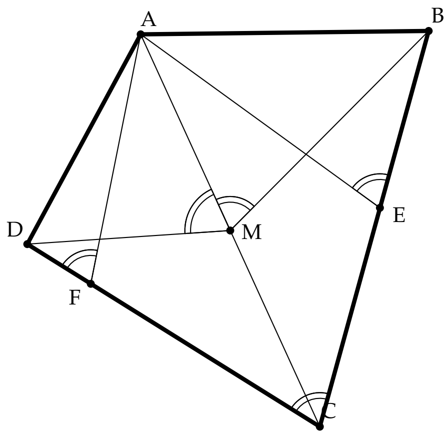
$$\widehat{BPC}-\widehat{BAC}=\widehat{CPA}-\widehat{CBA}=\widehat{APB}-\widehat{ACB}.$$

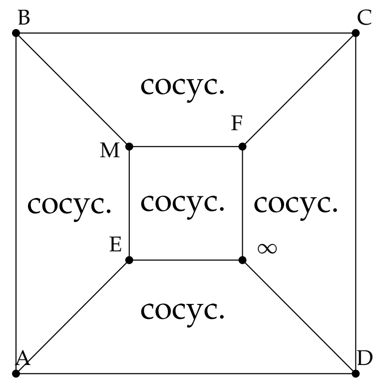
Montrer que $PA\cdot BC=PB\cdot CA=PC\cdot AB$.

Exercice 7 Soit $ABCDEF$ un 6-gone convexe ayant ses 6 côtés égaux, et tel que $\widehat{A}+\widehat{C}+\widehat{E}=\widehat{B}+\widehat{D}+\widehat{F}$. Montrer que AD, BE et CF sont concourantes.

- Corrigé -

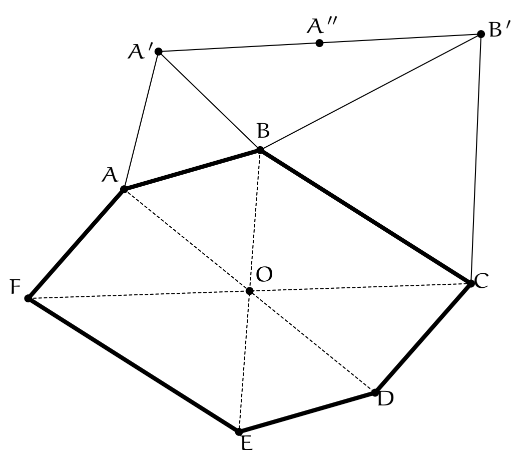
<u>Solution de l'exercice 1</u> *Solution de Lucas Perotin.* Soit $\alpha = \widehat{BMA} = \widehat{AMD} = \widehat{BCD}$. On commence par placer les points E et F sur BC et DC tels que $\widehat{BEA} = \widehat{AFD} = \alpha$.





Les quadrilatères $AMFD$, $BAME$, $DFC\infty$ et $BEC\infty$ sont cocycliques. $\widehat{BEA} = \widehat{BCD}$ donc $(EA)//(CD)$, de même $(AF)//(BC)$, donc $AECF$ parallélogramme, ses diagonales se coupent en leur milieu, E, F, M alignés. On peut utiliser le théorème du cube.

<u>Solution de l'exercice 2</u> (solution de Arthur Nebout) Par soucis de clarté nous n'avons dessiné que deux des six triangles equilatéraux sur la figure.

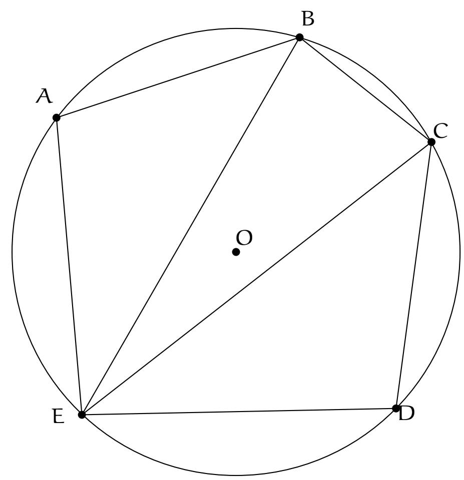


Nous allons raisonner en complexes, avec O l'origine et a, b, c les affixes de A, B, C, et on note $\omega = e^{\frac{2i\pi}{3}}$ (qui vérifie $1 + \omega + \omega^2 = 0$). On a $a' = a - \omega^2(b - a) = -\omega a - \omega^2 b$. De même $b' = -\omega b - \omega^2 c$ et $c' = -\omega c + \omega^2 a$.

$$a'' = \frac{-\omega a + b - \omega^2 c}{2}, \quad b'' = a'' = \frac{-\omega b + c + \omega^2 a}{2}$$

Et il est facile de vérifier que $-\omega a'' = b''$.

<u>Solution de l'exercice 3</u> (solution de Yassine Hamdi) On considère une triangulation :



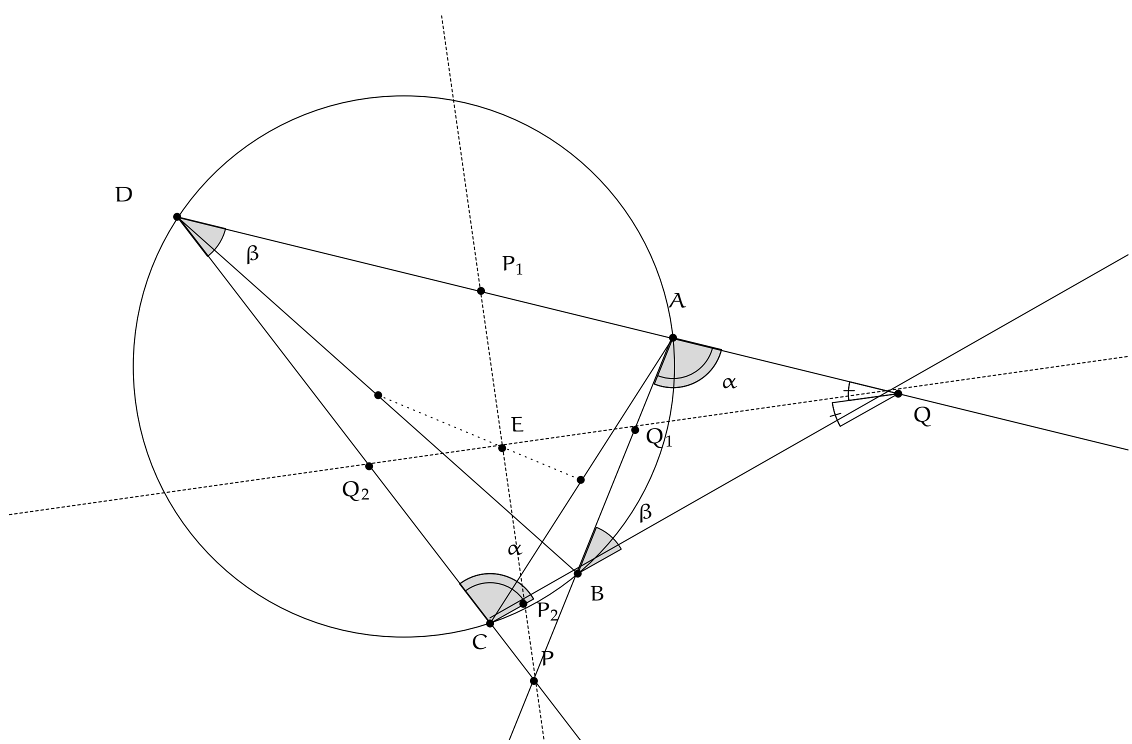
Les trois triangles ont le même centre du cercle circonscrit. Soit O_{BE} la projection orthogonale de O sur BE. On note r_{XYZ} le rayon du cercle inscrit du triangle XYZ. Par un lemme vu en cours :

$$\begin{aligned} OO_{BE} + OO_{CE} + OO_{BC} &= R + r_{BEC} \\ OO_{AB} + OO_{AE} - OO_{BE} &= R + r_{ABE} \\ OO_{CD} + OO_{DE} - OO_{CE} &= R + r_{CDE} \end{aligned}$$

$$r_{BEC} + r_{ABE} + r_{CDE} = OO_{AB} + OO_{BC} + OO_{CD} + OO_{DE} + OO_{EA} - 3R$$

qui est invariant. Lorsque O n'est pas à l'intérieur de $ABCDE$, cela se fait de la même façon.

<u>*Solution de l'exercice 4*</u> Introduisons Q_1 et Q_2 les intersections de la bissectrice de $\widehat{Q}$ avec AB et CD.



Par la loi des sinus,

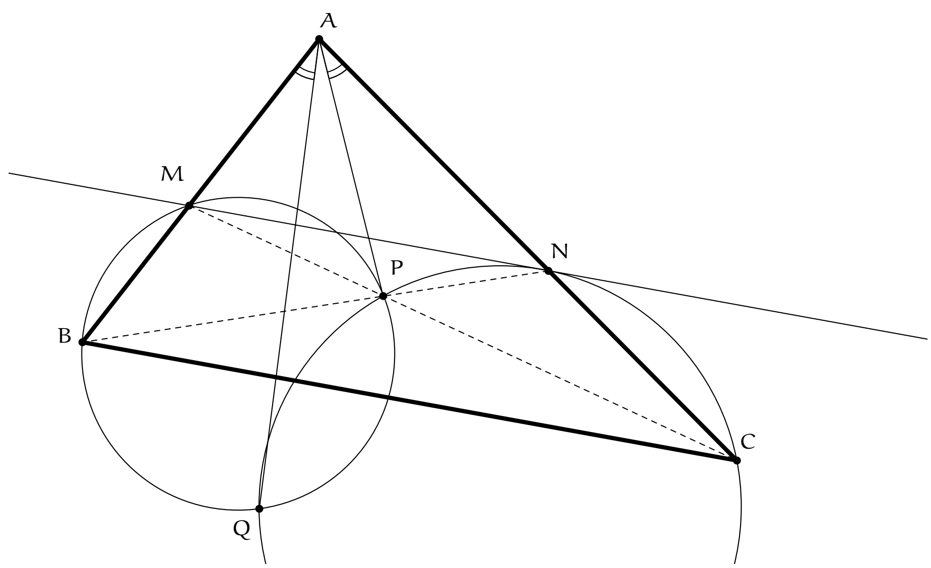
$$\frac{BQ_1}{\sin(\gamma)} = \frac{QQ_1}{\sin(\beta)} \text{ et } \frac{AQ_1}{\sin(\gamma)} = \frac{QQ_1}{\sin(\alpha)} \text{ donc } \frac{BQ_1}{AQ_1} = \frac{\sin(\alpha)}{\sin(\beta)},$$

et de même

$$\frac{DQ_2}{CQ_2} = \frac{\sin(\alpha)}{\sin(\beta)}$$

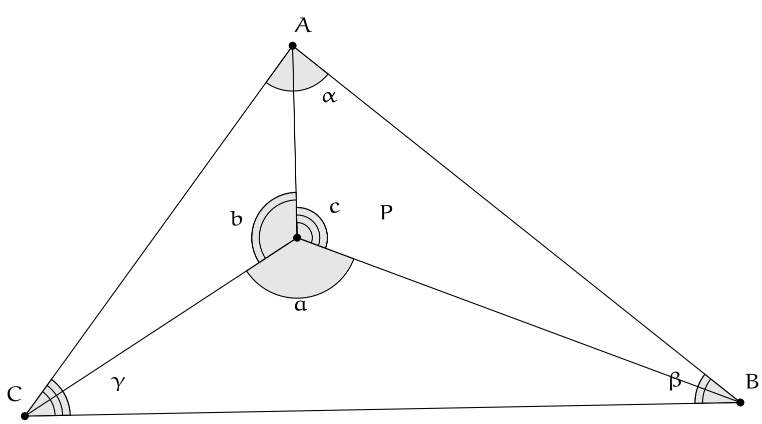
donc si X est le barycentre de $((A, \sin(\alpha)); (B, \sin(\beta)); (C, \sin(\alpha)); (D, \sin(\beta)))$, il est facile de montrer que X est sur le segment Q_1Q_2. On prouve de la même manière que X est sur le segment P_1P_2, et il est évident que X est sur le segment qui joint les milieux des diagonales.

Solution de l'exercice 5 Nous allons considérer l'involution $\mathcal{I}_A$ de centre A qui échange M et C.



On remarque également que Q est le point de Miquel de CM, BN, AB, AC. Donc les cercles circonscrits des triangles AMC, ANB, BPM et CNP passent tous par Q. L'involution $\mathcal{I}_A$ échange les droites (AB) et (AC). Par thalès, $AM \cdot AC = AN \cdot AB$, donc $N \leftrightarrow B$. On en déduit $(CM) \leftrightarrow C_{AMC}$, et de même $(BN) \leftrightarrow C_{ANB}$. Donc en regardant l'intersection, $P \leftrightarrow Q$. Après cela il est facile de vérifier que $\widehat{BAQ} = \widehat{PAC}$.

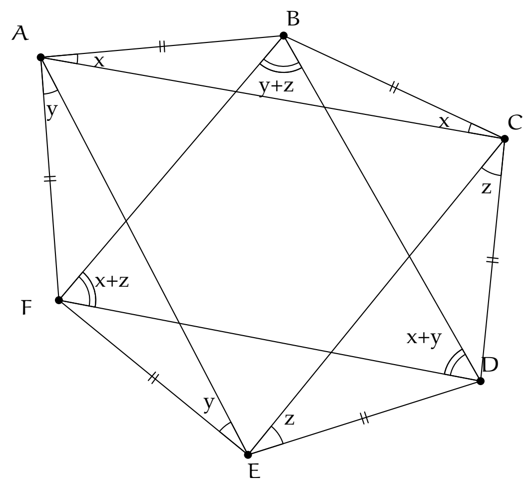
Solution de l'exercice 6 Commençons par nommer tous les angles :



Par hypothèse $a - \alpha = b - \beta = c - \gamma = \theta$. Comme $\alpha + \beta + \gamma = 180°$ et $a + b + c = 360°$, $\theta = 60°$.

On veut montrer que $PA \cdot BC = PB \cdot AC$, ou encore $|b_{ABCP}| = 1$ (le birapport). On vérifie avec les opérations sur les birapports que $b_{ABPC} + b_{ACBP} = 1$. De plus $\arg(b_{ABPC}) = -\arg(b_{ACBP}) = 60°$. Il est facile de voir qu'alors si on place les birapports sur le plan complexe avec les points 0 et 1, on se retrouve avec des triangles equilatéraux. Donc ça marche.

<u>*Solution de l'exercice 7*</u> On considère qu'on avait un triangle ACE auquel on a ajouté 3 triangles isocèles d'angle à la base x, y et z respectivement.



Par hypothèse, $\widehat{B} + \widehat{D} + \widehat{F} = 360°$, ce qui permet de vérifier que $x + y + z = 90°$

Ensuite, on vérifie que que le produit des rapports $r_{AEF} \cdot r_{ECD} \cdot r_{CAB} = 1$ (ce sont trois rotations puisque les longueurs sont égales, et la somme des angles fait 360°. Par une propriété du cours, on sait qu'il existe une involution telle que $A \leftrightarrow D$, $E \leftrightarrow B$ et $C \leftrightarrow F$. Donc $r_{DBF} \cdot r_{BCA} \cdot r_{CDE} = 1$, ce qui implique que $\widehat{BFD} = x + y$. Ensuite, si on appelle x', y', z' les angles de base des triangles DEF, BCD et EFA respectivement, et que l'on utilise la relation $x+y+z = 90°$, on trouve que $x = x'$, $y = y'$ et $z = z'$. Regardons maintenant les droites BF et EC : $\widehat{FBC} = 2y+z$ et $\widehat{BCE} = 2x + z$, donc $(BF)//(EC)$, le quadrilatère $BCFE$ est un parallélogramme, les diagonales se coupent en leur milieu, l'hexagone a un centre de symétrie, l'exo est fini.

III. Deuxième période

Contenu de cette partie

1 Incontournables (4èmes-3èmes) : stratégies de base

Nous renvoyons aux différents cours de stratégies de base sur le site d'Animath pour des détails et compléments (voir les liens en haut de la page 14).

1 Premier cours : récurrence

- Exercices vus en cours -

Exercice 1 Déterminer la somme $1 + 2 + \cdots + n$.

Exercice 2 Montrer que

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

Exercice 3 Déterminer

$$1^3 + 2^3 + \cdots + n^3.$$

Exercice 4 Déterminer les $n \in \mathbb{N}$ tels que $2^n \geqslant n^2$.

Exercice 5 Déterminer les $n \in \mathbb{N}$ tels que $3^n > n^2 - 2n + 91$.

Exercice 6 Montrer que

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2.$$

Solution de l'exercice 6 On peut montrer par recurrence que

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leqslant 2 - \frac{1}{n}.$$

Exercice 7 Si on enlève d'un damier deux coins opposés, ils reste 62 cases. Peut-on paver les 62 cases par 31 dominos ?

Exercice 8 Si on enlève d'un damier une case blanche et une case noire, peut-on paver les 62 cases qui restent par 31 dominos ?

2 Deuxième cours : principe des tiroirs

- Principe des tiroirs -

Le principe des tiroirs semble très évident lorsqu'on l'énonce, pourtant c'est un principe étonnamment puissant, utilisé dans un grand nombre de démonstrations mathématiques.

Si l'on place plus de n objets dans n tiroirs, l'un des tiroirs au moins contiendra au moins deux objets.

Il est important que le nombre d'objets soit strictement supérieur au nombre de tiroirs, sinon on pourrait placer un objet par tiroir. Il faut donc compter précisément le nombre d'objets et le nombre de tiroirs pour pouvoir appliquer ce principe.

La première utilisation mathématique de ce principe des tiroirs date du milieu du XIX° siècle. Il s'agissait de prouver que l'écriture décimale d'une fraction $\frac{p}{q}$ était périodique, de période strictement inférieure à q. Le résultat était déjà connu par ailleurs, mais avec une démonstration beaucoup plus laborieuse. Là, il suffit d'observer le processus de division : par exemple, si l'on divise 5 par 7, dans 50 il va 7 fois 7, il reste 1. Dans 10 il va 1 fois 7, il reste 3. Dans 30 il va 4 fois 7, il reste 2. Dans 20 il va 2 fois 7, il reste 6, et ainsi de suite... Les restes sont tous compris entre 0 et $q-1$, et si l'un des restes est nul, la division s'arrête : le quotient est de période 1 puisqu'il n'y a plus que des 0 à partir d'un certain rang. Sinon, parmi q restes consécutifs, compris entre 1 et $q-1$, au moins deux sont égaux, et à partir du moment où deux restes sont égaux les suivants le sont également, d'où la périodicité.

Le principe des tiroirs admet une variante : si l'on place dans n tiroirs strictement plus de kn objets, au moins un tiroir contiendra au moins $k+1$ objets. Un exemple tout bête : chaque Parisien a au plus 300 000 cheveux, or il y a 3 000 000 de Parisiens. On en déduit qu'on peut trouver dix Parisiens ayant le même nombre de cheveux. Les tiroirs, c'est les nombres de cheveux, et les objets, les Parisiens. Attention qu'il y a 300 001 tiroirs, à savoir tous les nombres entre 0 et 300 000. Pour pouvoir affirmer qu'on peut trouver onze Parisiens ayant le même nombre de cheveux, il faut qu'il y ait strictement plus que $10\times$ 300 001 Parisiens, donc au moins 3 000 011.

- Énoncés des exercices vus en cours -

Exercice 1

Un grand maître joue au moins une partie d'échecs chaque jour, mais au plus dix chaque semaine. Montrer que parmi six semaines consécutives, on peut trouver une période de n journées consécutives au cours desquelles il aura joué exactement 21 parties.

Exercice 2

Montrer que pour tout entier $n > 0$, il existe un multiple non nul de n d'au plus n chiffres tous égaux à 0 ou 1.

Exercice 3

On choisit dix entiers quelconques de deux chiffres, donc entre 10 et 99. Montrer que parmi eux, on peut trouver deux sous-ensembles disjoints d'entiers de même somme.

Exercice 4

On colorie chaque point du plan en rouge ou bleu.

a) Montrer que pour tout réel $x > 0$, il existe une couleur telle qu'on puisse trouver deux points du plan de cette même couleur distants de x.

b) Montrer qu'il existe une couleur telle que pour tout réel $x > 0$, on puisse trouver deux points du plan de cette même couleur distants de x.

Exercice 5

On place 51 points dans un carré de côté 1, de manière quelconque. Montrer qu'on peut trouver un cercle de rayon $\frac{1}{7}$ contenant au moins trois d'entre eux (le cercle peut déborder le carré).

Exercice 6

On considère dix entiers quelconques, $a_1, a_2, ... a_{10}$. Montrer qu'on peut choisir, parmi $\{-1, 0, 1\}$, dix nombres $b_1, b_2, ... b_{10}$ non tous nuls tels que : $b_1 a_1 + b_2 a_2 + ... + b_{10} a_{10}$ soit divisible par 1000.

- Solutions -

Solution de l'exercice 1

Appelons $a_1, a_2, ...a_k...$ le nombre de parties qu'il a jouées le premier jour, les deux premiers jours, ... les k premiers jours. Cette suite est strictement croissante, car chaque jour il joue au moins une partie, et en six semaines il aura joué au plus 60 parties : $1 \leqslant a_1 < a_2 < ... < a_{42} \leqslant 60$. Si le grand maître joue 21 parties au cours des n premiers jours, $a_n = 21$. S'il joue 21 parties entre le $(k+1)$ème jour et le $(k+n)$ème jour, $a_{k+n} = a_k + 21$. Il va donc falloir comparer les termes de la suite $a_1, a_2, ...a_k, ...a_{42}$ à ceux de la suite : $21, a_1 + 21, a_2 + 21 ... a_k + 21 ... a_{42} + 21$, et montrer qu'un terme de la première suite est égal à un terme de la seconde suite. Or $21 < a_1 + 21 < a_2 + 21 < ... < a_{42} + 21 \leqslant 81$. Les 42 termes de la première suite et les 43 de la seconde suite, soit en tout 85 entiers, se trouvent tous entre 1 et 81 : d'après le principe des tiroirs, il y en a nécessairement deux qui sont égaux, et comme ce ne peut pas être deux termes de la première suite, strictement croissante, ni deux termes de la seconde suite, ce sont nécessairement un terme de la première suite égal à un terme de la seconde suite, ce qui achève la démonstration.

Solution de l'exercice 2

Ici, les tiroirs seront les restes de la division par n, et les objets, des nombres dont la différence s'écrive seulement avec des 0 et des 1. Plus précisément, choisissons pour objets les nombres : $a_0 = 0, a_1 = 1, a_2 = 11, a_3 = 111, \ldots, a_n = 11\ldots, 1$ qui s'écrivent avec $0, 1, 2, ...n$ chiffres 1. Il y a $n+1$ objets, et leurs restes de la division par n peuvent prendre n valeurs distinctes : $0, 1, ...n-1$. Donc deux de ces nombres auront même reste de la division par n : $a_i = nq_i + r$ et $a_j = nq_j + r$, et leur différence (en supposant $i > j$) : $a_i - a_j = n(q_i - q_j)$ sera divisible par n. Or cette différence s'écrira avec $(i-j)$ fois le chiffre 1 suivis de j fois le chiffre 0, ce qui est conforme à l'énoncé.

Solution de l'exercice 3

Combien peut-on trouver de sous-ensembles de notre ensemble de dix entiers ? $2^{10} = 1024$. Pour chacun des dix entiers, on peut le choisir ou ne pas le choisir, ce qui constitue dix choix binaires indépendants. Et combien y a-t-il de sommes distinctes d'éléments d'un tel sous-ensemble ? En tout cas moins que mille. La plus grande somme possible est : $99 + 98 + ... + 90 < 1000$, et la plus petite est 10. Donc deux sous-ensembles A et B auront même somme. Rien ne prouve qu'ils sont disjoints, mais ils sont distincts, et s'ils ont une intersection non vide C, en retirant de chacun d'eux les éléments de l'intersection, les sous-ensembles restants deviendront disjoints, et ils auront encore même somme car chaque somme sera diminuée de la somme des éléments de l'intersection.

Solution de l'exercice 4

Les deux questions sont assez différentes, et la deuxième nécessite pas mal de logique.

Pour la question a), il suffit de construire un triangle équilatéral de côté x : nécessairement deux des sommets de ce triangle équilatéral sont de même couleur, ce sont les deux points cherchés.

Pour la question b) : raisonnons par l'absurde. La conclusion serait fausse si pour chacune des couleurs rouge et bleu, on pouvait trouver un réel (x pour rouge et y pour bleu) de telle sorte que deux points rouges ne soient jamais distants de x, ni deux points bleus de y. Supposons $x \geqslant y$. Si tous les points du plan étaient bleus, on aurait deux points bleus distants de y, ce qui contredit la négation de notre conclusion. On supposera donc qu'un point A au moins est rouge, et on construit un triangle ABC avec $AB = AC = x, BC = y$, ce qui est possible car $x \geqslant y$. Si l'un des points B ou C est rouge, on aura deux points rouges distants de x. Si B et C

sont tous deux bleus, on aura deux points bleus distants de y. Dans tous les cas, la négation de la conclusion est contradictoire, donc la conclusion (ce que l'on doit démontrer) est juste.

Solution de l'exercice 5

Pour appliquer le principe des tiroirs et prouver que l'un des n tiroirs contient au moins 3 points, il faut que $51 > 2n$ donc $n \leqslant 25$. Or il est facile de partager le carré en 25 carrés de côté $\frac{1}{5}$. Pour chacun des côtés communs à deux carrés, il faut convenir auquel des carrés on le rattache, de sorte qu'on ait une réelle partition du carré en sous-ensembles disjoints. Chaque point appartient à un petit carré, donc il existe un petit carré contenant au moins trois points. Reste à voir qu'il existe un cercle de rayon $\frac{1}{7}$ contenant ce carré, car la diagonale du carré, $\frac{\sqrt{2}}{5}$ est inférieure au diamètre du cercle $\frac{2}{7}$.

Solution de l'exercice 6

Cet exercice s'apparente à celui sur les dix entiers entre 10 et 99. Considérons toutes les sommes possibles $c_1a_1 + c_2a_2 + ... + c_{10}a_{10}$ où $c_1, c_2, ...c_{10}$ sont choisis parmi $\{0, 1\}$. Il y en a $2^{10} = 1024$, car chaque c_i peut être choisi indépendamment parmi deux valeurs. Les restes des divisions par 1000 de ces sommes peuvent prendre 1000 valeurs distinctes (les trois derniers chiffres du nombre s'il est positif), de 0 à 999. Donc parmi ces 1024 sommes, nécessairement deux au moins auront même reste de la division par 1000, ce qui signifie que leur différence sera divisible par 1000. Or une différence de deux sommes du type $c_1a_1 + ... + c_{10}a_{10}$ avec $c_i = 0$ ou 1 est précisément une somme du type $b_1a_1 + b_2a_2 + ... + b_{10}a_{10}$ avec $b_i = -1, 0$ ou 1.

3 Cours/TD : invariants, inclusion-exclusion

- Les invariants -

Le principe des invariants est assez vague, c'est plutôt une méthode qu'un énoncé mathématique précis.

PRINCIPE DES INVARIANTS - Si une quantité est conservée par certaines transformations, alors il est impossible de passer d'une situation à une autre où la quantité est différente en utilisant seulement ces transformations.

Nous avons déja utilisé ce principe pour l'exercice des dominos. Si on enlève une case à un échiquier de taille 8×8, on ne peut pas le paver avec des dominos de taille 1×2 car le nombre initial de cases à paver (63) est impair, et lorsqu'on pose un domino, cela ne change pas la parité du nombre de cases restant à paver. Pour montrer que si on enlève deux cases situées à des coins opposés de l'échiquier, on ne peut pas non plus le paver avec des dominos, nous avons également utilisé le principe des invariants : un domino recouvre toujours une case blanche et une case noire de l'échiquier, donc si le nombre de cases blanches n'est pas égal au nombre de cases noires, impossible de paver la zone avec des dominos.

Nous allons voir d'autres exemples d'utilisation d'invariants. Commençons tout doucement.

Exercice 1 Une feuille de papier est déchirée en trois parties. Ensuite, l'une de ces parties est déchirée de nouveau en trois parties, et ainsi de suite. Peut-on obtenir, en fin de compte, un total de cent parties ?

Exercice 2 On considère le tableau de signes suivant :

$$\begin{array}{cccc} + & + & - & + \\ - & - & + & + \\ + & + & + & + \\ + & + & + & + \end{array}$$

On répète plusieurs fois l'opération qui consigne à choisir une ligne ou une colonne et à en changer tous les signes en leurs opposés. Est-il possible d'atteindre un tableau constitué seulement de signes $-$?

Exercice 3 Est-il possible de répartir les entiers $1, 2, \ldots, 33$ en 11 groupes disjoints de trois éléments chacun, de sorte que dans chaque groupe, l'un des éléments soit la somme des deux autres ?

Exercice 4 On écrit les nombres $1, 2, 3, \ldots, 2013$ sur une feuille de papier, puis on choisit deux nombres quelconques qu'on efface et on les remplace par leur différence. Est-il possible que le dernier nombre restant soit 2 ?

Exercice 5 Sur une île vivent 34 caméléons, qui peuvent prendre 3 couleurs : jaune, rouge et vert. Au début 7 sont jaunes, 10 rouges et 17 verts. Lorsque deux caméléons de couleurs différentes se rencontrent, ils prennent simultanément la troisième couleur. Il se trouve qu'au bout d'un certain temps, tous les caméléons de l'île ont pris la même couleur. Quelle est cette couleur ? (Il faut en particulier montrer que c'est la seule possible.)

Exercice 6 A partir d'un triplet (a, b, c), on peut effectuer l'opération suivante :
– On choisit deux des nombres du triplet, mettons x et y
– On remplace x par $(x-y)/\sqrt{2}$ et y par $(x+y)/\sqrt{2}$, en laissant le troisième nombre inchangé.

Peut-on passer du triplet initial $(2, \sqrt{2}, 1/\sqrt{2})$ au triplet $(1, \sqrt{2}, 1+\sqrt{2})$ en respectant ces règles ?

Exercice 7 On écrit les nombres $1, 2, 3, \ldots, 100\,000$ sur une feuille de papier, puis on remplace chaque nombre par la somme de ses chiffres, et ainsi de suite, jusqu'à ce que chaque nombre ne soit constitué que d'un seul chiffre. Quel est le chiffre le plus fréquent de la liste obtenue ?

- Comptage et inclusion-exclusion -

PRINCIPE D'INCLUSION-EXCLUSION - On note $|A|$ le nombre d'objets d'un ensemble A. Si A, B, C sont des ensembles, alors on a :

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Pour démontrer ces formules, le plus simple est de dessiner des patates !

Exercice 8 Combien y a t-il de nombres à moins de quatre chiffres (de 0 à 9999) qui ne sont divisibles ni par 3, ni par 5, ni par 7 ?

Exercice 9 Un cube $20 \times 20 \times 20$ est divisé en 8000 cubes unités. On écrit un nombre dans chaque cube unité. Dans chaque ligne et dans chaque colonne de 20 petits cubes, parallèle à une des arêtes du cube, la somme des nombres fait 1. Dans un des petits cubes, le nombre écrit est 10. Par ce petit cube passent trois couches $1 \times 20 \times 20$ parallèles aux faces du cube. Trouver la somme de tous les nombres en dehors de ces trois couches.

- Solution des exercices -

Solution de l'exercice 1 L'invariant est simplement la parité du nombre de morceaux. A chaque étape, le nombre total de morceaux augmente de 2. Comme il vaut 1 au début, on ne peut atteindre 100.

Solution de l'exercice 2 L'invariant est la parité du nombre de $-$. Si dans la ligne ou colonne choisie, il y a n signes $-$, alors après inversion des signes, il y en a $4-n$. Et $4-n$ a même parité que n. Or, il y a initialement 3 signes $-$, donc le nombre de signes $-$ reste impair : il ne sera jamais égal à 16.

Solution de l'exercice 3 Dans un groupe donné (x, y, z), l'un des nombres, mettons z, est égal à la somme des deux autres. Donc la somme des trois nombres, qui vaut $x+y+z = x+y+(x+y) = 2*(x+y)$ est paire. S'il était possible d'effectuer une telle répartition, la somme totale des nombres de 1 à 33 serait donc paire, puisqu'elle pourrait se décomposer en la somme de 11 nombres pairs. Or, $1+2+3+\ldots+33 = 33 \times 34/2 = 33 \times 17$, c'est un nombre impair.

Solution de l'exercice 4 Un invariant est ici la parité du nombre de nombres impairs de la liste. Si les nombres x et y choisis sont tous les deux impairs, le nombre de nombres impairs diminue de 2. Dans les autres, cas, on vérifie qu'il ne change pas. Donc la parité du nombre de nombres impairs de la liste est conservée. Il y a initialement 1007 nombres impairs écrits, donc le dernier nombre de peut pas être 2.

Solution de l'exercice 5 La configuration initiale est $(7J, 10R, 17V)$. On commence par constater que les caméléons peuvent être tous verts : c'est le cas si les 7 jaunes rencontrent des caméléons rouges, on passe alors à $(0J, 3R, 31V)$. Puis un rouge rencontre un vert : $(2J, 2R, 30V)$. Et enfin, les 2 jaunes et les 2 rouges se rencontrent : $(0J, 0R, 34V)$. Il reste à montrer que le vert est la seule couleur pour laquelle c'est possible.

Si x, y, z sont respectivement les nombres de caméléons jaunes, rouges et verts, le reste dans la division euclidienne de $y-x$ par 3 est un invariant. En effet, selon les rencontres, on passera de (x, y, z) à $(x+2, y-1, z-1)$, à $(x-1, y+2, z-1)$ ou à $(x-1, y-1, z+2)$. Dans le dernier cas, la différence entre le nombre de caméléons rouges et le nombre de caméléons jaunes ne change pas. Dans les deux premiers cas, elle diminue ou augmente de 3. Or au départ, cette différence est un multiple de 3, donc c'est vrai à toute étape. Comme 34 n'est pas un multiple de 3, si tous les caméléons sont unis, ils sont forcément verts.

Solution de l'exercice 6 Ici, un invariant est donné par $a^2+b^2+c^2$. Or on constate que la somme des carrés n'est pas la même pour les deux triplets, donc on ne peut pas passer de l'un à l'autre avec la transformation indiquée.

Solution de l'exercice 7 Il s'agit ici de remarquer que pour tout entier n la somme des chiffres de n est congrue à n modulo 9. La suite obtenue est donc périodique : $1, 2, 3, 4, 5, 6, 7, 8, 9, 1, 2, 3, 4, \ldots$ et on termine par un 1, c'est donc lui qui apparaît le plus souvent.

Solution de l'exercice 8 On définit A comme l'ensemble des nombres divisibles par 3, B comme l'ensemble des nombres divisibles par 5 et C comme l'ensemble des nombres divisibles par 7.

Le résultat demandé vaut $10\,000 - |A \cup B \cup C|$. Il ne reste qu'à appliquer la formule d'inclusion-exclusion, en constatant que $A \cap B$ est l'ensemble des nombres divisibles par 15, etc. Si on ne se trompe pas, on tombe sur 4571.

Solution de l'exercice 9 Calculons la somme sur l'union des trois couches en utilisant le principe d'inclusion-exclusion. On obtient $20 + 20 + 20 - 1 - 1 - 1 + 10 = 67$. La somme de tous les nombres du cube vaut 400. Le résultat final est donc $400 - 67 = 333$.

4 TD

- Énoncés -

Exercice 1 On choisit 55 entiers distincts entre 1 et 99. Peut-on trouver parmi ces entiers 2 dont la différence est 9 ? Même question pour 10, 11, 12 et 13.

Exercice 2 Montrer que, pour tout $n > 5$, il est possible de découper un carré en n petits carrés. Montrer que ce n'est pas possible pour n valant 2 ou 3.

Exercice 3 On prend tous les piques d'un jeu de cartes, et on joue à la réussite suivante : on regarde le numéro i de la carte du dessus (avec la convention que le valet vaut 11, la dame 12 et le roi 13). On prend les i premières cartes du paquet, on les retourne, puis on les repose sur le dessus du paquet. Par exemple, on passe de V,4,9,1,D,10,3,5,R,2,8,6,7 à 8,2,R,5,3,10,D,1,9,4,V,6,7, où la carte la plus à gauche est celle au dessus du paquet. On gagne si, à un moment donné, la carte du dessus est l'as. Prouver que l'on gagne à tous les coups.

Exercice 4 Alice et Bob jouent au jeu suivant : 2012 points sont disposés régulièrement autour d'un cercle. Alice commence. Les deux joueurs jouent chacun leur tour, et ont le droit de retirer un des points, ou de retirer 2 points consécutifs (plus précisément, deux points qui étaient consécutifs dans la position de départ à 2012 points). Le gagnant est celui qui efface le dernier point. Qui gagne ? Même question si on modifie la définition des points consécutifs en disant qu'il ne devaient pas forcément être consécutifs dans la position de départ.

Exercice 5 Montrer qu'un polyèdre convexe possède toujours deux faces qui ont le même nombre d'arêtes. (Un polyèdre est convexe s'il n'a pas de "renfoncement" ou, plus formellement, si pour tout couple de points situés à l'intérieur du polyèdre, le segment reliant ces deux points est entièrement situé à l'intérieur du polyèdre).

- Corrigé -

Solution de l'exercice 1 La question demande de trouver deux éléments vérifiant une même propriété, il faut donc penser immédiatement au principe des tiroirs. Il nous faut choisir des tiroirs tels que, si deux éléments sont dans le tiroir, alors leur différence est 9. On veut donc des tiroirs du style : $(1, 10)$. Regardons combien de tels tiroirs on peut construire. On commence par :

$$(1, 10), (2, 11), (3, 12), \ldots, (8, 17), (9, 18).$$

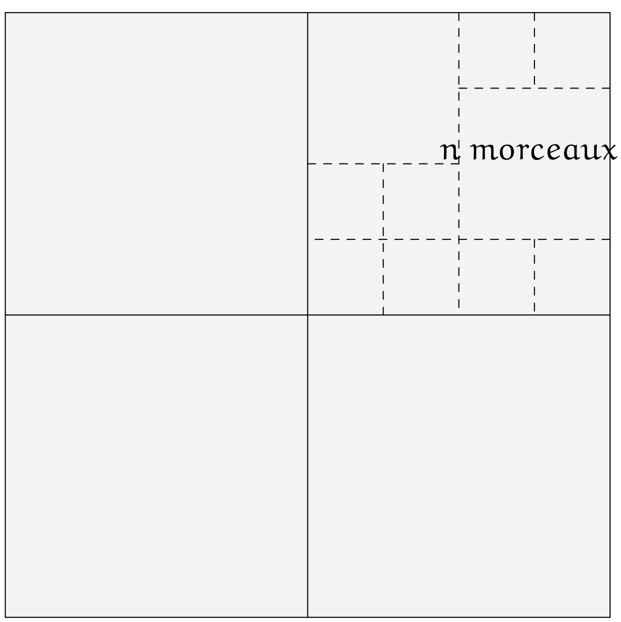
Ensuite, on ne peut pas mettre le tiroir $(10, 19)$, car 10 est déjà dans le tiroir $(1, 10)$. On continue donc par le tiroir $(19, 28)$, et ainsi de suite. Cette construction permet de grouper les entiers en tiroirs par paquets de 18. On peut donc grouper tous les entiers inférieurs à

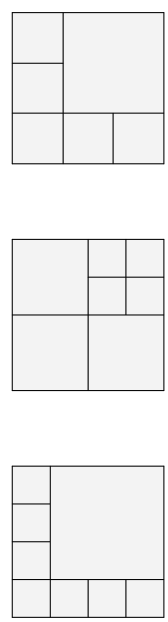
$18 \cdot 5 = 90$ en 45 tiroirs. Il nous reste les 9 entiers compris entre 91 et 99, que l'on ne peut plus grouper par paires. Ce n'est pas grave, on crée simplement un nouveau tiroir pour chacun de ces entiers. On a $45 + 9 = 54$ tiroirs, 55 entiers, il y en a donc deux dans le même tiroir, et leur différence est forcément égale à 9. Cette méthode marche de la même façon pour 10,12 et 13 (elle permet même de prouver des résultats plus forts : par exemple on n'a pas besoin de 55 entiers pour être sûr que deux d'entre eux ont pour différence 10).

Par contre, cela ne marche pas pour 11 : dans ce cas, les tiroirs commencent par $(1, 12)$, $(2, 13), \ldots, (11, 22)$: ils sont groupés par paquets de 22. On peut donc grouper les $22 \cdot 4 = 88$ premiers entiers en 44 tiroirs, et on met les 11 entiers restant de 89 à 99 dans des tiroirs à part, ce qui nous fait $44 + 11 = 55$ tiroirs au total, ce qui ne permet pas de conclure.

Cherchons donc un contre exemple permettant de prouver que ce n'est pas toujours possible. Pour cela, il faut que chacun de nos 55 tiroirs contienne exactement 1 entier (si un de nos tiroirs est vide, alors on a au plus 44 tiroirs non vides, et par principe des tiroirs un de ces 44 tiroirs contient deux entiers). On doit donc nécessairement prendre les entiers de 89 à 99. Maintenant, regardons le tiroir $(77, 88)$. On doit choisir un entier de ce tiroir, mais cela ne peut pas être 88 car on a déjà pris 99 et que $99 - 88 = 11$. On est donc forcé de prendre 77. En répétant ce raisonnement on voit que, pour avoir un contre exemple, il faut obligatoirement choisir les 55 entiers de la sorte : ceux de 1 à 11, puis ceux de 23 à 33, puis ceux de 45 à 55, puis ceux de 67 à 77, et enfin ceux de 89 à 99. On vérifie facilement que ce contre-exemple fonctionne. Il aurait certes été facile de trouver ce contre-exemple soi-même à la main, mais on voit que la méthode du principe des tiroirs permet de montrer quelque chose de plus fort : l'unicité du contre-exemple.

<u>*Solution de l'exercice 2*</u> En faisant des essais à la main, on voit facilement que le découpage est possible pour n valant 6, 7 ou 8, comme le montre la figure suivante :





Ces essais nous montrent aussi autre chose : si on a un découpage d'un carré en n petits carrés, alors on peut facilement construire un découpage en $n + 3$ petits carrés : il suffit de découper en 4 un carré du découpage d'origine.

Cela permet de terminer par récurrence, mais c'est une récurrence un peu plus générale que celle enseignée par Theresia, dans laquelle on se servait uniquement de la propriété au rang n pour la prouver au rang $n + 1$.

Proposition 19. Principe de récurrence forte : si une propriété P est vraie au rang 1 (initialisation), et si le fait que P est vraie pour tous les rangs inférieurs à n implique le fait qu'elle soit vraie au rang $n + 1$ (propagation), alors la propriété est vraie pour tout n.

Cela paraît logique. Une preuve par récurrence, c'est une façon plus formelle de rédiger des démonstrations "de proche en proche". Et si on démontre une propriété P de proche en proche, quand on veut la prouver au rang 100, on sait déjà qu'elle est vraie aux rangs allant de 1 à 99, donc on peut utiliser tout cela dans notre preuve du rang 100.

Voyons comment rédiger cette récurrence pour notre exercice : on initialise en prouvant que le découpage est possible aux rangs 6, 7 et 8. Maintenant, soit n plus grand que 8, supposons que le découpage est possible à tous les rangs compris entre 6 et n. Alors en particulier le découpage est possible au rang $n - 2$ (car comme $n \geqslant 8$, $n - 2 \geqslant 6$), et en découpant en 4 un carré du découpage en $n - 2$ carrés, on obtient un découpage en $n + 1$ carrés, ce qui clôt la récurrence.

Pour montrer que c'est impossible pour 2 ou 3, on pourrait faire des petits raisonnements géométriques plus ou moins vaseux. Mais, comme souvent avec les résultats qui paraissent intuitivement évidents, mais qui semblent délicats à rédiger de façon claire, le principe des tiroirs nous donne un argument massue permettant de tuer le problème. En effet, supposons que l'on ait un découpage en 3 carrés, alors par principe des tiroirs un de ces 3 carrés comporte 2 des sommets du carré d'origine, contradiction.

Solution de l'exercice 3 Après quelques essais, on se fait la réflexion suivante : si, au bout d'un moment, on tombe sur le roi, alors on le met au fond et on peut l'ignorer pendant le reste de la réussite, on s'est donc ramené à un cas plus simple, cela donne l'idée de faire une preuve par récurrence.

Montrons par récurrence sur n que, si on démarre la réussite avec un jeu de n cartes numérotées de 1 à n, alors on gagne. L'initialisation est évidente : avec un jeu de 1 carte on a immédiatement gagné. Supposons le résultat vrai pour un jeu de n cartes, et montrons-le avec un jeu de $n+1$ cartes. Supposons que, au bout d'un moment, on tombe sur la carte $n+1$. Alors on met cette carte au fond, et on peut l'ignorer pendant le reste de la réussite. On s'est donc ramené au cas avec n cartes, que l'on sait résoudre par hypothèse de récurrence. Supposons maintenant que l'on ne tombe jamais sur la carte $n + 1$ (et que cette carte n'est pas placée en dernier). Dans ce cas aussi, on peut ignorer cette carte, et on peut aussi ignorer la carte placée en dernière position, car elle ne bougera jamais. Échangeons donc la carte $n+1$ et la carte placée en dernier (par exemple, on passe de 34,4,5,$n + 1$,9,..., 8 à 34,4,5,8,9,..., $n + 1$). Cela ne changera pas le déroulement de la réussite, et comme la carte $n + 1$ est au fond, on s'est à nouveau ramené au cas du jeu à n cartes, qui gagne par hypothèse de récurrence. Cela termine la preuve.

Une autre observation qui permet de résoudre l'exercice est de remarquer que le paquet de carte se trie de plus en plus au cours de la réussite. Pour pouvoir l'exploiter, il faut trouver un moyen de l'énoncer formellement. Le nombre de cartes à la bonne position n'augmente pas forcément au cour de la réussite, un retournement pouvant changer les positions de plein de petites cartes, mais ce retournement met alors une carte plus grande à sa place, l'idée est donc d'attribuer une plus grande importance aux grandes cartes.

À chaque situation on va associer la liste des cartes qui sont à la bonne position, dans l'ordre décroissant. Par exemple, à la situation D, 2, 4, 6, 5, R, 10, 8, 1, 3, V, 9, 7, on associe la liste $(V, 8, 5, 2)$. On a envie de dire que la liste (5) est plus triée que la liste $(4, 3, 2)$, on décide donc d'utiliser l'ordre du dictionnaire (aussi appelé l'ordre lexicographique) : si on a deux listes, pour voire laquelle est la plus triée, on regarde l'élément le plus à gauche. Si ces deux éléments sont différents, on dit que la liste ayant le plus grand premier élément est la plus grande. S'ils sont identiques, on regarde l'élément suivant, et ainsi de suite. On voit facilement que, à chaque étape, notre opération de retournement trie un peu plus la liste (par exemple, après un retournement de D, 2, 4, 6, 5, R, 10, 8, 1, 3, V, 9, 7, on obtient la liste $(D, 3)$, plus triée que $(V, 8, 5, 2)$ car elle commence par une dame). Or le nombre de listes possibles est fini, donc on ne peut pas continuer à trier indéfiniment. , et bout d'un moment notre réussite s'arrête. On a même montré un résultat un peu plus fort : le nombre de listes est 2^{13}, donc notre réussite s'arrêtera toujours en moins de 2^{13} étapes.

La technique utilisée ici est la technique des monovariants. Un monovariant est une quantité qui, au cours d'un processus, se déplace toujours dans le même sens. Ici, c'était une liste qui se triait, cela peut aussi par exemple être un certain entier qui augmente. Si notre monovariant ne peut pas augmenter indéfiniment, alors cela prouve que le processus s'arête. C'est très important de retenir ceci pour traiter les problèmes parlant de processus. Pour résumer :

– si un problème demande si un processus peut atteindre un certain état, il faut essayer de trouver des invariants
– si un problème demande de prouver qu'un processus s'arête, il faut essayer de trouver des monovariants.

<u>*Solution de l'exercice 4*</u> Nous allons prouver que Bob gagne à tous les coups. Il y a un principe important à connaître pour traiter ces exercices de jeu : 2012, c'est beaucoup, et si on joue un peu n'importe comment, on arrive rapidement à des positions très embrouillés, et à des études de cas affreuses et totalement inextricables. Pour pouvoir prouver ce résultat, il faut donc, à tous les instants, essayer de conserver la position la plus simple possible. Bob à donc intérêt à essayer, après chaque coup d'Alice, de revenir à une position simple.

Ici, la façon de faire est de jouer symétriquement : après qu'Alice efface ses points, Bob efface les points situés à l'opposé des points effacés par Alice. Ainsi, après chaque tour de Bob, on sera revenu à une position symétrique. Avec cette stratégie, la symétrie est donc un invariant. Comme il n'est pas possible de gagner en un coup à partir d'une position symétrique, Alice ne pourra jamais gagner.

Si on change les règles, la situation devient différente. En effet la stratégie précédente ne marche pas toujours : Si Alice arrive à la position comportant 2 points diamétralement opposés, elle gagne en un coup. En fait, dans ce cas Alice possède même une stratégie gagnante : elle commence par enlever 2 points quelconques, pour se ramener à une position à 2010 points. Ensuite, à chaque coup, si Bob retire un point Alice en retire 2, et inversement. Ainsi, après chaque tour d'Alice, le nombre de points sera divisible par 3, et comme il est impossible de gagner en un coup à partir d'une position où le nombre de points est multiple de 3, Alice gagne. On a utilisé exactement les mêmes principes que dans le cas précédent : on a réussi à simplifier les positions, en remarquant que la seule chose importante était le reste de la division du nombre de points par 3, puis, en adoptant une stratégie symétrique, on a réussi à trouver un invariant résolvant le problème.

Solution de l'exercice 5 On doit montrer que deux objets vérifient ensemble une propriété, il faut donc penser au principe des tiroirs. La façon naturelle de faire est de prendre comme chaussettes les faces du polynôme, et comme tiroirs les nombres d'arêtes de chacune des faces. Ainsi, si on a deux chaussettes dans le même tiroir (par exemple deux faces dans le tiroir "3"), alors ces deux faces auront le même nombre d'arêtes (dans notre exemple, ce seront des triangles). Il faut maintenant essayer de compter les chaussettes et les tiroirs.

Comme le polyèdre est par définition fini, la plupart des tiroirs seront inutiles. Plus précisément, supposons que la face du polyèdre ayant le plus d'arêtes possède m arêtes. Alors, les seuls tiroirs utiles seront les tiroirs $(3, 4, 5, \ldots, m)$: il y en a $m - 2$. Pour conclure, il nous suffit de prouver que le polyèdre a plus de $m - 1$ faces. Regardons une face à m arêtes. Cette face a exactement m faces voisines (c'est la que l'on utilise l'hypothèse de convexité), ce qui termine l'exercice.

5 Test

- Énoncés (durée : 3h) -

Exercice 1 On pose, pour n un entier supérieur à 1, $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$. Trouver une formule (et la démontrer) pour la somme

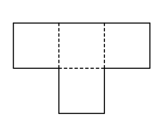
$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \ldots + n \cdot n!.$$

Exercice 2 Quel est le nombre maximal de pions que l'on peut placer sur un damier 12×12 de telle sorte que deux pions ne soient pas sur deux cases adjacentes ? (On dit que deux cases sont adjacentes si elles se touchent par un côté ou un coin).

Exercice 3 Soient A, B et C trois ensembles tels que :
- $|A| = 100$, $|B| = 50$ et $|C| = 48$,
- le nombre d'éléments appartenant à exactement un des trois ensembles est égal au double du nombre d'éléments appartenant à exactement deux des ensembles,
- le nombre d'éléments appartenant à exactement un des trois ensembles est égal au triple du nombre d'éléments appartenant à tous les ensembles.

Combien d'éléments appartiennent à tous les ensembles ?

Exercice 4 Peut-on paver un échiquier 10×10 avec des blocs T ? Un bloc T est de la forme suivante :



- Corrigé -

<u>*Solution de l'exercice 1*</u> En calculant les premières valeurs, on obtient : $1, 5, 23, 119, 719$. Montrons par récurrence que pour tout entier n, on a :

$$1 \cdot 1! + 2 \cdot 2! + \ldots + n \cdot n! = (n+1)! - 1.$$

Pour $n = 1$, on a bien $1 \cdot 1! = (1+1)! - 1 = 1$. Supposons la formule vraie pour un certain entier n. Alors,

$$\begin{gathered} 1 \cdot 1! + 2 \cdot 2! + \ldots + n \cdot n! + (n+1) \cdot (n+1)! \\ = (1 \cdot 1! + 2 \cdot 2! + \ldots + n \cdot n!) + (n+1) \cdot (n+1)! \\ = ((n+1)! - 1) + (n+1) \cdot (n+1)! \\ = (1 + (n+1)) \cdot (n+1)! - 1 \\ = (n+2)! - 1. \end{gathered}$$

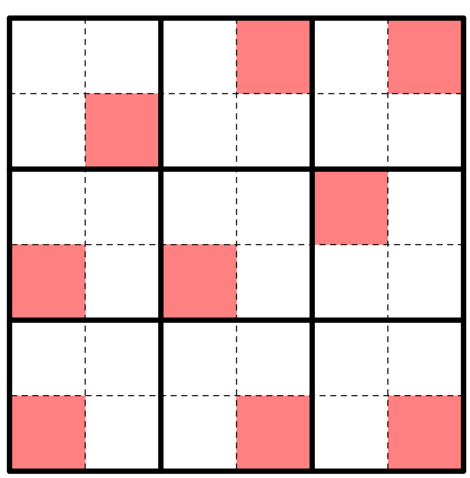
Nous avons montré que si la formule est vraie au rang n, alors elle est vraie au rang $n+1$. Comme elle est vraie pour $n = 1$, ceci termine notre démonstration par récurrence.

<u>*Solution de l'exercice 2*</u>

Il est facile de trouver une configuration avec 36 pions, par exemple en numérotant les lignes et les colonnes du damier, et en plaçant un pion sur chaque case dont les numéros de ligne et de colonne sont pairs. L'intuition nous dit que cette configuration est optimale, il faut maintenant le prouver.

Pour cela, on découpe notre damier en $6 \cdot 6 = 36$ petits blocs de taille 2×2, et on applique le principe des tiroirs. Le principe nous dit que si on place plus de 37 pions sur le damier, deux d'entres eux seront dans le même bloc 2×2, et ces deux pions seront adjacents. On ne peut donc pas faire mieux que 36.

La figure suivante illustre cette preuve dans le cas d'un damier 6×6 (cela marche pareil). Les cases colorées donnent une des configurations optimale. On remarque que cette configuration optimale n'est pas très régulière. En particulier, tous les essais de preuves foireuses à base de "pour que ce soit optimal, on est obligé de placer des pions dans les coins et de placer les autres le plus près possible" sont voués à l'échec.



<u>*Solution de l'exercice 3*</u> Notons x le nombre d'éléments qui appartiennent à exactement un des trois ensembles (c'est-à-dire, qui appartiennent à A mais ni à B ni à C, ou à B mais ni à A ni à C ou à C mais ni à A ni à B). De même, on note y le nombre d'éléments qui appartiennent à exactement deux des trois ensembles, et z le nombre d'éléments qui appartiennent à l'intersection des trois ensembles. D'après l'énoncé, on a $x = 2y = 3z$. Or, lorsqu'on calcule $|A| + |B| + |C|$, on compte deux fois les éléments qui appartiennent à deux ensembles, et trois fois ceux qui appartiennent aux trois ensembles. D'où : $|A| + |B| + |C| = x + 2y + 3z$, soit $100 + 50 + 48 = 198 = x + 2y + 3z$. On obtient donc $198 = 3x$. Ainsi, $x = 66$ et $z = x/3 = 22$. En conclusion, il a 22 éléments qui appartiennent à tous les ensembles.

<u>*Solution de l'exercice 4*</u> On colore les cases en blanc ou en noir selon le motif d'un échiquier classique. Plaçons un T sur cet échiquier. Si sa case centrale est posée sur une case blanche, alors ses trois autres cases sont posées sur une case noire, et inversement. Ainsi, un T couvre forcément un nombre impair de cases noires. Or, pour paver tout l'échiquier, on aurait besoin de 25 blocs T, et 25 blocs T couvrent forcément un nombre impair de cases noires. Comme l'échiquier a exactement 50 cases noires, un nombre pair, c'est impossible.

2 Incontournables (2ndes-1ères) : stratégies de base

Nous renvoyons aux différents cours de stratégies de base sur le site d'Animath pour des détails et compléments (voir les liens en haut de la page 14).

1 Principe des tiroirs

Nous renvoyons au polycopié de stratégies de base disponible sur le site d'Animath pour le cours.

Les exercices sont approximativement classés par thème et par ordre de difficulté.

- Géométrie -

Exercice 1 Montrer qu'un triangle équilatéral ne peut pas être complètement recouvert par deux triangles équilatéraux strictement plus petits.

Exercice 2 On a n points dans l'espace P_1, ..., P_n tels qu'il existe un point P tel que $P_iP < P_iP_j$ pour tout $j \neq i$. Montrer que $n < 15$.

Exercice 3 On place 6 points dans un rectangle 3×4. Montrer que deux points sont à distance $\leqslant \sqrt{5}$.

Exercice 4 On considère 5 points à coordonnées entières P_1, ..., P_5 dans le plan. Montrer qu'il existe un point à coordonnée entière sur un des segments $]P_i, P_j[$.

Exercice 5 Le plan est colorié en deux couleurs (d'une façon quelconque). Montrer qu'il existe une rectangle dont les sommets sont d'une même couleur.

Exercice 6 On colorie certains segments de $[0, 1]$ en rouge. On suppose que deux points rouges ne sont jamais à une distance de 0.1. Montrer que la somme des longueurs de ces segments est $\leqslant 0.5$.

Exercice 7 Prouver que dans un polygone convexe à $2n$ côtés, il existe une diagonale qui n'est parallèle à aucun côté.

- Coloriage -

Exercice 8 Est-il possible de paver un échiquier 8×8 auquel on a enlevé deux coins opposés par des dominos 2×1 ?

Exercice 9 Combien de rois peut-on mettre sur un échiquier 8×8 sans qu'ils se mettent en échec ?

Exercice 10 On pave un sol rectangulaire avec des pièces 1×4 et 2×2. On enlève une pièce. Est-il possible en ajoutant une pièce de type opposé de paver à nouveau le rectangle ?

Exercice 11 On colorie certaines cases d'un échiquier 8×8 en rouge. Combien de cases peut-on colorier au maximum si on veut qu'il n'y ait pas de trimino rouge ? Combien de cases peut-on colorier au minimum si on veut que tout trimino ait au moins une case rouge ?

Exercice 12 On considère un échiquier 9×9 tel que sur chaque case il y a une sauterelle. Chaque sauterelle saute une fois d'une case en diagonale. Combien de cases libres y-a-t-il au minimum ?

- Arithmétique -

Exercice 13 Soient a_1, ..., a_n des entiers. Montrer qu'il existe $1 \leqslant i_1 < ... < i_r \leqslant n$ tels que $a_{i_1} + ... + a_{i_r}$ soit divisible par n.

Exercice 14 Si on se donne $n + 1$ entiers distincts entre 1 et $2n$, au moins deux de ces entiers sont premiers entre eux.

Exercice 15 On se donne des entiers a_1, ..., a_m de $\{1, ..., m\}$. On suppose que toute somme constituée d'un sous-ensemble des a_i n'est pas divisible par $m + 1$. Montrer que tous les a_i sont égaux.

Exercice 16 Si on se donne $n + 1$ entiers (pas forcément distincts) entre 1 et $2n$, un de ces entiers divise un autre.

Exercice 17 Soient a_i des entiers tels que $0 < a_1 \leqslant a_2 \leqslant ... \leqslant a_n \leqslant 2n$. On suppose que pour tout $i \neq j$, $\mathrm{ppcm}(a_i, a_j) \geqslant 2n$. Montrer que $3a_1 > 2n$.

Exercice 18 On considère $\alpha \notin \mathbb{Q}$ (i.e. α ne s'écrit par sous la forme $\frac{a}{b}$ avec a, $b \in \mathbb{Z}$). Par exemple on peut prendre $\alpha = \sqrt{2}$.

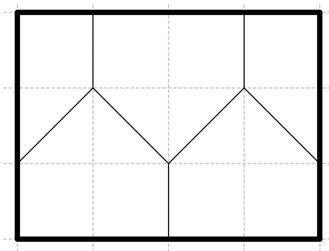
Montrer qu'on peut trouver p, $q \in \mathbb{Z}$ tels que $-\frac{1}{q^2} \leqslant \alpha - \frac{p}{q} \leqslant \frac{1}{q^2}$.

- Solutions de géométrie -

Solution de l'exercice 1 Au moins un des deux triangles contient deux sommets ce qui est impossible.

Solution de l'exercice 2 On a $\widehat{P_iPP_j} > 60$ (en appliquant Al-Kashi dans le triangle P_iPP_j en P par exemple). On considère E_i ($i = 1, ..., n$) qui est l'ensemble des points Q de la sphère unité tel que $\widehat{P_iPQ} \leqslant 30$. Les E_i sont disjoints et la surface de E_i est $2\pi(1 - \cos(30))$. On a donc $n \cdot 2\pi(1 - \cos(30)) < 4\pi$ (la surface de la sphère unité est 4π). Donc $n < 15$.

Solution de l'exercice 3 On pave le rectangle en 5 parties telles que deux points d'une même partie sont à distance $\geqslant \sqrt{5}$.



<u>*Solution de l'exercice 4*</u> On écrit $P_i = (x_i, y_i)$ avec $x_i, y_i \in \mathbb{Z}$. La "parité" du couple (x_i, y_i) peut prendre $2^2 = 4$ valeurs : (P, P), (P, I), (I, P), (I, I) (P pour pair, I pour impair). Par le principe des tiroirs, au moins deux points P_i et P_j sont de même parité. On considère alors le milieu de $[P_i, P_j]$ qui est bien à coordonnées entières.

<u>*Solution de l'exercice 5*</u> Appelons nos deux couleurs rouge et bleu. On considère une grille rectangulaire 7×3 (disons que les colonnes ont 7 points et les lignes ont 3 points). Parmi les 7 points de la première colonne, au moins 4 sont d'une même couleurs, disons bleu. On ne considère plus que le sous-réseau 4×3 qui correspond à supprimer les lignes ne passant pas par les 4 points précédents. Si deux points de la deuxième colonne sont bleus alors on a gagné. Sinon au moins trois points de la deuxième colonne sont rouges. Alors comme deux points de la troisième colonne sont de la même couleur, on a un rectangle rouge ou bleu.

<u>*Solution de l'exercice 6*</u> On divise le segment $[0,1]$ en dix segments $I_k = [\frac{k}{10}, \frac{k+1}{10}]$ $(k = 0, ..., 9)$. On note x_k la longueur des points rouge dans $[\frac{k}{10}, \frac{k+1}{10}]$. On translate les points rouges de I_k dans I_{k+1} : ceux-ci sont disjoints des points rouges de I_{k+1}, donc $x_k + x_{k+1} \leqslant 0.1$. En particulier $x_1 + x_2 \leqslant 0.1$, $x_3 + x_4 \leqslant 0.1$, $x_5 + x_6 \leqslant 0.1$, $x_7 + x_8 \leqslant 0.1$, $x_9 + x_{10} \leqslant 0.1$. En sommant ces 5 inégalités, on a $x_1 + ... + x_{10} \leqslant 0.5$.

<u>*Solution de l'exercice 7*</u> Supposons par l'absurde que toute diagonale est parallèle à un côté. Il y a $n(2n-3)$ diagonales dans un $2n$-gone (choisir le premier sommet de $2n$ façon différentes, puis le deuxième de $2n-3$ façons, mais on compte deux fois chaque diagonale). Une diagonale peut être parallèle à $n-2$ côtés au plus. Donc il y a au plus $2n(n-2) < n(2n-3)$ diagonales, absurde.

- **Solutions Coloriage** -

<u>*Solution de l'exercice 8*</u> Non : on colorie les cases en blanc et noir de la façon habituelle sur un échiquier. Alors il y a 30 cases d'une couleur et 32 d'une autre. Or un domino couvre une case de chaque couleur, donc il devrait y avoir autant de cases noires que de cases blanches.

<u>*Solution de l'exercice 9*</u> Réponse : 16. En effet, on découpe l'échiquier en 16 blocs 2×2 : il y a au plus un roi par bloc donc au plus 16 rois. Réciproquement il est immédiat de trouver 16 rois (on en met un en haut à gauche de chaque bloc).

<u>*Solution de l'exercice 10*</u> Non : on colorie l'échiquier en blanc et noir de façon à ce qu'une pièce 2×2 couvre 1 case noire et qu'une pièce 1×4 couvre 0 ou 2 cases noires. Alors la parité du nombre de cases noires permet de conclure.

<u>*Solution de l'exercice 11*</u> On découpe l'échiquier en 16 blocs 2×2. Il ne peut pas y avoir plus de deux cases rouges par bloc sinon il y aurait un trimino rouge. Donc il y a au plus 32 cases rouges. Réciproquement il est immédiat de trouver un exemple avec 32 cases (mettre deux

cases rouges en diagonale dans chaque bloc).
b) On utilise le même découpage et il y a au moins deux cases rouges par bloc, la réponse est donc 32 cases rouges minimum.

Solution de l'exercice 12 On colorie une colonne sur deux en blanc et les autres colonnes en noir. Alors il y a $4 \times 9 = 36$ cases blanches et $5 \times 9 = 45$ cases noires. Comme une sauterelle va d'une case noire à une case blanche, alors il y a au moins $45 - 36 = 9$ cases libres. réciproquement un exemple pour 36 cases libre est immédiat.

- Solutions d'aritthmétique -

Solution de l'exercice 13 On considère les sommes $s_i = a_1 + ... + a_i$. Il y en a n, donc si elles sont toutes non divisibles par n, au moins deux de ces sommes ont le même reste dans la division euclidienne par n. Disons que $s_i = n \times k + r$ et $s_j = n \times q + r$ avec $i < j$, $0 < r < n$. Alors n divise $s_j - s_i = a_{i+1} + ... + a_i$.

Solution de l'exercice 14 Comme souvent on va montrer quelque chose de plus fort que ce qui est demandé (c'est toute la difficulté ici). Parmi nos $n+1$ entiers, il y a deux entiers consécutifs donc deux entiers premiers entre eux.

Solution de l'exercice 15 Supposons par l'absurde que $a_1 \neq a_2$. On sait que les $s_i = a_1 + ... + a_i$ ont des restes distincts et non nuls par $m+1$. Il y a m tels restes. Donc les s_i prennent tous les restes possibles par la division par $m+1$. Donc il existe $i > 2$ tel que s_i ait le même reste que a_2, d'où n divise $s_i - a_2 = a_1 + a_3 + ... + a_i$ (on a $i \neq 1$ car $a_1 \neq a_2$ et $i \neq 2$ car $m+1$ ne divise pas $a_1 = s_2 - a_2$).

Solution de l'exercice 16 On note a_1, ..., a_{n+1} ces $n+1$ entiers. Si tous les a_i sont impairs, il y en a deux d'égaux donc le résultat est évident. En fait on peut toujours écrire $a_i = 2^{r_i} b_i$ où b_i est impair. Donc il existe $i \neq j$ tel que $b_i = b_j$ et alors a_i divise a_j ou a_j divise a_i.

Solution de l'exercice 17 Si $3a_1 \leqslant 2n$, on peut considérer l'ensemble d'entiers $2a_1, 3a_1, a_2, ..., a_n$ compris entre 1 et $2n$. Par l'exercice 4), un de ces entiers divise un autre, ce qui est impossible vu l'hypothèse sur le ppcm.

Solution de l'exercice 18 On considère $N \geqslant 1$ un entier. On divise l'intervalle $[0, 1]$ en N parties $I_k = [\frac{k}{N}, \frac{k+1}{N}]$. Alors par le principe des tiroirs, parmi les nombres α, 2α, ..., $N\alpha$, $(N+1)\alpha$, deux ont leur partie fractionnaire dans le même I_k, autrement dit il existe $1 \leqslant i < j \leqslant N+1$ tel que $(j-i)\alpha - p \in [-\frac{1}{N}, \frac{1}{N}]$ pour un certain entier p. Soit $q = j - i$. On a $1 \leqslant q \leqslant N$ et $-\frac{1}{q} \leqslant \frac{1}{N} \leqslant q\alpha - p \leqslant \frac{1}{N} \leqslant \frac{1}{q}$.

2 Récurrence

- Rappel de cours -

Soit $\mathcal{P}(n)$ une propriété sur les entiers (par exemple "n est un nombre premier", "un polygone à n côtés est triangulable" ou "$n^3 - n$ est divisible par 3") que l'on veut démontrer pour tout n.

Théorème 20. Si

1. $\mathcal{P}(0)$ est vraie ("initialisation") et
2. si on suppose que $\mathcal{P}(n)$ est vraie, on peut démontrer $\mathcal{P}(n+1)$ ("hérédité")

alors la propriété $\mathcal{P}(n)$ est vraie pour tout entier $n \geqslant 0$.

- Exercices -

Exercice 1 Trouver une formule pour $1 + 2^3 + 3^3 + \cdots + n^3$.

Exercice 2 Regardons la suite de Fibonacci : $F_1 = F_2 = 1$ et $F_{n+2} = F_{n+1} + F_n$. Soit ϕ (resp. ϕ') la solution positive (resp. négative) de l'équation $X^2 = X + 1$. Montrer que :

$$F_n = \frac{\phi^n - \phi'^n}{\sqrt{5}}.$$

Exercice 3 Définissons pour tout $n \geqslant 0$ et tout $0 \leqslant k \leqslant n$ les coefficients binomiaux $\binom{n}{k}$ (prononcez "k parmi n") de la manière suivante :

$$\binom{n}{0} = \binom{n}{n} = 1 \text{ et } \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$

Démontrer que

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

Exercice 4 On trace n cercles dans le plan tels que deux cercles ne soient jamais tangents. Montrer que l'on peut colorier les régions du plan ainsi délimitées de deux couleurs de telle façon que deux régions séparées par un arc de cercle soient de couleurs différentes.

Exercice 5 On trace n droites dans le plan, deux jamais parallèles, trois jamais concourantes. En combien de parties le plan est-il découpé ?

Exercice 6 Montrer que pour tout $n > 5$ il est possible de découper un carré en n carrés plus petits.

Exercice 7 Soit x un réel tel que $x + \frac{1}{x}$ est un entier. Montrer que pour tout n, $x^n + \frac{1}{x^n}$ est un entier.

Exercice 8 On choisit n points sur un cercle et on trace toutes les cordes associées (on se débrouille pour que 3 cordes n e soient jamais concourantes). En combien de parties le cercle est-il découpé ?

Exercice 9 (Les tours de Hanoi) Dans le temple de Bénarès sont érigées trois aiguilles de diamants. Sur l'aiguille de gauche sont enfilés 64 disques d'or pur, le plus large à la base et les autres, de plus en plus étroits, empilés jusqu'au sommet. Nuit et jour, les moines déplacent les disques d'une aiguille à l'autre en suivant deux règles : ils ne peuvent déplacer qu'un disque à la fois, et ils ne peuvent pas poser un disque sur un disque plus petit. Il est dit que lorsque les 64 disques seront sur l'aiguille de droite, le temple s'écroulera et ce sera la fin du monde. Combien de temps nous reste-t-il ?

Exercice 10 Montrer que pour tout entier $x < n!$, il existe $k \leqslant n$ un entier et $d_1, d_2, \ldots, d_k$ des diviseurs deux à deux distincts de $n!$ tels que $x = d_1 + d_2 + \cdots + d_k$.

- Corrigé -

Solution de l'exercice 1 Calculons les premiers termes pour se donner une idée :

$$1\ ;\ 1+8=9\ ;\ 1+8+27=36\ ;\ 1+8+27+64=100\ ;\ 1+8+27+64+125=225\ ;\dots$$

On remarque tout de suite que tous les termes sont des carrés, les carrés de la suite $1, 3, 6, 10, 15$, que l'on reconnait comme la suite $1, (1+2), (1+2+3)$, etc. Nous allons essayer de prouver la formule suivante par récurrence :

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

L'initialisation est facile. Maintenant supposons que la formule est vraie pour n et calculons

$$1+\cdots+n^3+(n+1)^3=\frac{n^2(n+1)^2}{4}+(n+1)^3=\frac{(n+1)^2(n^2+4(n+1))}{4}=\frac{(n+1)^2(n+2)^2}{4}$$

ce qui achève la récurrence.

Solution de l'exercice 2 Commençons par calculer ϕ et ϕ'. C'est un simple trinome du second degré :

$$\phi=\frac{1+\sqrt{5}}{2}\quad \phi'=\frac{1-\sqrt{5}}{2}$$

Il est facile de vérifier que la formule marche pour F_1. Ensuite pour F_2 nous utiliserons la relations $\phi^2=\phi+1$ (pareil pour ϕ') :

$$\frac{\phi^2-\phi'^2}{\sqrt{5}}=\frac{(\phi+1)-(\phi'+1)}{\sqrt{5}}=1=F_2.$$

Interessons nous maintenant à l'hérédité : supposons que la formule est vraie pour F_n et F_{n+1}. Nous utiliserons la formule suivante :

$$\phi^{n+1}+\phi^n=\phi^n(\phi+1)=\phi^n\cdot\phi^2=\phi^{n+2}.$$

$$F_{n+2}=F_{n+1}+F_n=\frac{\phi^{n+1}-\phi'^{n+1}+\phi^n-\phi'^n}{\sqrt{5}}=\frac{\phi^{n+2}-\phi'^{n+2}}{\sqrt{5}},$$

ce qui achève la récurrence.

Solution de l'exercice 3 Attention, ici il y a deux indices :n et k, il faut être minutieux sur la façons dont nous ferons la récurrence. Nous allons démontrer par récurrence sur n la propriété suivante :

$$\mathcal{P}(n)=\text{“}\forall 0\leqslant k\leqslant n,\ \binom{n}{k}=\binom{n}{k}=\frac{n!}{k!(n-k)!}\text{”}.$$

L'initialisation est évidente ($0!=1$). Intéressons nous maintenant à l'hérédité. Supposons que la formule est vraie pour la ligne n et regardons la ligne $n+1$. Débarassons-nous déjà des cas $k=0$ et $k=n+1$:

$$\frac{(n+1)!}{0!(n+1)!}=1=\binom{n+1}{0}\quad\text{et}\quad\frac{(n+1)!}{(n+1)!0!}=1=\binom{n+1}{n+1}.$$

Regardons à présent le reste des cas :

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

on met tout sur le même dénominateur $(k+1)!(n-k)!$:

$$= \frac{n!((k+1)+(n-k))}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!}$$

Ce qui achève la récurrence.

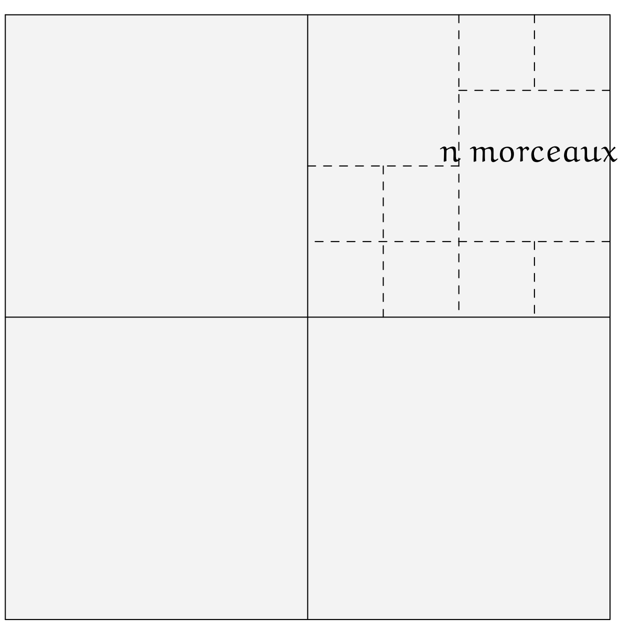
Solution de l'exercice 4 Nous allons faire la démonstration par récurrence sur n. Pour $n = 1$, c'est facile, il suffit de colorier l'intérieur du cercle en rouge et l'extérieur en bleu.

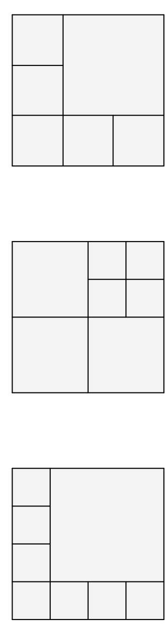
Maintenant supposons que pour n cercles il est toujours possible de trouver un bon coloriage. Prenons $n+1$ cercles et meetons-en un de côté. Il en reste n, donc par hypothèse de récurrence on peut trouver un bon coloriage. Maintenant rajoutons le dernier cercle et faisons la manipulation suivante : on inverse la couleur de tous les secteursà l'intérieur du cercle et on ne touche pas à l'extérieur. Il est facile de vérifier que le coloriage ainsi obtenu est bon.

Solution de l'exercice 5 Lorsqu'il n'y a aucune droites, il y a 1 secteur, avec une droite il y a 2 secteurs. Soit u_n le nombre de secteurs lorsqu'il y a n droites. Lorsqu'on rajoute la $n+1$-ème droite, elle va couper les n autres droites, ce qui signifie qu'elle passera par $n+1$ secteurs. Elle coupera chacun de ces secteurs en deux, donc elle rajoute $n+1$ régions. Nous obtenons la relation de récurrence suivante : $u_{n+1} = u_n + n + 1$. Il est facile de démontrer par récurrence qu'alors

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

Solution de l'exercice 6 Soit $\mathcal{P}(n)$ la propriété : "il est possible de découper un carré en n petits carrés". On remarque que si on sait découper un carré en n carré, alors il est facile de découper un carré en $n+3$ carrés : on coupe le gros carré en 4 et on découpe un des petits carrés en n morceaux (voir la figure de gauche).





Ceci règle son compte à l'hérédité : si on suppose $\mathcal{P}(n)$, vraie alors $\mathcal{P}(n+3)$ est vraie. Il suffit ensuite de s'occuper de l'initialisation. Attention, comme on passe de n à $n+3$, il faut prouver 3 cas : les cas 6, 7 et 8. Ils sont dans la partie droite de la figure.

Solution de l'exercice 7 Notons $\mathcal{P}(n)$ la propriété "$x^n + \frac{1}{x^n}$ est un entier". $\mathcal{P}(1)$ est vrai par hypothèse. Si on suppose $\mathcal{P}(n)$ et $\mathcal{P}(n-1)$ vraies,

$$\left(x^n + \frac{1}{x^n}\right)\left(x^n + \frac{1}{x^n}\right) = x^{n+1} + \frac{1}{x^{n+1}} + x^{n-1} + \frac{1}{x^{n-1}}$$

Les termes $x^n + \frac{1}{x^n}$, $x + \frac{1}{x}$ et $x^{n-1} + \frac{1}{x^{n-1}}$ sont entiers par hypothèse de récurrence, donc $x^{n+1} + \frac{1}{x^{n+1}}$ est aussi entier, ce qui achève la récurrence.

Solution de l'exercice 8 Comme dans l'exercice plus haut, nous allons dénombrer combien on rajoute de secteurs lorsqu'on place le $n+1$-ème point. Numérotons les sommets de 1 à n et plaçons un sommet supplémentaire entre le point 1 et le point n. Regardons la corde C_k qui relie le nouveau point au point k. Une autre corde Γ de la figure coupe la corde C_k ssi un des sommets de Γ est à droite de C_k et l'autre est à gauche. Pour trouver une corde qui coupe C_k il faut donc choisir un point parmi les $k-1$ à droite et un parmi les $n-k$ à gauche, ce qui en donne $(k-1)(n-k)$. Et comme dans l'exercice précédent, cela signifie que la corde C_k rajoute $(k-1)(n-k)+1$ secteurs. Donc

$$u_{n+1} - u_n = \sum_{k=1}^{n} (k-1)(n-k) + 1 = (n+1)\sum_{k=1}^{n} k - \sum_{k=1}^{n} k^2 - n(n-1) = u_n + \frac{n^3 - 3n^2 + 8n}{6}.$$

On initialise avec $u_0 = u_1 = 1$ et on trouve :

$$u_n = \frac{n(n-1)(n^2-5n+18)}{24} + 1 = \frac{n^4 - 6n^3 + 23n^2 - 18n + 24}{24}.$$

Solution de l'exercice 9 Appelons u_n le nombre minimal de mouvements pour déplacer une colonne de taille n d'une aiguille à une autre. Pour déplacer une colonne de taille $n+1$ de la colonne de droite à la colonne de gauche, il faut déplacer les n premiers disques sur la colonne du milieu, puis déplacer le gros disque sur la colonne de droite, puis redéplacer les n autes disques par dessus. Cela nous permet de trouver la formule de récurrence suivante : $u_{n+1} = 2u_n + 1$. On initialise avec $u_1 = 1$, et je laisse au lecteur le soin de démontrer par récurrence que $u_n = 2^n - 1$. Si on considère qu'il faut au moins une seconde aux moines pour faire un mouvement, la fin du monde n'est pas avant $2^64 - 1$ s $\approx$ 600 milliards d'années (on est larges).

Solution de l'exercice 10 Nous allons montrer la propriété par récurrence. L'initialisation est facil. Maintenant supposons que la propriété est vraie pour n et prenons un entier $k < (n+1)!$. Nous allons faire la division euclidienne de k par $n+1$:

$$k = (n+1)q + r.$$

L'entier q est strictement inférieur à $n!$, donc on peut appliquer l'hypothèse de récurrence : $q = d_1 + \cdots + d_k$ avec $k \leqslant n$ et

$$k = d_1(n+1) + d_2(n+1) + d_3(n+1) + \cdots + d_k(n+1) + r.$$

3 Combinatoire

- Introduction -

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

Le contenu de ce mini-cours est le suivant : coefficients binomiaux, double comptage, injections, surjections, méthodes bijections.

- Coefficients binomiaux -

1) Définitions

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

Définition 21. Pour des entiers $0 \leqslant k \leqslant n$, on note $\binom{n}{k}$ (et on prononce « k parmi n ») le nombre de manières de choisir un sous-ensemble à k éléments d'un ensemble à n éléments différents. Pour $k > n$, on pose $\binom{n}{k} = 0$.

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

Exemple 22. On a $\binom{4}{2} = 6$, car les sous-ensembles à 2 éléments de $\{1,2,3,4\}$ sont $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{3,4\}$ et il y en a 6

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

Proposition 23. Le nombre de manières d'ordonner n éléments est $n!$.

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

Proposition 24. Pour des entiers $0 \leqslant k \leqslant n$, on a :

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

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

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

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

2) Propriétés combinatoires

Exercice 1 Pour des entiers $0\leqslant k\leqslant n$, on a :

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

Solution de l'exercice 1 *Première méthode :* On utilise la formule $\binom{n}{k}=\frac{n!}{(n-k)!k!}$ et le résultat en découle immédiatement.

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

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

Exercice 2 (formule de Pascal) Soiet $0\leqslant k\leqslant n$ des entiers (avec $(k,n)\neq(0,0)$). Alors :

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

Solution de l'exercice 2 *Première méthode :* On utilise la formule.

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

Exercice 3 Pour $0\leqslant k\leqslant n$, on a :

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

Solution de l'exercice 3 *Première méthode :* On utilise la formule exprimant $\binom{n}{k}$ (le faire).

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

Exercice 4 Pour un entier $n \geqslant 1$, on a

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

<u>*Solution de l'exercice 4*</u> *Première méthode :* Si on n'a pas d'idée comment commencer de manière astucieuse, on peut essayer de procéder par récurrence sur n. Pour $n = 1$, le résultat est clair. Supposons le résultat acquis au rang n et montrons-le au rang $n+1$ en écrivant, avec l'exercice 4 :

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

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

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

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

Proposition 25 (Formule du binôme de Newton)**.** Soient x, y des nombres réels et $n \geqslant 1$ un entier. Alors :

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

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

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

Exercice 5 Quel est le cardinal moyen d'un sous-ensemble de $\{1, 2, \ldots, n\}$?

<u>*Solution de l'exercice 5*</u>

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

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

Autre méthodes : Il faut évaluer la somme

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

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

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

Troisième méthode : On utilise le résultat de l'exercice précédent :

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

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

Évaluons alors cette quantité en $x = 1$:

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

Le résultat en découle.

Exercice 6 Prouver que pour $0 \leqslant m \leqslant n$:

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

<u>*Solution de l'exercice 6*</u> On remarque d'abord que seuls les k tels que $k \geqslant m$ contribuent de manière non nulle. On va procéder à un double comptage en comptant le nombre N de sous-ensembles A, B de $\{1, 2, \ldots, n\}$ tels que $A \subset B$ et $\mathrm{Card}(A) = m$. En effet, d'une part, pour construire A, B on peut d'abord choisir A de cardinal m ($\binom{n}{m}$ choix), puis rajouter un sous-ensemble quelconque de l'ensemble $\{1, 2, \ldots, n\}$ privé des éléments de A, qui a $n-m$ éléments (et donc 2^{n-m} choix indépendants). En ainsi, $N = \binom{n}{m}2^{n-m}$.

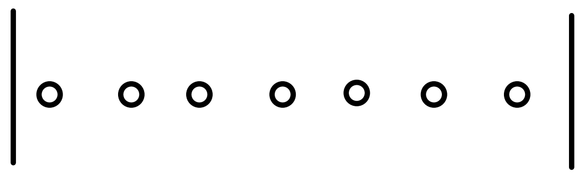
D'autre part, pour construire A, B on peut d'abord choisir B de cardinal quelconque entre m et n (si B est de cardinal k, $\binom{n}{k}$ choix), puis choisir A de cardinal m comme sous-ensemble de B ($\binom{k}{m}$ choix si B est de cardinal k). Ainsi, $N = \sum_{k=0}^{n}\binom{n}{k}\binom{k}{m}$.

Exercice 7 Combien y a-t-il de chemins sur $\mathbb{Z}^2$ issus de $(0, 0)$, faisant des pas $+(1, 0)$ ou $+(0, 1)$, et finissant en (m, n), où $m, n \geqslant 0$?

<u>*Solution de l'exercice 7*</u> Un tel chemin doit faire $m + n$ pas, dont m fois $+(1, 0)$ et n fois $+(0, 1)$. Il suffit donc de choisir parmi les $m + n$ pas possibles la position des m qui font $+(1, 0)$. Le nombre total vaut donc $\binom{m+n}{m}$.

Exercice 8 De combien de manières peut-on placer 5 pièces identiques dans 3 poches différentes ?

<u>*Solution de l'exercice 8*</u> Considérons la figure suivante (avec deux barres) :



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

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

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

- Principe d'Inclusion-Exclusion -

On sait que si A et B sont deux ensembles finis, alors $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$. La formule suivante, dite d'inclusion-exclusion, généralise cela au cas où nous en avons un nombre quelconque.

Proposition 26 (Formule d'inclusion-exclusion)**.** Si $A_1, \ldots, A_n$ sont des ensembles finis, alors :

$$\mathrm{Card}(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \mathrm{Card}\left(A_{i_1} \cup \cdots \cup A_{i_k}\right).$$

Exercice 9 Combien y a-t-il d'entiers strictement positifs inférieurs ou égaux à 120 et qui ne sont divisibles ni par 3, ni par 5, ni par 7 ?

Démonstration. Par récurrence (bon courage !) □

<u>*Solution de l'exercice 9*</u> Trouvons plutôt le nombre d'entiers strictement positifs inférieurs ou égaux à 120 divisibles par 3, 5, ou 7. D'après la formule d'inclusion-exclusion, ce nombre vaut :

$$40 + 24 + 17 - 8 - 5 - 3 + 1 = 66.$$

Ainsi, le nombre cherché vaut $120 - 66 = 54$.

Exercice 10 Les n stagiaires au stage de Montpellier vont se baigner et laissent leurs t-shirts Animath en vrac sur le sable. Ils reviennent et prennent un t-shirt complètement au hasard. Quelle est la probabilité que personne ne se retrouve avec son t-shirt ?

<u>*Solution de l'exercice 10*</u> On assigne à chaque stagiaire un chiffre différent entre 1 et n, et on note x_i le numéro de l'élève prenant le i-ième t-shirt. Ainsi, $(x_1, \ldots, x_n)$ est une permutation de $(1, \ldots, n)$. Calculons plutôt la probabilité qu'au moins une personne retrouve son t-shirt

en vue d'utiliser le principe d'inclusion-exclusion. Pour $1 \leqslant i \leqslant n$, soit A_i l'ensemble des permutations telles que $x_i = i$. Il est clair que pour $1 \leqslant i_1 < \cdots < i_k \leqslant n$, on a :

$$\text{Card}\left(A_{i_1} \cup \cdots \cup A_{i_k}\right) = (n-k)!.$$

Ainsi, d'après la formule d'inclusion-exclusion :

$$\begin{aligned}
\text{Card}(A_1 \cup A_2 \cup \cdots \cup A_n) &= \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \text{Card}\left(A_{i_1} \cup \cdots \cup A_{i_k}\right) \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (n-k)! \\
&= \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)! \\
&= \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!}.
\end{aligned}$$

La probabilité cherchée vaut $1 - \text{Card}(A_1 \cup A_2 \cup \cdots \cup A_n)/n!$, c'est-à-dire :

$$\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} + \cdots + (-1)^n \frac{1}{n!}.$$

- Injections, surjections, bijections -

1) Injections et surjections

Définition 27. Soient E, F deux ensembles et $f : E \to F$ une application.

(i) On dit que f est injective si pour tous $x, y \in E$ avec $x \neq y$, $f(x) \neq f(y)$.

(ii) On dit que f est surjective si pour fou $y \in F$, il existe $x \in E$ tel que $f(x) = y$.

On dit que E est l'ensemble de départ, F l'ensemble d'arrivée. Si $f(x) = y$, on dit que x est l'antécédent de y et y l'image de x.

Pour montrer que $f : E \to F$ est injective, on montre très souvent que si $x, y \in E$ sont tels que $f(x) = f(y)$, alors $x = y$ (voir le cours sur les équations fonctionnelles).

On introduit la notation $[n] = \{1, 2, \ldots, n\}$ pour un entier $n \geqslant 1$.

Proposition 28. Il existe une injection $[m] \to [n]$ si, et seulement si, $m \leqslant n$. Il existe une surjection de $[m] \to [n]$ si, et seulement si, $m \geqslant n$.

Démonstration. Exercice. □

En pratique, on utilise la proposition précédente en combinatoire comme suit : pour montrer que $a \leqslant b$, on construit deux ensembles A, B tels que $\text{Card}(A) = a$, $\text{Card}(B) = b$, ainsi qu'une injection de A dans B. Ou encore, pour montrer que $a \geqslant b$, on construit deux ensembles A, B tels que $\text{Card}(A) = a$, $\text{Card}(B) = b$, ainsi qu'une surjection de A dans B.

Exercice 11 (Olympiades Balkaniques de Mathématiques 1997) Soient $m, n > 1$ des entiers. Soit S un ensemble de cardinal n et $A_1, A_2, \dots, A_m$ des sous-ensembles de S. On suppose que pour tous éléments $x \neq y$ de S, il existe $1 \leqslant i \leqslant m$ tel que $x \in A_i$ et $y \notin A_i$, ou bien $x \notin A_i$ et $y \in A_i$. Prouver que $n \leqslant 2^m$.

Solution de l'exercice 11 À tout élément $x \in S$, on associe le m-uplet $(x_1, \dots, x_m)$ où $x_i = 0$ si $x \notin A_i$ et $x_i = 1$ si $x \in A_i$. Cette application est définie sur S, et son ensemble d'arrivée est $\{0,1\}^m$. Par hypothèse, si $x \neq y$, alors $f(x) \neq f(y)$. Ainsi, f est injective. Le cardinal de l'ensemble de départ est donc inférieur ou égal au cardinal de l'ensemble d'arrivée.

Exercice 12

(i) Combien existe-t-il de fonctions de $[m] \to [n]$?

(i) On suppose $m \leqslant n$. Combien existe-t-il d'injections de $[m] \to [n]$?

(ii) On suppose $m \geqslant n$. Combien existe-t-il de surjections de $[m] \to [n]$?

Solution de l'exercice 12 Pour (i), il y en a clairement n^m (n choix pour chacun des m entiers au départ)

Pour (ii), on a n choix pour l'image de 1, $n-1$ choix pour l'image de 2, et ainsi de suite jusqu'à m pour lequel on a $n-m+1$ choix pour son image. La réponse est donc

Pour (iii), on va utiliser le principe d'inclusion-exclusion et compter le nombre de fonctions $[m] \to [n]$ qui ne sont par surjectives. À cet effet, pour $1 \leqslant i \leqslant n$, notons A_i l'ensemble des fonctions $[m] \to [n]$ telles que i n'est pas atteint par la fonction. Il est clair que pour des entiers $1 \leqslant i_1 < \cdots < i_k \leqslant n$, on a $\text{Card}(A_{i_1} \cap \cdots A_{i_k}) = (n-k)^m$, car chaque élément de $[m]$ peut être envoyé sur un des $n-k$ entiers de $[n]$ autorisés. Ainsi, d'après le principe d'inclusion exclusion, si on note $s(m,n)$ le nombre de surjections de $[m] \to [n]$, on a :

$$
\begin{aligned}
n! - s(m,n) &= \text{Card}(A_1 \cup A_2 \cup \cdots \cup A_n) \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \text{Card}\left(A_{i_1} \cup \cdots \cup A_{i_k}\right) \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (n-k)^m \\
&= \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)^m
\end{aligned}
$$

Ainsi,

$$
s(m,n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.
$$

2) Preuves bijections en combinatoire

Définition 29. Soient E, F deux ensembles et $f : E \to F$ une application. On dit que f est bijective si elle est à la fois injective et à la fois surjective.

Proposition 30. Soient A et B deux ensembles finis. Alors A et B ont même cardinal si, et seulement si, il existe une bijection entre A et B

Démonstration. Exercice. □

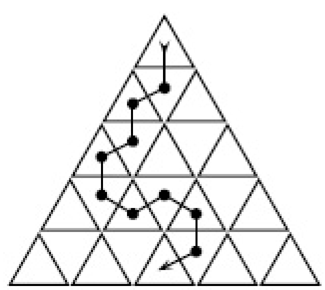
En combinatoire, cette proposition est souvent utilisée de la manière suivante. Si on veut montrer que $a = b$, où $a, b \geqslant 0$ sont des entiers, il suffit de trouver deux ensembles finis A et B tels que $\mathrm{Card}(A) = a$ et $\mathrm{Card}(B) = b$, et de construire une bijection entre A et B.

Pour vérifier qu'une fonction est bijective, il est parfois pratique d'exhiber la fonction réciproque. Plus précisément :

Proposition 31. Si $f : A \to B$ et $g : B \to A$ sont deux fonctions telles que $f(g(b)) = b$ pour tout $b \in B$ et $g(f(a)) = a$ pour tout $a \in A$, alors f et g sont bijections (on dit qu'elles sont réciproques, ou inverses, l'une de l'autre).

Démonstration. Montrons d'abord que f est surjective. Soit $b \in B$. On sait que $f(g(b)) = b$, ainsi $g(b)$ est un antécédent de b, de sorte que f est surjective. Pour montrer l'injectivité, soient $x, y \in E$ tels que $f(x) = f(y)$ et montrons que $x = y$. On a $x = g(f(x)) = g(f(y)) = y$. La fonction f est donc injective, et comme elle est surjective, elle est bien bijective. Par symétrie, g est aussi bijective. □

Exercice 13 (Canada 2005) Soit un triangle équilatéral dont le côté est de longueur n, divisé en triangles unitaires tel qu'illustré. Soit $f(n)$ le nombre de chemins allant du triangle de la rangée du haut jusq'au triangle au centre de la rangée du bas, de façon à ce que des triangles adjacents partagent une arête commune et que le chemin ne repasse jamais par le même triangle et qu'il n'aille jamais vers le haut (d'une rangée inférieure à une rangée supérieure). Un tel chemin est illustré ci-après avec $n = 5$. Déterminer la valeur de $f(2012)$.



<u>*Solution de l'exercice 13*</u> L'application qui à un chemin associe un $(n-1)$-uplet $(x_1, \ldots, x_{n-1})$ où x_i est l'entier x tel que le chemin traverse la i-ième ligne horizontale en partant du haut au x-ième segment en partant de la gauche. Cette application est clairement une bijection entre l'ensemble des chemins considérés et l'ensemble $[1] \times [2] \times \cdot \times [n-1]$, qui est de cardinal $(n-1)!$. Ainsi, $f(2012) = 2011!$.

4 Principe extrémal

- 1. Principe du minimum. -

Axiome 1 (Principe du minimum)**.** Tout ensemble non vide de nombres naturels possède un minimum.

Dans de nombreux problèmes, en particulier en arithmétique et en combinatoire, il est souvent utile de considérer une valeur minimale dans un certain ensemble. S'il s'agit d'entiers naturels, on peut le faire en utilisant le principe du minimum. Il est rare qu'on puisse résoudre un problème en utilisant uniquement ce principe ; en fait, celui-ci permet souvent de se ramener à certains cas particuliers d'un problème dont l'étude est plus simple que le cas général. Il se combine souvent bien avec le raisonnement par l'absurde : pour montrer qu'un objet n'existe pas, on suppose qu'il existe et on considère, dans un certain sens, le plus petit ; puis on montre qu'à partir de celui-ci, on peut en construire un encore plus petit, ce qui amène à une contradiction. Ceci sera illustré par les exercices 2 et 3, par exemple. Il existe aussi un principe analogue, assurant que tout ensemble non vide et majoré d'entiers admet un maximum. Attention, l'hypothèse de majoration est ici indispensable.

Exercice 1 On considère une feuille quadrillée infinie. On suppose que dans chaque case est inscrit un entier naturel, et que cet entier est toujours supérieur ou égal à la moyenne arithmétique de ses quatres voisins. Montrer que chaque case contient le même entier.

Solution de l'exercice 1 Notons a le plus petit entier parmi tous ceux écrits dans au moins une case. Alors si une case contient le nombre a, ses quatre voisins contiennent forcément aussi le nombre a. C'est aussi le cas des voisins de ses voisins, et des voisins des voisins de ses voisins, etc. Ainsi, en partant d'une case contenant a, on montre, de proche en proche, que toutes les cases contiennent a.

Exercice 2

Un carré est partitionné en $n > 1$ rectangles de côtés parallèles à ceux du carré. On suppose que toute droite parrallèle aux côtés du carré, qui coupe l'intérieur du carré, coupe également l'intérieur d'au moins un des rectangles de la partition. Montrer qu'il y a un rectangle qui ne touche pas les côtés du carré.

(Problème C1 *de la liste étendue de l'OIM* 2007.*)*

Solution de l'exercice 2

On note $ABDC$ le carré et on appelle horizontale et verticale les directions (AB) et (AC) respectivement. On suppose par l'absurde qu'il existe une partition sans rectangle intérieur. On en choisit une qui possède le nombre minimal de rectangles. On note a et b les rectangles situés au voisinage de A et B respectivement. Quitte à échanger A et B, on peut supposer que a a une hauteur inférieure à b. On note c l'unique rectangle qui partage un côté vertical avec a, et d l'unique rectangle qui touche a et c. On distingue trois cas.

$\mathrm{largeur}(a) = \mathrm{largeur}(c)$**.** Dans ce cas on peut recoller a et c et obtenir une partition avec moins de rectangles. Exclu par minimalité.

$\mathtt{largeur}(c) < \mathtt{largeur}(a)$**.** Alors d ne peut pas toucher ni (AB) (bloqué par a), ni (AC) (bloqué par c). Puisque $\mathtt{hauteur}(a) < \mathtt{hauteur}(b)$, d ne peut pas toucher (BD) non plus : il est bloqué par b. La seule possibilité restante est que d touche (CD). Mais, dans ce cas, on peut fusionner c, d, et tous les rectangles situés dans la zone délimitée par le coté bas de c, le coté gauche de d, et les droites (AC) et (CD), ce qui produit une partition convenable avec strictement moins de rectangles. Donc ce cas est impossible.

$\mathtt{largeur}(c) > \mathtt{largeur}(a)$**.** Alors d ne peut toucher ni (AC) (bloqué par a), ni (CD) (bloqué par c), ni (BD) (bloqué par b). La seule solution restante est qu'il touche (AB), mais alors on peut le fusionner avec a, ce qui fournit une partition convenable avec un rectangle de moins. Absurde.

- 2. Lien avec les principes de récurrence et de descente infinie -

Exercice 3

Montrer que tout entier naturel supérieur ou égal à 2 peut s'écrire comme un produit de nombres premiers.

Solution de l'exercice 3

Première méthode : principe du minimum. Par l'absurde, supposons qu'il existe un entier $n \geqslant 2$ ne pouvant pas s'écrire comme produit de nombres premiers. On suppose alors que n est le plus petit entier vérifiant cette propriété. L'entier n n'est donc pas premier ; il existe donc des entiers k et l tous deux strictement inférieurs à n tels que $n = kl$. Par minimalité de n, les entiers k et l sont produits de nombres premiers, donc n aussi, contradiction. Donc tout entier est produit de nombres premiers.

Seconde méthode : par récurrence. On montre le résultat par récurrence forte sur n. Si n est premier, c'est vrai ; si n n'est pas premier, on écrit $n = kl$ avec k et l des entiers strictement inférieurs ou égaux à n ; par hypothèse de récurrence, ils s'écrivent comme produits de nombres premiers, donc n aussi.

Troisième méthode : descente infinie. Supposons qu'il existe un entier n_0 ne pouvant pas s'écrire comme produit de nombres premiers. On va montrer qu'on peut en construire un strictement plus petit, n_1, vérifiant la même propriété. L'entier n_0 s'écrit $n_0 = kl$, où k et l sont des entiers strictement plus petits que n_0. Au moins l'un des deux, par exemple k, ne peut pas s'écrire comme produit de nombres premiers, sinon n_0 pourrait aussi s'écrire sous cette forme. On pose alors $n_1 = k$.

En réitérant ce procédé, on peut construire un entier naturel $n_2 < n_1$ qui ne s'écrit pas comme produit de nombres premiers, puis $n_3 < n_2$ de la même façon, et ainsi de suite... Ainsi, on construit une suite (n_i) d'entiers naturels strictement décroissante. Une telle suite ne peut pas exister, ce qui permet de conclure.

En fait, les trois méthodes utilisées pour cette preuve sont rigoureusement identiques : seule la formulation change. Le principe de récurrence est en fait équivalent au principe du minimum, et toute preuve par récurrence peut être reformulée en utilisant le principe du minimum combiné avec un raisonnement par l'absurde. Ces deux principes sont équivalents à un troisième principe que nous allons maintenant aborder : le principe de descente infinie.

Axiome 2 (Principe de descente infinie)**.** Il n'existe pas de suite strictement décroissante d'entiers naturels.

Théorème 32. On a équivalence entre :

(1) Le principe du minimum ;

(2) Le principe de récurrence ;

(3) Le principe de descente infinie.

Démonstration. **(1)** $\Rightarrow$ **(2)** Soit $P(n)$ une propriété telle que $P(0)$ est vraie et, pour tout $n \geqslant 0$, $P(n)$ implique $P(n+1)$. On pose $E = \{n \in \mathbb{N} \mid P(n)$ *est fausse*$\}$. Par l'absurde, supposons E non-vide. Par le principe du minimum, E admet alors un minimum n_0. $P(n_0)$ est donc fausse, donc $n_0 > 0$. Par mnimalité de n_0, $P(n_0 - 1)$ est vraie. Donc $P(n_0)$ est vraie aussi, contradiction. On en déduit que E est vide, donc que $P(n)$ est vraie pour tout n.

(2) $\Rightarrow$ **(1)** Soit E un ensemble d'entiers naturels qui n'a pas de minimum ; on va montrer que E est vide. On note $P(n)$ la propriété « E ne contient aucun entier inférieur ou égal à n ». Comme E n'a pas de minimum, $0 \notin E$, donc $P(0)$ est vraie. De plus, si $P(n)$ est vraie, alors $n+1$ n'appartient pas à E, sinon ce serait le minimum de E ; $P(n+1)$ est donc vraie. Par le principe de récurrence, $P(n)$ est vraie pour tout n ; ainsi E est vide.

(1) $\Rightarrow$ **(3)** Soit (u_n) une suite d'entiers naturels. Par le principe du minimum, il existe un entier naturel n_0 tel que u_{n_0} soit minimal. On a alors $u_{n_0} \leqslant u_{n_0+1}$, et la suite (u_n) n'est pas strictement décroissante.

(3) $\Rightarrow$ **(1)** Supposons qu'il existe un ensemble non vide d'entiers naturels, E, n'admettant pas de minimum. Pour tout $n_i \in E$, il existe donc $n_{i+1} \in E$ tel que $n_{i+1} < n_i$. En partant d'un entier $n_0 \in E$, on construit ainsi une suite strictement décroissante d'entiers naturels, dont l'existence contredit le principe de descente infinie.

□

Toute preuve pouvant être faite avec l'un des trois principes précédents peut se reformuler avec les deux autres. Néanmoins, contrairement à l'exercice 3, dans la plupart des cas, l'utilisation de l'un d'eux est beaucoup plus simple que celle des deux autres.

- 3. Utilisation de la descente infinie. -

Le principe de descente infinie s'utilise généralement de la manière suivante. On veut montrer qu'une propriété $P(n)$ n'est satisfaite par aucun entier naturel n. Pour cela, on commence par montrer que si la propriété est vérifiée par un entier n_i, alors elle est aussi vérifiée par un entier naturel $n_{i+1} < n_i$. Ainsi, en supposant l'existence d'un entier n_0 tel que $P(n_0)$ soit vraie, on arrive à construire une suite strictement décroissante d'entiers naturels vérifiant la propriété P, ce qui contredit le principe de descente infinie. Ce type de raisonnement, utilisé pour la première fois par Fermat, est très utile dans la résolution d'équations diophantiennes.

Exercice 4 Montrer que $\sqrt{2}$ est irationnel.

<u>*Solution de l'exercice 4*</u> Supposons par l'absurde qu'il existe $a,b \in \mathbb{N}$ avec $b \neq 0$ tels que $\sqrt{2} = \frac{a}{b}$. Alors on a $2b^2 = a^2$. On déduit que a est pair, notons-le $a = 2 \cdot a_1$. Alors $2b^2 = 4a_1^2$, donc $b^2 = 2a_1^2$. Comme b est pair, on le note $2b_1$ et on trouve $4b_1^2 = 2a_1^2$, d'où $2b_1^2 = a_1^2$. Ceci fournit un couple (a_1, b_1) vérifiant la même propriété que (a, b), avec $b_1 < b$. En continuant, on trouve une suite infinie de couples $(a_1, b_1), (a_2, b_2), \dots$ telle que $b > b_1 > b_2 > \cdots$. Le principe de descente infinie contredit l'existence d'une telle suite (b_i), donc il n'existe pas de couple (a, b) tel que $\sqrt{2} = \frac{a}{b}$.

Exercice 5 Montrer que l'unique solution dans $\mathbb{Z}^3$ de l'équation $x^3 + 2y^3 = 4z^3$ est $(0, 0, 0)$.

<u>*Solution de l'exercice 5*</u> Soit (x_0, y_0, z_0) un triplet solution. Alors x_0 est pair, et on peut poser $x_0 = 2x_1$. On a alors $4x_1^3 + y_0^3 = 2z_0^3$. Donc y_0 est pair, on pose $y_0 = 2y_1$, et on a $2x_1^3 + 4y_1^3 = z_0^3$. Donc z_0 est pair, et on peut poser $z_0 = 2z_1$; le triplet (x_1, y_1, z_1) est donc solution de la même équation que (x_0, y_0, z_0). On peut donc construire une suite (x_i, y_i, z_i) de triplets solutions, avec $x_i = 2x_{i+1}$, $y_i = 2y_{i+1}$, et $z_i = 2z_{i+1}$ pour tout i. Si l'un des entiers x_0, y_0 ou z_0 était non-nul, par exemple x_0, alors la suite $(|x_i|)$ serait une suite d'entiers naturels strictement décroissante, contradiction. Donc $(x_0, y_0, z_0) = (0, 0, 0)$.

- 4. Extréma d'un ensemble fini. -

Proposition 33. Un ensemble fini de réels admet un maximum et un minimum.

Démonstration. Par récurrence sur le cardinal de l'ensemble.

□

Même si trivial, ce résultat peut constituer le point de départ pour une solution. Avant d'essayer des techniques plus sophistiquées, il faut penser à considérer un élément extrémal.

Exercice 6 Soit $n \geqslant 1$ un entier naturel. Dans un système solaire il y a exactement $2n + 1$ planètes, qui abritent toutes de la vie, et qui se trouvent à des distances deux à deux distinctes. Les habitants de chaque planète lancent une expédition sur la planète la plus proche. Montrer qu'il existe une planète qui n'est pas visitée.

<u>*Solution de l'exercice 6*</u> Par récurrence sur n. Considérons les deux planètes les plus proches dans le système solaire, que l'on notera A et B. Celles-ci s'explorent réciproquement. Il reste $2n - 1$ planètes.

- Si $n = 1$ *(initialisation de la récurrence)* il reste une seule planète qui explore soit A, soit B, et qui n'est donc pas explorée.
- Si $n \geqslant 2$ *(hérédité)* alors on distingue deux cas. Soit au moins l'une des planètes restantes explore A ou B ; ces planètes sont au nombres de $2n - 1$, et peuvent donc être explorées par au plus $2n - 2$ expéditions, donc l'une d'elles n'est pas explorées. Soit les $2n - 1$ planètes restantes s'explorent entre elles, et par hypothèse de récurrence, l'une d'elles n'est pas explorée.

Exercice 7 On se donne un ensemble fini de points dans le plan, de cardinal pair, trois quelconques d'entre eux non alignés. Montrer qu'on peut les relier par des segments sorte que chaque point soit relié à exactement un autre et que les segments ne se coupent pas.

Solution de l'exercice 7 Considérons la façon de relier les points qui minimise la somme des longueurs des segments, avec pour unique contrainte que chaque point soit extrémité d'exactement un segment. Supposons, par l'absurde, que l'on a deux segments AD et BC qui se coupent en un point O (par hypothèse, celui-ci est forcément différent de A, B, C, et D). Si, à la place des segments AD et BC on choisit CD et AB, alors tout point est relié à exactement un autre. Par minimalité de la somme des longueurs, on en déduit :

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

Pour la même raison, on a :

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

En sommant les deux équations, on trouve

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

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

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

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

- 5. Invariants monotones -

Exercice 8

Soit $n \geqslant 1$ un entier naturel. Considérons un parlement composé de n députés. On suppose que chaque député a exactement trois ennemis. On suppose que la relation d'inimitié est symétrique (si a est ennemi de b, alors b est ennemi de a). Montrer qu'il est possible de séparer le parlement en deux commissions telles que chaque député ait au plus un ennemi dans sa commission.

Solution de l'exercice 8

On va utiliser une méthode algorithmique pour former les deux commissions. On va commencer par former deux commissions au hasard. Puis, tant qu'il restera au moins un député ayant au moins deux ennemis dans sa commission, on s'autorisera l'opération suivante : changer ce député de commission. On continue à effectuer ces opérations tant qu'il reste un député ayant au moins deux ennemis dans sa commission. Si à partir d'un certain moment, il n'est plus possible d'effectuer de telles opérations, cela signifie qu'on a obtenu la situation voulue. Le problème est que rien ne garantit, a priori, que ces opérations vont s'arrêter un jour.

Pour prouver que c'est en fait le cas, on va introduire m le nombre de paires $\{a, b\}$ où a et b sont deux députés ennemis faisant partie de la même commission. Autrement dit, c'est le nombre de relations d'inimitié à l'intérieur des commissions. m est un entier positif, et à chaque fois qu'on effectue une opération autorisée, il diminue strictement : en effet, en changeant de commission un député ayant au moins deux ennemis dans sa commission, on casse au moins deux relations d'inimitiés, et on en crée au plus une (car ce député a au plus un ennemi dans l'autre commission). Au bout d'un certain temps, m atteindra donc forcément sa valeur minimale, et dès lors, aucune opération ne sera plus possible. Ceci signifiera que la situation attendue est obtenue.

L'entier positif m utilisé dans cette preuve est appelé un *invariant monotone*. Les invariants monotones interviennent dans de nombreux problèmes, pour montrer qu'une suite d'opérations se termine forcément et permet d'arriver à une certaine situation.

Exercice 9

À chaque sommet d'un pentagone régulier, on associe un entier relatif de telle sorte que la somme de ces cinq nombres soit strictement positive.

Si, à trois sommets consécutifs, correspondent les nombres x, y, et z avec $y < 0$, alors l'opération suivante est permise : « remplacer le triplet (x, y, z) par $(x + y, -y, y + z)$ ».

Cette opération est répétée tant qu'au moins un des cinq nombres est strictement négatif. Déterminer si ce processus prend nécessairement fin après un nombre fini d'opérations.

(Problème 3 *de l'OIM* 1986.*)*

<u>*Solution de l'exercice 9*</u>

L'idée est de trouver un invariant monotone, dont la valeur soit toujours un entier positif, et qui diminue strictement à chaque opération. Ici, en notant x_i l'entier associé au $i^{\text{ème}}$ sommet du pentagone (les indices étant pris modulo 5, et les sommets du pentagone ordonnés dans le sens direct), on va poser $f(x_1, x_2, x_3, x_4, x_5) = \sum_{i=1}^{5}(x_{i-1} - x_{i+1})$.

Supposons, par exemple, que $x_3 < 0$, et qu'on applique une opération autorisée au triplet (x_2, x_3, x_4). Celle-ci remplacera le quintuplet $X = (x_1, x_2, x_3, x_4, x_5)$ par $Y = (x_1, x_2 + x_3, -x_3, x_3+x_4, x_5)$. Un calcul simple montre alors que $f(Y)-f(X) = 2x_3(x_1+x_2+x_3+x_4+x_5) < 0$ (en effet, la somme $x_1 + x_2 + x_3 + x_4 + x_5$ ne changeant pas au cours des opérations, elle reste strictement positive).

À chaque opération, la valeur de $f(X)$ diminue strictement, tout en restant positive. Lorsqu'elle atteindra sa valeur minimale, cela signifiera qu'aucune opération n'est plus possible, et donc que les nombres situés au sommets du pentagone sont tous positifs.

Remarque 34. On aurait pu aussi donner une autre formulation de cette solution, utilisant le principe du minimum : par l'absurde, supposons qu'il existe une suite infinie d'opérations autorisées. Alors on considère le quintuplet X obtenu au cours de cette suite d'opérations qui minimise la valeur de $f(X)$. En effectuant une opération supplémentaire, $f(X)$ diminue encore, absurde.

5 Test

- Énoncés (durée : 3h) -

Exercice 1 Les 67 stagiaires du stage de Montpellier vont manger au restaurant "La Muraille du Phénix" et s'assoient autour d'une table circulaire sur laquelle sont disposées 67 assiettes. Chaque assiette porte le nom d'un des stagiaires. Au début du repas, personne n'est assis en face de son assiette. Montrer qu'il est possible de tourner la table de sorte qu'il y ait au moins deux stagiaires assis en face de leur assiette.

Exercice 2 Peut-on paver un échiquier 8×8 auquel on a enlevé un coin par des triminos (qui sont des rectangles de taille 3×1) ?

Exercice 3 Soient $0 \leqslant m \leqslant n$ des entiers. Prouver que :

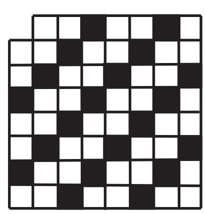
$$\sum_{k=0}^{m} \binom{m}{k}\binom{n}{k} = \binom{m+n}{m}.$$

Exercice 4 On considère les 26 villages suivants : Arras, Bergues, Cambrai, Dunkerque, Esquelbecq, ... , Zuydcoote. Deux de ces villages sont toujours reliés soit par tracteur, soit par train (à double sens). Montrer qu'il est possible de choisir un moyen de transport, tel que, en partant de n'importe quel des villages, on puisse atteindre n'importe quel autre village uniquement à l'aide de ce moyen de transport.

- Corrigé -

<u>*Solution de l'exercice 1*</u> Notons n_i le nombre d'élèves qui se retrouvent en face de leur assiette lorsqu'on a tourné la table de i crans (avec $1 \leqslant i66$). Pour chaque élève, on peut trouver un moment lors de cette rotation où il était en face de son assiette. Ainsi, $n_1 + n_2 + \cdots + n_{66} = 67$. Il existe donc forcément $1 \leqslant i \leqslant 66$ tel que $n_i \geqslant 2$ (dans le cas contraire, la somme $n_1 + n_2 + \cdots + n_{66}$ ne pourrait dépasser 66).

<u>*Solution de l'exercice 2*</u> On considère le coloriage suivant : Un trimino recouvre exactement une



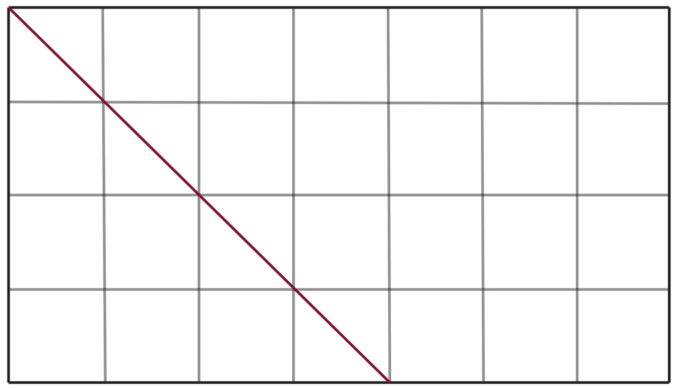
case coloriée. Comme il y a 20 cases coloriées, on pourra poser au plus 20 trimions. Or pour recouvrir 63 cases il faut 21 triminos. Il n'est donc pas possible de paver un échiquier 8×8 auquel on a enlevé un coin par des trimions.

<u>*Solution de l'exercice 3*</u> *Première solution (de Yassine Hamdi)* On considère un groupe de m filles et n garçons et on compte de deux manières le nombre de manières de choisir un sous-groupe de n personnes. D'une part, ce nombre vaut clairement $\binom{m+n}{n}$. D'autre part, choisir ce sous-groupe revient à choisir d'abord le nombre k de filles qui vont y être ($0 \leqslant k \leqslant m$), puis choisir les filles ($\binom{m}{k}$ choix), puis les garçons ($\binom{n}{n-k}$ choix). Ainsi :

$$\binom{m+n}{m} = \sum_{k=0}^{m} \binom{m}{k}\binom{n}{n-k} = \sum_{k=0}^{m} \binom{m}{k}\binom{n}{k},$$

où on a utilisé le fait que $\binom{n}{n-k} = \binom{n}{k}$ pour la deuxième égalité.

Deuxième solution (Hizir Nuhoglu) Considérons un rectangle de longueur n et de largeur m : On s'intéresse aux chemins partant du sommet en bas à gauche (coordonnées $(0,0)$) et



finissant en haut à droite (coordonnées (n,m)) en faisant uniquement des pas d'une unité vers la droite ou vers le haut. D'après un exercice de TD, leur nombre vaut $\binom{m+n}{m}$. D'autre part, n'importe quel de ces chemins traverse un point de coordonnées $(k, m-k)$ avec $0 \leqslant k \leqslant m$ (points sur la diagonale rouge sur la figure). Or le nombre de chemins allant de $(0,0)$ à $(k, m-k)$ vaut $\binom{m}{k}$, et le nombre de chemins allant de $(k, m-k)$ à (n,m) vaut $\binom{n}{n-k} = \binom{n}{k}$. Ainsi

$$\binom{m+n}{m} = \sum_{k=0}^{m} \binom{m}{k}\binom{n}{k},$$

Troisième solution et généralisation (Nicolas Heutte) Si on considère $m+1$ nombres alignés $a_0, a_1, \dots, a_m$ et qu'on forme un triangle de Pascal "descendant" à partir de cette ligne originelle, la $m+1$-ième ligne contiendra un unique nombre qui sera

$$a_0\binom{m}{0} + a_1\binom{m}{1} + \cdots + \cdots a_m\binom{m}{m}.$$

On effectue cette opération à partir des $m+1$ premiers nombres de la n-ième ligne du triangle de Pascal, qui sont $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{m}$. On obtient donc que le nombre sur la $n+m-1$-ième ligne en m-ième place est

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

Or par construction du triangle de Pacal, ce nombre est aussi $\binom{m+n}{m}$, ce qui conclut.

Il est possible de généraliser cette formule : soit $u \geqslant 0$ un entier tel que $u \leqslant n-m+2$. Alors en faisant le raisonnement précédant, mais en partant des $m+1$ nombres consécutifs à partir du u-ième nombre de la n-ième ligne du triangle de Pascal, on obtient :

$$\sum_{k=0}^{m} \binom{m}{k}\binom{n}{k+u} = \binom{m+n}{m+u}.$$

Quatrième solution (par récurrence) On rappelle que $\binom{m}{n} = 0$ si $n > m$ ou si $n < 0$. On raisonne par récurrence sur $m+n$. Plus précisément, pour un entier $j \geqslant 0$, soit P_j la propriété

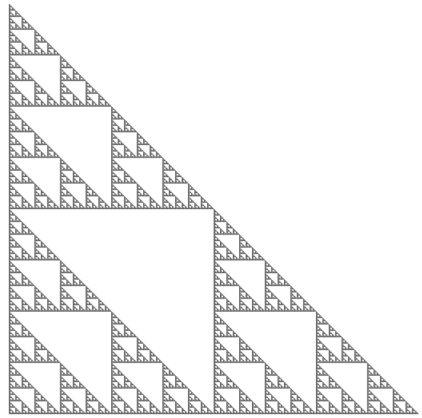


FIGURE 1 – Interlude : le triangle de Sierpinski

"Pour tous entiers $m, n \geqslant 0$ tels que $m + n = j$, on a :

$$\sum_{k \geqslant 0} \binom{n}{k}\binom{m}{k} = \binom{m+n}{m} \quad \textbf{et} \quad \sum_{k \geqslant 0} \binom{n}{k-1}\binom{m}{k} = \binom{m+n}{m-1}".$$

Initialisation : P_0 est vraie.

Hérédité : supposons P_j vraie et démontrons P_{j+1}. Soient $m, n \geqslant 0$ des entiers tels que $m + n = j + 1$. On écrit, en utilisant de nombreuses fois la relation de Pascal :

$$\begin{aligned}
\sum_{k \geqslant 0} \binom{n}{k}\binom{m}{k} &= \sum_{k \geqslant 0} \left(\binom{n-1}{k} + \binom{n-1}{k-1}\right)\binom{m}{k} \\
&= \sum_{k \geqslant 0} \binom{n-1}{k}\binom{m}{k} + \sum_{k \geqslant 0} \binom{n-1}{k-1}\binom{m}{k} \\
&= \binom{m+n-1}{m} + \binom{m+n-1}{m-1} \\
&= \binom{m+n}{m},
\end{aligned}$$

où on a utilisé l'hypothèse de récurrence pour écrire l'avant-dernière égalité (ce qui est licite, car $m + n - 1 = j$).

De même, on a :

$$\begin{aligned}
\sum_{k \geqslant 0} \binom{n}{k-1}\binom{m}{k} &= \sum_{k \geqslant 0} \binom{n}{k-1}\left(\binom{m-1}{k} + \binom{m-1}{k-1}\right) \\
&= \sum_{k \geqslant 0} \binom{n}{k-1}\binom{m-1}{k} + \sum_{k \geqslant 0} \binom{n}{k-1}\binom{m-1}{k-1} \\
&= \binom{m+n-1}{m-2} + \binom{m+n-1}{m-1} \\
&= \binom{m+n}{m-1}.
\end{aligned}$$

où on a utilisé l'hypothèse de récurrence pour écrire l'avant-dernière égalité (ce qui est licite, car $m+n-1=j$).

Solution de l'exercice 4 Supposons que le nombre de villages est une entier $n \geqslant 2$, et que deux villages quelconques sont reliés soit par train, soit par tracteur, et montrons qu'il est possible de choisir un moyen de transport, tel que, en partant de n'importe quel des villages, on puisse atteindre n'importe quel autre village uniquement à l'aide de ce moyen de transport.

Pour avoir une intuition de ce qui se passe, il est conseillé de tester différentes configurations pour des petites valeurs de n. Pour $n = 2$, il n'y a un qu'un seul moyen de transport. Pour $n = 3$, soient A, B, C les trois villages. Sans perte de généralité, supposons que $A - B$ est une liaison tracteur. Alors soit C peut être relié à A ou B par un tracteur, auquel cas le tracteur convient, soit C est relié à A et B par un train, auquel cas le train convient.

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

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

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

En particulier, P_{26} est vraie, ce qui est le résultat demandé.

3 Intermédiaires : équations fonctionnelles

Nous renvoyons aux cours d'équations fonctionnelles disponible sur le site d'Animath pour des détails et compléments (voir les liens en haut de la page 14).

1 Premier cours

- Énoncés -

Exercice 1 Trouver toutes les fonctions croissantes $f : \mathbb{R} \to \mathbb{R}$, telle que $f(1) = 1$ et, pourt tous $x, y \in \mathbb{R}$, $f(x+y) = f(x) + f(y)$.

Exercice 2 Trouver les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que, pour tous x, y on a

$$f(x - f(y)) = f(f(y)) + xf(y) + f(x) - 1. \tag{III.5}$$

Exercice 3 Soit $f : \mathbb{N} \to \mathbb{N}$ satisfaisant :

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

1. $\forall n \in \mathbb{Z}^+, f(n!) = f(n)!$;
2. $\forall m \neq n, (m-n) \mid (f(n) - f(m))$.

Montrer les affirmation suivantes.

1. Si f a un point fixe $n_0 \geqslant 3$, alors $f = \mathbf{id}_{\mathbb{N}}$.
2. Si $f(3) \neq 3$, alors, pour tout n, $3 \nmid f(n!)$ et f est constante.

Exercice 4 Prouver que l'équation

$$x^2 + 2y^2 = z^2 + 2t^2 \tag{III.6}$$

a une infinité de solutions entières positives. Ensuite, trouver les fonctions $f : \mathbb{N}^* \to \mathbb{N}^*$ telles que, pour tous m et n entiers positifs, on a :

$$f\left(f(n)^2 + 2f(m)^2\right) = n^2 + 2m^2. \tag{III.7}$$

Exercice 5 Soient $f_1, f_2 : [0,1] \to \mathbb{R}$ telles que pour tous $a_1, a_2 \in \mathbb{R}$, $a_1f_1 + a_2f_2$ est monotone. On suppose que f_2 n'est pas constante. Montrer qu'il existe un réel a tel que $f_1 - af_2$ est constante.

Exercice 6 Trouver les fonctions $f : \mathbb{Q} \to \mathbb{Q}$ telles que $f(1) = 2$, $\forall x, y \in \mathbb{Q} : f(xy) = f(x)f(y) - f(x+y) + 1$.

- Corrigé -

Solution de l'exercice 1 En posant $x = y = 0$ on trouve $f(0) = 0$. En posant $y = -x$ on a $f(0) = f(x) + f(-x)$, donc $f(-x) = -f(x)$. Soit $x \in \mathbb{R}$. On a $f(2x) - f(x) + f(x)$. Par récurrence on a pour tout n naturel,

$$f((n)x) = nf(x). \tag{III.8}$$

Pour tout $m \in \mathbb{N}$, on a $f(1 \cdot \frac{1}{m} = mf(\frac{1}{m})$, donc $f(\frac{1}{m}) = \frac{1}{m}$. En injectant dans (III.8) on obtient $f(q) = q$ pour tout $q \in \mathbb{Q}_+$. Comme f est impaire, $f(q) = q$ pour tout q rationnel.

Soit $r \in \mathbb{R}$ et supposons $f(r) \neq r$. On suppose $f(r) > r$, le cas $f(r) < r$ étant analogue. Comme entre n'importe quels deux nombres réels il y a un nombre rationnel, on prend q_0 tel que $f(r) < q_0 < r$. Comme f est croissante, on a $f(f(r)) < f(q_0) \leqslant f(r)$. Contradiction. Ainsi, $f(x) = x$ pour tout x.

Solution de l'exercice 2 On note $c = f(0)$. Soit $z \in \mathrm{Im}(f)$, et y tel que $z = f(y)$. Pour $x = z$ on a

$$c = f(z - z) = f(z) + z^2 + f(z) - 1. \tag{III.9}$$

Cela donne $f(z) = \frac{1}{2}(c - z^2 + 1)$ pour tout $z \in \mathrm{Im}(f)$. On est tenté de poser $z = 0$ et d'obtenir $c = 1$, mais on ne sait pas si $0 \in \mathrm{Im}(f)$. En posant $x = y = 0$ dans (III.5) on $c \neq 0$. On fait $y = 0$ dans (III.5) et on voit que tout réel est la différence de 2 éléments de l'image :

$$x = \frac{f(x-c) - f(c) - f(x) + 1}{c}. \tag{III.10}$$

Soit z un réel et y_1, y_2 tels que $z = f(y_1) - f(y_2)$.On note $u = f(y_1)$ et $v - f(y_2)$. On injecte $f(y_1)$ et y_2 dans (III.5) et on trouve

$$f(f(y_1) - f(y_2)) - f(f(y_1)) + f(y_1)f(y_2) + f(f(y_2)) - 1. \tag{III.11}$$

Or, on connait l'expressions de $f(u)$ pour tout $u \in \operatorname{Im}(f)$, donc on trouve $f(z) = c - \frac{z^2}{2}$. En comparant avec l'expression $f(z) = \frac{1}{2}(c - z^2 + 1)$ pour tout $z \in \operatorname{Im}(f)$, on en déduit que $c = 1$. La seule possibilité est donc $f(z) = 1 - \frac{z^2}{2}$, qui est effectivement solution de l'équation.

Solution de l'exercice 3 (Adaptation d'après un problème de BMO 2012.)

1. On pose $a_0 = n_0$ et, pour tout $k \geqslant 0$, $a_{k+1} = a_k!$. Une récurrence simple montre que, pour tout k, a_k est un point fixe. Comme $a_0 \geqslant 3$, $a_1 = a_0! > a_0$ et par récurrence $a_0 < a_1 < a_2 < \cdots$, donc on a une suite infinie de points fixes. Pour un n fixé et un k arbitraire on a :
$$n - a_k \mid (f(n) - f(a_k)) - (n - a_k) = f(n) - n. \tag{III.12}$$
Comme k est arbitraire, $f(n) - n$ a une infinité de diviseurs, donc $f(n) = n$.

2. Puisque $f(1)! = f(1)$ et $f(2)! = f(2)$, $f(1), f(2) \in \{1,2\}$. Si $f(3) > 3$, alors $4 \mid f(3)!$. D'autre part, $3! - 2 \mid f(3!) - f(2)$. Cela implique $4 \mid f(2)$. Faux. Ainsi $f(3) \in \{1,2\}$. Pour tout $n \geqslant 3$, $3 \mid n!$, donc $3 \mid (n! - 3)$. D'autre part, $n! - 3 \mid f(n!) - f(3)$, donc, puisque $f(3) \in \{1,2\}$, $3 \nmid f(n!)$. Or, alors, pour tout n, $f(n) \in \{1,2\}$. La deuxième condition implique $f(n) = f(m)$ ou $|n - m| \leqslant |f(n) - f(m)|$ pour tout couple n, m. Ainsi $f(n) = f(1)$ pour $n \geqslant 3$ et $f(n) = f(2)$ pour $n \geqslant 4$, donc f est constante.

Solution de l'exercice 4 (BMO 2009) Pour comprendre une équation, il est toujours pratique de commencer par trouver quelques solutions. Pour cela on calcule $x^2 + 2y^2$ pour tout couple déléments de $\{1,2,3,4,5\}$; la case (n, m) du tableau suivant indique $n^2 + 2m^2$.

	1	2	3	4	5
1	3	9	19	*33*	51
2	6	12	22	36	54
3	11	17	**27**	41	59
4	18	24	34	48	66
5	**27**	*33*	43	57	75

On conclut que $(5,1,3,3)$ et $(1,4,5,2)$ sont solutions.

Une méthode simple de montrer qu'on a une infinité de solution est de trouver une formule, dépendant d'un paramètre, qui produit une infinité de solutions. On cherche une formule du type
$$(x+\alpha)^2 + 2(x+\beta)^2 = (x+\gamma)^2 + 2(x+\delta)^2. \tag{III.13}$$

Pour cela on doit avoir :

$$\alpha + 2\beta = \gamma + 2\delta \tag{III.14}$$
$$\alpha^2 + 2\beta^2 = \gamma^2 + 2\delta^2 \tag{III.15}$$

Parmi les deux solutions que l'on connaît pour (III.15), seule $(1,4,5,2)$ vérifie (III.14). On a obtenu la formule :
$$(x+1)^2 + 2(x+4)^2 = (x+5)^2 + 2(x+2)^2. \tag{III.16}$$

Passons maintenant à la deuxième partie de l'exercice. Commençons par remarquer que f est injective car, si $f(n_1) = f(n_2)$, alors $3n_1^2 = f(3f(n_1)^2) = f(3f(n_2)^2) = 3n_2^2$. On note $a = f(1)$. En posant $n = m = f(1)$ dans (III.7) on trouve $f(3a^2) = 3$.

Si (x, y, z, t) est une solution de (III.6), alors on peut injecter $n = xa^2$, $m = ya^2$, puis $n = za^2$ et $m = ta^2$ dans (III.7) et trouver :

$$f(f(xa^2)^2 + 2f(ya^2)^2) = (xa^2)^2 + 2(ya^2)^2 = (za^2)^2 + 2(ta^2)^2 = f(f(za^2)^2 + 2f(ta^2)^2). \quad \text{(III.17)}$$

Par l'injectivité de f, on a $f(xa^2)^2 + 2f(ya^2)^2 = f(za^2)^2 + f(ta^2)^2$. En conclusion, (x, y, z, t) solution implique $(f(xa^2), f(ya^2), f(za^2), f(ta^2))$ solution.

Pour $(x, y, z, t) = (5xt, z, , 1, 3, 3)$ on trouve $f(5a^2)^2 + 2f(a^1)^2 = 3f(3a^2) = 27$. L'équation $u^2 + 2v^2 = 27$, n'a pas de solutions autres que $(5, 1)$ et $(3, 3)$. Comme $(3, 3)$ est interdite par l'injectivité de f, $f(5a^2) = 5$ et $f(a^2) = 1$.

Pour $(x, y, z, t) = (1, 4, 5, 2)$ on trouve $f(a^2)^2 + 2f(4a^2)^2 = f(5a^2)^2 + 2f(2a^2)^2$. Comme $f(5a^2) = 5$ et $f(a^2) = 1$, $f(4a^2)$ et $f(2a^2)$ vérifie l'équation $1 + 2g^2 = 5^2 + 2h^2$. Cela équivaut à $(g - h)(g + h) = 12$. Comme $(g - h)$ et $g + h$ ont la même parité, $g - h = 2$ et $g + h = 6$, d'où $f(4a^2) = 4$ et $f(2a^2) = 2$.

On montre par récurrence sur k que $f(ka^2) = k$. On l'a déjà prouvé pour $k \in \{1, 2, 3, 4, 5\}$. On suppose le résultat connu pour $k+1, k+2, k+4$ et on le montre pour $k+5$. Pour $(x, y, z, t) = (k + 1, k + 4, k + 5, k + 2)$ on trouve :

$$f((k + 1)a^2)^2 + 2f((k + 4)a^2)^2 = f((k + 5)a^2)^2 + 2f((k + 2)a^2). \quad \text{(III.18)}$$

Ceci prouve $f((k + 5)a^2) = (k + 5)a^2$. Donc, pour tout $k \in \mathbb{Z}_+^*$, $f(ka^2) = k$.

En prenant $k = a$ on trouve $f(a^3) = a$. En mettant $n = m = a^3$ dans (III.7) on a $f(f(a^3)^2 + 2f(a^3)^2) = 3a^6$. Or $f(a^3) = a$, donc $f(3a^2) = 3a^6$. Ainsi $a^6 = 1$, donc $a = 1$. La seule possibilité pour f est l'identité, qui réciproquement vérifie (III.7).

<u>*Solution de l'exercice 5*</u> Si on montre le résultat pour $\overline{f_1} = f_1 - c_1$ et $\overline{f_2} = f_2 - c_2$ pour deux constantes réelles c_1 et c_2, alors on aura le résultat aussi pour f_1 et f_2. En prenant $c_1 = f_1(0)$ et $c_2 = f_2(0)$ on peut supposer $f_1(0) = f_2(0) = 0$.

Remarquons que si $f_2(1) = 0$, alors f_2 est constante, ce qui est interdit par l'hypothèse. On pose $g = f_1(x) - \frac{f_1(1)}{f_2(1)} f_2(x)$. On a $g(1) = 0$, $g(0) = 0$. Or, d'après l'hypothèse, g est monotone, donc g est constante.

<u>*Solution de l'exercice 6*</u> En posant $y = 1$ on a $f(x + 1) = f(x) + 1$. Une récurence immédiate montre que $f(x + n) = f(x) + n$ pour tout n entier. Comme $P(1) = 2$, $f(m) = m + 1$ pour tout entier m. Soit $x = \frac{m}{n}$ un rationnel. En posant $y = n$ ddans l'équation de l'énoncé on a $f(m) = f(x)f(n) - f(x + n) + 1$. Or $f(x + n) = f(x) + n$, donc $f(x) = \frac{m}{n} = x$.

2 Deuxième cours

- Énoncés des exercices vus en cours -

Exercice 1 (Cauchy, trois fonctions) Trouver toutes les fonctions $f, g, h : \mathbb{Q} \to \mathbb{Q}$ telles que $\forall x, y \in \mathbb{Q}$:

$$f(x) + g(y) = h(x + y).$$

Exercice 2 (Cauchy, positif) Trouver toutes les fonctions $f : \mathbb{R}_+ \to \mathbb{R}_+$ telle que $\forall x, y \in \mathbb{R}$:

$$f(x+y) = f(x) + f(y).$$

Exercice 3 (Cauchy multiplicatif sur $\mathbb{N}$) Trouver toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ telle que $\forall x, y \in \mathbb{N}$:

$$f(xy)) = f(x)f(y).$$

Exercice 4 (OIM 1990) Trouver une fonctions $f, g, h : \mathbb{Q}_+^* \to \mathbb{Q}_+^*$ telles que $\forall x, y \in \mathbb{Q}_+^*$:

$$f(xf(y)) = \frac{f(x)}{y}.$$

Exercice 5 (Substitutions cycliques 1) Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telle que $\forall x \in \mathbb{R} \setminus \{0, 1\}$:

$$f(x) = 2f(1-x) + \frac{1-3x}{x(1-x)}.$$

Exercice 6 (Substitutions cycliques 2) Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telle que $\forall x \in \mathbb{R} \setminus \{0, 1\}$:

$$f(x) + f\left(\frac{1}{1-x}\right) = \frac{2(1-2x)}{x(1-x)}.$$

Exercice 7 (Itérations 1) Existe-t-il une fonction $f : \mathbb{N} \to \mathbb{N}$ telle que $\forall n \in \mathbb{N}$:

$$f(f(n)) = n + 1?$$

Exercice 8 (Itérations 2) Existe-t-il une fonction $f : \mathbb{N} \to \mathbb{N}$ telle que $\forall n \in \mathbb{N}$:

$$f(f(n)) = n^2?$$

Exercice 9 (Itérations 3) Existe-t-il une fonction $f : \mathbb{R} \to \mathbb{R}$ telle que $\forall x \in \mathbb{R}$:

$$f(f(x)) = x^2 - 2?$$

Exercice 10 (Composition) Existe-t-il des fonctions $f, g : \mathbb{R} \to \mathbb{R}$ telle que $\forall x \in \mathbb{R}$:

$$f \circ g(x) = x^2 \text{ et } g \circ f(x) = x^3?$$

Exercice 11 (Bonus) Trouver toutes les fonctions $f, g : \mathbb{N} \to \mathbb{N}$ telles que $\forall n \in \mathbb{N}$:

$$f(n) + f(n + g(n)) = f(n + 1).$$

Solution de l'exercice 11 On constate que $f(n+1) = f(n)+f(n+g(n)) \geqslant f(n)$, alors la fonction f est croissante.

Similairement, on trouve que $f(n + 1) \geqslant f(n + g(n))$.

Si $g(n) \geqslant 1$, la croissance de f implique qu'on a deja $f(n + 1) = f(n + g(n))$, donc $f(n) = f(n+1) - f(n+g(n)) = 0$.

Donc, on a montré que pour chaque n, soit $g(n) = 0$, soit $f(n) = 0$.

Cas 1 : $f(n) \equiv 0 \ \forall n \in \mathbb{N}$.

Dans ce cas, l'équation fonctionnelle est correcte, on peut choisir la fonction g librement.

Cas 2 : Il existe n_0 qui est le plus petit nombre naturel tel que $f(n_0) \neq 0$.

Comme f est croissante, $f(n) \neq 0$ pour $n \geqslant n_0$, donc $g(n) = 0$ pour $n \geqslant n_0$.

Donc, pour $n \geqslant n_0$ l'équation fonctionnelle devient $2f(n) = f(n + 1)$, alors $f(n) = f(n_0) \cdot 2^{n-n_0}$ pour $n \geqslant n_0$.

Il reste à déterminer les valeurs de $g(n)$ pour $n < n_0$.

Pour $n = n_0 - 1$, l'équation fonctionnelle donne

$$\begin{aligned} f(n_0 - 1) + f(n_0 - 1 + g(n_0 - 1)) &= f(n_0) \\ 0 + f(n_0 - 1 + g(n_0 - 1)) &= f(n_0) \end{aligned}$$

Mais comme n_0 est le seul argument où f prend la valeur $f(n_0)$, on a $n_0-1+g(n_0-1) = n_0$ et donc

$$g(n_0 - 1) = 1.$$

Pour $n < n_0 - 1$, l'équation fonctionnelle donne $0 + f(n + g(n)) = 0$. Donc, il faut juste assurer que $n + g(n) < n_0$.

Conclusion : On a trouvé la solution triviale $f(n) \equiv 0$, g arbitraire et la famille des solutions avec paramètres $n_0, c \in \mathbb{N}$ et $c_k < n_0 - k$:

$$f(n) = \begin{cases} 0 \text{ si } n < n_0 \\ c \cdot 2^{n-n_0} \text{ si } n \geqslant n_0 \end{cases}$$

$$g(n) = \begin{cases} c_k \text{ si } n < n_0 - 1 \\ 1 \text{ si } n = n_0 - 1 \\ 0 \text{ si } n \geqslant n_0 \end{cases}$$

3 Premier TD

- Énoncés -

Exercice 1 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x et y, $f(\frac{x+y}{2}) = \frac{f(x)+f(y)}{2}$.

Exercice 2 Trouver toutes les fonction $f : [0,1] \to [0,1]$ telles que $f(f(x)) = x$, $f(0) = 0$ et $f(1) = 1$.

Exercice 3 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que f est monotone et $\exists n_0 \geqslant 0$ tel que $\forall x$, $f^{n_0}(x) = -x$.

Exercice 4 Soit E un ensemble fini (non vide). Trouver toutes les fonctions $f : \mathcal{P} \to \mathbb{R}$ telles que pour toutes parties A et B de E, $f(A \cap B) + f(A \cup B) = f(A) + f(B)$, et pour toute bijection $\sigma : E \to E$ et toute partie A de E, $f(\sigma(A)) = f(A)$.

Exercice 5 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous $x, y \in \mathbb{R}$, $f(xf(x) + f(y)) = y + f(x)^2$.

Exercice 6 Soient P et Q deux polynômes tels que $\forall x \in \mathbb{R}$, $P(Q(x)) = Q(P(x))$. Montrer que si $P(x) = Q(x)$ n'a pas de solutions alors $P(P(x)) = Q(Q(x))$ n'a pas de solutions.

- Corrigé -

Solution de l'exercice 1 L'idée est de se ramener à l'équation de Cauchy $f(x+y) = f(x)+f(y)$. Le problème est que $f(0) \neq 0$ a priori. On pose donc $g(x) = f(x) - f(0)$. Alors $g(\frac{x+y}{2}) = \frac{g(x)+g(y)}{2}$ et $g(0) = 0$. Donc en faisant $y = 0$ il vient $g(\frac{x}{2}) = \frac{g(x)}{2}$. D'où $g(x + y) = g(x) + g(y)$ et par l'équation de Cauchy (g est continue), g est affine donc f aussi. Réciproquement les fonctions $ax + b$ sont solutions.

Solution de l'exercice 2 f est bijective. En effet, $f(a) = f(b)$ implique $f(f(a)) = a = f(f(b)) = b$ et f est surjective car $f(f(x)) = x$. On admet le résultat d'analyse connu qui dit qu'une fonction continue injective est tristement monotone. En l'occurrence comme $f(0) < f(1)$, on a f strictement croissante. Si il existe x tel que $f(x) < x$, alors $x = f(f(x)) < f(x)$ contradiction. Si $f(x) > x$, alors $x = f(f(x)) > f(x)$ contradiction. Donc $f(x) = x$ pour tout $x \in [0,1]$.

Solution de l'exercice 3 Déjà, n est impair car sinon f^n est croissante et $x \to -x$ n'est pas croissante. De plus f est strictement décroissante (évident). Soit $x \in \mathbb{R}$. Posons $u_n(x) = f^{2n+1}(x)$ pour $n \geqslant 0$. Alors u_n est monotone car $u_{n+1} = f^2(u_n)$ et f^2 est strictement croissante : ainsi si $u_0 < u_1$, alors $f(u_0) < f(u_1)$, i.e. $u_1 < u_2$ et de même $u_n < u_{n+1}$. Si $u_0 > u_1$, alors $u_n > u_{n+1}$ par le même argument. Comme $u_{kn_0} = -x$ pour tout $k \geqslant 0$, alors si $u_1 = f(x) < -x$, il existe un plus petit indice $k \geqslant 1$ tel que $u_k < u_{k+1}$ (on a même $k < n_0$). Donc à partir de ce rang k, par le raisonnement précédent, notre suite est strictement croissante, contradiction car elle prend une infinité de fois la valeur $-x$. De même on ne peut pas avoir $f(x) > -x$ sinon la suite serait strictement croissante à partir d'un certain rang. Donc $f(x) = -x$, qui est bien une solution réciproquement.

Solution de l'exercice 4 On va montrer que les solutions sont les fonctions affines en le cardinal, i.e. de la forme $f(A) = a \cdot \mathrm{Card}(A) + b$. Déjà, si $A = \{x\}$, $f(A)$ ne dépend pas de x. En effet on a une bijection σ de E vers E telle que $\sigma(x) = y$, pour tout x et y. Posons $b = f(\emptyset)$ et $a = f(\{x\})$ pour un $x \in E$ (c'est indépendant du choix de x). Alors par récurrence sur $\mathrm{card}(A)$, $f(A) = a \cdot \mathrm{Card}(A) + b$. En effet si $x \in A$, $A = (A \setminus \{x\}) \cup \{x\}$. Donc $f(A) = f(A \setminus \{x\}) + f(\{x\}) = a \cdot (\mathrm{Card}(A) - 1) + b + a = a \cdot \mathrm{Card}(A) + b$.

Solution de l'exercice 5 Pour $x = 0$, $f(f(y)) = y + f(0)^2$. Donc f est bijective. Soit x_0 tel que $f(x_0) = 0$. Alors pour $x = x_0$ et y quelconque, $f(f(y)) = y$ donc $f(0) = 0$. En posant $x = f(t)$,

$f(tf(t)+f(y)) = y+t^2 = y+f(t)^2$, donc $f(t)^2 = t^2$. Donc $f(t) = t$ ou $f(t) = -t$, pour chaque t. Attention, le signe peut a priori dépendre de t.

Premier cas : $f(1) = 1$. Alors pour $x = 1$, $f(1+f(y)) = y+1$. En élevant au carré, $(1+f(y))^2 = (y+1)^2$. Si $f(y) = -y$, alors $(1-y)^2 = (1+y)^2$ donc $y = 0$. Donc $f = \mathrm{Id}$. De même si $f(-1) = -1$, $f(x) = -x$.

<u>*Solution de l'exercice 6*</u> Comme les polynômes sont des fonction continues sur $\mathbb{R}$, dire que l'équation $P(x) = Q(x)$ n'a pas de solutions revient à dire que $P(x) > Q(x)$ pour tout x ou que $Q(x) > P(x)$ pour tout x (sinon considérer $P - Q$: il prend une valeur < 0 et une valeur > 0, donc par le TVI une valeur nulle). Sans perte de généralité on peut donc supposer $P > Q$. Alors $P(P(x)) > Q(P(x)) = P(Q(x))$. Si on a un x tel que $P(P(x)) = Q(Q(x))$, alors $Q(Q(x)) > P(Q(x))$, absurde car $P > Q$.

4 Deuxième TD

- Énoncés -

Exercice 1 Déterminer toutes les fonction $f : \mathbb{R} \to \mathbb{R}$ telles que, pour tout réel x :

$$f(x^3+x) \leqslant x \leqslant (f(x))^3 + f(x).$$

Exercice 2 Déterminer les fonctions $f : \mathbb{Z} \to \mathbb{Z}$ telles que, pour tous entiers m, n :

$$f(m+f(f(n))) = -f(f(m+1)) - n.$$

Exercice 3 Soit $f : \mathbb{R} \to \mathbb{R}$ telle que pour tout réel x, on ait $|f(x)| \leqslant 1$ et

$$f\left(x+\frac{13}{42}\right) + f(x) = f\left(x+\frac{1}{6}\right) + f\left(x+\frac{1}{7}\right).$$

Montrer que f est périodique.

- Corrigé -

<u>*Solution de l'exercice 1*</u> Soit $g : x \mapsto x^3 + x$. La fonction g est continue et strictement croissante sur $\mathbb{R}$, et $g(\mathbb{R}) = \mathbb{R}$. Par suite, g est une bijection de $\mathbb{R}$ sur $\mathbb{R}$. On note g^{-1} sa bijection réciproque. Alors, g^{-1} est également strictement croissante sur $\mathbb{R}$.

Soit f une solution éventuelle. Alors, l'énoncé devient : pour tout réel x, on a $f(g(x)) \leqslant x \leqslant g(f(x))$. En appliquant la première égalité à $g^{-1}(x)$, il vient $f(x) \leqslant g^{-1}(x)$. En composant par g^{-1} (qui est croissante) la seconde inégalité, il vient $g^{-1}(x) \leqslant f(x)$.

Et donc $f(x) = g^{-1}(x)$.

Réciproquement, il est facile de vérifier que g^{-1} est bien solution du problème.

<u>*Solution de l'exercice 2*</u> L'idée est de "créer" de la symétrie dans l'équation fonctionnelle. Soit f une solution éventuelle. On note f^k la k-ième itérée de f. Pour tous entiers m, n, on a alors

$$f(f^2(m) + f^2(n)) = -f^2(f^2(m) + 1) - n.$$

Le membre de gauche étant symétrique en m et n, celui de droite doit l'être également, d'où

$$f^2(f^2(m) + 1) + n = f^2(f^2(n) + 1) + m$$

c.à.d.

$$m - n = f^2(f^2(m) + 1) - f^2(f^2(n) + 1).$$

Or, d'après l'équation fonctionnelle initiale $f^2(f^2(m) + 1) = f(-f^2(2) - m) = f(-k - m)$, où $k = f^2(2)$. Donc, pour tous entiers m, n, on a :

$$m - n = f(-k - m) - f(-k - n).$$

Pour $n = -k$ et $p = -m - k$, on déduit que pour tout entier p, $f(p) = f(0) - p$. Notons qu'en particulier, $f(f(p)) = f(f(0) - p) = f(0) - (f(0) - p) = p$. Réciproquement, si $f : p \mapsto q - p$ où $q \in \mathbb{Z}$ est constante, alors pour tous entiers m, n, on a d'une part $f(m + f(f(n))) = f(m + n) = q - m - n$ et, d'autre part $-f(f(m + 1)) - n = -m - 1 - n$. Par suite, la seule solution du problème est $f : p \mapsto 1 - p$.

<u>*Solution de l'exercice 3*</u> Soit f une fonction vérifiant les conditions de l'énoncé (notons qu'il existe bien de telles fonctions, par exemple la fonction $x \mapsto k$ où $k \in [-1, 1]$ est une constante).

On pose $g : x \mapsto f(x + \frac{1}{6}) - f(x)$. D'après l'équation fonctionnelle, pour tout réel x, il vient :

$$g\left(x + \frac{1}{7}\right) = f\left(x + \frac{13}{42}\right) - f\left(x + \frac{1}{7}\right) = f\left(x + \frac{1}{6}\right) - f(x) = g(x).$$

Par suite, la fonction g est $\frac{1}{7}$-périodique. Elle est donc également 1-périodique (puisque $1 = 7 \times \frac{1}{7}$). Ainsi, pour tout réel x, on a $g(x+1) = g(x)$, c.à.d $f(x+1+\frac{1}{6}) - f(x+1) = f(x+\frac{1}{6}) - f(x)$, ou encore

$$f\left(x + 1 + \frac{1}{6}\right) - f\left(x + \frac{1}{6}\right) = f(x + 1) - f(x).$$

Cela signifie que la fonction $h : x \mapsto f(x + 1) - f(x)$ est $\frac{1}{6}$-périodique. Et donc elle est aussi 1-périodique. Par suite, pour tout réel x, on a $h(x + 1) = h(x)$ c.à.d. :

$$f(x + 2) - f(x + 1) = f(x + 1) - f(x).$$

Soit $a \in \mathbb{R}$ fixé, on en déduit que la quantité $f(a + n) - f(a + n - 1)$ est indépendante de n. Notons c cette valeur commune. Alors, pour tout entier $k \geqslant 1$:

$$f(a + k) = f(a) + \sum_{i=1}^{k} f(a + i) - f(a + i - 1) = kc + f(a).$$

Si l'on fait tendre k vers $+\infty$, on constate que, puisque f est bornée, c'est donc que $c = 0$. Mais alors $f(a + 1) - f(a) = 0$, et ce pour tout réel a. Par suite, f est 1-périodique.

5 Test

- Énoncés (durée : 3h) -

Exercice 1 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous $x, y \in \mathbb{R}$:

$$f(f(f(x) + f(y))) = f(x) + y.$$

Exercice 2 Trouver toutes les fonctions $f : \mathbb{Q} \to \mathbb{Q}$ telles que pour tous $x, y \in \mathbb{Q}$:

$$f(x + y) + f(x - y) = 2f(x) + 2f(y).$$

Exercice 3 Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction telle que pour tous $x, y \in \mathbb{R}$:

$$f(f(x + y)) = f(x + y) + f(x)f(y) - xy.$$

On pose $\alpha = f(0)$. Prouver que :

(i) $f(\alpha)f(-\alpha) = 0$,

(ii) $\alpha = 0$,

(iii) $f(x) = x$ pour tout $x \in \mathbb{R}$.

- Corrigé -

Solution de l'exercice 1 Tout d'abord, f est surjective. En effet, en prenant $x = 0$ et $y = z - f(0)$:

$$f(f(f(0) + f(z - f(0)))) = f(0) + z - f(0) = z.$$

Soit alors x_0 un antécédent de 0. On injecte $x = x_0$:

$$f(f(0 + f(y))) = y. \tag{III.19}$$

On injecte $y = x_0$:

$$f(f(f(x) + 0)) = f(x). \tag{III.20}$$

De (III.19) et (III.20), on en tire que $f(z) = z$ pour tout $z \in \mathbb{R}$.

Solution de l'exercice 2 On commence par remarquer que les fonctions $c \cdot x^2$ sont solutions ($c \in \mathbb{Q}$). Montrons que ce sont les seules.
En prenant $x = y = 0$, on a $2f(0) = 4f(0)$ donc $f(0) = 0$. Pour $x = 0$, on obtient $f(-y) = f(y)$ donc f est paire. Montrons que $f(nx) = n^2 f(x)$, pour tout entier $n \geqslant 0$ et pour tout $x \in \mathbb{Q}$. C'est vrai pour $n = 0$ et $n = 1$. On fixe x et on montre la propriété par récurrence sur n. On remplace x par nx et y par x dans l'équation fonctionnelle, on obtient :

$$f((n + 1)x) = 2f(nx) + 2f(x) - f((n - 1)x) = (2n^2 + 2 - (n - 1)^2) \cdot f(x) = (n + 1)^2 f(x)$$

Posons $a = f(1)$ et montrons que $\forall x \in \mathbb{Q}$, $f(x) = ax^2$. C'est vrai $x \in \mathbb{N}$ car $f(x) = f(x \times 1) = x^2 \cdot f(1) = ax^2$, et par parité c'est vrai pour $x \in \mathbb{Z}$.

Dans le cas général, si $x = \frac{p}{q}$, $f(p) = f(qx) = q^2 f(x) = ap^2$, donc $f(x) = ax^2$.

<u>*Solution de l'exercice 3*</u> (i) On injecte $x = y = 0$ et on obtient

$$f(\alpha) = \alpha^2 + \alpha. \tag{III.21}$$

On injecte ensuite $x = \alpha$ et $y = -\alpha$:

$$f(\alpha) = \alpha + f(\alpha)f(-\alpha) + \alpha^2. \tag{III.22}$$

De (III.21) et (III.22) on en tire $f(\alpha)f(-\alpha) = 0$.

(ii) Supposons que $\alpha \neq 0$. Dans un premier temps, supposons $f(\alpha) = 0$. Alors par (III.22), $\alpha + \alpha^2 = 0$ et donc $\alpha = 0$ ou $\alpha = -1$. Donc $\alpha = -1$, et donc en prenant $y = 0$, $f(f(x)) = 0$ pour tout $x \in \mathbb{R}$. Ainsi pour tous $x, y \in \mathbb{R}$,

$$f(x+y) + f(x)f(y) - xy = 0.$$

En prenant $y = \alpha$, il vient $f(x+\alpha) = -x$, et donc $f(x) = -x + \alpha$. On vérifie aisément que cette solution ne convient pas.

Dans un second temps, supposons $f(-\alpha) = 0$. En prenant $x = 0$ et $y = -\alpha$, on obtient

$$f(f(-\alpha)) = f(-\alpha) + \alpha f(-\alpha) - 0,$$

et donc $f(0) = 0$. Ainsi, $\alpha = 0$.

(iii) On fait $y = 0$: $f(f(x)) = f(x)$. Donc $f(x)f(y) = xy$. En prenant $y = 1$, on voit que f est injective, et donc $f(x) = x$.

4 Avancés : combinatoire avancée

1 Premier cours : graphes

Nous renvoyons au cours de graphes disponible sur le site d'Animath pour des détails et compléments (voir les liens en haut de la page 14).

- Énoncés -

Exercice 1 Dans une fête, chaque personne a au moins un ami, et parmi tout groupe d'au moins trois personnes, il n'y a jamais exactement deux paires d'amis. Montrer que tout le monde s'aime ! Que se passe-t-il si on suppose cette propriété vraie seulement pour les groupes de trois personnes ?

Exercice 2 Un tournoi entre les chevaliers du Roi Arthur a été organisé, et toutes les joutes possibles ont été livrées. Montrer qu'il est possible d'ordonner les chevaliers de telle sorte que le premier ait battu le second, le second ait battu le troisième, et ainsi de suite jusqu'au dernier.

Bonus : s'il y a n chevaliers ayant gagné $v_1, v_2, \dots v_n$ combats, montrer que le tournoi est transitif (au sens où si A a vaincu B et B a vaincu C, alors A a vaincu C) si et seulement si :

$$\sum_{i=1}^{n} v_i^2 = \frac{n(n-1)(2n-1)}{6}$$

Exercice 3 Soit G un graphe à n sommets tel que G ne contient pas de triangle (cycle de longueur 3). Prouver que G a au plus $\lfloor n^2/4 \rfloor$ arêtes. Montrer que ce résultat est optimal.

Bonus : montrer que dans un graphe ayant k arêtes, il existe au plus $\lfloor \frac{\sqrt{2}}{3} k^{3/2} \rfloor$ triangles.

Exercice 4 Soit G un graphe complet à n sommets. On fait une suite d'opérations élementaires consistant à choisir un 4-cycle (s'il en existe) et à retirer une arête. Quel est le plus petit nombre d'arêtes possible parmi les graphes que l'on peut atteindre ?

Exercice 5 A la suite du tournoi, les chevaliers du Roi Arthur se sont querellés. Des semaines de patientes négociations par Merlin ont fait en sorte que chaque chevalier est fâché avec moins de la moitié de tous les chevaliers (au sens strict s'ils sont en nombre impair). Est-il possible d'enfin les arranger autour de la Table Ronde de manière à ce que deux ennemis ne soient assis côte à côte ?

Exercice 6 Existe-t-il un polyèdre dont toutes les faces sont des triangles sauf une qui est un pentagone, et tel que tous les sommets sont de degré pair ?

Exercice 7 On oriente arbitrairement les arêtes d'un polyèdre convexe, de telle sorte que tout sommet aie au moins une arête entrante et une arête sortante. Montrer qu'il existe deux faces qui sont orientées de manière cohérente. On pourra introduire pour chaque $s \in G$, $c(s)$ le nombre $c(s)$ de changements d'orientation dans l'ordre cyclique des arêtes autour de s, et pour chaque face F, le nombre $c(F)$ de changement d'orientation dans l'ordre cyclique des arêtes autour de F.

- Corrigé -

Solution de l'exercice 1 On peut supposer qu'il y a au moins 4 personnes. Supposons par l'absurde qu'il y ait deux personnes A et B qui ne s'aiment pas. Soit C un ami de A et D un ami de B. Par hypothèse, B et C ne s'aiment pas, donc $C \neq D$. Si C et D sont amis, on obtient que C et B sont amis, ce qui est une contradiction. D'autre part, si C et D ne s'aiment pas, alors A, B, C, D est un groupe de quatre personnes avec exactement deux paires d'amis, et on a encore une contradiction.

Sous l'hypothèse plus faible, on montre facilement en "suivant les chemins" que la fête sécrit comme une réunion de graphes complets disjoints.

Solution de l'exercice 2 Reformulation en termes de graphe : on donne une direction à chaque arête du graphe complet K_n. Montrons qu'il existe un chemin respectant les orientations et passant exactement une fois par chaque sommet.

On le fait par récurrence sur n. C'est vrai pour $n = 1$! Soit $n \geqslant 2$. On se donne une direction sur chaque arête de K_n. Soit x un sommet quelconque. Par récurrence, $K_n - x$ (qui est un graphe complet à $n-1$ sommets) admet un chemin $P = x_1 \dots x_{n-1}$ respectant les orientations et passant par tous les sommets. Il y a trois possibilités pour les arêtes reliant x à P : soit l'arête xx_1 est orienté vers x_1, soit l'arête xx_{n-1} est orientée vers x, soit ces deux choses ne se produisent pas. Dans le premier et le second cas, on rajoute x en début où en fin de chemin et on a gagné. Dans le second, on considère le plus petit indice i tel que xx_i est orientée vers x et xx_{i+1} est orientée vers x_{i+1}, et on insère x entre x_i et x_{i+1}.

Pour la preuve du bonus, la première question donne l'implication "tournoi transitif"$\Leftarrow$ $\sum_{i=1}^{n} v_i^2 = \sum_{i=1}^{n} (i-1)^2 = \frac{n(n-1)(2n-1)}{6}$. Pour la réciproque, on remarque que la somme des

v_i est constante ($\frac{n(n-1)}{2}$). On montre alors que si le tournoi n'est pas transitif, alors on peut trouver une arête dont le renversement fait baisser la valeur de la somme.

Solution de l'exercice 3 On le démontre par récurrence sur $n \leqslant 1$. Pour $n = 1$ et $n = 2$, le nombre d'arêtes possible est 0 et 1, ce qui correspond bien à la borne. Soit $n \geqslant 3$ et G un graphe à n sommets sans triangle. On choisit une arête $e = xy$ quelconque dans G, et on regarde le graphe $G' = G - \{x, y\}$. Par hypothèse de récurrence, il admet au plus $\lfloor (n-2)^2/4 \rfloor$ arêtes. D'autre part, chaque sommet de G' est relié à au plus l'un de x, y (car sinon on aurait un triangle). Donc le nombre d'arêtes de G est au plus :

$$\lfloor (n-2)^2/4 \rfloor + (n-2) + 1 \leqslant (n-2)^2/4 + (n-2) + 4 = n^2/4$$

Comme ce nombre d'arêtes est bien sûr entier, ceci conclut.

Un graphe qui réalise la borne est le graphe biparti $K_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}$. On peut montrer qu'il est en fait unique. C'est un cas particulier dû à Montel d'un théorème de Turan (cf. poly de Pierre Bornzstein, section 3.5 et exercice 18).

Solution de l'exercice 4 Le graphe complet est connexe, et l'opération élémentaire préserve la connexité car on détruit des cycles. Les graphes obtenus sont donc connexes, et ont au moins $n - 1$ arêtes. Il reste à voir si on peut obtenir un arbre.

L'observation-clé est qu'un arbre est biparti, alors que K_n (pour $n \geqslant 3$, seul cas intéressant) ne l'est pas ! Soit G un graphe et G' un graphe obtenu par opération élémentaire à partir de G. Supposons G' biparti, disons avec $S(G') = S' \cup S''$. Le graphe G est obtenu à partir de G' en rajoutant une arête à un chemin $v_1v_2v_3$ de longueur 3 pour former un 4-cycle. Comme G' est biparti, on doit avoir v_1 et v_3 tous deux dans S' ou dans S'', et rajouter l'arête v_3v_1 donne encore un graphe biparti. Donc G est biparti. Donc on ne peut obtenir un arbre à partir du graphe complet, et le nombre d'arêtes minimal est $\geqslant n$.

La borne n est accessible. Soit G_n le graphe à n arêtes formé par un chemin de longueur $n - 2$ auquel on ajoute un triangle à une extrémité. Montrons par récurrence sur $n \geqslant 3$ que l'on peut obtenir G_n à partir de K_n. Pour $n = 3$, c'est clair. Mais à partir de K_n pour $n \geqslant 4$, on peut utiliser des opérations élémentaires pour supprimer toutes les arètes reliant un sommet fixé aux autres sauf une, et applique la récurrence au K_{n-1} sur les autres.

Solution de l'exercice 5 La reformulation en termes de théorie des graphes est un théorème de Dirac. Soit G un graphe à $n \geqslant 3$ sommets tel que tout sommet est de degré $\geqslant \lceil \frac{n}{2} \rceil$. Montrons qu'il existe un cycle hamiltonien dans G, c'est-à-dire un cycle passant exactement une fois par chaque sommet.

Tout d'abord, G est clairement connexe (regarder le degré maximal des sommets dans la plus petite composante connexe). Considérons un chemin $P = x_0 \dots x_k$ de longueur maximale k dans G. Par maximalité, tous les voisins de x_0 et x_k sont dans P. Par la condition sur le degré et le principe des tiroirs, il existe un indice $0 \leqslant i \leqslant n-1$ tel que $x_0x_{i+1} \in G$ et $x_ix_k \in G$. Mais alors on a un cycle $C = x_0x_{i+1}Px_kx_iPx_0$. Supposons par l'absurde que C n'est pas hamiltonien, i.e. qu'il existe $y \in G - C$. Alors par connexité de G, C a un voisin dans $G - C$, et on voit que l'on a un chemin de longueur $> k$. Donc C est un chemin hamiltonien de G.

Solution de l'exercice 6 On fait un double décompte des arêtes :

$$3(f-1) + 5 = 2a$$

que l'on réinjecte dans la formule d'Euler, ce qui donne :

$$f = 2s - 6$$
$$a = 3s - 8$$

Il n'y a pas de contradiction à ce stade, il faut exploiter la condition sur les degrés. Pour cela, on remarque que si tous les degrés de G sont pairs, on peut colorier les faces en noir et blanc de sorte que deux faces adjancentes n'aient pas la même couleur : en effet, le graphe dual de G est biparti (il n'a pas de cycle de longueur impaire), donc est bicoloriable ! Maintenant, soit f_n (resp. f_b) le nombre de faces noires (resp. blanches). On peut supposer que le pentagone est noir. On refait un double décompte par couleur :

$$a = 3(f_n - 1) + 5$$
$$a = 3f_b$$

d'où l'on tire $3 \mid a$, puis $3 \mid 5$, ce qui est absurde.

Solution de l'exercice 7 La formule clé est :

$$\sum_{s \in S(G)} c(s) + \sum_{F \in F(G)} c(F) = 2e$$

Elle se démontre par exemple par récurrence sur le nombre de sommets, en regardant ce qui se passe quand on introduit un nouveau sommet. (Il y a sans doute aussi un double décompte astucieux...). Combiné avec la formule d'Euler, cela donne :

$$\sum_{s \in S(G)} c(s) + \sum_{F \in F(G)} c(F) = 2s + 2f - 4$$

Or l'hypothèse se traduit par : $\forall s \in S(G),\ c(s) \geqslant 2$. On en déduit :

$$\sum_{F(G)} c(F) \leqslant 2f - 4$$

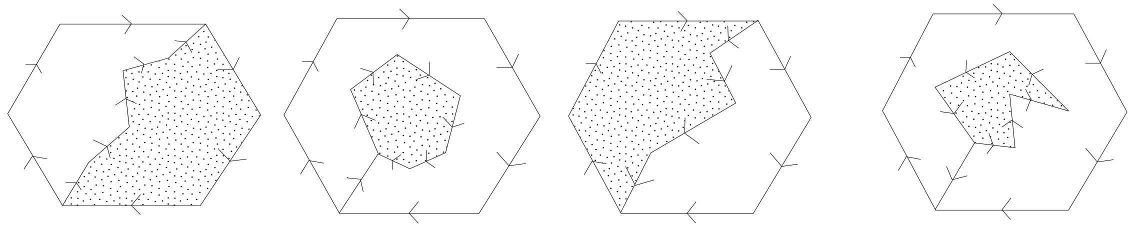
Or $c(F) = 0 \Leftrightarrow$ F est orientée de manière cohérente, et $c(F)$ est toujours pair. On en déduit immédiatement qu'il y a au moins deux faces orientées de manière cohérente.

Cette approche assez étrange à première vue est l'analogue discret d'un théorème sur la topologie des surfaces, à savoir la formule de Poincaré-Hopf sur l'indice d'un champ de vecteur sur la sphère.

Autre solution (proposée par Séginus Mowlawi) : On commence par construire, comme application du fait que tout sommet à une arête sortante et du théorème de la poêle à frire, un cycle orienté correctement. On raisonne ensuite sur les deux "moitiés" du polyèdre découpées par ce cycle. Dans chacune d'entre elles, on montre l'existence d'une face orientée de manière cohérente, par récurrence descendante sur le nombre de faces encloses, en utilisant suivant les cas l'existence d'arêtes entrantes ou d'arêtes sortante. La figure suivante décrit tous les cas possibles et vaut mieux qu'un long discours :

2 Deuxième cours

Ce cours avait pour l'objet l'étude du théorème de dualité de la programmation linéaire.



3 Premier TD

Cette séance est consacrée aux preuves combinatoires. Il est donc interdit d'utiliser d'autres méthodes pour résoudre les exercices. En particulier, les récurrences sont bannies, ainsi que l'utilisation des formules donnant les coefficients binomiaux ou les nombres de Fibonacci.

- Double comptage -

Dans cette partie, seule les preuves par double comptage sont autorisées. Comme son nom l'indique, la méthode de double comptage consiste à compter le nombre d'éléments d'un ensemble de deux façons différentes. On obtient alors deux expressions donnant le nombre d'éléments de A, ce qui nous donne une identité algébrique. Pour prouver une identité par double comptage, il faut commencer par essayer de comprendre ce que compte un des membre de l'identité, puis il faut essayer de faire ce compte d'une autre manière en essayant de faire apparaître les termes de l'autre membre de l'identité.

Exercice 1 Essayez de prouver deux des égalités suivantes :
- $n! = \binom{n}{k}k!(n-k)!$
- $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
- $\binom{n}{k} = \binom{n}{n-k}$
- $k\binom{n}{k} = n\binom{n-1}{k-1}$
- $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Exercice 2 Essayez de prouver deux des égalités suivantes :
- $\binom{\binom{n}{2}}{2} = 3\binom{n}{4} + 3\binom{n}{3}$
- $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$
- $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$
- $\sum_{m=k}^{n} \binom{m}{k} = \binom{n+1}{k+1}$
- $\sum_{m=k}^{n-k} \binom{m}{k}\binom{n-m}{k} = \binom{n+1}{2k+1}$

Nous allons maintenant nous concentrer sur des identités concernant les termes de la suite de Fibonacci. Pour pouvoir obtenir des preuves combinatoires de ce type d'identités, il nous faut tout d'abord un moyen de donner du sens combinatoire aux termes de la suite de Fibonacci. Il y a de nombreuses façons de le faire, on en propose une dans le prochain exercice.

Exercice 3 Soit F_n le n-ième terme de la suite de Fibonacci (avec la convention usuelle $F_0 = 0$ et $F_1 = 1$), et soit f_n le nombre de façons de paver un rectangle $1 \times n$ avec des carrés 1×1 et des dominos 1×2. Montrer que $F_n = f_{n-1}$.

Exercice 4 Montrer que $f_{m+n} = f_m f_n + f_{m-1} f_{n-1}$.

Exercice 5 Montrer que

$$f_0 + f_2 + \ldots + f_{2n} = f_{2n+1}.$$

Exercice 6 Montrer que

$$\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \ldots = f_n.$$

Exercice 7 Montrer que si m divise n alors f_{m-1} divise f_{n-1}.

Exercice 8 Montrer que

$$f_{2n+1} = \sum_{i \geqslant 0} \sum_{j \geqslant 0} \binom{n-i}{j} \binom{n-j}{i}.$$

Exercice 9 Montrer que

$$f_n + f_{n-1} + \sum_{k=0}^{n-2} f_k 2^{n-2-k} = 2^n.$$

Notre méthode ne se limite pas aux seuls termes de la suite de Fibonacci : cette interprétation combinatoire se généralise à une classe bien plus large de suites récurrentes, comme le montre l'exercice suivant, et il est donc possible de prouver de façon combinatoire de nombreux résultats sur les suites récurrentes.

Exercice 10 Trouver une interprétation combinatoire des termes de la suite $(u_n)_{n \in \mathbb{Z}}$ vérifiant $u_n = 0$ si $n < 0$, $u_0 = 1$ et, pour $n \geqslant 1$,

$$u_n = c_1 u_{n-1} + c_2 u_{n-2} + \ldots + c_k u_{n-k},$$

où les c_i sont des entiers positifs.

Pour finir, un petit exemple d'exercice de type olympique faisant appel au double comptage.

Exercice 11 Dans une école, il y a 2007 filles et 2007 garçons. Chaque élève appartient à au plus 100 clubs, et toute paire formée d'un garçon et d'une fille appartient à exactement un club. Montrer qu'il y a un club comportant au moins 11 filles et 11 garçons.

- Bijections -

On dit que deux ensembles A et B sont en bijection s'il existe une application f allant de l'un dans l'autre (disons de A dans B), telle que chaque élément de B est atteint précisément une fois par f. Autrement dit, f apparie les éléments de A avec ceux de B. Si deux ensembles sont en bijection, alors ils ont le même nombre d'éléments. Cela nous donne une nouvelle méthode pour obtenir des identités : si le membre de gauche (resp. de droite) d'une identité compte le nombre d'éléments d'un ensemble A (resp. B), et si ces deux ensembles sont en bijection, alors l'identité est vérifiée.

Exercice 12 On pave un triangle équilatéral de côté n par n^2 petits triangles équilatéraux de côté 1. Combien la figure obtenue comporte-t-elle de parallélogrammes ?

Exercice 13 Une partition de n est une écriture de n comme somme d'entiers. Par exemple, $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$ possède 7 partitions.

Montrer que le nombre de partitions de n à k termes est égal au nombre de partitions de n dont le plus grand élément est k.

Exercice 14 Montrer que le nombre de partitions de n dont tous les éléments sont distincts est égal au nombre de partitions de n dont tous les éléments sont impairs.

Exercice 15 Montrer que $3f_n = f_{n+2} + f_{n-2}$.

Exercice 16 Montrer que $\sum_{k=0}^{n} f_k^2 = f_n f_{n+1}$.

Exercice 17 Montrer que $f_n^2 = f_{n+1}f_{n-1} + (-1)^n$.

Exercice 18 Essayez de fabriquer de nouvelles identités en construisant à la main des bijections.

Une dernière remarque pour terminer : dans cette séance, nous avons surtout prouvé des identités faciles, c'est à dire des identités qui pourraient aisément se prouver par des méthodes classiques de type récurrence (essayez !). Mais n'allez pas croire que la méthode combinatoire est une méthode faible ! En particulier, des preuves combinatoires du même type que celles utilisées dans cette séance permettent de montrer dès identités très fortes sur les suites récurrentes, dont les preuves "classiques" utilisent des techniques algébriques relativement poussées (par exemple des fonctions génératrices ou des fonctions hyperboliques). Si ce sujet vous intéresse, je recommande vivement le livre "Proofs that really count" de Arthur T. Benjamin et Jennifer J. Quinn (la séance correspond au premier chapitre du livre).

Solution de l'exercice 1

- Comptons de deux façons différentes le nombre de façon d'ordonner n personnes. Il y a n choix pour la première personne, puis $n-1$ pour la seconde (car il ne faut pas choisir à nouveau la première personne), et ainsi de suite. Il y a donc $n!$ ordres. Mais on peut aussi commencer par choisir les k personnes qui seront placées devant ($\binom{n}{k}$ possibilités), puis ordonner ces k personnes ($k!$ possibilités) et finir par ordonner les $n-k$ dernières personnes ($(n-k)!$) possibilités). Il y a donc $\binom{n}{k}k!(n-k)!$ ordres.
- On considère une classe de n élèves, un des élèves s'appelant Georges. Comptons de deux façons combien il existe de groupes de k élèves. Par définition, cela vaut $\binom{n}{k}$. Mais on peut aussi dire qu'il y a précisément $\binom{n-1}{k-1}$ groupes contenant Georges (on met Georges d'office dans le groupe, puis on choisit $k-1$ élèves parmi les $n-1$ élèves autres que Georges), et $\binom{n-1}{k}$ groupes ne contenant pas Georges, d'où le résultat.
- Pour choisir un groupe de k élèves dans une classe de n, on peut soit choisir directement les k élèves qui seront dans le groupe ($\binom{n}{k}$ façons de le faire), soit ce qui revient au même choisir les $n-k$ élèves qui ne seront pas dans le groupe ($\binom{n}{n-k}$ façons de le faire).
- On compte le nombre de façons de choisir dans notre classe de n élèves un groupe de k élèves comportant un président. On peut commencer par choisir le groupe ($\binom{n}{k}$ possibilités), puis le président parmi les k élèves du groupe (k possibilités). Le nombre cherché est donc $k\binom{n}{k}$. Mais on peut aussi choisir le président en premier (n possibilités), puis choisir les $k-1$ autres élèves du groupe parmi les $n-1$ élèves restants. Le nombre cherché vaut donc aussi $n\binom{n-1}{k-1}$.
- On compte le nombre de façons de choisir un groupe dans une classe de n élèves. Pour chaque élève, on choisit s'il est dans le groupe ou non (2 possibilités par élève). Le nombre de groupes vaut donc 2^n. On peut aussi distinguer selon le nombre d'élèves du groupe : pour $0 \leqslant k \leqslant n$ il y a $\binom{n}{k}$ groupes de k élèves, d'où le résultat.

Solution de l'exercice 2

– Le nombre de gauche compte le nombre de paires de paires d'entiers de 1 à n (par définition, une paire est non ordonnée, par exemple $(1,2)$ et $(2,1)$ sont considérées comme la même paire). Parmi ces paires, certaines comme la paire $((1,2),(3,4))$ comportent 4 nombres différents. Il y en a $3\binom{n}{4}$ (on choisit d'abord les 4 entiers, puis on regarde le plus petit de nos quatre entiers, et on choisit celui de trois autres qui ira dans la même paire). Les autres paires ont un entier en commun (c'est le cas par exemple de la paire $((1,2),(1,3)))$, il y en a $3\binom{n}{3}$ (on choisit d'abord les 3 entiers, puis on choisit celui des 3 qui sera commun aux deux paires).
– Le terme de gauche est égal au nombre de façons dans une classe de n de choisir un groupe de k élèves contenant un sous groupe de m élèves. Pour compter cela on peut aussi commencer par choisir le sous-groupe de m élèves ($\binom{n}{m}$ choix), puis par le compléter en choisissant $k-m$ élèves à rajouter pour former le groupe de k ($\binom{n-m}{k-m}$ choix).
– Le terme de gauche compte le nombre de groupes d'élèves possédant un président. Or on peut aussi choisir le président (n choix), puis choisir un groupe quelconque parmi les $n-1$ autres élèves ($2^{n-1}\mathrm{choix}$).
– On veut compter les ensembles de $k+1$ entiers parmi $\{1,\dots n+1\}$. Il y a précisément $\binom{m}{k}$ tels ensembles dont le plus grand élément est $m+1$.
– On veut compter les ensembles de $2k+1$ entiers parmi $\{1,\dots 2n+1\}$. Il y a précisément $\binom{m}{k}\binom{n-m}{k}$ tels ensembles dont l'élément médian est $m+1$.

Solution de l'exercice 3 C'est vrai pour n valant 1 ou 2, il suffit donc pour conclure de montrer que les deux suites vérifient la même relation de récurrence. Or il y a deux sortes de pavages du rectangle $1\times n+1$: ceux qui se terminent par un carré (il y en a f_n) et ceux qui se terminent par un domino (il y en a f_{n-1}), et donc $f_{n+1} = f_n + f_{n-1}$.

Solution de l'exercice 4 Petit point de vocabulaire : s'il n'y a pas de domino à cheval entre les deux cases i et $i+1$ d'un pavage, alors on dit que ce pavage a une coupure en position i (car on peut séparer le pavage en deux pavages plus petits en coupant entre les cases i et $i+1$).

On va essayer de couper notre pavage en position m. Si c'est possible, on obtient un pavage du rectangle $1\times m$ ainsi qu'un pavage du rectangle $1\times n$, il y a donc $f_m f_n$ pavages pour lesquels la coupure est possible en m. Si cette coupure est impossible, alors il y a un domino à cheval sur les cases m et $m+1$. En effaçant ce domino, on se retrouve avec deux pavages des rectangles $1\times m-1$ et $1\times n-1$: il y a $f_{m-1}f_{n-1}$ cas où la coupure est impossible.

Solution de l'exercice 5 Tout pavage du rectangle $1\times 2n+1$ comporte nécessairement un carré. Intéressons nous au dernier carré de notre pavage (celui placé le plus à droite). Il est suivi d'une succession de dominos, donc il est placé en position impaire dans le pavage. Il y a exactement f_{2k} pavage du rectangle ou le dernier carré est en position $2k+1$, d'où la formule.

Solution de l'exercice 6 On distingue selon le nombre de dominos appartenant à notre pavage du rectangle $1\times n$. Un pavage comportant k dominos comporte $n-k$ blocs, pour compter ces pavages, il suffit donc de compter le nombre de façons de positionner nos k dominos parmi ces $n-k$ blocs, il y a donc $\binom{n-k}{k}$ partitions à k dominos.

Solution de l'exercice 7 Devant une expression compliquée de la sorte, il faut se demander ce que compte le terme de gauche, en essayant d'interpréter combinatoirement chacun de ses termes. On se rappelle que $\binom{n-i}{j}$ est le nombre de pavages du rectangle $1\times n+j-i$ ayant précisément j dominos (et donc $n-i-j$ carrés). L'autre coefficient $\binom{n-j}{i}$ correspond lui au nombre de pavages du rectangle $1 \times n+i-j$ ayant précisément $n-i-j$ carrés. Les deux termes comptent des pavages ayant le même nombres de carrés. Cela nous donne l'idée d'introduire le carré médian.

Un pavage du rectangle $1 \times 2n+1$ possède un nombre impair de carrés, et possède donc un carré médian. On essaye de compter le nombre de pavages tels qu'il y a i dominos à gauche de ce carré médian, et j dominos à droite. Alors le pavage possède $2n+1-2i-2j$ carrés au total, dont $n-i-j$ sont à gauche du médian. Il y a donc $\binom{n-i}{j}\binom{n-j}{i}$ tels pavages, ce qui conclut.

<u>*Solution de l'exercice 8*</u> Soit q tel que $n = qm$. Il nous faut trouver un moyen de dénombrer le nombre de pavages du rectangle $1 \times qm-1$ faisant apparaître des pavages du rectangle $1 \times m-1$. L'idée naturelle est de regarder les $m-1$ premières cases de notre rectangle. Il y a $f_{m-1}f_{(q-1)m}$ pavages pour lesquelles une coupure est possible en $m-1$. On suppose maintenant cette coupure impossible, et on regarde le prochain bloc potentiel de taille $m-1$: celui compris entre les cases $m+1$ et $2m-1$. Il y a $f_{m-2}f_{m-1}f_{(q-2)m}$ cas où la coupure est possible en $2m-1$ (le f_{m-2} correspond au pavage des $m-2$ cases avant le domino empêchant la première coupure).

Plus généralement, il y a précisément $f_{m-2}^{j-1}f_{m-1}f_{(q-j)m}$ pavages pour lesquels la coupure est impossible en $im-1$ pour $i < j$, mais possible en $jm-1$. Enfin, si les coupures sont impossibles en $im-1$ pour tout $i < q$, alors le domino recouvrant les cases $(q-1)m-1$ et $(q-1)m$ est suivi d'un bloc de taille $m-1$, il y a donc $f_{m-2}^{n-1}f_{n-1}$ tels pavages (je mets ce dernier cas en évidence, car c'est là que l'on se sert de l'hypothèse m divise n). On a donc au final obtenu la formule :

$$f_{n-1} = f_{m-1}\sum_{j=1}^{q} f_{m-2}^{j-1}f_{(q-j)m}.$$

Remarque : l'idée que des résultats de divisibilités peuvent se prouver par des méthodes combinatoires est cruciale et à retenir absolument.

<u>*Solution de l'exercice 9*</u> Il nous faut choisir une interprétation combinatoire de 2^n, on choisit par exemple le nombre de nombres binaires à n chiffres. Il nous faudrait maintenant un moyen d'inclure nos pavages dans cet ensemble de nombres binaires. On va par exemple décider de coder un carré par le chiffre 0 et un domino par la série de chiffre 10, ce qui nous permet de coder un pavage par un nombre binaire (par exemple, le pavage "carré-carré-domino-carré" est codé par 00100). On remarque enfin que les codes correspondant à des pavages sont ceux qui ne comportent pas deux 1 consécutifs, et qui se terminent par 0, ce qui nous donne une nouvelle interprétation combinatoire des nombres de Fibonacci, mieux adaptée au problème. (Il y aurait bien sûr de nombreuses autres façons d'aboutir à une interprétation satisfaisante).

Maintenant, comptons le nombre de nombres binaires à n chiffres. Il y en a $f_{n-1}+f_n$ n'ayant pas deux 1 consécutifs (il y en a f_n qui se terminent par 0, et f_{n-1} qui se terminent par 01). Maintenant, comptons ceux ayant deux 1 consécutifs, en distinguant selon la position de la première telle paire de 1. Si cette première paire est en position $k+1$ et $k+2$, alors le k-ième chiffre est un 0 et donc k premiers chiffres du nombre binaire codent un pavage du rectangle $1 \times k$, les valeurs des $n-2-k$ chiffres à partir de la position $k+3$ sont arbitraires, il y a donc $f_k 2^{n-2-k}$ tels nombres, ce qui montre le résultat.

<u>*Solution de l'exercice 10*</u> Si n est positif u_n est le nombre de façon de paver un rectangle $1 \times n$ en utilisant des carrés 1×1 de c_1 couleurs différentes, des dominos 1×2 de c_2 couleurs différentes, des tuiles 1×3 de c_3 couleurs différentes, ..., et des tuiles $1 \times k$ de c_k couleurs différentes.

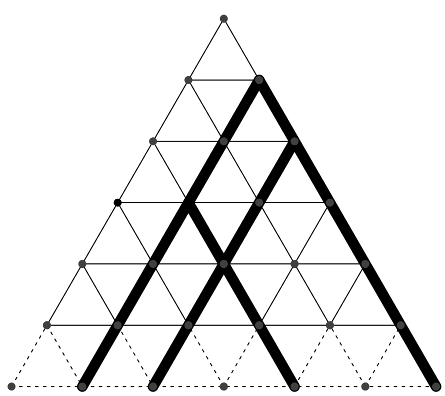
<u>*Solution de l'exercice 11*</u> Quand on voit ce type de problème, il faut immédiatement penser à une approche par double comptage. En effet, les deux hypothèses, ainsi que ce que l'on nous demande de prouver, sont des hypothèses de comptage, et on a donc beaucoup de façon de dénombrer des choses. Il est possible que parmi ces dénombrements, il y en ai un qui résolve le problème.

Raisonnons par l'absurde et supposons que dans chaque club, il y a soit au plus 10 filles (on appelle un tel club un club de type A), soit au plus 10 garçons (club de type B). Dénombrons le nombre de triplets (f, g, c) où f et g sont une fille et un garçon appartenant au club c. Comme chaque paire appartient à exactement un club, il y a exactement 2007^2 tels triplets.

Maintenant, comptons le nombre de triplets où c est un club de type A. On a 2007 choix pour le garçon g, puis au plus 100 choix pour le club c de type A (un élève appartenant à au plus 100 clubs), puis au plus 10 choix pour la fille par définition du club de type A : il y a au plus $10 \times 100 \times 2007$ triplets où c est de type A, et de même pour ceux où c est de type B.

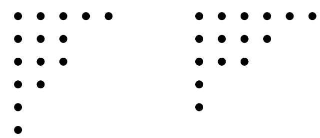
On a donc montré que $2007^2 \leqslant 2 \times 10 \times 100 \times 2007$, une contradiction.

<u>*Solution de l'exercice 12*</u> Tout d'abord, les parallélogrammes n'ont que 3 orientations possibles, et par symétrie il y a autant de parallélogrammes de chaque orientation. On se contente de compter ceux avec une pointe vers le haut. Pour cela, on prolonge notre pavage d'une ligne comme sur le dessin. Pour chacun des parallélogrammes, on prolonge ses côtés, et on obtient quatre intersection avec la ligne rajoutée sous notre triangle. On vérifie que cela donne une bijection entre les parallélogrammes pointant vers le haut et les ensembles de quatre points de notre grille sur la dernière ligne rajoutée. Comme il y a $n+2$ points de la grille sur cette ligne, il y a $\binom{n+2}{4}$ parallélogrammes pointant vers le haut, et donc $3\binom{n+2}{4}$ parallélogrammes au total.



<u>*Solution de l'exercice 13*</u> On va introduire une interprétation plus combinatoire des partitions d'un entier. Ce n'est pas indispensable, mais ça aide à mieux voir les choses. À la partition $n = a_1 + \ldots + a_k$, où les a_i sont classés par ordre décroissant, on associe la figure comportant a_i points, alignés à gauche, dans la ligne i, appelé diagramme de Ferrar. Par exemple, la partition $15 = 5+3+3+2+1+1$ est représentée dans le diagramme de gauche sur la figure.

Le nombre d'éléments de la partition est le nombre de lignes du diagramme, et le plus grand élément est le nombre de points dans la première ligne. La symétrie d'axe la diagonale (qui transforme le diagramme de droite en le diagramme de gauche, qui correspond à la partition $15 = 6+4+3+1+1$) donne une bijection entre les diagrammes de k lignes et ceux de première ligne de longueur k, ce qui conclut.



<u>*Solution de l'exercice 14*</u> On part d'une partition à éléments distincts, par exemple $30 = 12 + 7 + 6 + 4 + 1$. On décompose chaque élément de la partition en parties paire et impaire (on les écrit sous la forme $2^n k$ avec k impair), par exemple $30 = 4 \cdot 3 + 7 + 2 \cdot 3 + 4 \cdot 1 + 1$, puis on casse chaque produit en remplaçant $2^n k$ par $k + k + \ldots + k$, par exemple $30 = 3 + 3 + 3 + 3 + 7 + 3 + 3 + 1 + 1 + 1 + 1 + 1$, et on obtient une partition à nombres impairs.

Pour montrer que cette opération est bijective, exhibons sa réciproque : à partir d'une partition en nombres impairs, on commence par regrouper les termes identiques entre eux (par exemple $30 = 3 + 3 + 3 + 3 + 7 + 3 + 3 + 1 + 1 + 1 + 1 + 1$ devient $30 = 1 \cdot 7 + 6 \cdot 3 + 5 \cdot 1$). Ensuite on décompose chaque coefficient en sommes de puissance de 2 (notre décomposition devient $30 = 1 \cdot 7 + (4 + 2) \cdot 3 + (4 + 1) \cdot 1$), et enfin on casse les sommes de puissance de 2 (ce qui donne $30 = 1 \cdot 7 + 4 \cdot 3 + 2 \cdot 3 + 4 \cdot 1 + 1 \cdot 1$), on vérifie que l'on retombe bien sur la partition de départ.

Dans toute la suite, on notera P_n l'ensemble de tous les pavages du rectangle $1 \times n$ par des carrés et des dominos (par convention P_0 possède un seul élément : le pavage vide).
<u>*Solution de l'exercice 15*</u> Ici, à cause du facteur 3, une bijection fonctionnera mal. L'idée est donc d'essayer d'associer à chaque élément de P_n trois pavages des rectangles $1 \times n - 2$ ou $1 \times n + 2$ (c'est-à-dire trois éléments de $P_{n-2} \cup P_{n+2}$). Le premier est obtenu en rajoutant un domino à l'extrémité droite de notre pavage, le second en rajoutant deux carrés. Pour le troisième, on distingue selon le bloc final du pavage $1 \times n$: si ce pavage se termine par un domino, on lui associe le pavage $1 \times n - 2$ obtenu en supprimant ce domino, mais si ce pavage se termine par un carré, on lui associe le pavage $1 \times n + 2$ obtenu en insérant un domino juste avant ce carré. On vérifie aisément que chaque élément de $P_{n-2} \cup P_{n+2}$ est atteint précisément une fois, d'où le résultat.

<u>*Solution de l'exercice 16*</u> On part d'un élément de $P_n \times P_{n+1}$ (c'est-à-dire d'une paire de pavages des rectangles $1 \times n$ et $1 \times n + 1$). On voudrait essayer de lui associer un élément de P_k^2 (une paire de pavages de deux rectangles de même longueur k) pour un certain k. On place les deux pavages l'un au dessus de l'autre, et soit k la dernière position à laquelle on peut couper les deux pavages (s'il n'y en a pas, on dit que l'on coupe en position 0). En retirant la partie à droite de la coupure, on obtient un élément de P_k^2. Or, la partie à droite de notre coupure est entièrement déterminée : le rectangle possédant un nombre pair de cases est rempli de dominos, l'autre commence par un carré, puis est rempli de dominos. Ceci permet, à partir de l'élément de P_k^2, de remonter à la paire initiale, et notre application de découpage est une bijection entre $P_n \times P_{n+1}$ et $\bigcup_{k=0}^{n} P_k^2$.

<u>*Solution de l'exercice 17*</u> Il faut trouver un moyen d'associer à un élément de P_n^2 une élément de $P_{n-1} \times P_{n+1}$. Pour cela, l'idée est de disposer nos deux rectangles $1 \times n$ les uns sous les

autres, en en décalant un d'un cran. Si les deux pavages ont une coupure au même endroit, on les découpe au niveau de leur dernière coupure commune, et on échange les extrémités des deux pavages. On peut alors facilement revenir en arrière : on découpe les pavages $1 \times n - 1$ et $1 \times n + 1$ obtenus au niveau de leur dernière coupure commune, et on échange à nouveau les extrémités.

Dans quel cas est-il impossible de réaliser l'opération d'échange ? Quand les deux pavages n'ont pas de coupure commune. Ainsi, si n est pair, on ne peut pas procéder à l'échange sur la paire de pavages composés uniquement de dominos, et si n est impair on ne peut faire l'échange à partir de la paire de pavages $1 \times n - 1$ et $1 \times n + 1$ composés uniquement de dominos. C'est de là que vient le terme en $(-1)^n$.

4 Deuxième TD

- Exercices généraux -

Exercice 1 Il y a $n > 1$ clous et $\binom{n}{2}$ ficelles relient deux à deux les clous. Chaque ficelle a une couleur et, pour tout triplet de couleurs, il y a un triangle ayant précisément ces trois couleurs. Décider si n peut être égal à 6. Même question pour $n = 7$.

Exercice 2 On se donne 18 points dans le plan de façon que tout triplet est noncolinéaire. On note A la somme des aires des 816 triangles formés. On choisit une couleur pour chaque point de façon que l'on ait 6 bleus, 6 jeunes et 6 rouges. Montrer que la somme des aires des triangles monochromes (3 sommets de la même couleur) est inférieur à $\frac{A}{4}$.

Exercice 3

1. Pour tout n naturel on a l'égalité :

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}. \tag{III.23}$$

2. Pour tous a, N et k naturels on a :

$$\binom{N+a+1}{k+1} - \binom{N}{k+1} = \sum_{j=0}^{a} \binom{N+j}{k}. \tag{III.24}$$

Exercice 4 De combien de façons peut-on ranger n chaussettes identiques dans un placard avec $k \geqslant 1$ tiroirs.

Exercice 5 Soit $E = \{1, 2, \ldots, n\}$. Compter le nombre de paires non-ordonnées (A, B) telles que $A \bigcup B \subset E$, $A \bigcap B = \emptyset$ et $A \neq \emptyset \neq B$.

Exercice 6 Calculer les chiffres imédiatement à gauche et à doite de la virgule dans $(\sqrt{2} + \sqrt{3})^{2012}$.

Exercice 7 On appelle arangement chaque façon d'asseyer n couples à une table ronde de $2n$ places. On dit qu'un couple est ensemble si ses deux membres sont assis l'un à côté de l'autre. Quel est le nombre moyen de couples ensemble par arangement.

Exercice 8 Les mots d'un langage sont définis de la manière suivante. ab et bb sont les seuls mots de longueur 2. Pour tout $a \geqslant 3$, tous les mots de longurur n s'obtiennent d'un mot de longueur inférieure en remplaçant chaque occurence de b par un mot. Deux occurence différentes peuvent ne pas être remplacées par le même mot. Il y a combien de mots de longueur n ?

- Permutations -

Si E est un ensemble on appelle permutation de E toute fonction bijective $f : E \to E$. On note $\mathcal{S}_n$ l'ensemble de permutations de $\{1, 2, \ldots, n\}$. La définition suivante sert à partager $\mathcal{S}_n$ en deux sous-ensemble : les permutations qui peuvent être transformées en l'identit´e par un nombre pair d'échanges.

Définition 35. Pour tout $\sigma \in \mathcal{S}_n$ on pose

$$\epsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Proposition 36. Pour tout $\sigma \in \mathcal{S}_n$, $\epsilon\sigma \in \{1, -1\}$.

Démonstration. Les ensembles $\{|i-j| \mid i, j \in \{1, 2, \ldots, n\}\}$ et $\{|\sigma(i) - \sigma(j)| \mid i, j \in \{1, 2, \ldots, n\}\}$ sont égaux car σ est une bijection. □

Définition 37. On appelle paire toute permutation σ telle que $\epsilon(\sigma) = 1$. On dit que σ est impaire si $\epsilon(\sigma) = -1$.

Proposition 38. Pour toutes permutations σ et τ, on a $\epsilon(\tau \circ \sigma) = \epsilon(\tau)\epsilon(\sigma)$.

Démonstration.

$$\begin{aligned}
\epsilon(\tau \circ \sigma) &= \Pi_{\{i,j\}} \frac{\tau(\sigma(i)) - \tau(\sigma(j))}{\sigma(i) - \sigma(j)} && \text{(III.25)} \\
&= \Pi_{\{i,j\}} \left(\frac{\tau(\sigma(i)) - \tau(\sigma(j))}{\sigma(i) - \sigma(j)} \cdot \frac{\sigma(i) - \sigma(j)}{i - j} \right) && \text{(III.26)} \\
&= \left(\Pi_{\{i,j\}} \frac{\tau(\sigma(i)) - \tau(\sigma(j))}{\sigma(i) - \sigma(j)} \right) \cdot \left(\Pi_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} \right) && \text{(III.27)} \\
&= \left(\Pi_{\{i,j\}} \frac{\tau(i) - \tau(j)}{i - j} \right) \cdot \left(\Pi_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} \right) && \text{(III.28)} \\
&= \epsilon(\tau)\epsilon(\sigma). && \text{(III.29)}
\end{aligned}$$

Le passage de (III.26) à (III.27) provient du fait qu'un produit de nombre réels peut se faire dans n'importe quel ordre. Le passage de (III.27) à (III.28) provient du faite que l'ensemble $\{\frac{\sigma(i)-\sigma(j)}{i-j} \mid i, j \in \{1, 2, \ldots, n\}\}$ coincide avec l'ensemble $\{\frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \mid i, j \in \{1, 2, \ldots, n\}\}$. □

Proposition 39. Il y a autant de permutations paires et impaires.

Démonstration. On appelle τ_{i_1,i_2} la permutation qui écahnge i_1 et i_2 et laisse les autres éléments inchangés. L'application $f : \epsilon^{-1}(1) \to \epsilon^{-1}(-1)$, $\sigma \mapsto \sigma \circ \tau_{1,2}$ est une bijection. □

Exercice 9 Trouver le nombre de permutations $(a_1, a_2, \dots, a_6)$ de $(1, 2, 3, 4, 5, 6)$ telles que le nombre minimal de transpositions à utiliser pour transformer $(a_1, \dots, a_6)$ en $(1, \dots, 6)$ est 4.

Exercice 10 Le jeu du Taquin consiste de 15 carrés d'aire 1 placé sur un carré d'aire 16 comme dans la Figure 10. Peut-on partir de la configuration où tout carré est à sa place et arriver dans la configuration où on a échangé 15 et 14 en laissant les autres sur place ? On précise qu'un mouvement consiste à bouger le "trou" dans un espace voisin horizontal ou vertical.

- Corrigé des exercices -

<u>*Solution de l'exercice 1*</u> Avant de répondre à la question on peut remarquer que n peut valoir 3 et 5, mais pas 4, ce qui laisse deviner qu'on doit trouver une propriété arithméthique pour les n possibles.

Pour $i \in [1, n]$, on note c_i le nombre de ficelles de couleur i. Comme chaque ficelle participe à exactement $n-2$ triangles et comme il y a $\binom{n}{3}$ triangles, ayant $3\binom{n}{3}$ côtés, on a :

$$\sum_{i=1}^{n} c_i \binom{n}{2} \geqslant 3\binom{n}{3}. \tag{III.30}$$

Comme, $\sum_{i=1}^{n} c_i = \binom{n}{2}$, le nombre de ficelles, (III.30) est possible seulement en tant qu'égalité et cela si chaque ficelle forme le nombre maximal de triangles tricolores. Ainsi, on doit avoir le même nombre de ficelles de chaque couleur. Ainsi :

$$n \mid \binom{n}{2}. \tag{III.31}$$

Cela caractérise les nombres impaires, donc $n = 6$ est impossible.

Pour n impair on appelle les couleurs par des éléments de $\mathbb{Z}/n\mathbb{Z} = \{0, \dots, n-1\}$ l'ensemble des restes modulo n. On associe à chaque clou un élément i différent. Si $i + j$ donne reste k modulo n, alors on donne la couleur k à la ficelle $[i, j]$. Si un triangle i_1, i_2, i_3 a le coloriage (k_1, k_2, k_3) alors il vérifie $2i_1 \equiv k_2 + k_3 - k_1$ et les analogues. Si $2i_1 \equiv 2i_1' \mod n$ pour un certain $i_1' \in \{0, \dots, n-1\}$, alors $n \mid 2(i_1' - i_1)$. Comme n est impair, $i_1 = i_1'$. Donc les triangles sont deux à deux distincts. Comme il y a le même nombre de coloriages que de triangles, tous les coloriages sont obtenus. Donc $n = 7$ est possible.

<u>*Solution de l'exercice 2*</u> On note A_1 la somme des aires des triangles monochromes et A_2 la somme des triangles qui contiennent exactement deux couleurs. On considère un des triangle monochrome ABC et M un point d'une autre couleur. On a clairement :

$$S[ABC] < S[ABM] + S[BCM] + S[ACM]. \tag{III.32}$$

On écrit toutes les équations du type de celle ci-dessus. Chaque triangle monochrome apparait exactement 12 fois dans le membre droit car il y a 12 points d'une couleur autre que celle du triangle ABC. Chaque triangle à deux couleurs apparait exactement 4 fois à doite car son côté monochrome fait partie d'exactement 4 triangles monochromes. Ainsi $12A_1 < 4A_2$, soit $4A_1 < A_1 + A_2$. On conclut que $A_1 < \frac{A}{4}$.

Solution de l'exercice 3

1. On s'intéresse au coefficient de n dans $(x+1)^{2n}$. D'une part on a trivialement $\binom{2n}{n}$. D'autre part on a $(1+x)^{2n} = (1+x)^n(1+x)^n = (\sum_{k=0}^{n} x^k \binom{n}{k})(\sum_{k=0} x^{n-k}\binom{n}{k})$. D'où le résultat.
2. On s'intéresse au coefficient de k dans $\sum_{j=0}^{a}(1+x)^{N+j}$. D'une part il est égal à $\sum_{i=0}^{a}\binom{N+j}{k}$. D'autre part on a l'égalité :
$$\sum_{j=0}^{a}(1+x)^{N+j} = \frac{(1+x)^{(N+a+1)}-1}{x}. \tag{III.33}$$
Ainsi le coefficient de k dans le membre de gauche est celui de $k+1$ dans $(1+x)^{(N+1+a)} - (1+x)^N$, donc $\binom{N+1+a}{k+1} - \binom{N}{k+1}$.

Solution de l'exercice 4 On associe un nombre de 1 à k à chaque tiroir. On représente chaque façon de ranger les chaussettes à l'aide d'un tube transparent et de $n+k-1$ billes de ping-pong dont n blanches et $k-1$ oranges. En effet, si le tube commence par a_1 billes blanches alors on met a_1 chaussettes dans le tiroir 1. Si le tube continue par une bille orange et a_2 blanches, alors on range a_2 chaussetes oranges dans le tiroir 2. Comme il y a $\binom{n+k-1}{k-1}$ façons de mettres les billes de ping-pong dans le tube (positions des billes oranges), il y a autant de façons de ranger les chaussettes dans les tiroirs.

Solution de l'exercice 5 On compte d'abords le nombre de pairs ordonnées (A, B), incluses en E, en leur permettant d'être vides. Pour cela, à chaque fonction $f : E \to \{a, b, 0\}$ on associe la pair (A, B) ordonnée telle que $x \in A \Leftrightarrow f(x) = a$ et $x \in B \Leftrightarrow f(x) = b$. Comme il y a 3^n telles fonctions, on a 3^n pairs ordonnées. Pour passer des pairs ordonnées aux pairs non-ordonnées on sostrait le couple $(\emptyset, \emptyset)$ et on divise par 2 :$\frac{3^n-1}{2}$. Pour trouver le résultat on soustrait les couples de type $(\emptyset, C)$ qui sont en nombre de $2^n - 1$. Ainsi, la réponse est $\frac{3^n+1}{2} - 2^n$.

Solution de l'exercice 6 On montre que $(\sqrt{2}+\sqrt{3})^{2012} = \ldots 7, 9 \ldots$. On pose $a = (\sqrt{2}+\sqrt{3})^2 = 5+\sqrt{24}$ et $b = (\sqrt{2}-\sqrt{3})^2 = 5-\sqrt{24}$. On doit étudier a^{1006}. Le point de départ est la remarque que $a^{1006} + b^{1006}$ est un nombre entier, alors que b^{1006} est petit. En effet, $a^{1006} + b^{1006} = (S_1 + \sqrt{24}S_2) + (S_1 - \sqrt{24}S_2)$ avec $S_1 = \sum_{k=0}^{503} 5^{2k}24^{503-k}\binom{1006}{2k}$ et $S_2 = \sum_{k=0}^{502} 5^{2k+1}24^{503-k}\binom{1006}{2k+1}$. De plus $ab = 25 - 24 = 1$, donc $0 < b < \frac{1}{5}$ et ainsi $b^{1006} < \frac{1}{5^{1006}} < \frac{1}{10}$. En tant qu'entier moins une quantité inférieure à $\frac{1}{10}$, a^{1006} vaut $\ldots, 9 \ldots$.

Pour évaluer le dernier chiffre de a^{1006} il suffit d'évaluer le dernier chiffre de $a^{1006} + b^{1006} = 2S_1$ et d'enlever 1. Chaque terme de S_1 divisible par 5 ne contribue pas au dernier chiffre de $2S_1$. Ainsi, le dernier chiffre est celui de $2 \cdot 24^{503}$. Comme $24^{503} \equiv 4^{503} \mod 10$ et une réurrence imédiate montre que pour tout k, $4^k \equiv 4 \mod 10$ si et seulement si $k \equiv 1 \mod 2$, le dernier chiffre de $2S_1$ est 8. On conclut que $a^{1006} = \ldots 7, 9 \ldots$.

Solution de l'exercice 7 On compte le nombre de couples ensemble dans tous les arangements. Pour tout i on note N_i le nombre de fois où il est ensemble. Par symétrie, pour tout i, $N_i = N_1$.

Le nombre d'arangements où le couple 1 est ensemble est $4n \cdot (2n-2)!$, $4n$ choix pour les places du couple 1 et $(2n-2)!$ pour asseyer les autres couples. Finalement, le nombre de couples ensemble dans tous les arangements cumulés est $N_1 + \cdots + N_n$, soit nN_1. La réponse est donc $\frac{4n(2n-2)!}{(2n)!} = \frac{2n}{2n-1}$.

Solution de l'exercice 8 Pour $n = 2$ et $n = 3$ on remarque que tous les mots commencent par un nombre pair de lettres b, possiblement 0, et finissent par (au moins) un b. Montront par récurrence que cette propriété est vraie pour tout n. Supposons le résultat pour $1, 2, \ldots, n-1$. Si w est un mot obtenu à partir de $c_1 \ldots c_k$ avec $k < n$, alors w ne peut pas finir par a. En effet, $c_k \neq a$ par hypothèse de récurrence, donc la fin de w est un mot de longueur inférieure, obtenu par remplacement. Par l'hypothèse de récurrence ce dernier finit par b, donc w finit par b. Maintenant, la parité du nombre de lettres b au début du mot est gardée par tout remplacement. Comme ab et bb commencent par un nombre pair de lettres b, tout autre mot fait de même.

Montrons maintenant réciproquement que toute suite qui commence par un nombre pair de lettres b et finit par b. Si une suite est de type $bbx \ldots xb$, alors on l'obtient de bb en remplaçant le premier b par bb et le deuxième par $x \ldots xb$ qui est un mot par l'hypothèse de récurrence. Si une suite w est de type $w = aBax \ldots xb$ avec B une suite finie de lettres b, alors on distingue deux cas. Si B est de longueur paire, alors on obtient w de ab en relmplaçant b par $Bax \ldots b$, qui est un mot par l'hypothèse de récurrence. Si B est de longueur impaire, on obtient w comme $bb \to (ab)(u)$ où u est $Bax \ldots b$ sauf la première lettre b. Par l'hypothèse de récurrence u est un mot. Cela finit la description des mots.

Il reste à compter le nombre de suites de n lettres qui commencent par un nombre pair de lettres b et fnissent par b . On note N_n cette quantité. Un mot de $n+2$ lettres peut être bbu avec u un mot de n lettres ou avb avec v n'importe quelle suite. On a N_n choix pour u et 2^n choix pour v. Ainsi on a :

$$N_{n+2} = N_n + 2^n. \tag{III.34}$$

Cela donne $N_n = 2^{n-2} + 2^{n-4} + \cdots$, où la somme finit quand l'exposant devient négatif. Cela vaut $N_n = \frac{2^n + 2(-1)^n}{3}$.

Solution de l'exercice 9 On note n_i le nombre de permutations $(a_1, \ldots, a_6)$ qui ont besoin d'exactement i transpositions pour obtenir $(1, 2, \ldots, 6)$. Comme on a $\frac{6!}{2}$ permutations paires, $n_0 + n_2 + n_4 + n_6 = 360$. Pour toute permutation on peut mettre a_1 à sa place, puis a_2 et ainsi de suite jusqu'à a_5, ce qui implique que a_6 est également à sa place. Ainsi $a_6 = 0$. Clairement $a_0 = 1$. Si on calcule a_2 on aura le résultat.

Une permutation qui se transforme en $(1, \ldots, 6)$ par deux transposition est soit le produit de deux permutations de supports disjoints, soit un $3-$cycle. Le nombre de produits de 2 transpositions à supports disjoints est $\binom{\binom{6}{2}}{2}$. Le nombre de 3 cycles et 2 fois le nombre de supports à 3 éléments, donc $2\binom{6}{3}$. Ainsi $a_4 = 274$.

Solution de l'exercice 10 La configuration de départ et d'arrivée ont des parités différentes. Chaque mouvement est une trasposition, de signature -1, donc on a besoin d'un nombre impair de mouvements.

On colorie les cases du grand carré comme les cases d'un échiquier. À chaque mouvements le trou change de couleur. Au début et 'a la fin il a la même couleur. Ainsi le nombre de mouvements est pair. Contradiction.

5 Test

- Énoncés (durée : 3h30) -

Exercice 1 Soit $d \geqslant 1$ et G un graphe de degré moyen supérieur ou égal à 2d.

1. Montrer que G admet un sous-graphe de degré minimal strictement supérieur à d.
2. Soit T un arbre avec un nombre de sommets inférieur ou égal à d+2. Montrer que G admet une copie de T comme sous-graphe.

Exercice 2 Soit $n \geqslant 0$. On dit qu'une permutation $c : \{1, \ldots, n\} \to \{1, \ldots n\}$ est un 3-cycle s'il existe $i_1, i_2, i_3 \in \{1, \ldots n\}$ distincts tels que $c(i_1) = i_2$, $c(i_2) = i_3$, $c(i_3) = i_1$ et $c(j) = j$ pour tout $j \notin \{i_1, i_2, i_3\}$. Soit $\sigma : \{1, \ldots n\} \to \{1, \ldots, n\}$ une permutation paire. Montrer que σ peut s'écrire comme une composition de 3-cycles.

Exercice 3 Pour tout $k \geqslant 0$, on note F_k le k-ième nombre de Fibonacci. Soient $m, n \geqslant 0$. Montrer :

$$F_{n+1}^m = \sum_{k_1,\ldots,k_{n-1} \geqslant 0} \binom{m}{k_1} \binom{m-k_1}{k_2} \cdots \binom{m-k_{n-2}}{k_{n-1}}$$

Exercice 4 On considère un nombre fini d'intervalles de la droite réelle. Montrer qu'il est possible de les colorier en blanc et rouge de manière à ce que tout point de la droite soit dans le même nombre d'intervalles blancs et rouges, à ± 1 près.

- Corrigé -

<u>*Solution de l'exercice 1*</u>

1. L'énoncé ne le précisait pas, mais on suppose G non-vide et on cherche alors H non-vide...

   Soit G un graphe de degré moyen supérieur ou égal à 2d. Considérons un sous-graphe non-vide H de G de degré moyen $\geqslant 2d$ et minimal (pour la relation de sous-graphe) pour ces propriétés. Il est clair que H a au moins 2 sommets. Supposons par l'absurde que H a un sommet x de degŕe inférieur où égal à d : alors $H - x$ est de degré moyen supérieur ou égal à $(2kd - d * 1 - d)/(k - 1) = 2d$, ce qui contredit la minimalité de H. Donc G a un sous-graphe de degré minimal strictement supérieur à d.
2. On commence par énumérer les sommets de T, disons $\{v_1, \ldots, v_t\}$, de manière à ce que pour tout $2 \leqslant i \leqslant t$, v_i aie exactement un voisin $v_{f(i)}$ parmi $v_1, \ldots, v_{i-1}$. On prend ensuite un sous-graphe H de degré minimal strictement supérieur à d comme en 1. On construit ensuite une copie de T par récurrence sur $1 \leqslant i \leqslant t$: on part de n'importe quel sommet s_1, et on passe de $i - 1$ à i en introduisant un nouveau sommet s_i voisin de $s_{f(i)}$: la condition sur le degré minimum et la borne sur le nombre de sommets de T assure que de tels sommets existent toujours.

<u>*Solution de l'exercice 2*</u> On rappelle que toute permutation $\sigma : \{1, \ldots n\} \to \{1, \ldots n\}$ est composée de transpositions, que la parité p du nombre de transposition dans une telle décomposition ne dépend pas de la transposition (la signature de σ vaut alors $(-1)^p$). On dit que σ est paire si p est pair. On utilise dans ce qui suit la notation en cycles pour les permutations.

D'après ce qui précède, il suffit de montrer que tout produit de deux transpositions distinctes peut être écrit comme composée de 3-cycles. En particulier, on peut supposer $n \geqslant 3$. Soient $\tau = (ab)$, $\tau' = (cd)$ deux transpositions distinctes. Deux cas se présentent : $\{a, b\} \cap \{c, d\} \neq \emptyset$ or $\{a, b\} \cap \{c, d\}\emptyset$.

Dans le premier cas, supposons par exemple que $a = c$. On calcule :

$$(ab) \circ (ad) = (dba)$$

qui est un 3-cycle.

Dans le second cas, on a nécessairement $n \geqslant 4$. On écrit :

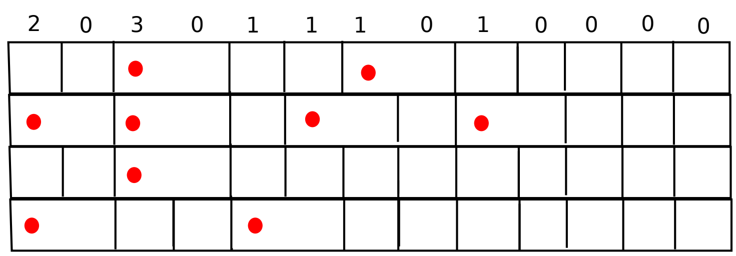
$$(ab) \circ (cd) = (abc) \circ (bcd)$$

qui est une composée de 3-cycles.

<u>*Solution de l'exercice 3*</u> On utilise l'interprétation combinatoire suivante, vue en TD, des nombres de Fibonacci : F_{n+1} est le nombre de pavages du rectangle $1 \times n$ par des carrés 1×1 et des dominos 1×2.

Le membre de gauche compte donc le nombre de m-uplets de pavages de $1 \times n$, que l'on se représente alignés horizontalement. Pour le membre de droite, on sépare les pavages suivant les nombres $k_1, \ldots k_{n-1}$ de dominos qui commencent à la hauteur de la 1ère,... n-ième colonne : il s'agit alors de choisir leurs k_i positions parmi les $m - k_{i-1}$ places laisées par les k_{i-1} dominos de la colonne précédente, soit un total de :

$$\binom{m}{k_1}\binom{m-k_1}{k_2}\cdots\binom{m-k_{n-2}}{k_{n-1}}$$



<u>*Solution de l'exercice 4*</u> Rappelons que les intervalles de $\mathbb{R}$ sont exactement les sous-ensembles convexes, et qu'en particulier l'intersection de deux intervalles est un intervalle.

Notons $I_1, \ldots I_n$ les intervalles en question. On considère les intersections maximales non-vides des I_k : elles forment un nombre fini d'intervallesdisjoints $J_1, \ldots J_m$.

On forme alors la matrice d'incidence de $(I_k)_k$ et de $(J_l)_l$: c'est une matrice $\mathcal{J}$ de taille $n \times m$ avec :

$$\mathcal{J}_{k,l} = \begin{cases} 1, \text{ si } J_l \subseteq I_k \\ 0, \text{ sinon} \end{cases}$$

Montrons que $\mathcal{J}$ est totalement unimodulaire. D'après le théorème de Ghouila-Houri pour les colonnes, il suffit de vérifier que pour tout sous-ensemble $S \subset \{1, \ldots m\}$ de ses colonnes, il est possible d'attribuer des coefficients $(\epsilon_l^S)_{l \in S} \in \{-1, 1\}^S$ tels que pour tout k :

$$\sum_{l \in S} \epsilon_l^S \mathcal{J}_{k,l} \in \{-1, 0, 1\}$$

Pour choisir ces coefficients, on ordonne les intervalles disjoints $(J_l)_{l \in S}$ le long de la droite réelle, puis on leur attribue alternativement le coefficient 1 et -1. Par convexité, les indices l pour lesquels un I_k fixé rencontre J_l sont alors consécutifs, et leur somme alternée vaut bientoujours 1 ou -1. Donc $\mathcal{I}$ est totalement unimodulaire.

Le théorème de Ghouila-Houri appliqué à toutes les lignes de $\mathcal{I}$ dit alors qu'il est possible d'attribuer des coefficients 1 ou -1 aux I_k (que l'on voit comme des couleurs blanches et rouges) de manière à ce, pour tout l, le nombre d'intervalles I_k blancs avec $J_l \subset I_k$ est égal au nombre d'intervalles I_k rouges avec $J_l \subset I_k$, à ± 1 près. Or tout point x de $\mathbb{R}$ contenu dans au moins un des I_k est dans exactement l'un des J_l, et les intervalles I_k dans lesquels le point x se trouve ne dépendent que de l. On a donc terminé.

IV. Troisième période

Contenu de cette partie

1 Incontournables (4èmes-3èmes) : arithmétique

Nous renvoyons au cours d'arithmétique disponible sur le site d'Animath pour des détails et compléments (voir les liens en haut de la page 14).

1 Premier cours

L'arithmétique est l'étude des nombres entiers $0, 1, 2 \dots$. On note $\mathbb{N}$ l'ensemble des nombres entiers et on utilisera aussi la notation $n \in \mathbb{N}$, qui se lit « n appartient à $\mathbb{N}$ » pour dire que n est un nombre entier.

- Identités remarquables -

On commence par rappeler quelques identités remarquables :

$$(a+b)^2 = a^2 + 2ab + b^2, \;\; (a-b)^2 = a^2 - 2ab + b^2, \;\; a^2 - b^2 = (a+b)(a-b).$$

$$1 + a + \cdots + a^{k-1} + a^k = \sum_{i=0}^{k} a^i = \frac{1 - a^{k+1}}{1-a}, \text{ si } a \neq 1.$$

Exercice 1

1. Montrer que si n est somme des carrés de deux entiers consécutifs alors $2n-1$ est le carré d'un entier.
2. Montrer que si $2n-1$ est le carré d'un entier alors n est somme des carrés de deux entiers consécutifs.

Solution de l'exercice 1

1. Par hypothèse, il existe un entier a tel que $n = a^2 + (a+1)^2$. On développe ce qui donne :

   $$n = 2a^2 + 2a + 1.$$

   Un calcul donne maintenant que

   $$2n - 1 = 4a^2 + 4a + 1 = (2a)^2 + 2 \times (2a) \times 1 + 1^2.$$

   On reconnaît une identité remarquable :

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

   ce qui prouve bien que $2n-1$ est le carré d'un entier.
2. Par hypothèse, il existe un entier b tel que $2n - 1 = b^2$. De plus, comme $2n-1$ est impair, on remarque que b est aussi forcément impair (le carré d'un entier pair est pair et le carré d'un entier impair est impair). Ainsi, il existe un entier a tel que $b = 2a+1$. On a donc

   $$2n - 1 = (2a+1)^2 = 4a^2 + 4a + 1.$$

   Ainsi un calcul donne que

   $$n = 2a^2 + 2a + 1 = a^2 + (a^2 + 2a + 1) = a^2 + (a+1)^2.$$

   Comme a est entier, on a bien montré que n est somme de deux entiers consécutifs.

- Divisibilité -

On dit qu'un entier $n \in \mathbb{N}$ divise un entier $m \in \mathbb{N}$ s'il existe un troisième entier $k \in \mathbb{N}$ tel que $m = kn$. On dit aussi que m est un multiple de n. On note alors $n \mid m$.

Exemple 40. – $4 \mid 12$, 4 divise 12 car $12 = 4 \times 3$;
– 5 ne divise pas 12 (on le note $5 \nmid 12$) ;
– 0 est un multiple de tout nombre car si $n \in \mathbb{N}$, alors $0 = 0 \times n$;
– 1 divise tout nombre car si $n \in \mathbb{N}$, alors $n = 1 \times n$.

Nombres premiers : on dit qu'un nombre $p \in \mathbb{N}$ est premier s'il possède exactement deux diviseurs : 1 et p. Attention, 1 n'est pas premier d'après cette définition, en effet il n'a qu'un diviseur.

Exercice 2 Déterminer les nombres premiers inférieurs à 100. Critère d'Eratosthène.

Solution de l'exercice 2 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Exercice 3 Montrer qu'il existe une infinité d'entiers $a \in \mathbb{N}$ tels que $n^4 + a$ n'est premier pour aucun entier $n \in \mathbb{N}$.

Solution de l'exercice 3 Il faut bien choisir la forme de a. Pour $a = 4k^4$, on peut utiliser les identités remarquables comme suit :

$$n^4 + 4k^4 = (n^2 + 2k^2)^2 - 4n^2k^2 = (n^2 + 2k^2 - 2nk)(n^2 + 2k^2 + 2nk).$$

De plus $n^2 + 2k^2 - 2nk = (n-k)^2 + k^2$, donc $n^4 + 4k^4$ n'est pas premier (sauf si $k = 1$ et $n = 1$).

Une propriété importante des nombres premiers est qu'il sont en nombre infini. Voici la preuve qu'en donne Euclide (à peu près 300 ans avant J.C.).

On raisonne par l'absurde, c'est-à-dire qu'on suppose qu'il n'existe qu'un nombre fini, N, de nombres premiers. On les note $p_1, \ldots, p_N$. On considère alors l'entier $n = 1 + p_1 \times \cdots \times p_N$. Soit maintenant p un nombre premier tel que $p \mid n$. Comme p est premier, c'est forcément l'un des p_i, pour un certain $1 \leqslant i \leqslant N$. Donc $p \mid p_1 \times \cdots \times p_N$. Mais $p \mid n$, donc p divise la différence, soit

$$p \mid n - p_1 \times \cdots \times p_N = 1.$$

C'est absurde car aucun nombre premier ne divise 1. Ainsi, il existe une infinité de nombres premiers.

Décomposition en facteurs premiers : une propriété fondamentale est que tout entier $n \neq 0$ peut s'écrire de manière unique sous la forme

$$n = (1\times) p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

où les p_i sont des nombres premiers distincts $p_1 < \cdots < p_k$ et les α_i strictement positifs. Bien sûr, k dépend de n.

Exemple 41.

$$30 = 2 \times 3 \times 5, \quad 135 = 3^3 \times 5.$$

Exercice 4 Énumérer les diviseurs de 30 et de 135, les compter.

Solution de l'exercice 4 Pour 30 : $1, 2, 3, 5, 6, 10, 15, 30$ soit $8 = 2 \times 2 \times 2$ diviseurs. Pour 135 : $1, 3, 5, 9, 15, 27, 45, 135$ soit $8 = 4 \times 2$ diviseurs.

Plus généralement, on peut deviner de l'exercice précédent que si un entier n se décompose en facteurs premiers :

$$n = (1\times)p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

alors n possède exactement $(1 + \alpha_1) \times \cdots \times (1 + \alpha_k) = \prod_{i=1}^{k}(1 + \alpha_i)$ diviseurs. En effet, si m divise n, alors il ne possèdera dans sa décomposition en facteurs premiers que des nombres premiers qui apparaissent dans la décomposition de n, et à une puissance inférieure. Ainsi, m peut s'écrire

$$m = p_1^{\beta_1} \times \cdots \times p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta_i},$$

où pour chaque i, on a $0 \leqslant \beta_i \leqslant \alpha_i$. (Attention au fait que l'écriture de m ci-dessus n'est pas forcément sa décomposition en facteurs premiers ; en effet certaines puissances peuvent-être nulles.) Ainsi, choisir un diviseur de n revient à choisir les puissances $\beta_1, \ldots, \beta_k$ sui vérifient les inégalités ci-dessus, et pour β_i il y a $1 + \alpha_i$ choix.

pgcd, ppcm : le **pgcd** de deux entiers n et m, noté $n \wedge m$ est le plus grand commun diviseur de m et n (noter que 1 est toujours un diviseur commun) c'est-à-dire le plus grand entier l tel que $l \mid n$ et $l \mid m$.

Exemple 42. Le pgcd de 30 et de 135 est $30 \wedge 135 = 15$.

On peut déterminer le pgcd de deux nombres d'après leur décomposition en facteurs premiers. En effet, les facteurs premiers du pgcd doivent apparaître dans les 2 nombres, et à une puissance inférieure à celle des deux nombres (mais quand même maximale). On obtient donc la formule suivante : si

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

$$m = p_1^{\beta_1} \times \cdots \times p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta_i},$$

alors

$$n \wedge m = p_1^{\min(\alpha_1, \beta_1)} \times \cdots \times p_k^{\min(\alpha_k, \beta_k)} = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}.$$

Vérifier que ça coïncide bien avec l'exemple précédent.

On dit que deux entiers m et n sont **premiers entre eux** si $m \wedge n = 1$. Dans le cas général, si a et b sont deux entiers quelconques, et si l'on pose $d = a \wedge b$, alors on peut écrire $a = d \times a'$ et $b = d \times b'$ où a' et b' sont deux entiers tels que $a' \wedge b' = 1$.

Le **ppcm** de deux entiers m et n, noté $m \vee n$, est le plus petit commun multiple de m et de n (noter que $m \times n$ est toujours un commun multiple de m et n) c'est-à-dire le plus petit entier l tel que $n \mid l$ et $m \mid l$.

Exemple 43. Le ppcm de 30 et de 135 est $30 \wedge 135 = 270$.

On peut déterminer le ppcm de deux nombres d'après leur décomposition en facteur premier. En effet, les facteurs premiers du ppcm doivent apparaître dans au moins l'un des 2 nombres, et à une puissance supérieure à celle des deux nombres (mais quand même minimale). On obtient donc la formule suivante : si

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

$$m = p_1^{\beta_1} \times \cdots \times p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta_i},$$

alors

$$n \wedge m = p_1^{\max(\alpha_1,\beta_1)} \times \cdots \times p_k^{\max(\alpha_k,\beta_k)} = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)}.$$

Vérifier que ça coïncide bien avec l'exemple précédent.

Des formules précédentes, on déduit immédiatement que

$$m \times n = \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i} = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)} = (m \wedge n) \times (m \vee n).$$

Exercice 5 Combien existent-ils de couples n, m tels que $n \wedge m = 50$ et $n \vee m = 75$?

Et tels que $n \wedge m = 50$ et $n \vee m = 600$?

<u>*Solution de l'exercice 5*</u> Pour le premier, la réponse est 0 ! En effet, un peu de réflexion montre qu'on doit toujours avoir $n \wedge m \mid n \vee m$, or $50 \nmid 75$.

Pour le second, on commence par décomposer en facteurs premiers : $50 = 2 \times 5^2$ et $600 = 2^3 \times 3 \times 5^2$. On sait aussi que si n, m sont solutions, on a $nm = 50 \times 600 = 2^4 \times 3 \times 5^4$. Enfin $50 \mid n$ et $50 \mid m$.

En conclusion, les solutions seront exactement de la forme $m = 50 \times 2^a \times 3^b$ et $n = 50 \times 2^{2-a} \times 3^{1-b}$, avec $0 \leqslant a \leqslant 2$ et $0 \leqslant b \leqslant 1$. En conclusion, on a 3 choix pour a et 2 pour b soit en tout 6 couples de solutions.

On conclut cette section par un résultat fondamental dû à Gauss, d'où son nom.

<u>*Lemme de Gauss*</u> : soit trois entiers a, b et c tels que $a \mid b \times c$. Si $a \wedge b = 1$ alors $a \mid c$.

Avec ce que l'on a vu précédemment, ce résultat est assez intuitif. L'hypothèse $a \mid b \times c$ peut se traduire par le fait que l'on retrouve tous les éléments de la décomposition en facteurs premiers de a dans le produit $b \times c$. Mais comme $a \wedge b = 1$, aucun de ces éléments ne figure dans la décomposition de b. Ils doivent donc tous venir de c, d'où la conclusion.

Exercice 6 Déterminer tous les triplets d'entiers a, b et c tels que $a^2 + b^2 = c^2$.

<u>*Solution de l'exercice 6*</u> C'est un grand classique, on appelle de tels triplets, des triplets pythagoriciens. On raisonne par analyse-synthèse. On commence par considérer un tel triplet, a, b,

c. Soit $d = a \wedge b$. Alors on a aussi $d \mid c$. Soit $a = da'$, $b = db'$ et $c = dc'$. De plus, on a alors $a' \wedge b' = 1$.

On s'intéresse ensuite à la parité. On a deux possibilités, ou bien a et b sont de parité différente, soit ils sont tous les deux impairs (ils ne peuvent pas être pairs tous les deux car ils sont premiers entre eux). S'ils sont tous les deux impairs, alors on peut écrire $a = 2k + 1$, et $b = 2l + 1$ et alors

$$c^2 = a^2 + b^2 = 4(k^2 + k + l^2 + l) + 2.$$

Donc c^2 est pair, mais n'est pas divisible par 4. Or si c^2 est pair, alors c aussi et on peut écrire $c = 2k'$ et $c^2 = 4c'^2$ qui est donc divisible par 4, c'est absurde.

Ainsi, on a nécessairement que a' et b' sont de parité différente, quitte à les échanger, supposons que $a' = 2A$ et $b' = 2B + 1$. Alors $c = 2C + 1$ est impair. Maintenant on réécrit l'équation initiale comme suit

$$4A^2 = c'^2 - b'^2 = (c' - b')(c' + b').$$

D'abord, montrons que $a' \wedge c' = 1$. Par l'absurde, soit p un nombre premier qui divise b' et c', alors il divise aussi $a'^2 = c'^2 - b'^2$ donc il divise a'. C'est absurde car $a' \wedge b' = 1$. Enfin, on montre que $c' - b' \wedge c' + b' = 2$. En effet, si k divise $c' - b'$ et $c' + b'$ alors il divise leur somme et leur différence, soit $2c'$ et $2b'$. Donc k vaut 1 ou 2. De plus 2 divise bien $c' - b'$ et $c' + b'$.

Enfin, on observe que si $x^2 = yz$ avec $y \wedge z = 1$ alors y et z sont tous les deux des carrés (observer la décomposition en facteurs premiers de x).

Ici, la situation est presque identique, et on trouve qu'il existe deux entiers p et q, premiers entre eux, tels que $c' - b' = 2p^2$ et $c' + b' = 2q^2$, ou encore

$$c = dc' = d(p^2 + q^2), \quad b = db' = d(q^2 - p^2), \quad a = da' = 2dpq.$$

Réciproquement, on vérifie que de tels triplets sont bien pythagoriciens.

- **Division euclidienne** -

Étant donnés deux nombres entiers m et n, il existe un unique couple d'entiers q et r tels que

- $n = m \times q + r$,
- $0 \leqslant r < m$.

Dans ce qui précède, on appelle n le dividende, m le diviseur, q le quotient et r le reste. L'opération qui à (n, m) associe le couple (q, r) s'appelle la division euclidienne de n par m.

Exemple 44. $135 = 30 \times 4 + 15$.

On peut constater que $m \mid n$ si et seulement si le reste de la division euclidienne de n par m est 0.

Exercice 7 Montrer que tout entier n possède un multiple qui ne s'écrit qu'avec des 1 et des 0.

Montrer que si n est impair et n'est pas divisible par 5, alors il possède un multiple qui ne s'écrit qu'avec des 1.

Solution de l'exercice 7 Soit $n \in \mathbb{N}$. On pose pour tout $k \in \mathbb{N}$, a_k le nombre qui s'écrit en base 10 par k fois le chiffre 1. Enfin, on fait la division euclidienne de a_k par n : $a_k = n \times q_k + r_k$.

Comme r_k ne peut prendre qu'un nombre fini de valeurs, par le principe des tiroirs, il existe deux entiers $k < l$ tels que $r_k = r_l$. Mais alors $a_l - a_k = n(q_l - q_k)$ est un multiple de n qui ne s'écrit qu'avec des 0 et des 1.

Pour la seconde question, on reprend le multiple trouvé précédemment qui est de la forme plus précise de un groupe de 1 à gauche puis un groupe de 0 à droite.

L'algorithme d'Euclide : prenons un autre exemple, et amusons nous à continuer les divisions euclidiennes. On va diviser $135 = 3^3 \times 5$ par $105 = 3 \times 5 \times 7$:

$$135 = 105 \times 1 + 30,$$

$$105 = 30 \times 3 + 15,$$

$$30 = 15 \times 2 + 0.$$

Comme les restes successifs des divisions euclidiennes forment une suite strictement décroissante, il y a forcément un moment où l'on ne peut plus continuer, c'est-à-dire où le reste vaut 0. L'avant dernier reste, ci-dessus 15 s'avère être le pgcd de 135 et de 105. Ce n'est pas un hasard. C'est l'algorithme d'Euclide :

étant donnés des entiers r_0 et r_1, l'algorithme d'Euclide consiste à l'étape k à effectuer la division euclidienne de r_{k-1} par r_k : $r_{k-1} = r_k \times q_k + r_{k+1}$ etc.

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, \\
r_1 &= r_2 q_2 + r_3, \\
\vdots &\qquad \vdots, \\
r_{l-2} &= r_{l-1} q_{l-1} + r_l, \\
r_{l-1} &= r_l q_l + 0.
\end{aligned}$$

La suite des r_k est une suite strictement décroissante d'entiers, donc elle doit finir par s'annuler. Le dernier reste non nul (ici r_l) est alors le pgcd de r_0 et de r_1.

Démontrons ce fait. Notons $d = r_0 \wedge r_1$. Il nous faut montrer deux choses : que $d \mid r_l$ puis $r_l \mid d$, ce qui suffit pour conclure.

Pour montrer la première relation, on va montrer que pour tout $k \leqslant l$, $d \mid r_k$. On le fait par récurrence (sur deux indices). Pour commencer, on initialise la récurrence : par définition du pgcd, d divise r_0 et r_1.

Pour l'hérédité, on suppose que pour une certain k, d divise r_{k-1} et r_k. Alors $d \mid r_{k-1} - q_k r_k = r_{k+1}$. Ceci conclut la récurrence.

Montrons maintenant la seconde relation. Pour la première, on a descendu l'échelle des divisions euclidiennes successives, ici on va la remonter. On va montrer par récurrence que pour tout $k \leqslant l$, $r_l \mid r_{l-k}$. Encore une fois, la récurrence se fait sur deux indices, donc il faut vérifier l'initialisation pour $k = 0$ et $k = 1$. La relation est évidente pour $k = 0$, en effet on sait que $r_l \mid r_l$ est automatiquement vrai. Pour $k = 1$ on remarque que $r_l \mid r_{l-1}$ est exactement ce que nous dit la dernière ligne de l'algorithme d'Euclide.

Maintenant, on peut faire l'hérédité. On suppose pour pour un certain k, r_l divise $r_{l-(k-1)}$ et r_{l-k}. On utilise alors que r_l divise aussi $r_{l-k} q_{l-k} + r_{l-(k-1)} = r_{l-(k+1)}$ ce qui conclut la

récurrence. Maintenant, pour $k = l$ et $k = l - 1$, on trouve que r_l divise r_0 et r_1. Il divise donc leur pgcd.
Exercice 8 Déterminer $2^m - 1 \wedge 2^n - 1$.

<u>*Solution de l'exercice 8*</u> Écrivons la division euclidienne de n par m : $n = qm + r$. Maintenant on cherche à faire celle de $2^n - 1$ par $2^m - 1$:

$$2^n - 1 = (2^{mq} - 1)2^r + 2^r - 1 = (2^m - 1)(1 + 2^m + 2^{2m} + \cdots + 2^{(q-1)m}) + 2^r - 1.$$

De plus, $2^r - 1 < 2^m - 1$. Ainsi, l'algorithme d'Euclide associé à $2^n - 1$ et $2^m - 1$ peut être fait parallèlement à celui de n et m. Si $d = n \wedge m$, on aura

$$2^m - 1 \wedge 2^n - 1 = 2^d - 1.$$

<u>*Le théorème de Bezout*</u> : le dernier jeu auquel nous allons nous prêter consiste encore une fois à remonter l'algorithme d'Euclide, à la manière de ce qu'on a fait à la fin de la démonstration précédente. On sait donc que

$$d = r_l = r_{l-2} - r_{l-1}q_{l-1} = r_{l-2}u_1 + r_{l-1}v_1.$$

On remplace alors r_{l-1} par sa valeur donnée par la ligne précédente :

$$r_l = r_{l-2} - (r_{l-3} - r_{l-2}q_{l-2})q_{l-1} = r_{l-3}(-q_{l-1}) + r_{l-2}(1 + q_{l-2}q_{l-1}) = r_{l-3}u_2 + r_{l-2}v_2.$$

Et ainsi de suite, à chaque étape, on trouve deux entiers (relatifs) u_k et v_k tels que $d = r_{l-k-1}u_k + r_{l-k}v_k$. Ainsi, à la fin, on obtient deux entiers relatifs u et v tels que $d = ur_0 + vr_1$.

On vient de montrer la moitié du célèbre **théorème de Bezout** : deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que $1 = au + bv$.

En effet, le fait que si $a \wedge b = 1$ alors il existe u et v vient de l'analyse faite ci-dessous quand $d = 1$. La réciproque doit maintenant être facile. S'il existe u et v tels que $1 = au + bv$, et si d divise a et b, alors il divise $au + bv$ donc $d = 1$.
Exercice 9 Soit a, b et c trois entiers. Trouver tous les couples d'entiers relatifs x, y (possiblement avec un signe - devant) tels que $ax + by = c$.

<u>*Solution de l'exercice 9*</u> On raisonne encore par analyse synthèse. Soit $d = a \wedge b$. Si $ax + by = c$ alors $d \mid c$. On en déduit que si $d \nmid c$, alors il n'y a pas de solution.

Sinon, quitte à tout diviser par d, on peut supposer sans perte de généralité que $a \wedge b = 1$. On commence maintenant par chercher une solution particulière. Soient u et v, donnés par l'algorithme d'Euclide, tels que $au + bv = 1$. Alors, en posant $x_0 = cu$ et $y_0 = cv$ on a bien $ax_0 + by_0 = c$.

Soit maintenant x et y une solution quelconque. En soustrayant $ax + by = c$ et $ax_0 + by_0 = c$ on obtient

$$a(x - x_0) = b(y_0 - y).$$

Comme $a \wedge b = 1$, d'après le lemme de Gauss, $a \mid y_0 - y$, donc il existe un entier k tel que $y = y_0 - ka$. On trouve alors que nécessairement $x = x_0 + kb$.

Réciproquement, pour tout entier relatif k, les couples $x = x_0 + kb, y = y_0 - ka$ sont bien solutions.

2 Deuxième cours

Le sujet de ce cours était l'introduction aux congruences.

3 Premier TD

- Énoncés -

Exercice 1 Pour quels entiers n strictement positifs, le nombre n^2+1 divise-t-il $n+1$?

Exercice 2 Soient $a, b \geqslant 1$ des entiers.

(i) Est-ce que a divise b^2 si, et seulement si, a divise b ?

(ii) Est-ce que a^2 divise b^2 si, et seulement si, a divise b ?

Exercice 3 Trouvez tous les entiers n tels que 2^n+1 est un carré parfait.

Exercice 4 Si n admet un diviseur impair, montrer que 2^n+1 n'est pas premier.

Exercice 5 Montrez que pour tout premier p et tout entier $0 < k < p$, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ est divisible par p. Que se passe-t-il pour $k=0$ ou $k=p$?

Exercice 6 Montrez que la fraction $\frac{39n+4}{26n+3}$ est toujours irréductible.

Exercice 7 Pour quelles valeurs de $n \in \mathbb{N}$ la fraction $\frac{2n^2+11n-18}{n+7}$ est-elle irréductible ?

Exercice 8 Trouver tous les entiers relatifs x, y tels que $2x^3+xy-7=0$.

Exercice 9 Trouver tous les entiers relatifs x tels que $x^3+(x+1)^3+(x+2)^3=(x+3)^3$.

Exercice 10

(i) Trouver tous les entiers $m \geqslant 1$ tels que $m(m+1)$ est une puissance d'un nombre premier.

(ii) Trouver tous les entiers $m \geqslant 1$ tels qu'il existe deux entiers $a \geqslant 1$ et $k \geqslant 2$ tels que $m(m+1)=a^k$.

Exercice 11 Soit m un entier strictement positif. Peut-on trouver m nombres entiers positifs a_1, a_2, ..., a_m placés sur un cercle tels que si on prend deux nombres consécutifs sur ce cercle, le quotient du plus grand sur le plus petit est un nombre premier ?

- Corrigé -

Solution de l'exercice 1 Si n^2+1 divise $n+1$, on doit avoir $n^2+1 \leqslant n+1$, ou encore $n^2 \leqslant n$, c'est-à-dire $n \leqslant 1$. La seule possibilité est donc $n=1$. Réciproquement, $n=1$ convient bien.

Solution de l'exercice 2

(i) Si a divise b, alors comme b divise b^2, a divise b^2 par transitivité de la division. En revanche, si a divise b^2, alors a ne divise pas forcément b : par exemple 9 divise 3^2 mais 9 ne divise pas 3. La réponse est donc *non*.

(ii) Si a divise b, écrivons $b = ka$ avec $k \geqslant 1$ un entier. On élève cette égalité au carré : $b^2 = k^2a^2$. Donc a^2 divise b^2. Maintenant, supposons que a^2 divise b^2 et montrons que a divise b. Notons $v_p(n)$ la plus grande puissance de p divisant n. Il suffit de montrer que pour chaque nombre premier p divisant a, on a $v_p(a) \leqslant v_p(b)$. Comme a^2 divise b^2, $v_p(a^2) \leqslant v_p(b^2)$. Or $v_p(a^2) = 2v_p(a)$ et $v_p(b^2) = 2v_p(b)$. On a donc $2v_p(a) \leqslant 2v_p(b)$, ce qui impliquer $v_p(a) \leqslant v_p(b)$ et conclut la solution.

Solution de l'exercice 3 On réécrit l'équation $2^n = x^2 - 1 = (x+1)(x-1)$, donc $(x+1)$ et $(x-1)$ sont tous les deux des puissances de 2. Les seules puissances de 2 de différence 2 sont 2 et 4, donc la seule solution est $n = 3, 8+1 = 9$.

Solution de l'exercice 4 Écrivons $n = km$ avec $k, m \geqslant 1$ des entiers avec m impair. Comme $a^m + b^m$ set factorise par $a + b$ quand m est impair, l'entier $\left(2^k\right)^m + 1^m$ est divisible par $2^k + 1 \geqslant 2$, et n'est donc pas premier.

Solution de l'exercice 5 Écrivons une égalité sans dénominateurs : $k!(p-k)!\binom{p}{k} = p!$. Comme $0 < k < p$, on a $k < p$ et $p - k < p$. Ainsi, p divise $k!(p-k)!\binom{p}{k}$ sans diviser $k!(p-k)!$. Il divise donc $\binom{p}{k}$ d'après le lemme de Gauss.

Solution de l'exercice 6 Si un entier k divise $39n+4$ et $26n+3$, alors il divise aussi $3(26n+3) - 2(39n+4) = 1$, donc $k = 1$.

Solution de l'exercice 7 On veut calculer le PGCD de $2n^2 + 11n - 18$ et de $n + 7$, essayons donc l'algorithme d'Euclide :

$$2n^2 + 11n - 18 = (n+7) \times (2n-3) + 3$$

Donc le PGCD recherché est un diviseur de 3. Mais 3 divise $2n + 7$ ssi $n \equiv 2[3]$, donc si $n \equiv 0$ ou $1[3]$, alors la fraction est irréductible. Inversement, on vérifie que si $n \equiv 2[3]$ alors la fraction peut être simplifiée par 3.

Solution de l'exercice 8 Tout d'abord, il est clair que $x \neq 0$ et $y \neq 0$. L'entier x divise 7 d'après l'égalité. On a donc $x = -7, -1, 1$ ou 7. Pour chacune de ces valeurs, on obtient une valeur correspondante de y :

- pour $x = -7$, $-2 \cdot 7^3 - 7y - 7 = 0$, donc $y = -2 \cdot 7^2 - 1 = -99$,
- pour $x = -1$, $y = -9$,
- pour $x = 1$, $y = 5$,
- pour $x = 7$, $y = -97$.

Les solutions sont donc $(-7, -99)$, $(-1, -9)$, $(1, 5)$ et $(7, -97)$.

Solution de l'exercice 9 Développons les deux membres de l'égalité :

$$9 + 15x + 10x^2 + 2x^3 = 27 + 27x + 9x^2 + x^3.$$

On obtient, en faisant passer tout d'un seul côté :

$$-18 - 12x + x^2 + x^3 = 0.$$

Ainsi, x divise -18. Mais si x est pair, $-12x + x^2 + x^3$ serait divisible par 4 et donc -18 serait divisible par 4, ce qui n'est pas le cas. Il suffit donc de tester les valeurs $x = -3, -1, 1, 3$. On voit que $x = -3$ est la seule solution.

Solution de l'exercice 10

(i) Écrivons $m(m+1) = p^k$ avec p un nombre premier et $k \geqslant 1$. Alors m et $m+1$ sont tous les deux des puissances de p. Écrivons donc $m = p^a$ et $m+1 = p^b$ avec $a, b \geqslant 0$ et $a + b = k$. Comme $p^b = m+1 \geqslant m = p^a$, on a $b \geqslant a$. Mais on a $p^b - p^a = 1$. Ainsi, si $a \geqslant 1$, p divise $p^b - p^a$ et donc p divise 1, absurde. Donc $a = 0$. Ainsi, $p^b = 2$, et donc $p = 2$ et $b = 1$, ce qui entraine forcément $m = 1$.

(ii) Par l'absurde, supposons qu'il existe des entiers $m \geqslant 1$, $a \geqslant 1$ et $k \geqslant 2$ tels que $m(m+1) = a^k$. Comme m et $m+1$ sont premiers entre eux, il existe deux entiers positifs b, c premiers entre eux tels que $m = b^k$, $m+1 = c^k$ et $bc = a$. Alors $c^k - b^k = 1$. Or $c - b$ divise $c^k - b^k$. Donc $c - b$ divise 1. Donc, comme $c \geqslant b$, on a $c = b + 1$. Donc $1 + b^k = (b+1)^k$. En développant $(b+1)^k$, on obtient :

$$1 + b^k = 1 + \binom{k}{1} b + \binom{k}{2} b^2 + \cdots + \binom{k}{k-1} b^{k-1} + b^k.$$

En simplifiant :

$$0 = \binom{k}{1} b + \binom{k}{2} b^2 + \cdots + \binom{k}{k-1} b^{k-1}.$$

Comme $b > 0$ et $k > 2$, le terme de droite est strictement positif, contradiction.

<u>*Solution de l'exercice 11*</u> Pour m pair on trouve aisément un exemple (avec q premier) : $a_1 = p$, $a_2 = pq$, $a_3 = p$, $a_4 = pq$, ..., $a_{m-1} = p$, $a_m = pq$. Pour m impair on se rend compte qu'il n'est pas possible de trouver un exemple. Une première solution (expéditive) consiste à remarquer que $\frac{a_1}{a_2} \cdot \frac{a_2}{a_3} ... \frac{a_{m-1}}{a_m} \cdot \frac{a_m}{a_1} = 1$. Donc 1 est un produit nombres premiers ou inverses de nombres premiers. On peut donc regrouper deux à deux les terme du produit sous la forme $(p, \frac{1}{p})$. Contradiction car m est impair.

Deuxième solution : On considère ν_i la somme des exposants dans la décomposition de a_i en nombres premiers. Alors ν_i et ν_{i+1} ont parité contraire. Impossible car il y a un nombre impair de ν_i et que ν_1 et ν_m ont parité contraire.

4 Deuxième TD

- Énoncés -

Exercice 1 Montrer qu'un nombre est divisible par 3 si et seulement si la somme de ses chiffres dans la décomposition en base 10 de ce nombre est divisible par 3. Montrer ensuite le même résultat pour 9.

Exercice 2

Montrer que parmi 2008 nombres, on peut toujours en trouver dont la somme est divisible par 2008 (une somme peut éventuellement n'être constituée que d'un seul nombre).

Exercice 3

Montrer que si (x, y, z) est une solution de l'équation suivante alors x ou y est un multiple de 2 :

$$x^2 + y^2 = z^2$$

Exercice 4 Écrire sous forme d'une fraction (si possible) le nombre :

$$x = 0,51234123412341234123412341234123412341234\ldots$$

Pouvez-vous généraliser cette méthode à tous les nombres réels avec un développement périodique ? Et réciproquement ?

Exercice 5 On appelle addichiffrer un nombre le fait d'additionner tous les chiffres d'un nombre. Par exemple, lorsqu'on addichiffre 124, on trouve 1+2+4=6.

Qu'obtient-on lorsqu'on addichiffre 1998^{1998} puis qu'on addichiffre le résultat obtenu et ainsi de suite trois fois de suite ?

Exercice 6 Montrer que le produit de 5 nombres consécutifs ne peut pas être un carré.

Exercice 7 Il y a 40 passagers dans un bus. Ils ont sur eux des pièces de monnaie de 10, 15 et 20 euros. Ils ont en tout 49 pièces de monnaie. Le prix du ticket d'autobus est égal à 5 euros. Montrer qu'il est impossible que tout le monde paye le prix du ticket et obtienne la monnaie en retour.

Exercice 8 Montrer que l'équation :

$$x^3 + 3y^3 + 9z^3 = 9xyz$$

n'a pas d'autre solution rationnelle que $x = y = z = 0$. Indice : commencer par chercher les solutions entières.

Exercice 9 Trouver tous les entiers n tels que $2^n + 3$ est un carré parfait. Même question avec $2^n + 1$.

- Corrigé -

<u>*Solution de l'exercice 1*</u> Soit n un entier naturel et a_1, a_2 et a_k les chiffres de la décomposition de n en base 10 (c'est-à-dire que pour tout i on a $0 \leqslant a_i \leqslant 9$ et $n = a_0 10^0 + a_1 10^1 + \cdots + a_k 10^k$).

On a $10 \equiv 1 \pmod 3$ et donc par récurrence pour $k \geqslant 1$ on a $10^k \equiv 1 \pmod 3$. Donc on a

$$n = a_0 10^0 + a_1 10^1 + \cdots + a_k 10^k \equiv a_0 + a_1 + \ldots a_k \pmod 3$$

et donc les restes de la division par 3 de n et de la somme des chiffres de la décomposition de n en base 10 sont les mêmes.

La preuve précédente est exactement la même pour 9.

<u>*Solution de l'exercice 2*</u>

On note $a_1, a_2, ..., a_{2008}$ les nombres. On considère alors les sommes :
$S_1 = a_1$
$S_2 = a_1 + a_2$
$\vdots$
$S_{2008} = a_1 + a_2 + ... + a_{2008}$
Deux cas sont alors possibles :

- soit une de ces sommes est divisible par 2008, alors on a fini.
- sinon ces sommes ont au plus 2007 restes possibles par division euclidienne, alors il existe S_i et S_j différents (on suppose par exemple $i < j$), tels que $S_i \equiv S_j (\text{mod } 2008)$. On a donc $S_j - S_i = s_{i+1} + ... + s_j \equiv 0 (\text{mod } 2008)$ et on a donc le résultat souhaité.

<u>*Solution de l'exercice 3*</u> Regardons l'équation modulo 4. Si x et y sont impairs alors on a $1+1 = z^2 \pmod 4$ ce qui est impossible car un carré ne peut pas être congru à 2 modulo 4.

<u>*Solution de l'exercice 4*</u> On a

$$10x = 5,12341234123412341234123412341234123412341234\ldots \quad \text{et}$$

$$100000x = 51234,1234123412341234123412341234123412341234\ldots$$

Donc 100000x10x $= 99990x = 51229$ et finalement :

$$x = \frac{51229}{99990}$$

qui est irréductible. Cette méthode se généralise facilement et montre que tout nombre qui admet un développement décimal périodique peut s'écrire sous forme d'une fraction. Et réciproquement, dans le calcul du développement décimal on a seulement un nombre fini de restes et donc le développement décimal d'une fraction est nécessairement périodique.

<u>*Solution de l'exercice 5*</u> 1998 et 1998^{1998} sont des multiples de 9 et donc leurs addichiffres le sont aussi. Par récurrence tous les addichiffres obtenus par une répétition d'opérations d'addichiffre à partir de 1998^{1998} sont multiples de 9.

De plus :

$$1998^{1998} \leqslant 2000^{1998} = (2 \cdot 1000)^{1998} = 2^{1998}10^{3.1998} = 2^{1998}10^{5994}$$

et on sait que $2^9 = 512 < 10^3$ et donc $2^{1998} = 2^{9.222} < 10^{3.222} = 10^{666}$ et donc $1998^{1998} < 10^{5994+666} = 10^{6660}$. Donc l'addichiffre de 1998^{1998} est inférieur à $9.6660 = 59940$. L'addichiffre d'un nombre inférieur à 59940 est nécessairement inférieur à $5 + 9.4 = 41$. L'addichiffre d'un nombre inférieur à 41 est inférieur à $4 + 9 = 13$ et comme cet addichiffre est multiple de 9 et non nul ce nombre est nécessairement 9.

<u>*Solution de l'exercice 6*</u> Supposons que a, b, c, d, e soient des entiers strictement positifs consécutifs tels que $a.b.c.d.e$ soient le carré d'un entier.

Si un des nombres contient un facteur premier supérieur à 5, alors, nécessairement ce facteur doit avoir un exposant pair, car il n'apparait que dans un seul des nombres du produit. Ainsi selon la puissance des facteurs 2 et 3 dans chaque nombre, chacun des nombres a, b, c, d, e est :

1. un carré parfait ou,
2. deux fois un carré parfait ou,
3. trois fois un carré parfait ou,
4. six fois un carré parfait.

D'après le principe des tiroirs, il existe au moins 2 nombres dans la même catégorie. Si les deux nombres sont tous les deux dans le cas 2, 3 ou 4 alors leur différence est au moins 6, ce qui est impossible car a, b, c, d, e sont des entiers consécutifs. Si les deux nombres sont dans le cas 1, alors il sont tous les deux des carrés parfaits. Il est donc impossible que e dépasse 5 car les seuls carrés qui sont à une distance inférieure à 5 sont 1 et 4, or $1.2.3.4.5 = 120$ et 120 n'est pas un carré. Il est donc impossible que le produit de 5 nombres consécutifs strictement positifs soit un carré parfait.

Remarque : Paul Erdös a montré que le produit de $k > 1$ nombres consécutifs n'est jamais un carré.

Solution de l'exercice 7 Le prix total des quarante tickets est 200 euros. Supposons le problème possible. Après avoir réglé les comptes entre eux pour faire l'appoint, chaque passager a récupéré au moins une pièce. Le règlement des tickets a donc nécessité au plus 9 pièces. Mais $9 \cdot 20 = 180 < 200$.

Solution de l'exercice 8 Si on a une solution rationnelle non nulle alors en multipliant par le cube du PPCM des dénominateurs de x, y et z alors on obtient une solution entière non nulle.

Il suffit donc de prouver le théorème pour les valeurs entières. Supposons qu'on ait un triplet d'entiers (x_0, y_0, z_0) dont au moins un est non nul et qui vérifie l'équation. Si on regarde l'équation modulo 3 alors on a

$$x_0 \equiv 0 \pmod 3$$

donc x_0 doit être multiple de 3. On peut donc noter $x_0 = 3x_1$ pour un x_1 entier. Donc l'équation devient :

$$27x_1^3 + 3y_0^3 + 9z_0^3 - 27x_1y_0z_0 = 0 \quad \text{donc :}$$

$$y_0 + 3z_0 + 9x_1 - 9x_1y_0z_0 = 0$$

donc une autre solution est (y_0, z_0, x_1) et de la même façon on peut montrer que $y_0 = 3y_1$ et $z_0 = 3z_1$ avec y_1 et z_1 entiers et donc (x_1, y_1, z_1) est une nouvelle solution. Ainsi x_0, y_0 et z_0 sont divisibles par toute puissance de 3, ce qui est impossible pour des entiers non nuls.

Solution de l'exercice 9 Un carré n'est jamais congru à 3 modulo 4 (si vous ne me croyez pas, essayez vous verrez !), donc 2^n+3 ne peut pas être un carré si $n \geqslant 2$. Et si $n = 1$ alors $2^1+3 = 5$ n'est pas un carré et si $n = 0$ alors $2^0 + 2 = 3$ est un carré. La deuxième question est moins facile. On cherche n et x, deux entiers, tels que $2^n + 1 = x^2$. Autrement dit :

$$2^n = x^2 - 1 = (x1)(x+1)$$

donc $x+1$ et $x-1$ sont tous les deux des puissances de 2. Les seules puissances de 2 à distance 2 sont 2 et 4 donc $2^n = (x^2-1)(x+1) = 2 \cdot 4 = 8$ donc $n = 3$ est la seule solution.

5 Test

- Énoncés -

Exercice 1 Trouver tous les entiers strictement positifs a et n tels que

$$3^n + 1 = a^2.$$

Exercice 2 Pour quelles valeurs de n la fraction

$$\frac{3n^2 + 2n + 4}{n+1}$$

est-elle irréductible ?

Exercice 3 Pour quels entiers $n \geqslant 1$ l'entier $3^{2n} - 2^n$ est-il premier ?.

Exercice 4 Existe-t-il un carré parfait dont l'écriture décimale se termine par 2012 ?

- Corrigé -

Solution de l'exercice 1 Soient $a, n \geqslant 1$ des entiers tels que $3^n + 1 = a^2$. Comme nous savons factoriser une différence de carrés, écrivons $3^n = (a-1)(a+1)$. L'entier 3 étant premier, $a-1$ et $a+1$ sont tous les deux une puissance de 3. il existe donc deux entiers $b, c \geqslant 0$ tels que $a - 1 = 3^b$ et $a + 1 = 3^c$ (avec $b + c = n$ et $c > b$). Alors $3^b + 2 = 3^c$, et donc $2 = 3^c - 3^b$. Si $b > 0$, le terme de droite de l'égalité est divisible par 3, et donc 3 doit diviser 2, ce qui est absurde. Donc $b = 0$, et $2 = 3^c - 1$ et donc $c = 1$. Ainsi $a = 2$ et $n = 1$, et on vérifie réciproquement que cette solution convient.

Solution de l'exercice 2 On effectue la division euclidienne de $3n^2 + 2n + 4$ par $n + 1$:

$$3n^2 + 2n + 4 = (3n - 1)(n + 1) + 5.$$

Notons d le PGCD de $3n^2+2n+4$ et $n+1$. D'après l'égalité précédente, d divise 5. Donc $d = 1$ ou $d = 5$. Or 5 divise $n + 1$ si, et seulement $n \equiv 4 \mod 5$, et lorsque $n \equiv 4 \mod 5$, on a

$$3n^2 + 2n + 4 \equiv 3 \cdot 4^2 + 2 \cdot 4 + 4 \equiv 0 \mod 5.$$

Ainsi, la fraction est irréductible si, et seulement si, $n \not\equiv 4 \mod 5$, autrement dit si, et seulement si, $n - 4$ n'est pas divisible par 5.

Solution de l'exercice 3 On écrit

$$3^{2n} - 2^n = 9^n - 2^n.$$

Cet entier est divisible par 7 (pour le voir, on se rappelle que $9^n - 2^n$ se factorise par $9 - 2 = 7$, ou bien on utilise les modulos : $9^n - 2^n \equiv 2^n - 2^n \equiv 0 \mod 7$). De plus, pour $n > 1$, $9^n - 2^n > 7$. Démontrons-le par exemple par récurrence sur n :

- Initialisation : pour $n = 2$, c'est le cas.

- Hérédité : supposons que pour un entier $n \geqslant 2$, $9^n - 2^n > 7$ et montrons que $9^{n+1} - 2^{n+1} > 7$. On a :

$$9^{n+1} = 9 \cdot 9^n \geqslant 9 \cdot (7 + 2^n) = 9 \cdot 2^n + 63 > 2 \cdot 2^n + 7 = 2^{n+1} + 7,$$

où nous avons utilisé l'hypothèse de récurrence pour la première inégalité.

Ainsi, lorsque $n \geqslant 2$, $9^n - 2^n$ est divisible par 7 et est différent de 7 : il ne peut donc pas être premier. Lorsque $n = 1$, $9^n - 2^n = 7$ est premier.

La réponse est donc $n = 1$.

Solution de l'exercice 4 Si a est un entier tel que l'écriture décimale de a^2 se termine par 2012, alors $x^2 \equiv 2 \mod 10$. Or on vérifie aisément qu'un carré ne peut pas être congru à 2 modulo n. La réponse est donc : non, il n'en existe pas.

2 Incontournables (2ndes-1ères) : arithmétique

Nous renvoyons au cours d'arithmétique disponible sur le site d'Animath pour des détails et compléments (voir les liens en haut de la page 14).

1 Premier cours/TD

Programme : Nombres entiers, partie entière, divisibilité, division euclidienne, décomposition en base b, pgcd, ppcm, algorithme d'Euclide, théorème de Bezout, lemme de Gauss. Pour le détail du cours, voir le poly d'Arithmétique d'Animath.

- Énoncés des exercices vus en cours -

Exercice 1 Soit m un entier strictement positif, et soient $r_1, \dots r_m$ des nombres rationnels tels que $r_1 + \ldots + r_m = 1$. Quelles sont les valeurs minimale et maximale atteintes par la fonction $f(n) = n - \sum_{i=1}^{m} [r_i n]$ pour $n \in \mathbb{N}^*$?

Exercice 2 Montrer que pour tout n, $n^2 + n$ est divisible par 2.

Exercice 3

1. Déterminer le reste de la division euclidienne de 9^{100} par 8.
2. Trouver le dernier chiffre de 2012^{2012}.

Exercice 4 (Problème des poids de Bachet) On dispose d'une balance à deux plateaux avec laquelle on veut pouvoir peser tout objet d'une masse entière comprise entre 1 et 40kg. Quel est le nombre minimal de poids de masse entière qui sont nécessaires à cela :

1. si on ne peut poser ces poids que sur un plateau de la balance ?
2. si on peut les poser sur les deux plateaux ?

Exercice 5 Montrer que pour tout n entier la fraction $\frac{21n+4}{14n+3}$ est irréductible.

Exercice 6 Soient m, n des entiers strictement positifs. Déterminer le pgcd de $\underbrace{1 \dots 1}_{m \text{ chiffres}}$ et de $\underbrace{1 \dots 1}_{n \text{ chiffres}}$

Exercice 7 Déterminer le pgcd de tous les nombres de la forme

$$(a - b)(b - c)(c - d)(d - a)(a - c)(b - d)$$

où a, b, c, d sont des entiers.

Exercice 8 Soit p un nombre premier, k un entier compris entre 1 et $p-1$. Montrer que p divise $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ (qui, on le rappelle, est entier).

- Corrigé -

<u>*Solution de l'exercice 1*</u> Commençons par encadrer $f(n)$ pour avoir une idée des extréma : pour tout i, $r_i n - 1 < [r_i n] \leqslant r_i n$, d'où $n - m < \sum_{i=1}^{m} r_i n \leqslant n$, d'où $0 \leqslant f(n) \leqslant m - 1$. Nous allons montrer qu'en fait les valeurs 0 et $m-1$ sont atteintes. Soit A un dénominateur commun pour tous les r_i (on peut avoir l'idée de le considérer car il réalise l'égalité dans la toute première inégalité écrite), alors puisque $r_i A$ est entier pour tout i, $f(A) = 0$. D'autre part, $f(A - 1) = A - 1 - \sum_{i=1}^{m} [r_i(A - 1)] = A - 1 - \sum_{i=1}^{m} (r_i A - 1) = m - 1$.

<u>*Solution de l'exercice 2*</u>

Méthode 1 : n et n^2 sont de la même parité, donc leur somme est paire.

Méthode 2 : $n^2 + n = n(n + 1)$ est le produit de deux entiers consécutifs, dont un est nécessairement pair.

<u>*Solution de l'exercice 3*</u>

1. Puisque $9 = 1 + 8$, en développant on a $9^{100} = (1 + 8)^{100} = 1 + 8A$ où A est un entier. Donc le reste est 1.

2. Remarquons d'abord que cela revient à chercher le reste de la division euclidienne de 2012^{2012} par 10, qui est le même que celui de 2^{2012}. Or les derniers chiffres successifs des puissances de deux sont $2, 4, 8, 6, 2 \ldots$, périodiques de période 4, et 2^n avec n divisible par 4 a toujours pour dernier chiffre 6, donc puisque 2012 est divisible par 4, la réponse est 6.

Solution de l'exercice 4

1. On est obligé de prendre un poids de 1kg pour pouvoir peser 1kg. Ensuite, pour pouvoir peser 2kg, on a deux possibilités : soit ajouter un autre poids de 1kg, soit ajouter un poids de 2kg. La 2ème solution est plus avantageuse car elle permet en même temps de peser 3kg. De même, pour peser 4kg, il est plus avantageux de choisir un poids de 4kg plutôt qu'un poids de 1 ou de 2kg, car cela permet de peser tout jusqu'à 7kg. Pour la même raison, ensuite on choisit 8kg. On remarque que le choix de poids qui apparait est en fait la suite des puissances de deux. Pour en comprendre la raison, reformulons un peu le problème : nous voulons des entiers $p_1, \ldots p_k$ (les poids) tels que tout entier n entre 1 et 40 puisse s'écrire $n = e_1 p_1 + \ldots + e_k p_k$ avec $e_i \in \{0, 1\}$ ($e_i = 1$ si le poids est utilisé pour peser n, $e_i = 0$ sinon) de la manière « la plus unique possible », car pour avoir un nombre de poids optimal, il faut que chaque pesée puisse se faire de peu de façons différentes, voire d'une unique façon. Or nous venons de voir un telle possibilité de décomposition, la décomposition en base 2, qui est même unique ! Prendre donc des poids égaux aux puissances de deux inférieures à 40, à savoir $1, 2, 4, 8, 16, 32$, répond au problème. Mieux, avec cela on peut même mesurer tous les poids jusqu'à $1 + \ldots + 32 = 2^6 - 1 = 63$.

2. Commençons de même par trouver à la main les premiers poids qu'il faut, en commençant avec un poids de 1kg. Pour peser 2kg, on pourrait prendre 2, mais aussi 3, et c'est cette solution-là qui s'avère la plus avantageuse, car elle permet aussi de peser 4. D'autre part, on ne peut prendre 4 directement car avec 1 et 4 on ne peut peser 2. On choisit donc 1 et 3. De même, la meilleure solution ensuite est de choisir 9, car cela permet de couvrir tous les poids de 5 à 13. On voit que cette fois-ci, les poids qui apparaissent sont des puissances de 3. Pour expliquer cela, écrivons la décomposition unique en base 3 d'un nombre n : $n = e'_0 3^0 + \ldots + e'_k 3^k$ avec des $e'_i \in \{0, 1, 2\}$. Comme dans notre problème il nous faut des coefficients dans $\{-1, 0, 1\}$ (pour indiquer si un poids est utilisé, et si oui, de quel côté de la balance), nous allons appliquer à notre décomposition l'algorithme suivant : remplacer tous les termes de la forme 2×3^k par $3^{k+1} - 3^k$, puis regrouper par puissances de 3 et simplifier, et recommencer jusqu'à n'avoir que des coefficients -1,0 ou 1. L'algorithme termine nécessairement car de nouveaux 2 ne peuvent apparaitre que devant des puissances de 3 de plus en plus grandes. Sur un exemple, cela donne :

$$\begin{aligned} 17 &= 1 \times 3^2 + 2 \times 3 + 2 \times 1 \\ &= 1 \times 3^2 + 3^2 - 3 + 3 - 1 \\ &= 2 \times 3^2 - 1 \\ &= 3^3 - 3^2 - 1 \end{aligned}$$

   Ainsi, tout entier n s'écrit comme somme de puissances de 3 avec des coefficients $-1, 0, 1$, et on prouve que celle-ci est unique de la même manière que la décomposition en base 3 l'est. Donc les puissances de 3 donnent bien une solution à notre problème, et il suffit de quatre poids 1, 3, 9, 27, pour peser tous les poids entre 1 et 40, et cette fois-ci, ce système de poids est même optimal au sens où il ne peut peser que ces poids-là (41 ne peut être pesé).

Solution de l'exercice 5 2(21n+4) - 3(14n+3) = -1, donc pgcd $(21n+4, 14n+3) = 1$.

Solution de l'exercice 6 Supposons que $m < n$ et écrivons $n = mq + r$ la division euclidienne de n par m. Alors la division euclidienne de $\underbrace{1\dots1}_{n \text{ chiffres}}$ par $\underbrace{1\dots1}_{m \text{ chiffres}}$ s'écrit

$$\underbrace{1\dots1}_{n \text{ chiffres}} = \underbrace{1\dots1}_{m \text{ chiffres}} (10^{m(q-1)+r} + \dots 10^{m+r} + 10^r) + \underbrace{1\dots1}_{r \text{ chiffres}}.$$

En appliquant l'algorithme d'Euclide on voit donc que le pgcd cherché est $\underbrace{1\dots1}_{\mathrm{pgcd}(m,n)}$.

Solution de l'exercice 7 Nous allons montrer que le pgcd cherché est 12. En effet, par le principe des tiroirs, parmi a, b, c, d il y a deux nombres congrus modulo 3, et donc leur différence est divisible par 3. Maintenant si on regarde modulo 4, on a deux possibilités : soit il y a deux nombres parmi a, b, c, d congrus modulo 4, et à ce moment-là leur différence est divisible par 4, soit a, b, c, d sont distincts modulo 4. Mais dans ce dernier cas, deux d'entre eux sont pairs et deux sont impairs, donc le produit qui nous intéresse a deux facteurs pairs. Ainsi, dans tous les cas, ce produit est divisible par 3 et par 4, donc par 12.

D'autre part, prenant $a = 0, b = 1, c = 2, d = 3$, le produit obtenu vaut -12 donc le diviseur que nous avons trouvé est bien le pgcd.

Solution de l'exercice 8 Il suffit pour cela de prouver que $k!(p-k)!$ divise $(p-1)!$, sachant que l'on sait qu'il divise $p!$. Or p est premier avec $k!$ et avec $(p-k)!$ (on a bien $1 \leqslant k \leqslant p-1$), donc $k!(p-k)!$ est premier avec p, ce qui conclut.

2 Deuxième cours/TD

- Nombres premiers -

Définition 45 (Nombres premiers)**.** Un entier naturel $p > 1$ est dit *premier* s'il possède exactement deux diviseurs naturels, à savoir 1 et p.

Les nombres premiers inférieurs à 20 sont $2, 3, 5, 7, 11, 13, 17, 19$. Parmi les nombres suivants : $67, 77, 87, 97$, lesquels sont-ils premiers ? Le nombre 67 est premier car il n'est divisible par aucun des entiers $2, 3, 5, 7$ et comme $11^2 > 67$, si 67 avait un facteur premier plus grand que 11, il aurait aussi un facteur premier plus petit. Le nombre 77 n'est pas premier car il est divisible par 7. Le nombre 87 n'est pas premier car il est divisible par 3. Le nombre 97 est premier car il n'est pas divisible par $2, 3, 5, 7$.
Exercice 1 Soit $p > 3$ un nombre premier. Montrer que $p^2 - 1$ est un multiple de 12.

Théorème 46 (Théorème fondamental de l'arithmétique)**.** Tout entier naturel $n > 1$ se décompose de manière unique en produit de nombres premiers.

Théorème 47. L'ensemble des nombres premiers est infini.

Démonstration. Supposons par l'absurde qu'il n'y a qu'un nombre fini n de nombre premiers. Notons ces nombres premiers $p_1, \dots, p_n$, et posons $N = p_1 p_2 \dots p_n + 1$. L'entier N n'est divisible par aucun des p_i. Donc soit il est premier, soit il admet un diviseur premier différent de $p_1, \dots, p_n$. Dans tous les cas, on obtient une contradiction. □

Exercice 2 Montrer que pour tout entier naturel k, il est possible de trouver un entier n tel que les nombres $n+1, \dots, n+k$ soient tous composés.

Exercice 3 Montrer qu'il existe une infinité de nombres premiers de la forme $4k-1$.

Si la décomposition en facteurs premiers de l'entier $n \geqslant 1$ est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors les diviseurs positifs de n sont les entiers de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $1 \leqslant i \leqslant k$. Comme conséquence, on obtient une expression du pgcd et du ppcm de deux entiers lorsqu'on connaît leur décomposition en facteurs premiers. Précisément, si

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

où les p_i sont deux à deux distincts, mais les α_i et β_i sont éventuellement nuls, on a :

$$\mathrm{pgcd}(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_k^{\min(\alpha_k,\beta_k)}$$

$$\mathrm{ppcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_k^{\max(\alpha_k,\beta_k)}$$

Si l'on remarque que pour α et β des entiers (ou des réels), on a toujours $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$, on déduit directement des deux expressions précédentes la relation suivante :

$$\mathrm{pgcd}(a, b) \cdot \mathrm{ppcm}(a, b) = ab.$$

Définition 48 (Valuation p-adique)**.** Si p est un nombre premier, et n un entier non nul, la valuation p-adique de n est le plus grand entier k tel que p^k divise n. On la note $v_p(n)$. Si $n = 0$, on convient que $v_p(0) = +\infty$ pour tout nombre premier p.

Si n non nul se décompose sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors $v_{p_i}(n) = \alpha_i$ pour tout $1 \leqslant i \leqslant k$, et $v_p(n) = 0$ si p est distinct des p_i. Ainsi, $v_p(n) = 0$ sauf pour un nombre fini de p premiers. Si a et b sont deux entiers, on a, pour tout nombre premier p :

$$v_p(ab) = v_p(a) + v_p(b)$$

$$v_p(a+b) \geqslant \min(v_p(a), v_p(b))$$

et la dernière inégalité est une égalité dès que $v_p(a) \neq v_p(b)$.

Exercice 4 Soient a et b des entiers strictement positifs tels que a^n divise b^{n+1} pour tout entier $n \geqslant 1$. Montrer que a divise b.

Exercice 5 (Formule de Legendre) On note $[x]$ la partie entière du réel x. Montrer que si p est un nombre premier et n est un entier positif, on a :

$$v_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots.$$

Lorsque $p^i > n$, on a $[\frac{n}{p^i}] = 0$. Ceci assure qu'il n'y a bien qu'un nombre fini de termes non nuls dans la somme précédente.

Exercice 6 Par combien de zéros se termine le nombre 2012! ?

Exercice 7 Montrer que le nombre

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

est un entier, quels que soient les entiers naturels m et n.

Exercice 8 Montrer que si la décomposition en facteurs premiers de n est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors le nombre de diviseurs positifs de n vaut :

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

et le produit des diviseurs positifs de n vaut :

$$p(n) = n^{\frac{d(n)}{2}}.$$

Exercice 9 Montrer que si deux entiers m et n sont tels que $p(m) = p(n)$, alors $m = n$.

- Solutions des exercices -

Solution de l'exercice 1 On factorise : $p^2 - 1 = (p+1)(p-1)$. Comme p est un nombre premier différent de 2, il est impair. Ainsi, $p-1$ et $p+1$ sont tous les deux pairs et le produit est un multiple de 4. De même $p > 3$ et donc p ne peut-être un multiple de 3. On en déduit que soit $p-1$, soit $p+1$ est un multiple de 3, et donc p^2-1 en est également un. En conclusion, p^2-1 est multiple de 3 et de 4, et donc de 12.

Solution de l'exercice 2 Il suffit de prendre $n = (k+1)! + 1$.

Solution de l'exercice 3 On raisonne par l'absurde en supposant qu'il n'existe qu'un nombre fini de nombres premiers de cette forme, notés $p_1, p_2, \dots p_k$. On considère alors $N = 4p_1p_2 \dots p_k - 1$. Les diviseurs premiers de N sont distincts de 2 et des $p_i, 1 \leqslant i \leqslant k$. Or s'ils étaient tous de la forme $4n+1$, N s'écrirait aussi sous cette forme, donc il en existe au moins un qui est de la forme $4k-1$. Contradiction.

Solution de l'exercice 4 Soit p un nombre premier. L'hypothèse nous dit que $n v_p(a) \geqslant (n + 1) v_p(b)$, soit encore :

$$v_p(a) \geqslant \left(1 + \frac{1}{n}\right) v_p(b)$$

et par passage à la limite $v_p(a) \geqslant v_p(b)$ pour tout nombre premier p. On en déduit que a divise b.

Solution de l'exercice 5 Pour un entier positif ou nul i, appelons n_i le nombre d'entiers compris entre 1 et n dont la valuation p-adique est exactement i. On a alors : $v_p(n!) = n_1 + 2n_2 + 3n_3 + \dots$. D'autre part, les entiers dont la valuation excède i sont exactement les multiples de p^i et sont au nombre de $\left[\frac{n}{p^i}\right]$, d'où :

$$\left[\frac{n}{p^i}\right] = n_i + n_{i+1} + \dots + n_{i+2} + \dots$$

Les deux formules précédentes mises ensemble démontrent la proposition.

Solution de l'exercice 6 L'entier 10 n'est pas premier : on ne peut donc pas appliquer directement la formule de Legendre. En décomposant 10 en facteurs premiers, on se rend compte que le plus grand exposant n tel que 10^n divise 2012! est le plus petit des deux nombres $v_2(2012!)$ et $v_5(2012!)$. La formule de Legendre prouve directement que c'est $v_5(2012!)$. Il vaut :

$$\left[\frac{2012}{5}\right] + \left[\frac{2012}{25}\right] + \left[\frac{2012}{125}\right] + \left[\frac{2012}{625}\right] + \left[\frac{2012}{3125}\right] + \ldots = 402 + 80 + 16 + 3 + 0 + \ldots = 501.$$

Le nombre 2012! se termine donc par 501 zéros.

Solution de l'exercice 7 Compte tenu de la formule de Legendre, il suffit de montrer que pour tout nombre premier p et pour tout entier k,

$$\left[\frac{2m}{p^k}\right] + \left[\frac{2n}{p^k}\right] \geqslant \left[\frac{m}{p^k}\right] + \left[\frac{n}{p^k}\right] + \left[\frac{m+n}{p^k}\right].$$

Or l'inégalité $[2a] + [2b] \geqslant [a] + [b] + [a+b]$ est vraie pour tous réels a et b.

Solution de l'exercice 8 On ne démontre que l'expression de $p(n)$ qui est la plus difficile. Un diviseur positif de n s'écrit $n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ où $0 \leqslant \beta_i \leqslant \alpha_i$. Le produit de tous ces nombres est de la forme $p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k}$. Il suffit donc de calculer les exposants γ_i. Fixons un entier $v \in \{0, 1, \ldots, \alpha_1\}$. Il y a exactement $(\alpha_2+1)\ldots(\alpha_k+1)$ diviseurs de n pour lesquels $\beta_1 = b$. Lorsque l'on multiplie tous ces diviseurs, on aura donc :

$$\gamma_1 = (\alpha_2+1)\ldots(\alpha_k+1)\sum_{v=0}^{\alpha_1} v = \frac{1}{2}\alpha_1(\alpha_1+1)\ldots(\alpha_k+1) = \alpha_1 \cdot \frac{d(n)}{2}.$$

On a bien entendu une formule analogue pour γ_i. En remettant tout bout à bout, on obtient la formule annoncée.

Solution de l'exercice 9 Écrivons : $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ et $n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ où les p_i sont des nombres premiers deux à deux distincts et les exposants α_i et β_i sont des entiers positifs ou nuls. On a vu que le produit des diviseurs de m s'écrit : $p(m) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k}$ pour :

$$\gamma_i = \frac{1}{2}\alpha_i(\alpha_1+1)\ldots(\alpha_k+1).$$

L'hypothèse de l'énoncé assure que pour tout i :

$$\frac{1}{2}\alpha_i(\alpha_1+1)\ldots(\alpha_k+1) = \frac{1}{2}\beta_i(\beta_1+1)\ldots(\beta_k+1)$$

et donc il existe un rationnel q, indépendant de i, tel que $\alpha_i = q\beta_i$. Quitte à intervertir m et n, on peut supposer $q \geqslant 1$. L'hypothèse se réécrit alors :

$$q(q\beta_1+1)\ldots(q\beta_k+1) = (\beta_1+1)\ldots(\beta_k+1)$$

et on voit directement que si $q > 1$, le membre de gauche est strictement supérieur à celui de droite. On a donc $q = 1$ et $m = n$.

3 Troisième cours/TD

- Énoncé des exercices vus en cours -

Exercice 1 Trouver les entiers a tels que 5 divise $a^3 + 3a + 1$.

Exercice 2 Trouver les entiers a, b et c tels que $a^2 + b^2 + 1 = 4c$.

Exercice 3 Trouver un entier x tel que $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$ et $x \equiv 1 \pmod 5$.

Exercice 4 Existe-t-il un entier x tel que $x \equiv 1 \pmod 6$, $x \equiv 9 \pmod{14}$ et $x \equiv 7 \pmod{15}$?

Exercice 5 Le nombre $\underbrace{20122012\ldots2012}_{2012 \text{ fois } ''2012''}$ est-il divisible par 19 ?

Exercice 6 Soit a un entier. Montrer que $a^{561} \equiv a \pmod{561}$.

Exercice 7 Soit p et q deux nombres premiers distincts, d et e deux entiers tels que $de \equiv 1 \pmod{(p-1)(q-1)}$ et a un entier quelconque. Montrer que $\left(a^d\right)^e \equiv a \pmod{pq}$.

- Solutions -

<u>*Solution de l'exercice 1*</u> La condition se réécrit $a^3+3a+1 \equiv 0 \pmod 5$. En essayant les 5 résidus, on constate que les seules solutions sont les entiers congrus à 1 et 2 modulo 5.

<u>*Solution de l'exercice 2*</u> Le problème revient à rechercher les entiers a et b tels que $a^2+b^2+1 \equiv 0 \pmod 4$. Les seuls carrés modulo 4 sont 0 et 1, et on constate donc que l'équation $a^2 + b^2 + 1 \equiv 0 \pmod 4$ n'admet aucune solution. Il s'ensuit que nul triplet d'entiers (a, b, c) ne vérifie $a^2 + b^2 + 1 = 4c$.

<u>*Solution de l'exercice 3*</u> Tout d'abord, le théorème chinois indique qu'un tel x existe bien, car 3, 4 et 5 sont premiers entre eux deux à deux. En outre, il indique également qu'il existe un unique entier naturel $a < 3 \times 4 \times 5 = 60$ tel que $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$ et $x \equiv 1 \pmod 5$ si et seulement si $x \equiv a \pmod{60}$.

Cherchons alors un tel entier a. On sait que $a \equiv 2 \pmod 3$ et que $a \equiv 3 \pmod 4$. On peut donc écrire $a = 3k + 2$. Il faut alors que k satisfasse l'égalité $3k + 2 \equiv 3 \pmod 4$, ou encore $3k \equiv 1 \pmod 4$.

Puisque 3 est inversible modulo 4 et que son inverse est 3 , cela signifie que $k \equiv 3 \pmod 4$. On peut ainsi écrire $k = 4l + 3$, et donc $a = 12l + 11$.

On veut alors que l satisfasse l'égalité $12l + 11 \equiv 1 \pmod 5$, ou encore $12l \equiv 0 \pmod 5$. Puisque 12 est inversible modulo 12, il s'ensuit que $l \equiv 0 \pmod 5$. On peut donc écrire $l = 5m$ et $a = 60m + 11$.

On a donc montré que $a = 11$. En particulier, il s'ensuit que $x = 11$ satisfait simultanément les trois égalités $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$ et $x \equiv 1 \pmod 5$.

<u>*Solution de l'exercice 4*</u> On souhaiterait appliquer directement le théorème chinois, mais on ne le peut pas, parce que 6 et 14 ne sont pas premiers entre eux (et que 6 et 15 ne sont pas premiers entre eux non plus).

Il faut alors ruser dans l'utilisation du théorème chinois : en factorisant $6 = 2\times3$, $14 = 2\times7$ et $15 = 3 \times 5$, on remarque que

- $x \equiv 1 \pmod 6$ si et seulement si $x \equiv 1 \pmod 2$ et $x \equiv 1 \pmod 3$;
- $x \equiv 9 \pmod{14}$ si et seulement si $x \equiv 9 \equiv 1 \pmod 2$ et $x \equiv 9 \equiv 2 \pmod 7$;

– $x \equiv 7 \pmod{15}$ si et seulement si $x \equiv 7 \equiv 1 \pmod 3$ et $x \equiv 7 \equiv 2 \pmod 5$.

On a donc montré que $x \equiv 1 \pmod 6$, $x \equiv 9 \pmod{14}$ et $x \equiv 7 \pmod{15}$ si et seulement si $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$ et $x \equiv 2 \pmod 7$. Le théorème chinois indique alors qu'il existe bien un tel entier x, et même, après un peu de travail, que ces entiers sont les entiers congrus à 37 (mod 210).

Solution de l'exercice 5 Dans la suite, on note N le nombre $\underbrace{20122012\ldots2012}_{2012 \text{ fois } "2012"}$, pour plus de simplicité dans les notations. Remarquons que $N = 2012\sum_{k=0}^{2011} 10^{4k} = 2012\dfrac{10^{8048}-1}{10^4-1}$.

L'idée est alors de regarder les puissances de 10 modulo 7 : $10 \equiv 10 \pmod{19}$, $10^2 \equiv 5 \pmod{19}$, $10^3 \equiv 12 \pmod{19}$, … En outre, le petit théorème de Fermat indique que $10^{18} \equiv 1 \pmod{19}$. Ceci montre que $2012 \equiv 2 \times 10^3 + 10 + 2 \equiv 2 \times 12 + 12 \equiv 17 \pmod{19}$.

De surcroit, puisque $8048 \equiv 2 \pmod 9$ et $8048 \equiv 0 \pmod 2$, alors $8048 \equiv 2 \pmod{18}$: on peut écrire 8048 sous la forme $8048 = 18k + 2$. Il s'ensuit que $10^{8048} \equiv \left(10^{18}\right)^k \times 10^2 \equiv 5 \pmod{19}$.

On a ainsi prouvé que 19 ne divise ni 2012 ni $10^{8048} - 1$. En particulier, cela montre que 19 ne divise pas $2012\left(10^{8048}-1\right)$, et donc ne divise pas N non plus.

Solution de l'exercice 6 On commence par factoriser 561 en produit de facteurs premiers : $561 = 3 \times 11 \times 17$. D'après le théorème chinois, il suffit alors de montrer que $a^{561} \equiv a \pmod 3$, $a^{561} \equiv a \pmod{11}$ et $a^{561} \equiv a \pmod{17}$.

En particulier, on note que $561 = 2 \times 280 + 1 = 10 \times 56 + 1 = 16 \times 35 + 1$, donc que $a^{561} \equiv \left(a^2\right)^{280} \times a \equiv a \pmod 3$, $a^{561} \equiv \left(a^{10}\right)^{56} \times a \equiv a \pmod{11}$ et $a^{561} \equiv \left(a^{16}\right)^{35} \times a \equiv a \pmod{17}$.

Cela signifie que $a^{561} - a$ est divisible à la fois par 3, par 11 et par 17, c'est-à-dire que $a^{561} \equiv a \pmod{561}$.

Solution de l'exercice 7 Soit k un entier tel que $de = k(p-1)(q-1)+1$. Si p divise a, alors $a^{de} \equiv 0 \equiv a \pmod p$. Sinon, alors $a^{de} \equiv \left(a^{p-1}\right)^{k(q-1)} \times a \equiv a \pmod p$. Dans tous les cas, cela signifie que $a^{de} \equiv a \pmod p$.

De même, on montre que $a^{de} \equiv a \pmod p$. Le théorème chinois indique alors que $a^{de} \equiv a \pmod{pq}$.

4 Quatrième cours/TD

- L'indicatrice d'Euler -

Soit $n \in \mathbb{N}$, on définit $\varphi(n)$ comme étant le nombre d'entiers $k \in \mathbb{N}$ tels que $k \wedge n = 1$, $k < n$. Cette fonction s'appelle l'indicatrice d'Euler. On notera aussi $\mathcal{A}(n)$ l'ensemble des tels k.

Le nombre $\varphi(n)$ correspond aussi au nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ (on dit que u est inversible s'il existe v tel que $uv \equiv 1[n]$). En effet, si $k \wedge n = 1$ par Bezout, on trouve u et v tels que $ku + nv = 1$, donc la classe de u est inverse de la classe de k modulo n. Réciproquement, s'il existe u tel que $ku \equiv 1[n]$ alors il existe v tel que $ku + nv = 1$, et donc $k \wedge n = 1$.

Pour calculer l'indicatrice d'Euler, on commence par montrer :

l'indicatrice d'Euler est une fonction multiplicative, c'est-à-dire que si $m \wedge n = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$.

Pour le montrer on considère la fonction :

$$\begin{aligned} \mathcal{A}(mn) &\to \mathcal{A}(m) \times \mathcal{A}(n) \\ x &\mapsto (x_1, x_2), \end{aligned}$$

où x_1 est le reste de la division euclidienne de x par m et x_2 de x par n.

Cette application est bien définie, car comme $x \wedge m = 1$, alors $x_1 \wedge m = 1$ et par définition, $x_1 < m$. De même, $x_2 \wedge n = 1$ et $x_2 < n$.

Elle est injective : en effet si x et x' ont même image (x_1, x_2), alors $x - x'$ est divisible par m et par n, donc par mn (car $m \wedge n = 1$). Donc $x = x'$ (car $|x - x'| < mn$).

Enfin, elle est surjective, en effet, si $(x_1, x_2) \in \mathcal{A}(m) \times \mathcal{A}(n)$, on applique Bezout pour obtenir $um + vn = 1$ et on a alors que $X = umx_1 + vnx_2$ vérifie

$$X \equiv x_1[m], \quad X \equiv x_2[n].$$

Enfin x, le reste de la division de X par mn appartient bien à $\mathcal{A}(mn)$ et a pour image (x_1, x_2).

Comme l'application considérée est une bijection, on a bien montré, par identification des cardinaux des ensembles, que $\varphi(mn) = \varphi(m)\varphi(n)$.

Pour calculer $\varphi(n)$ il suffit maintenant de calculer $\varphi(p^\alpha)$, pour p premier. Mais il est clair que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, les seuls nombres non premiers avec p^α étant les nombres divisibles par p.

En résumé, si

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

alors

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

On montre ensuite le *théorème d'Euler* : si $a \wedge n = 1$, alors

$$a^{\varphi(n)} \equiv 1[n].$$

On considère ici l'application de $\mathcal{A}(n)$ dans lui-même qui à x associe le reste de la division de ax par n. Comme a et x sont premiers avec n, ax aussi, et l'application est bien définie. Cette application est injective car si x et x' ont même image, alors n divise $a(x - x')$ et donc n divise $x - x'$ par Gauss et enfin $x = x'$. C'est donc aussi une bijection.

Notons maintenant les x_i les éléments de $\mathcal{A}_n$, on a

$$\prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} ax_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i[n].$$

On peut maintenant simplifier par le gros produit pour obtenir $a^{\varphi(n)} \equiv 1[n]$.

Exercice 1 Déterminer le nombre des dizaines de milliers de $A = 5^{5^{5^{5^5}}}$.

<u>*Solution de l'exercice 1*</u> On va déterminer le reste de la division euclidienne de A par $10000 = 2^5 \times 5^5$. On commence par diviser par 2^5. Comme $\varphi(2^5) = 16$, il suffit de déterminer le reste de la division euclidienne de $5^{5^{5^5}}$ par 16 et enfin, comme $\varphi(16) = 8$, il faut déterminer le reste de 5^{5^5} par 8. Et enfin 5^5 par 4 soit 1.

Donc on remonte $5^{5^5} \equiv 5[8]$, $5^{5^{5^5}} \equiv 5^5 \equiv 13[16]$. Et enfin, $A \equiv 5^{13} \equiv 5^5[2^5]$.

Ouf, il vient que l'on n'est pas obligé de refaire tout le travail pour 5^5, on a immédiatement $A \equiv 5^5 = 3125[10000]$. Ainsi, le chiffre de dizaines de milliers de A est 0.

Revenons à notre couple (a, n) avec $a \wedge n = 1$. Une question pertinente maintenant est de savoir pour quels entiers $k \in \mathbb{N}$ on a $a^k \wedge 1[n]$. La solution utilise la notion d'ordre de a.

L'**ordre de** a **modulo** n est le plus petit entier k_0 tel que $a^{k_0} \wedge 1[n]$. L'ensemble des entiers k tels que $a^k \wedge 1[n]$ est exactement l'ensemble des multiples de k_0. Enfin, il vient du théorème d'Euler que $k_0 \mid \varphi(n)$.

En effet, si k vérifie $a^k \wedge 1[n]$, on effectue la division euclidienne de k par k_0 : $k = lk_0 + r$ et on trouve que

$$a^k \equiv a^{lk_0+r} \equiv a^r \equiv 1[n].$$

Ainsi, par minimalité de k_0 on doit avoir $r = 0$.

Exercice 2 Existe-t-il des entiers $n \geqslant 1$ tels que 9 divise $7^n + n^3$?

<u>*Solution de l'exercice 2*</u> La réponse est non, voyons pourquoi. Soit n comme demandé. On a que n^3 est congru à 0, 1 ou -1 modulo 9 (c'est toujours vrai). Mais ici, n^3 ne peut pas être divisible par 9, donc on obtient que $n^6 \equiv 1[9]$. En particulier, $7^{2n} \equiv 1[n]$. Donc $2n$ est un multiple de l'ordre de 7 modulo 9. Cet ordre étant 3, n est un multiple de 3. C'est problématique vu que n^3 n'est pas divisible par 9.

- En vrac -

Exercice 3 Déterminer tous les couples d'entiers a, b tels que $a^b = b^a$.

<u>*Solution de l'exercice 3*</u> On commence, comme d'habitude, par introduire $d = a \wedge b$ et écrire $a = da'$ et $b = db'$ où $a' \wedge b' = 1$.

On constate d'abord que $a = b$ est toujours solution.

On cherche les autres solutions. Sans perte de généralité (quitte à inverser les rôles de a et b), on va supposer que $a < b$. Ainsi, l'équation se réécrit

$$d^{b-a} a'^b = b'^a.$$

On voit tout de suite que $a' = 1$ car $a' \mid b'^a$ alors que $a' \wedge b'^a = 1$. Et donc $d = a$ et $b' \geqslant 2$:

$$d^{d(b'-1)} = b'^d.$$

On prend les racines d-ièmes :

$$d^{b'-1} = b',$$

et on a encore quelques cas à traiter. Si $d = 1$, alors $b' = 1$ ce qui n'est pas possible, on a exclu ce cas.

Si $d = 2$, on voit que pour $b' = 2$ on a une solution qui correspond à $a = 2, b = 4$. Ensuite, on montre (par récurrence ou par une étude de fonction) que pour $b' > 2$, alors $2^{b'-1} > b'$.

Enfin, si $d \geqslant 3$, la situation est encore plus dramatique et on montre que

$$d^{b'-1} \geqslant 3^{b'-1} > b'.$$

Ainsi, les seules solutions sont les couples (a, a), $(2, 4)$ et $(4, 2)$.

Exercice 4 Trouver tous les entiers a et b tels que $7^a - 3 \times 2^b = 1$.

<u>*Solution de l'exercice 4*</u> On voit que $a = 0$ ou $b = 0$ sont impossibles. On réécrit l'équation comme suit :

$$7^a - 1 = 6 \times \sum_{i=0}^{a-1} 7^i = 6 \times 2^{b-1}.$$

Si $a = 1$, alors $b = 1$ est l'unique solution. Si $a = 2$ alors $b = 4$ est l'unique solution.

Supposons maintenant que $a > 2$ ce qui implique que $b > 4$. Comme la somme de gauche est paire, mais constituée d'éléments impairs, il doit y avoir un nombre pair de termes, a est donc pair. On regroupe termes pairs et impairs pour obtenir

$$(7+1) \sum_{i=0}^{a/2-1} 7^{2i} = 8 \times 2^{b-4}.$$

On simplifie, et on se rappelle que comme $b > 4$, la somme de gauche est paire mais encore constituée de termes impairs. Il y a donc un nombre pair de termes ($a/2$ est pair) et on peut recommencer la procédure :

$$(7^2+1) \sum_{i=0}^{a/4-1} 7^{4i} = 2^{b-4},$$

on aboutit à une contradiction car une puissance de 2 n'est pas divisible pas 50.

Les seules solutions sont donc $(1, 1)$ et $(2, 4)$.

Exercice 5 (OIM 99-4) Déterminer les couples d'entiers strictement positifs (n, p) tels que

- p est un nombre premier,
- $n \leqslant 2p$,
- $(p-1)^n + 1$ est divisible par n^{p-1}.

<u>*Solution de l'exercice 5*</u> On trouve d'abord des solutions évidentes : $(1, p)$ est toujours solution.

Si $p = 2$, et $n > 1$ alors seul $n = 2$ fonctionne et $(2, 2)$ est solution.

On suppose désormais que $p \geqslant 3$. Ainsi, n est nécessairement impair. Comme il est toujours plus simple de travailler avec des nombres premiers, soit q premier tel que $q \mid n$. Alors, les hypothèses impliquent $(p-1)^n \equiv -1[q]$, et plus généralement, $(p-1)^{an} \equiv (-1)^a[q]$. Fermat nous apprend aussi que $(p-1)^{b(q-1)} \equiv 1[q]$ car $p-1$ n'est pas divisible par q. On résume :

$$(p-1)^{an+b(q-1)} \equiv (-1)^a[q].$$

On se demande maintenant pour quelles valeurs de a et b on peut obtenir quelquechose d'intéressant, et on pense à Bezout. Mais il faut pour l'utiliser que $q - 1 \wedge n = 1$. Pour ce faire, on suppose que q est le plus petit diviseur premier de n (qui est impair) et on prend a et b donnés par Bezout, de sorte que $an + b(q-1) = 1$. On voit immédiatement que a doit être impair, et donc

$$p - 1 \equiv -1[q]$$

soit $q \mid p\,!$ Comme $n < 2p$ on a même que $n = p$, par minimalité de q.

On est prêt du but. En développant

$$(p-1)^p + 1 = \sum_{i=1}^{p} (-1)^{p-k} p^k \binom{p}{k} = p^2 + A,$$

on observe que A est divisible par p^3, donc $(p-1)^p + 1$ n'est pas divisible par p^3. Ainsi, on obtient que $p \leqslant 3$, soit $p = 3$ et $(3, 3)$ est bien une solution du problème, la dernière.

Exercice 6 (OIM 2002-4) Soit n un entier strictement plus grand que 1. On note $d_1, d_2, \cdots, d_k$ les diviseurs positifs de n avec

$$1 = d_1 < d_2 < \cdots < d_k = n.$$

On pose $D = d_1 d_2 + d_2 d_3 + \cdots + d_{k-1} d_k$.

Montrer que $D < n^2$.

Trouver les n tels que D est un diviseur de n^2.

<u>*Solution de l'exercice 6*</u> Il est clair que pour tout m, $d_{k-m} \leqslant n/(m+1)$. Ainsi, il vient que

$$\begin{aligned} D \leqslant n^2 \Big(\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{1}{(k-1) \times k}\Big) \\ = n^2 \Big(\frac{1}{1} - \frac{1}{\times 2} + \frac{1}{\times 2} - \frac{1}{\times 3} + \cdots + \frac{1}{k-1} - \frac{1}{k}\Big) \\ = n^2 \Big(1 - \frac{1}{k}\Big) < n^2. \end{aligned}$$

Pour la seconde partie de la question, on commence par remarquer que si n est premier, alors $D = d_1 d_2 = n \mid n^2$.

Si n est composé, soit $p = d_2$ les plus petit diviseur premier de n. Alors

$$n^2 > D > d_{k-1} d_k = n \times \frac{n}{p} = \frac{n^2}{p}.$$

Mais c'est alors impossible que $D \mid n^2$ car n^2/p est le plus grand diviseur strict de n^2.

Exercice 7 Soit A la somme des chiffres de 2012^{2012}. On pose B la somme des chiffres de A, et C la somme des chiffres de B. Déterminer C.

<u>*Solution de l'exercice 7*</u> On commence par majorer brutalement C. Comme $2012^{2012} \leqslant 10000^{2012}$, il possède moins de $4 \times 2012 + 1 < 10000$ chiffres, donc $A < 9 \times 10000 = 90000$. De même, $B < 9 \times 5 = 45$ et finalement $C \leqslant 13$.

Maintenant on regarde modulo 9 car on sait que l'opération de prendre la somme des chiffres laisse invariant cette congruence. Ainsi

$$2012^{2012} \equiv 5^{2012} \equiv 5^2 \equiv 7[9].$$

Ainsi, $C = 7$.

Exercice 8 (OIM 1990-4) Déterminer les entiers $n \in \mathbb{N}$ tels que $n^2 \mid 2^n+1$. <u>*Solution de l'exercice 8*</u>

Les solutions évidentes sont 1 et 3. Supposons dorénavant que $n > 1$. Au hasard, considérons p le plus petit entier qui divise n. Il est clair que n doit être impair, et donc que p aussi. L'hypothèse implique que $2^n \equiv -1[p]$ et donc que $2^{2n} \equiv 1[p]$. Ainsi, l'ordre de 2 modulo p divise $2n$. Mais il divise également $p-1$ (petit théorème de Fermat) et par définition de p, $p-1 \wedge n = 1$. Ainsi on obtient que cet ordre vaut 1 ou 2. Dans le premier cas, on trouve $2 \equiv 1[p]$ ce qui est impossible, la seconde possibilité, implique que $p = 3$. On écrit donc $n = 3^l \times k$ et on va déterminer les valeurs possibles de l. Pour cela, on factorise

$$2^{3^l k} + 1 = (2^{3^{l-1}k} + 1)(2^{2\times 3^{l-1}k} - 2^{3^{l-1}k} + 1).$$

On voit que cette formule (en particulier le terme de gauche) ce prête particulièrement bien à une récurrence. On évalue le terme de droite modulo 9. 2 est d'ordre 6 modulo 9 et ses premières puissances sont $2, 4, -1, -2, -4, 1$. En se rappelant que k est impair, on obtient immédiatement que

$$2^{2\times 3^{l-1}k} - 2^{3^{l-1}k} + 1 \equiv 3[9].$$

Enfin, $2^k + 1$ est aussi divisible par 3, mais pas par 9, du fait que k est pair, mais pas divisible par 3. En conclusion, la valuation de 3 dans $2^{3^l k} + 1$ est exactement $l + 1$. Mais par hypothèse, $3^{2l} \mid 2^n + 1$, ainsi, la seule possibilité est que $l = 1$.

Maintenant qu'on a réglé son compte à 3, on passe au diviseur premier suivant. On suppose $k \geqslant 2$, sinon on a la solutions $n = 3$. Soit encore p le plus petit diviseur de k. Ainsi, $p \geqslant 5$, et on recommence comme tout à l'heure. De $2^{6k} \equiv 1[p]$ on déduit que l'ordre de 2 modulo p divise $6l$ mais aussi $p-1$ et donc par définition de p, il doit diviser 6. Il vaut dont 1, 2, 3, ou 6. Et on a que 2, 4, 8 ou 64 est congru à 1 modulo p. De tous ces cas, comme p n'est ni 2 ni 3, la seule possibilité est $p = 7$. Mais 7 ne divise jamais $2^n + 1$, en effet les puissances successives de 2 modulo 7 sont $2, 4, 1$. Il n'y a donc pas d'autre solution.

Exercice 9 Soient $a > b$ deux entiers premiers entre eux. Montrer que pour tout m, n entiers,

$$(a^m - b^m) \wedge (a^n - b^n) = a^{m\wedge n} - b^{m\wedge n}.$$

<u>*Solution de l'exercice 9*</u> On pose $D = (a^m - b^m) \wedge (a^n - b^n)$ et $d = a \wedge b$. Posons $n = mq + r$ la division euclidienne de n par m. Essayons d'effectuer celle de $a^n - b^n$ par $a^m - b^m$:

$$a^n - b^n = a^{mq+r} - b^{mq+r} = a^r(a^{mq} - b^{mq}) + b^{mq}(a^r - b^r).$$

Or $a^{mq} - b^{mq} = (a^m - b^m)(a^{(q-1)m} + a^{(q-2)m}b^m + \cdots + a^m b^{(q-2)m} + b^{(q-1)m})$.

On n'a pas forcément la division euclidienne cherchée, mais on apprend tout de même que, comme $b^{mq} \wedge (a^m - b^m) = 1$ par le lemme de Gauss que $D \mid a^r - b^r$.

Ainsi, si $r_1, r_2, \ldots, d$ est la suite des restes dans l'algorithme d'Euclide, on obtient par récurrence immédiate que $D \mid a^d - b^d$.

Montrons maintenant que $a^d - b^d \mid D$ c'est-à-dire que c'est un diviseur commune à $a^m - b^m$ et $a^n - b^n$. Soit l tel que $n = ld$, alors on a vu comment $a^{ld} - b^{ld}$ est divisible par $a^d - b^d$. De même $a^m - b^m$ est divisible par $a^d - b^d$ donc $D = a^d - b^d$.

5 Test

- Énoncés -

Exercice 1 Soient a et b des entiers. Montrer que si 9 divise $a^2 + ab + b^2$, alors a et b sont multiples de 3.

Exercice 2 Montrer que $n!$ est divisible par 2^{n-1} si et seulement si n est une puissance de 2.

Exercice 3 Soit n un entier naturel. Montrer que si $2 + 2\sqrt{28n^2+1}$ est entier, alors c'est un carré.

Exercice 4

(i) Trouver tous les entiers $n \geqslant 1$ tels que n divise $2^n - 1$.

(ii) Trouver tous les entiers $n \geqslant 1$ impairs tels que n divise $3^n + 1$.

- Corrigé -

<u>*Solution de l'exercice 1*</u> On a $a^2 + ab + b^2 = (a-b)^2 + 3ab$. C'est un multiple de 9, donc de 3. On en déduit que 3 divise $(a-b)^2$, et donc 3 divise $a-b$. Du coup, 9 divise $(a-b)^2$, et donc 9 divise aussi $3ab$. Par conséquent, a ou b est multiple de 3. Or 3 divise $a-b$, d'où le résultat.

<u>*Solution de l'exercice 2*</u> Par la formule de Legendre, l'exposant de 2 dans la décomposition en facteurs premiers de $n!$ est égal à

$$S_n = \sum_{k \geqslant 1} \left[\frac{n}{2^k}\right].$$

Cette somme est strictement inférieure à n puisque $\sum_{k\geqslant 1} \frac{n}{2^k} = n$, et les $n/2^k$ ne sont pas tous entiers.

Soit $n = \sum_{i=1}^{r} 2^{\alpha_i}$ l'écriture en base 2 de n. On vérifie que :

$$\left[\frac{n}{2^k}\right] = \sum_{i;\ \alpha_i \geqslant k} 2^{\alpha_i - k}.$$

En réordonnant les termes de S_n, on obtient alors :

$$S_n = \sum_{i=1}^{r} \sum_{j=0}^{\alpha_i - 1} 2^j = \sum_{i=1}^{r} 2^{\alpha_i} - 1 = n - r.$$

Donc $S_n = n - 1$ si et seulement si n est une puissance de 2.

<u>*Solution de l'exercice 3*</u> Posons $2 + 2\sqrt{28n^2+1} = m$. Alors $m(m-4) = 4(28n^2+1) - 4 = 4 \times 28n^2 = 7(4n)^2$. Ainsi, parmi m et $m-4$, il y en a un qui est un carré et un autre qui est 7 fois un carré. Si m n'est pas un carré, alors c'est 7 fois un carré, et $m-4$ est un carré congru à 3 modulo 7, ce qui est impossible car 3 n'est pas un carré modulo 7.

<u>*Solution de l'exercice 4*</u>

(i) Soit $n > 1$ tel que n divise $2^n - 1$. Il est clair que n est impair. Soit p le plus petit facteur premier de n, qui est donc impair. Alors $2^n \equiv 1 \bmod p$. Soit ω l'ordre de 2 modulo p. Alors ω divise n. D'autre part, d'après le petit théorème de Fermat, $2^{p-1} \equiv 1 \bmod p$. Ainsi ω divise $p-1$. D'après la condition sur p, on a nécessairement $\omega = 1$. Alors $2 \equiv 1 \bmod p$, ce qui est absurde. On a donc forcément $n = 1$.

(ii) Soit $n > 1$ tel que n divise $3^n + 1$. Soit p le plus petit facteur premier de n, qui est donc impair, qui vérifie donc $p > 3$. Alors $3^{2n} \equiv 1 \bmod p$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1 \bmod p$. Ainsi ω divise $p-1$. On en déduit que ω divise $\operatorname{pgcd}(2n, p-1)$. D'après la condition sur p, on a nécessairement $\omega = 1$ ou 2. Dans le premier cas de figure, $3 \equiv 1 \bmod p$ et donc $p = 2$, ce qui est exclu. Dans le deuxième cas, $3^2 \equiv 1 \bmod p$ et donc p divise 8, ce qui est exclu également. On en déduit que $n = 1$.

3 Intermédiaires : algèbre

Nous renvoyons au cours de polynômes disponible sur le site d'Animath pour des détails et compléments (voir les liens en haut de la page 14).

1 Premier TD sur les polynômes

- Énoncés -

Exercice 1 Trouver tous les couples (n, r), n entier > 0, r réel, tels que $(x+1)^n - r$ soit divisible par $2x^2 + 2x + 1$.

Exercice 2

Pour quelles valeurs de $m \in \mathbb{R}$ l'équation :

$$\left(x^2 - 2mx - 4(m^2+1)\right)\left(x^2 - 4x - 2m(m^2+1)\right) = 0$$

admet-elle exactement trois racines distinctes ?

Exercice 3

Soit a un réel et $P(x) = x^2 - 2ax - a^2 - \frac{3}{4}$. Trouver toutes les valeurs de a telles que $|P(x)| \leqslant 1$ pour tout $x \in [0, 1]$.

Exercice 4

a) Déterminer le polynôme Q tel que pour tout réel α, $Q(\cos\alpha) = \cos 3\alpha$.

b) Soient a, b, c trois réels quelconques, $P(x) = 4x^3 + ax^2 + bx + c$ et M la valeur maximale de $|P(x)|$ sur $[-1, 1]$. Montrer que $M \geqslant 1$. Dans quel cas a-t-on l'égalité ?

Exercice 5

α, β, γ étant les trois racines de $x^3 - x - 1$, calculer : $\frac{1-\alpha}{1+\alpha} + \frac{1-\beta}{1+\beta} + \frac{1-\gamma}{1+\gamma}$

Exercice 6

Trouver (a, b, c) réels vérifiant :

$a + b + c = 3$, $a^2 + b^2 + c^2 = 35$, $a^3 + b^3 + c^3 = 99$.

- Corrigé -

Solution de l'exercice 1

$2x^2+2x+1$ admettant deux racines distinctes, en l'occurrence deux racines complexes $\frac{-1+i}{2}$ et $\frac{-1-i}{2}$, il faut et il suffit que chacune d'elles soit racine de $(x+1)^n - r$, donc que $\left(\frac{1+i}{2}\right)^n = r = \left(\frac{1-i}{2}\right)^n$. Or $\left(\frac{1+i}{2}\right)^n$ est réel si et seulement si n est multiple de 4, auquel cas, si $n = 4k$, $\left(\frac{1+i}{2}\right)^{4k} = \left(\frac{1-i}{2}\right)^{4k} = \left(\frac{-1}{4}\right)^k$. Les solutions cherchées sont donc tous les couples : $(4k, \left(\frac{-1}{4}\right)^k)$

Solution de l'exercice 2

Le premier trinôme $x^2 - 2mx - 4(m^2+1)$ admet toujours deux racines réelles distinctes. Il faut donc soit que le second trinôme admette une racine double, soit qu'il admette une racine en commun avec le premier.

Il admet une racine double lorsque $-2m(m^2+1) = 4$, soit $m^3 + m + 2 = 0$. Ce polynôme admet pour racine évidente $m = -1$, il se factorise donc en : $(m+1)(m^2-m+2)$ et m^2-m+2 n'admet pas de racine réelle. Or pour $m = -1$, la racine double 2 de $x^2 - 4x - 2m(m^2+1$ est aussi racine de $x^2 - 2mx - 4(m^2+1)$, de sorte que l'équation de l'énoncé n'admet que deux racines distinctes (dont une racine triple).

Si $x^2-2mx-4(m^2+1)$ et $x^2-4x-2m(m^2+1)$ admettent une racine commune, celle-ci est racine de la différence : $(4-2m)(x-(m^2+1))$. Soit $m = 2$ auquel cas les deux trinômes sont identiques, égaux à $x^2 - 4x - 20$, et l'équation admet seulement deux racines distinctes (deux racines doubles), soit $x = m^2 + 1$, auquel cas chacun des trinômes est égal à $(m^2+1)(m^2 - 2m - 3)$ et s'annule à condition que $m = -1$ ou $m = 3$. $m = -1$ est exclu (c'est la racine triple déjà vue), reste $m = 3$ pour lequel l'équation $(x^2 - 6x - 40)(x^2 - 4x - 60)$ a bien trois racines : $-4, -6$ et 10 (racine double). C'est donc l'unique solution de l'exercice.

Solution de l'exercice 3

Le trinôme atteint son minimum en $x = a$, donc sur l'intervalle qui nous intéresse lorsque $a \in [0,1]$. Hormis ce point, il ne peut être maximum ou minimum qu'aux bornes de l'intervalle, donc en -1 ou 1. Il suffit donc de voir quand chacune des trois valeurs $P(0), P(1)$ et $P(a)$ si $0 \leqslant a \leqslant 1$ est comprise entre -1 et 1. Pour $P(0) = -a^2 - \frac{3}{4}$, c'est lorsque $-\frac{1}{2} \leqslant a \leqslant \frac{1}{2}$. $P(1) = \frac{1}{4} - 2a - a^2$ est inférieur ou égal à 1 lorsque $a \leqslant -\frac{3}{2}$ ou $a \geqslant -\frac{1}{2}$, et supérieur ou égal à -1 lorsque $-\frac{5}{2} \leqslant a \leqslant \frac{1}{2}$. Enfin, pour $0 \leqslant a \leqslant 1$, $P(a) = -2a^2 - \frac{3}{4}$ est toujours < 1 et est $\geqslant -1$ lorsque $|a| \leqslant \frac{\sqrt{2}}{4}$. A l'intersection de tous ces intervalles se trouve l'intervalle solution : $a \in \left[\frac{-1}{2}, \frac{\sqrt{2}}{4}\right]$.

Solution de l'exercice 4

$\cos 2\alpha = \cos(\alpha+\alpha) = \cos^2\alpha - \sin^2\alpha = 2\cos^2\alpha - 1$, et $\cos 3\alpha = \cos(2\alpha+\alpha) = (2\cos^2\alpha - 1)\cos\alpha - (2\sin\alpha\cos\alpha)\sin\alpha = 4\cos^3\alpha - 3\cos\alpha$, donc $Q(x) = 4x^3 - 3x$.

Ce polynôme nous est utile pour la question b). En effet, il vaut 1 lorsque 3α est multiple de 2π, donc lorsque $x = \cos\alpha = 1$ ou $\frac{-1}{2}$, et vaut -1 lorsque 3α est multiple impair de π, donc lorsque $x = \cos\alpha = \frac{1}{2}$ ou -1. Pour toute autre valeur de $x = \cos\alpha \in [-1,1]$, $Q(x)$ est compris entre -1 et 1. Donc pour $a = 0, b = -3, c = 0, M = 1$.

Si un polynôme $P(x)$ vérifiait pour tout $x \in [-1,1]$ $|P(x)| < 1$, il vérifierait cette relation en particulier en $-1, \frac{-1}{2}, \frac{1}{2}, 1$, d'où $(P-Q)(-1) > 0$, $(P-Q)(\frac{-1}{2} < 0$, $(P-Q)(\frac{1}{2} > 0$ et $(P-Q)(1) < 0$. Il en résulterait que le polynôme $P - Q$ s'annulerait trois fois dans l'intervalle $[-1,1]$, ce qui est impossible vu que $P - Q$ est un polynôme du second degré. Donc on ne peut pas avoir $|P(x)| < 1$ pour tout $x \in [-1,1]$.

Pour le cas d'égalité : si $M = 1$, $(P-Q)(-1) \geqslant 0$, $(P-Q)(\frac{-1}{2} \leqslant 0$, $(P-Q)(\frac{1}{2} \geqslant 0$ et $(P-Q)(1) \leqslant 0$. Soit le trinôme est identiquement nul, $P = Q$ est effectivement solution, soit il s'annule sur $\left[\frac{-1}{2}, \frac{1}{2}\right]$ et sa deuxième racine est soit $> \frac{1}{2}$ auquel cas $P(-1) < 0$, soit $< \frac{-1}{2}$ auquel cas $P(1) > 0$: contradiction dans les deux cas. Le polynôme Q est donc l'unique cas d'égalité.

Solution de l'exercice 5

Une méthode sûre même si, en l'occurrence, on peut trouver plus rapide, est de chercher l'équation ayant pour racines $\frac{1-\alpha}{1+\alpha}, \frac{1-\beta}{1+\beta}, \frac{1-\gamma}{1+\gamma}$ et de calculer la somme des racines de cette dernière équation à partir de ses coefficients. Si x est racine de $x^3 - x - 1$, de quelle équation est racine $y = \frac{1-x}{1+x}$? On remarque que $x = \frac{1-y}{1+y}$ (la fonction est involutive), donc $\left(\frac{1-y}{1+y}\right)^3 - \left(\frac{1-y}{1+y}\right) - 1 = 0$, soit : $(1-y)^3 - (1-y)(1+y)^2 - (1+y)^3 = 0$. L'équation en y s'écrit donc : $-y^3 + y^2 - 7y - 1$, la somme de ses racines vaut 1.

Solution de l'exercice 6

Il faut se ramener à une équation du troisième degré en utilisant le fait que toute expression symétrique des racines d'une équation peut s'exprimer rationnellement en fonction des polynômes symétriques élémentaires (coefficients de ladite équation du troisième degré). En l'occurrence, $a^2 + b^2 + c^2 = (a+b+c)^2 - 2(ab+bc+ca)$, donc $ab + bc + ca = -13$. Et $a^3 + b^3 + c^3 = (a+b+c)(a^2+b^2+c^2) - (a^2b + b^2a + a^2c + c^2a + b^2c + c^2b)$ et $(a^2b + b^2a + a^2c + c^2a + b^2c + c^2b) = (a+b+c)(ab+ac+bc) - 3abc$. D'où : $99 - 3 \times 35 = -((3 \times -13) - 3abc$, d'où : $abc = -15$. a, b et c sont donc les racines de : $x^3 - 3x^2 - 13x + 15$. Cette équation admet 1 pour racine évidente, elle se factorise en : $(x-1)(x^2 - 2x - 15)$ et admet donc pour autres racines : -3 et 5. Donc (a, b, c) vaut à permutation près : $(1, -3, 5)$.

2 Deuxième TD sur les polynômes

- Énoncés -

Exercice 1 Soit $x \in \mathbb{R}$ tel que $x^2 - x \in \mathbb{Z}$ et il existe un entier positif $n \geqslant 3$ tel que $x^n - x \in \mathbb{Z}$. Montrer que x est entier.

Exercice 2 Trouver x tel que $x = (1 - \frac{1}{x})^{\frac{1}{2}} + (1 - \frac{1}{x})^{\frac{1}{2}}$.

Exercice 3 Soit n un entier, $n > 1$. On note $d_1, \ldots, d_k$ les diviseurs positifs de n avec $1 = d_1 < d_2 < \ldots < d_k = n$. On pose $D = d_1 d_2 + \ldots + d_{k-1} d_k$. Montrer que $D < n^2$. Trouver tous les entiers n pour lequels D est un diviseur de n^2.

Exercice 4 Montrer que les seules polynômes $P \in \mathbb{Z}[X]$ bornés sont ceux de degré 0.

Proposition 49. Soit $\alpha \in \mathbb{C}$. On suppose qu'il existe $P \in \mathbb{Q}[X]$ tel que $P(\alpha) = 0$. Alors il existe un polynôme μ_α unitaire (c-à-d de coefficient dominant 1) qui divise tout autre polynôme annulé par α. De plus, μ_α est irréductible et il est unique avec sa propriété.

Démonstration. Soit μ un polynôme annulé par α, unitaire et de degré minimal. Supposons par l'absurde qu'il existe $Q \in \mathbb{Q}[X]$ un polynôme annulé par α, non divisible par μ. On divise avec retenu Q par μ : $Q(X) = q(X)\mu + r(X)$, avec $\deg(r) < \deg(\mu)$. Comme Q et μ sont annulés par α, r l'est également. Or, $\deg(r) < \deg(\mu)$ et μ a été choisi de degré minimal. Donc $r = 0$, ce qui est absurde.

Si μ_α était réductible, disons $\mu_{alpha} = P_1P_2$ alors μ ne serait pas de degré minimal. Si on a deux valeurs μ et ν qui divise tous les autre polynômes annulateurs, alors $\mu \mid \nu$ et $\nu \mid \mu$, donc $\mu = k\nu$ pour une constante k. Comme μ_{alpha} est unitaire, il est unique. $\square$

Exercice 5 Montrer que pour tout $n > 1$ naturel le polynôme $P_n = x^{4n+3} + x^{4n+1} + x^{4n-2} + x^8$ est divisible par $x^2 + 1$.

Exercice 6 On se donne $2n$ réels distincts $a_1, a_2, \ldots, a_n, b_1, \ldots, b_n$. On ramplit une table $n \times n$ en mettant $a_i + b_j$ dans la case (i, j). On suppose qu'il existe une constante c telle que le produit de chaque ligne est c. Montrer qu'il existe une constante d telle que le produit de chaque colonne soit d.

Exercice 7 Soit p un nombre premier et $k \leqslant n$ deux nombre naturels. On considère les décompositions de n et k en base p :

$$n = n_d p^d + \cdots + n_1 p + n_0$$
$$k - k_d p^d + \cdots + k_1 + k_0.$$

k_d peut être 0. Montrer que $\binom{n}{k} \equiv \binom{n_d}{k_d} \cdots \binom{n_0}{k_0} \mod p$.

Exercice 8 Trouver tous les polynômes autre que les polynômes constants, à coefficients dans $\mathbb{R}$ et tels que, pour tout $z \in \mathbb{C}$,

$$P(z^2) = P(z)P(z-1).$$

Exercice 9 Factoriser de tête 8051.

- Corrigé -

<u>*Solution de l'exercice 1*</u> On note $a = x^2 - x$. Si $a = 0$, $x = 0$ ou $x = 1$. Si, $a \leqslant -1$, l'équation $x^2 - x$ n'a pas de racines réelles, donc $a \geqslant 1$.

Montrons par récurrence que, pour tout $\ell \in \mathbb{N}$, $\ell \geqslant 3$, in existe deux entiers positifs A_ℓ et B_ℓ tels $A_\ell \geqslant 2$ et

$$x^\ell = A_\ell x + B_\ell.$$

Pour $\ell = 3$ on a $x^3 = (a+1)x + a$. Supposons le résultat vrai pour ℓ. Ainsi $x^\ell = A_\ell x + B_\ell$. D'où $x^{\ell+1} = (A_\ell + B_\ell)x + aA_\ell$. $A_{\ell+1} := A_\ell + B_\ell$ et $B_{\ell+1} = aA_\ell$ conviennent. Cela finit la récurrence.

Ainsi, pour $\ell = n$, on a $x^n = A_n x + B_n$. D'autre par, d'après l'énoncé, $x^n = x + b$ pour un b entier. Donc $x = \frac{b - B_n}{A_n - 1}$. On peut diviser car $A_n \geqslant 2$. Ainsi $x \in \mathbb{Q}$.

Comme x vérifie $x^2 - x - a$ qui est à coefficients entiers, le dénominateur de x divise le coefficient de tête. Ainsi x est entier.

<u>*Solution de l'exercice 2*</u> On préfère toujours avoir une équation du type $P(x) = 0$ avec P polynôme. Pour se ramener à une telle forme, on a des calculs plus simples en posant $a = 1 - \frac{1}{x}$. On a $x = (a - 1 + a)^{\frac{1}{2}} + a^{\frac{1}{2}}$. Tout calcul fait, on a $x^2 - 2x\frac{2}{x} + \frac{1}{x^2} - 1 = 0$. Un polynôme de ce type "demande" toujours l'astuce $y = x - \frac{1}{x}$. On trouve $y^2 + 1 - 2y = 0$. La seule solution est $y = 1$. Ainsi $x^2 - 2xy + 1 = 0$ donne $x^2 - x - 1 = 0$, avec racines $\frac{1 \pm \sqrt{5}}{2}$.

<u>*Solution de l'exercice 3*</u> On a $d_i d_{i+1} = \frac{n^2}{d_{n-i}d_{n-i-1}}$ pour tout $i \in [1, n-1]$. Donc

$$\begin{aligned} D &= n^2\left(\frac{1}{d_1 d_2} + \ldots + \frac{1}{d_k d_{k-1}}\right) \\ &\leqslant n^2\left(\frac{1}{1 \cdot 2} + \ldots + \frac{k}{k-1}\right) \\ &= n^2\left((1-\frac{1}{2}) + (\frac{1}{2} - \frac{1}{3}) + \ldots + (\frac{1}{k-1} - \frac{1}{k})\right) \\ &< n^2. \end{aligned}$$

Les nombres $n = p$ avec p premier conviennent car $D = p \mid p^2$. Si n n'est pas premier, $k \geqslant 3$. On note p le plus petit facteur premier de n. Ainsi $D \geqslant n^2(\frac{1}{d_1 d_2} + \frac{1}{d_2 d_3}) > n^2(\frac{1}{d_1 d_2} = \frac{1}{p})$. Comme $D \mid nr$, $\frac{n^2}{D}$ divise n^2. Or $\frac{n^2}{D} < p$. Ainsi, $D = n^2$, impossible. Donc $D \mid n^2$ si et seulement si n est premier.

<u>*Solution de l'exercice 4*</u> Soit n le degré de P. On note B un nombre naturel tel que $|P(x)| \leqslant B$. Alors, $P(1), P(2), \ldots, P(n \cdot (2B+1))$ sont tous dans l'ensemble {-B,...,B-1,B} qui a $2B+1$ éléments. Par le principe du tiroir on a $n+1$ valeurs égales, disons à c. Alors $P(X) - c$ a $n+1$ racines, donc il est nul.

<u>*Solution de l'exercice 5*</u> On applique la proposition précédente au nombre i. Le polynôme x^2+1 est annulé par i. x^2+1 n'a pas de racine réelles, donc il n'a pas de racines rationnelles non plus. Ainsi x^2+1 est irréductible. Comme $\mu_i \mid x^2+1$, $\mu_i = x^2+1$. Comme $i^4 =$ on a $P_n(i) = i^3+i^1+i^2+i^4 = -i+i-1+1 = 0$. Comme P_n est annulé par i, il est divisible par Ö$mu_i = x^2+1$.

<u>*Solution de l'exercice 6*</u> On pose $P(x) - \Pi_{j=1}^{n}(x+b_j) - c$. D'après l'hypothèse $a_1, \ldots, a_n$ sont racines de P. Comme P est unitaire, $P = \Pi_{i=1}^{n}(x - a_i)$. Soit j un indice de colonne. Le produit de $\Pi_{i=1}^{n}(b_j + a_i)$ vaut $(-1)^n P(-b_j) = -c$. Comme c ne dépend pas de j, les produits des colonnes sont tous égaux.

<u>*Solution de l'exercice 7*</u> On calcule de deux facons différentes le coefficient de x^k dans $(1+x)^n$. D'une part il est trivialement $\binom{n}{k}$. Or, on a $(1+x)^n = (1+x)^{p^d n_d} \cdots (1+x)^{p n_1}(1+x)^{n}_{0}$. Comme , $\binom{p^r}{k} \equiv 0 \mod p$ pour tout $r \geqslant 1$ et tout $k \in \{2, p^r - 1\}$, $(1+x)^{p^r n_r} - (1+x^p)^{n_r} \in p\mathbb{Z}[x]$. Le coefficient de x^k dans ce dernier polynôme est $\binom{n_d}{k_d} \cdots \binom{n_0}{k_0}$.

<u>*Solution de l'exercice 8*</u> Supposons par l'absurde que P n'est pas constant. Si z_0 est une racine, alors $z_0^2, z_0^4, \ldots$ sont aussi des racines. Si on a des racines $|z_0| < 1$ ou $|z_0| > 1$ alors P aurait une infinité de racines. Donc toute les racines sont de module 1.

L'équation s'écrit également $P((x+1)^2) = P(x+1)P(x)$. Donc si z_0 est une racine , alors $(z+1)^2$ est une racine aussi. Comme toute racine est de module 1, on a $|z_O + 1| = 1$. Pour chercher les nombres complexes qui vérifient $|z| = |z+1| = 1$ on pose $z = a + ib$. On trouve $a^2 + b^2 = 1 = a^2 + b^2 + 2a + 1$. Alors $a = \frac{-1}{2}$ et $b = \pm\frac{\sqrt{3}}{2}$. Donc $P(x) = (x-\epsilon)^a(x - \frac{1}{\epsilon})^b$ pour $\epsilon = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$. Comme $P \in \mathbb{R}[x]$, $a = b$, donc $P = (x^2+x+1)^a$. Réciproquement tout polynôme de ce type convient.

<u>*Solution de l'exercice 9*</u> Si on trouve $P \in \mathbb{Z}[x]$ tel que $8051 = P(a) - P(b)$ on aurait le facteur $a - b$. Pour $P = x^2$ on a $8051 = 90^2 - 7^2$. Donc $8051 = 97 \cdot 83$, tous les deux premiers.

3 Suites

Une *suite* d'éléments d'un ensemble E est une application $u : \mathbb{N} \to E$. On écrit en général u_n à la place de $u(n)$. La suite est notée $(u_n)_{n\in\mathbb{N}}$ ou simplement (u_n). Dans la suite, sauf mention contraire, on prendra $E = \mathbb{C}$.

- 1. Suites classiques. -

Une *suite arithmétique* est une suite vérifiant une relation de récurrence de la forme $u_{n+1} = u_n + r$. Le nombre r est appelé la raison de la suite. On a $u_n = u_0 + nr$, et

$$\sum_{k=0}^{n} u_k = \frac{(u_0 + u_n)(n+1)}{2}.$$

Une *suite géométrique* est une suite vérifiant une relation de récurrence de la forme $u_{n+1} = q \cdot u_n$. Le nombre q est appelé la raison de la suite. On a $u_n = q^n \cdot u_0$, et si $q \neq 1$, $\sum_{k=0}^{n} u_k = u_0 \cdot \frac{q^{n+1} - 1}{q - 1}$.

Connaissant une suite (u_n) définie par une relation de récurrence, on peut parfois en trouver une expression explicite (c'est-à-dire une expression de u_n en fonction de n) en se ramenant à une suite de la forme $v_n = f(u_n)$ (où f est une bijection de l'ensemble E, par exemple une transformation affine) pour laquelle on connaît une formule explicite.

Exercice 1

Considérons une suite arithmético-géométrique, c'est-à-dire définie par une relation de récurrence de la forme $u_{n+1} = au_n + b$. Exprimer u_n en fonction de n.

Solution de l'exercice 1

Première méthode. Tentons de nous ramener à une relation de récurrence plus simple en posant $v_n = u_n + c$, où c est un complexe que l'on déterminera plus tard. La suite v_n vérifie la relation de récurrence $v_{n+1} - c = a(v_n - c) + b$, c'est-à-dire $v_{n+1} = av_n + (1-a)c + b$. En prenant $c = \frac{b}{a-1}$, (v_n) est une suite géométrique de raison a. Donc $v_n = a^n v_0$, et $u_n = a^n u_0 + \frac{a^n - 1}{a-1} \cdot b$.

Seconde méthode. En calculant formellement les premiers termes de la suite, on peut conjecturer que $u_n = a^n u_0 + a^{n-1} b + \ldots + ab + b = a^n u_0 + \frac{a^n - 1}{a-1} \cdot b$. Il ne reste plus qu'à montrer par récurrence que cette formule est vraie pour tout n.

- 2. Récurrences linéaires d'ordre 2 -

Une relation de *récurrence linéaire d'ordre* 2 est relation de récurrence de la forme $u_{n+2} = au_{n+1} + bu_n$. Son *polynôme caractéristique* est le polynôme $\chi(x) = x^2 - ax - b$.

Théorème 50. – Si le polynôme $\chi(x)$ à deux racines complexes distinctes r_1 et r_2, alors il existe $(\lambda, \mu) \in \mathbb{C}^2$ tels que pour tout $n \in \mathbb{N}$, on ait $u_n = \lambda r_1^n + \mu r_2^n$.
– Si le polynôme $\chi(x)$ à une racine double r, alors il existe $(\lambda, \mu) \in \mathbb{C}^2$ tels que pour tout $n \in \mathbb{N}$, on ait $u_n = (\lambda + \mu n) r^n$.

On calcule λ et μ à partir des deux premiers termes u_0 et u_1.

Exercice 2

Déterminer toutes les fonctions $f : \mathbb{R}_+ \to \mathbb{R}_+$ telles que pour tout $x \geqslant 0$, on ait $f(f(x)) + f(x) = 6x$.

Solution de l'exercice 2

Soit $x \geqslant 0$. On définit la suite (x_n) par $x_0 = x$ et $x_{n+1} = f(x_n)$. D'après l'équation fonctionnelle, cette suite vérifie la relation de récurrence $x_{n+2} = -x_{n+1} + 6x_n$. Le polynôme caractéristique, $t^2 + t - 6$, admet deux racines distinctes -3 et 2, donc il existe des réels λ et μ tels que pour tout n, $x_n = \lambda \cdot (-3)^n + \mu \cdot 2^n$. Supposons λ non-nul ; alors pour n assez grand, x_n est du signe de $\lambda \cdot (-3)^n$. Si $\lambda > 0$, alors x_n est négatif pour n impair, et si $\lambda < 0$, alors x_n est négatif pour n pair. Dans les deux cas, on aboutit à une contradiction, donc $\lambda = 0$. En utilisant le fait que $x_0 = x$, on trouve que $\mu = x$. Donc $f(x) = x_1 = 2x$.

Réciproquement, $f(x) = 2x$ est bien solution de l'équation fonctionnelle.

Exercice 3

Montrer que les cent premiers chiffres après la virgule dans l'écriture décimale de $(5 + 3\sqrt{3})^{200}$ sont des 9.

Solution de l'exercice 3

L'idée est de montrer que $(5 + 3\sqrt{3})^{200} + (5 - 3\sqrt{3})^{200}$ est entier, et que le second terme de la somme est très petit. Pour cela, posons $u_n = (5 + 3\sqrt{3})^{200} + (5 - 3\sqrt{3})^{200}$. On reconnaît une suite vérifiant une relation de récurrence linéaire d'ordre 2, de polynôme caractéristique $(x - 5 - 3\sqrt{3})(x - 5 + 3\sqrt{3}) = x^2 - 10x - 2$. On a donc, pour tout n, $u_{n+2} = 10u_{n+1} + 2u_n$. De plus, $u_0 = 2$ et $u_1 = 10$ sont entiers, donc il est clair par une récurrence immédiate que u_n est entier pour tout n, donc en particulier u_{200} l'est. On n'a donc plus qu'à vérifier que $(5 - 3\sqrt{3})^{200} \geqslant 10^{-100}$; mais à partir de l'inégalité $\sqrt{3} \leqslant \frac{7}{4}$, on obtient $3\sqrt{3} - 5 \leqslant \frac{1}{4}$, donc $(3\sqrt{3} - 5)^2 \leqslant \frac{1}{10}$, d'où le résultat voulu.

On remarquera que la méthode de résolution de cet exercice permet aussi de montrer le résultat connu suivant : si x est un complexe tel que $x + \frac{1}{x}$ est entier, alors $x^n + \frac{1}{x^n}$ est entier pour tout n.

Autre remarque : si on se retrouve avec une formule du type $u_n = \lfloor (5 + 3\sqrt{3})^n \rfloor$, il faut toujours penser à ajouter un terme en puissance de la quantité conjuguée (du type $(5+3\sqrt{3})^n$), ce qui permet, si celui-ci est assez petit à partir d'un certain rang, d'obtenir une expression de u_n sans partie entière, et éventuellement ensuite une relation de récurrence.

- 3. Autres récurrences -

Exercice 4

Déterminer des formules explicites pour les suites définies par récurrence suivantes :

(1) $u_0 = 2$ et $u_{n+1} = 3u_n^2 - 4u_n + 2$;

(2) $u_0 = \dfrac{5}{2}$ et $u_{n+1} = u_n^2 - 2$.

Solution de l'exercice 4

(1) On essaye de se ramener, via une transformation affine, à une relation de récurrence du type $x_{n+1} = x_n^2$, la plus simple a priori parmi les récurrences de degré 2. Si on pose $x_n = ay_n + b$ et qu'on suppose que (x_n) vérifie la relation de récurrence $x_{n+1} = x_n^2$, on trouve que $y_{n+1} = ay_n^2 + 2by_n + \dfrac{b^2 - b}{a}$; on voit que pour $a = 3$ et $b = -2$, il s'agit de la relation de récurrence vérifiée par (u_n). Avec $x_n = 3u_n - 2$, on trouve donc que $x_0 = 4$ et $x_{n+1} = x_n^2$, donc par une récurrence immédiate, $x_n = 4^{2^n}$ et $u_n = \dfrac{4^{2^n} + 2}{3}$ pour tout n.

(2) La formule trouvée à la question précédente montre qu'on ne peut pas se ramener à une récurrence du type $x_{n+1} = x_n^2$ via une transformation affine ; il faut donc trouver autre chose. La solution est dans l'identité $\left(x + \dfrac{1}{x}\right)^2 = x^2 + \dfrac{1}{x^2} + 2$: si on pose $x_n = x^{2^n} + \dfrac{1}{x^{2^n}}$ pour un certain complexe x, alors il est immédiat que $x_{n+1} = x_n^2 - 2$. Il suffit donc de trouver x tel que $x + \dfrac{1}{x} = \dfrac{5}{2}$; $x = 2$ convient. On a donc, pour tout n, $u_n = 2^{2^n} + \dfrac{1}{2^{2^n}}$.

On peut ainsi trouver des formules explicites pour toutes les suites dont la relation de récurrence se ramène, via une transformation affine, à une récurrence de ce type. À ma connaissance, à transformation affine près, il n'existe pas d'autres relations de récurrences de degré 2 que $x_{n+1} = x_n^2$ et $x_{n+1} = x_n^2 - 2$ pour lesquelles on connaisse une formule explicite.

Exercice 5

Soient $0 < a \leqslant b$. On définit les suites (a_n) et (b_n) par $a_0 = a$, $b_0 = b$, et les relations de récurrence suivantes :

$$a_{n+1} = \frac{a_n + b_n}{2}, \qquad b_{n+1} = \sqrt{a_{n+1} b_n}.$$

Montrer que les suites (a_n) et (b_n) convergent vers une limite commune et déterminer cette limite (ou, si vous n'êtes pas à l'aise avec les limites, déterminer une expression explicite de (a_n) et (b_n), après tout c'est ça qui est le plus intéressant).

Solution de l'exercice 5

On peut montrer que les deux suites admettent une limite commune en montrant qu'elles sont adjacentes, mais on va en fait directement montrer qu'elles convergent en en déterminant une expression explicite. Celle-ci est quasiment introuvable sans l'idée de départ : comme $0 < a \leqslant b$, on peut poser $a = b\cos\theta$ avec $\theta \in]0, \frac{\pi}{2}]$. L'dentité qui va nous aider ici est $\dfrac{\cos\alpha + 1}{2} = \cos^2\dfrac{\alpha}{2}$. En appliquant cette relation, on trouve successivement :

$$a_1 = b \cdot \frac{1+\cos\theta}{2} = b\cos^2\frac{\theta}{2}, \qquad b_1 = b\cos\frac{\theta}{2}\ ;$$

$$a_2 = b\cos\frac{\theta}{2} \cdot \frac{1+\cos\frac{\theta}{2}}{2} = b\cos\frac{\theta}{2}\cos^2\frac{\theta}{4}, \qquad b_2 = b\cos\frac{\theta}{2}\cos\frac{\theta}{4}\ ;$$

Et on peut naturellement conjecturer que :

$$a_n = b\cos\frac{\theta}{2}...\cos\frac{\theta}{2^{n-1}}\cos^2\frac{\theta}{2^n}, \qquad a_n = b\cos\frac{\theta}{2}...\cos\frac{\theta}{2^{n-1}}\cos\frac{\theta}{2^n},$$

ce qui se montre facilement par récurrence par la même méthode.

À partir de ce moment là, il est déjà clair que si (b_n) converge, alors (a_n) converge vers la même limite : en effet, $a_n = b_n \cos\frac{\theta}{2^n}$, et $\cos\frac{\theta}{2^n} \xrightarrow[n\to+\infty]{} 1$. Il suffit donc, à partir de maintenant, d'étudier la suite (b_n).

Pour simplifier un peu l'expression de b_n, on va utiliser l'identité $\sin 2\alpha = 2\sin\alpha\cos\alpha$. En utilisant successivement cette identité, on trouve :

$$b_n \sin\frac{\theta}{2^n} = b\cos\frac{\theta}{2}...\cos\frac{\theta}{2^{n-1}}\cos\frac{\theta}{2^n}\sin\frac{\theta}{2^n},$$

$$b_n \sin\frac{\theta}{2^n} = \frac{b}{2}\cos\frac{\theta}{2}...\cos\frac{\theta}{2^{n-1}}\sin\frac{\theta}{2^{n-1}},$$

...

$$b_n \sin\frac{\theta}{2^n} = \frac{b}{2^{n-1}}\cos\frac{\theta}{2}\sin\frac{\theta}{2},$$

$$b_n \sin\frac{\theta}{2^n} = \frac{b}{2^n}\sin\theta,$$

ce qui nous donne une expression explicite de b_n, $b_n = \dfrac{b\sin\theta}{2^n\sin\frac{\theta}{2^n}}$. En posant $x = \dfrac{\theta}{2^n}$, on trouve donc que $\lim\limits_{n\to\infty} 2^n \sin\dfrac{\theta}{2^n} = \lim\limits_{x\to 0}\theta \cdot \dfrac{\sin x}{x} = \theta$. On en déduit finalement que $\lim\limits_{n\to+\infty} b_n = \dfrac{b\sin\theta}{\theta}$, et comme $\theta \in]0, \frac{\pi}{2}]$, $\sin\theta = \sqrt{1-\cos^2\theta} = \sqrt{1-\frac{a^2}{b^2}}$, donc on a finalement $\lim\limits_{n\to+\infty} b_n = \dfrac{\sqrt{b^2-a^2}}{\arccos\frac{a}{b}}$.

Parfois, une bonne relation de récurrence vaut mieux qu'une expression explicite.

Exercice 6

Montrer que les nombres de Fermat, c'est-à-dire les entiers de la forme $2^{2^n}+1$ pour $n \in \mathbb{N}$, sont deux à deux premiers entre eux.

Solution de l'exercice 6

Posons $f_n = 2^{2^n} + 1$ le $n^{\text{ième}}$ nombre de Fermat. Les f_n sont liés par la relation de récurrence $f_{n+1} = (f_n - 1)^2 + 1$. Pour montrer que f_n et f_m sont premiers entre eux, si $m > n$ par exemple, on va calculer f_m modulo f_n. On a $f_{n+1} \equiv (0-1)^2 + 1 = 2 \mod f_n$, puis on montre par récurrence que pour tout $m > n$, $f_m \equiv 2 \mod f_n$: si c'est vrai au rang m, alors $f_{m+1} \equiv (2-1)^2 + 1 \equiv 2 \mod f_n$. Si $m > n \geqslant 0$, on a alors $f_m = kf_n + 2$ pour un certain $k \in \mathbb{N}$, donc si d est un diviseur commun à f_m et f_n, alors $d \mid 2$, donc $d = 1$ puisque comme $m \geqslant 1$, f_m est impair. f_m et f_n sont donc premiers entre eux.

- 4. La suite de Fibonacci -

La suite de Fibonacci est un cas particulier particulièrement célèbre de récurrence linéaire d'ordre 2. Elle est définie de la façon suivante :

$$F_0 = 0, \qquad F_1 = 1, \qquad , F_{n+2} = F_{n+1} + F_n.$$

Son polynôme caractéristique est $\chi(x) = x^2 - x - 1$, dont les racines sont $\phi = \dfrac{1+\sqrt{5}}{2}$ et $\dfrac{1-\sqrt{5}}{2}$. La première des deux racines, ϕ, est le célèbre nombre d'Or. L'équation dont elle est solution montre que $\phi - 1 = \phi^{-1}$. De plus, le produit des racines de $\chi(x)$ vaut -1, donc l'autre racine est $-\phi^{-1} = 1 - \phi$.

À partir des valeurs des termes initiaux, on peut calculer les coefficients dans l'expression explicite de F_n donnée par le théorème 50. On en déduit finalement la formule de Binet :

$$F_n = \frac{1}{\sqrt{5}}(\phi^n - (-\phi^{-1})^n).$$

Exercice 7

Calculer les sommes $\displaystyle\sum_{i=0}^{n} F_i$, $\displaystyle\sum_{i=0}^{n} F_{2i}$, et $\displaystyle\sum_{i=0}^{n} F_{2i+1}$.

Solution de l'exercice 7

En calculant les premières valeurs de chaque somme, on conjecture facilement que $\displaystyle\sum_{i=0}^{n} F_i = F_{n+2} - 1$, $\displaystyle\sum_{i=0}^{n} F_{2i} = F_{2n+1}$, et $\displaystyle\sum_{i=0}^{n} F_{2i+1} = F_{2n+2}$. Ces formules se prouvent ensuite très facilement par récurrence, en utilisant la relation de récurrence définissant les F_n.

On peut aussi trouver d'autres identités entre les termes de la suite de Fibonacci. Pour cela, plusieurs méthodes sont possibles : soit par des méthodes matricielles, très pratiques et que je n'aborderai pas, mais vous pouvez trouver ces méthodes expliquées dans le Soulami ; soit des méthodes combinatoires, que vous trouverez dans le poly de ce stage, dans le cours de combinatoire avancée ; soit en utilisant la formule de Binet, méthode certes laide mais fonctionnelle, et que l'on va utiliser ici.

L'idée est de tenter de comparer des expressions dans lesquelles ϕ et $-\phi^{-1}$ sont élevées aux mêmes puissances. Par exemple, calculons $F_{n+1}F_{n-1}$ avec la formule de Binet. On a :

$$F_{n+1}F_{n-1} = \frac{1}{5}(\phi^{n+1} - (-\phi^{-1})^{n+1}))(\phi^{n-1} - (-\phi^{-1})^{n-1}))$$

$$F_{n+1}F_{n-1} = \frac{1}{5}(\phi^{2n} + (-\phi^{-1})^{2n}) + (-1)^n(\phi^2 + \phi^{-2}))$$

$$F_{n+1}F_{n-1} = \frac{1}{5}(\phi^{2n} + (-\phi^{-1})^{2n})) + (-1)^n\frac{3}{5}$$

Pour obtenir une autre formule dans laquelle les ϕ et $-\phi^{-1}$ soit élévés à la puissance $2n$, on a alors l'idée de multiplier des termes de la suite dont la somme des indices vaut $2n$. Par exemple F_n et F_n. Après un calcul du même type, on trouve que :

$$F_n^2 = \frac{1}{5}(\phi^{2n} + (-\phi^{-1})^{2n}) - (-1)^n\frac{2}{5}$$

On en déduit finalement que $F_{n+1}F_{n-1} = F_n^2 + (-1)^n$. Ce type de formules est bien évidemment aussi démontrable par récurrence... Mais il faut déjà les connaître à l'avance !

Exercice 8

Exprimer F_{m+n} en fonction de F_{m-1}, F_m, F_n, et F_{n+1}.

<u>*Solution de l'exercice 8*</u>

On aimerait exprimer F_{m+n} comme une somme de produits du type F_kF_l avec k proche de m et l proche de n. On se rend compte que c'est les termes à la puissance $k-l$ qui devront être supprimés, et on a intérêt à choisir k et l dans chaque produit de sorte que $k - l$ soit constant. D'où l'idée de calculer $F_{m-1}F_n$ et F_mF_{n+1}. On trouve :

$$F_{m-1}F_n = \frac{1}{5}(\phi^{m+n-1} + (-\phi^{-1})^{m+n-1} - (-1)^n(\phi^{m-n-1} + (-\phi^{-1})^{m-n-1}))\ ;$$

$$F_mF_{n+1} = \frac{1}{5}(\phi^{m+n+1} + (-\phi^{-1})^{m+n+1} - (-1)^{n+1}(\phi^{m-n-1} + (-\phi^{-1})^{m-n-1})).$$

Pour éliminer les termes parasites, on additionne les égalités précédentes. On prend soin, en même temps, de transformer tous les termes avec des puissances « proches » de $m+n$ en des termes en puissance $m+n$, quitte à faire apparaître des facteurs multiplicatifs. On obtient finalement :

$$F_{m-1}F_n + F_mF_{n+1} = \frac{1}{5}((\phi + \phi^{-1})\phi^{m+n} - (\phi + \phi^{-1})(-\phi^{-1})^{m+n})).$$

Puis en utilisant le fait que $\phi + \phi^{-1} = \sqrt{5}$ et en simplifiant, on obtient finalement $F_{m-1}F_n + F_mF_{n+1} = F_{m+n}$.

La suite de Fibonacci possède de nombreuses propriétés artihmétiques intéressantes.

Exercice 9

(1) Montrer que si $m \mid n$, alors $F_m \mid F_n$.

(2) Montrer que $\mathrm{PGCD}(F_m, F_n) = F_{\mathrm{PGCD}(m,n)}$.

Solution de l'exercice 9

(1) On montre par récurrence sur k que $F_m \mid F_{km}$. C'est vrai pour $k = 0$ et $k = 1$. Si c'est vrai au rang k, alors par la formule trouvée à l'exercice précédent, on a $F_{(k+1)m} = F_{km-1}F_m + F_{km}F_{m+1}$, et chacun des deux termes de cette somme possède un facteur divisible par F_m. Donc $F_{(k+1)m}$ est aussi divisible par F_m.

Une autre méthode permet de montrer le même résultat pour toutes les suites (u_n) définies par une récurrence du type $u_{n+2} = au_{n+1} + bu_n$, avec a, b, et u_1 entiers, $u_0 = 0$, et dont le polynôme caractéristique a deux racines distinctes. En effet, considérons cette suite et notons r_1 et r_2 les racines de son polynôme caractéristique, et λ et μ des complexes tels que $u_n = \lambda r_1^n + \mu r_2^n$. Soit $m \geqslant 1$; on cherche à montrer que $u_m \mid u_{km}$ pour tout k. Considérons la suite $v_k = u_{km}$. Alors $v_k = \lambda(r_1^m)^k + \mu(r_2^m)^k$, donc v_k vérifie une relation de récurrence linéaire d'ordre 2 de polynôme caractéristique $x^2 - (r_1^m + r_2^m)x + (r_1 r_2)^m$. Comme $r_1 r_2 = -b$, le coefficient constant de ce polynôme est entier. Admettons pour l'instant que le coefficient du terme en x est aussi entier. Alors v_k vérifie une relation de récurrence du type $v_{k+2} = cv_{k+1} + dv_k$, avec c et d entiers. Comme $v_0 = 0$ et $v_1 = u_m$ sont tous les deux divisibles par u_m, il est alors immédiat par récurrence que u_m divise tous les termes de cette suite, ce qu'il fallait démontrer.

Il ne reste plus qu'à montrer que $r_1^m + r_2^m$ est entier. Si on note $w_m = r_1^m + r_2^m$, alors $w_0 = 2$ et $w_1 = a$ sont entiers. De plus, la suite (w_m) vérifie la même relation de récurrence linéaire d'ordre 2 que (u_n), puisqu'elle a le même polynôme caractéristique. En particulier, cette relation est à coefficients entiers, donc les termes de la suite (w_m) aussi.

(2) Déjà, il est clair, par la question précédente, que $F_{\mathrm{PGCD}(m,n)} \mid \mathrm{PGCD}(F_m, F_n)$. Il s'agit maintenant de montrer la réciproque. Pour cela, posons $d = \mathrm{PGCD}(m, n)$ et considérons $u, v \in \mathbb{Z}$ tels que $um + vn = d$. On aimerait exprimer F_d comme une combinaison linéaire de F_{um} et F_{vn}, le problème étant que u et v ne sont pas positifs. En fait, ce n'est pas un problème, puisqu'en utilisant la formule de Binet, on peut définir F_n pour n négatif. (F_n) vérifie toujours la même relation de récurrence linéaire, même pour n négatif, et on peut en déduire par récurrence descendante que F_n est entier pour tout $n \leqslant 0$ (en initialisant en 0 et 1). De même, la formule de l'exercice 8 reste vraie pour les négatifs, puisqu'elle a été démontrée avec la formule de Binet. Enfin, le résultat de la question précédente reste lui aussi vrai, on peut le montrer par récurrence descendante en utilisant la seconde méthode. Il est donc tout à fait correct d'écrire $F_d = F_{um-1}F_{vn} + F_{um}F_{vn+1}$. $D = \mathrm{PGCD}(F_m, F_n)$ divise F_{um} et F_{vn} par la généralisation de la question précédente, donc $D \mid F_d$, ce qui conclut la preuve.

- 5. Ensembles finis -

Considérons un ensemble fini E, et une suite (u_n) d'éléments de E vérifiant une relation de récurrence du type $u_{n+1} = f(u_n)$, où $f : E \to E$ est une application. Alors u_n ne pouvant prendre qu'un nombre fini de valeurs, par le principe des tiroirs il va exister deux entiers $k < l$

tels que $u_k = u_l$. Il est alors immédiat, par récurrence, que $u_{k+n} = u_{l+n}$ pour tout $n \geqslant 0$: la suite u_n est périodique à partir d'un certain rang.

Si on suppose de plus f injective, on peut obtenir un résultat encore plus intéressant. En effet, considérons le couple (k, l) tel que $k < l$ et $u_k = u_l$, avec k minimal. Si k était supérieur où égal à 1, on aurait $f(u_{k-1}) = f(u_{l-1})$, donc par injectivité de f, $u_{k-1} = u_{l-1}$, ce qui contredirait la minimalité de k. Donc $k = 0$, et $u_n = u_{l+n}$ pour tout n : la suite (u_n) est périodique.

Exercice 10

Le palais du Minotaure est constitué d'un million de salles reliées par des couloirs. De chaque salle partent exactement trois couloirs. Le Minotaure, parti d'une des salles, parcourt son palais, en tournant alternativement à droite et à gauche dans les salles par lesquelles il passe. Montrer qu'il finira par revenir dans la salle de départ.

Solution de l'exercice 10

Notons E l'ensemble des triplets (s, p, d), où s est une salle du palais du Minotaure, p la porte par laquelle il est entré dans la salle, et d une direction (droite où gauche) ; soit $f : E \to E$ la fonction qui à un triplet (s, p, d) associe (s', p', d'), où s' est la salle dans laquelle arrive le Minotaure s'il vient de la salle s, dans laquelle il est entré par la porte p, et en prenant la direction d, p' la porte par laquelle il entré dans cette salle, et d' la direction opposée à d. On note u_n le triplet (s_n, p_n, d_n), où s_n est la salle dans laquelle se situe le Minotaure après son $n^{\text{ième}}$ déplacement, p_n la porte par laquelle il y est entré, et d_n la direction qu'il a l'intention de prendre à son déplacement suivant. On a alors clairement $u_{n+1} = f(u_n)$. Comme E est fini, et f injective, on en déduit que (u_n) est périodique. En particulier, il existe un entier n tel que $u_n = u_0$; après son $n^{\text{ième}}$ déplacement, le Minotaure se retrouvera donc dans sa salle de départ.

Exercice 11

Définissons la suite (u_n) par $u_0 = u_1 = 0$ et $u_{n+2} = u_{n+1} + u_n + 1$. Montrer qu'il existe un entier $N \geqslant 1$ tel que u_N et u_{N+1} soient tous les deux divisibles par 2011^{2012}.

Solution de l'exercice 11

Posons $A = 2011^{2012}$, et réduisons tous les termes de la suite modulo A. Posons, par exemple, u'_n le reste de la division euclidienne de u_n par A. Considérons la suite des couples (u'_n, u'_{n+1}). Cette suite est à valeurs dans un ensemble fini, et la relation de récurrence qui la définit est bijective : on peut retrouver (u'_n, u'_{n+1}) en fonction de (u'_{n+1}, u'_{n+2}) (prendre pour u'_n le reste de la division euclidienne de $u'_{n+2} - u'_{n+1} - 1$ par A). Elle est donc périodique, et on peut trouver $N \geqslant 1$ tel que $(u'_N, u'_{N+1}) = (u'_0, u'_1) = (0, 0)$. N est bien l'entier recherché.

- 6. Téléscopages -

Lorsqu'on veut sommer les termes d'une suite (u_n) (ou multiplier les termes d'une suite (a_n)), il est souvent pratique de pouvoir écrire $u_n = v_{n+1} - v_n$ (ou $a_n = \dfrac{b_{n+1}}{b_n}$), où (v_n) et (b_n) sont des suites connues : on a alors $\displaystyle\sum_{i=k}^{l} u_i = v_{l+1} - v_k$ et $\displaystyle\prod_{i=k}^{l} a_i = \frac{b_{l+1}}{b_k}$.

Exercice 12

Soit (a_n) la suite définie par $a_1 = 1$ et $a_{n+1} = 1 + a_1 a_2 ... a_n$. Déterminer $\sum_{n=1}^{+\infty} \frac{1}{a_n}$.

Solution de l'exercice 12

Il est clair que pour tout $n \geqslant 2$, on a $a_{n+1} - 1 = a_n(a_n - 1)$, et en inversant cette relation, on obtient $\frac{1}{a_{n+1}-1} = \frac{1}{a_n - 1} - \frac{1}{a_n}$, autrement dit $\frac{1}{a_n} = \frac{1}{a_n - 1} - \frac{1}{a_{n+1}-1}$. En sommant, on obtient $\sum_{k=1}^{n} \frac{1}{a_k} = 1 + \frac{1}{a_2 - 1} - \frac{1}{a_{n+1}-1} = 2 + \frac{1}{a_{n+1}-1}$. Pour conclure que $\sum_{n=1}^{+\infty} \frac{1}{a_n} = 2$, il suffit de montrer que $\frac{1}{a_{n+1}-1} \xrightarrow[n\to+\infty]{} 0$, autrement dit que $a_n \xrightarrow[n\to+\infty]{} +\infty$. Mais ceci est clair car la définition de (a_n) montre que $a_{n+1} \geqslant 1 + a_n$, donc que $a_n \geqslant n$ pour tout n.

4 Test

Exercice 1 Montrer que si $x \in]0, \infty[$, alors

$$x^8 - x^5 - \frac{1}{x} + \frac{1}{x^4} \geqslant 0.$$

Exercice 2 Trouver les polynômes $P \in \mathbb{C}[X]$ tels que

$$P(2X) = P(X-1)P(1).$$

Exercice 3 Soit p, q, r trois rationnels tels que $\sqrt[3]{p^2q} + \sqrt[3]{q^2r} + \sqrt[3]{r^2p}$ est rationnel. Montrer que $\frac{1}{\sqrt[3]{p^2q}} + \frac{1}{\sqrt[3]{q^2r}} + \frac{1}{\sqrt[3]{r^2p}}$ est rationnel..

Exercice 4

Montrer que les entiers de la forme $\left\lfloor \frac{(3+\sqrt{10})^{2^n}}{4} \right\rfloor + 1$, où n est un entier naturel, sont deux à deux premiers entre eux ($\lfloor \cdot \rfloor$ désigne la partie entière).

- Corrigé -

Solution de l'exercice 1 Supposons par l'absurde que P a une racine $\alpha \neq -2$. En posant $X = \alpha + 1$ on trouve $P(2\alpha + 2) = 0$, ainsi $2\alpha + 2$ est aussi racine. Comme $\alpha \neq -2$, $2\alpha + 2 \neq -2$. Ainsi on obtient une suite $\alpha_1 = \alpha, \alpha_2, \alpha_3, \dots$ avec $\alpha_{n+1} = 2\alpha_n + 2$. Par récurrence on trouve $\alpha_n = 2^{n-1}\alpha + 2$. Ainsi P a une infinité de racines distinctes. Impossible.

Supposons que P n'est pas constant. Alors $P = a(x+2)^n$ pour $a \in \mathbb{C}$. On trouve $a = (\frac{2}{3})^n$.

Parmi les polynômes constants il y a seulement 0 et 1 qui conviennent.

Solution de l'exercice 2 On est tenté de factoriser l'expression. Le facteur $x^3 - 1$ est un bon candidat. On fait la division euclidienne et on trouve : $x^8 - x^5 - \frac{1}{x} + \frac{1}{x^4} = \frac{1}{x^4}(x^{12} - x^9 - x^3 + 1) =$

$\frac{1}{x^4}(x^3-1)^2(x^9-1)$. Or pour x^9-1 on applique la formule $a^3-b^3=(a-b)(a^2+ab+b^2)$, donc $x^9-1=(x^3-1)(x^6+x^3+1)$. Ainsi l'expression n'a que des facteurs positifs.

Solution de l'exercice 3 On pose $a = \mathrm{sqrt}[3]p^2q$, $b = \mathrm{sqrt}[3]q^2r$ et $c = \mathrm{sqrt}[3]r^2p$. On a $abc = pqr \in \mathbb{Q}$. Aussi $a^3 + b\neg 3 + c^3 = p^2q + q^2r + r^2p \in \mathbb{Q}$. L'hypothèse dit $a + b + c \in \mathbb{Q}$.

On pose $s_1 = a+b+c$, $s_2 = ab+bc+ca$ et $s_3 = abc$. On a $a^3+b^3+c^3 = 3s_3+s_1(s_1^2-3s_2)$. Comme s_1, s_3, et $a^3 + b\neg 3 + c\neg 3$ sont tous rationnels, $s_2 \in \mathbb{Q}$. Donc $\frac{s_2}{s_3} \in \mathbb{Q}$. CQFD

Solution de l'exercice 4

Posons $u_n = \left\lfloor \dfrac{(3+\sqrt{10})^{2^n}}{4} \right\rfloor + 1$. On aimerait trouver une relation de récurrence entre les u_n de laquelle il soit facile de déduire la propriété voulue.

La première chose à faire est de se débarasser de la partie entière, et pour cela on va introduire la quantité conjuguée $3-\sqrt{10}$ qui, élevée à une puissance suffisante, deviendra très petite. On va donc poser $v_n = (3+\sqrt{10})^{2^n} + (3-\sqrt{10})^{2^n}$. On a $v_0 = 6$, et comme $3-\sqrt{10} = (3+\sqrt{10})^{-1}$, on en déduit, comme dans le cours, la relation de récurrence $v_{n+1} = v_n^2 - 2$. En particulier, tous les termes de la suite (v_n) sont entiers, et il est même immédiat par récurrence qu'ils sont tous congrus à 2 modulo 4. Étant donné $n \in \mathbb{N}$, on peut alors choisir $k \in \mathbb{Z}$ tel que $v_n = 4k+2$; comme $-1 < 3-\sqrt{10} < 0$, on en déduit que $0 < (3-\sqrt{10})^{2^n} < 1$, donc que $k + \dfrac{1}{4} < \dfrac{(3+\sqrt{10})^{2^n}}{4} < k + \dfrac{1}{2}$, et donc $u_n = k+1 = \frac{v_n+2}{4}$. On a donc $v_0 = 2$, et de la relation de récurrence liant les v_n, on peut tirer celle liant les u_n : $u_{n+1} = 4u_n^2 - 4u_n + 1$.

Il y a deux méthodes possibles pour conclure. La première est de calculer u_m modulo u_n pour $m > n$: la relation de récurrence donne $u_{n+1} \equiv 1 \mod u_n$, puis une récurrence immédiate donne $u_m \equiv 1 \mod u_n$ pour tout $m \geqslant n+1$. En écrivant $u_m = ku_n + 1$, il est immédiat que u_m et u_n sont premiers entre eux. La seconde méthode est de montrer une autre relation de récurrence pour (u_n) : pour tout $n \geqslant 1$, $u_n = 4^n u_{n-1} \ldots u_1 u_0 + 1$, sur laquelle il est immédiat que tous les termes de la suite sont premiers entre eux. On démontre cette relation par récurrence à partir de la première.

4 Avancés : arithmétique avancée

Nous renvoyons aux cours d'arithmétique disponible sur le site d'Animath pour des détails et compléments (voir les liens en haut de la page 14).

1 Premier cours/TD

- STRUCTURE DE $\mathbb{Z}/n\mathbb{Z}$ -

Certains théorèmes et certaines propositions de la versions polycopiée de ce cours ont été présentés en tant qu'exercices en classe. Je les ai ici mis sous forme de théorèmes pour souligner leur importance, par rapport aux autres exercices.

- **L'anneau** $\mathbb{Z}/n\mathbb{Z}$ -

Soit $n \geqslant 2$ un entier naturel. Dans $\mathbb{Z}$, on dispose de la relation de congruence modulo n. Celle-ci est une *relation d'équivalence*, c'est-à-dire qu'elle est *réflexive* (pour tout $x \in \mathbb{Z}$, $x \equiv x \mod n$), *symétrique* (pour tous x, $y \in \mathbb{Z}$, si $x \equiv y \mod n$, alors $y \equiv x \mod n$) et *transitive* (pour tous x, y, $z \in \mathbb{Z}$, si $x \equiv y \mod n$ et $y \equiv z \mod n$, alors $x \equiv z \mod n$). De plus, elle est compatible avec les opérations $+$ et $\times$. Elle possède en fait des propriétés tout à fait similaires à l'égalité, et on aimerait bien la « transformer » en une égalité, en « faisant de deux entiers congrus modulo n un seul et même nombre ».

Si x est un entier, on appelle *classe d'équivalence de* x *modulo* n l'ensemble des entiers congrus à x modulo n. On note $\overline{x}$ la classe de x. Attention, si $x \equiv y \mod n$, alors $\overline{x}$ et $\overline{y}$ sont deux notations pour un seul et même objet. On obtient exactement n classes d'équivalence, et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de ces classes d'équivalence. On munit $\mathbb{Z}/n\mathbb{Z}$ de deux opérations $+$ et $\times$ en posant $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$. Il est clair que ces opérations sont bien définies (c'est-à-dire, par exemple pour $+$, que si $\overline{x} = \overline{x'}$ at $\overline{y} = \overline{y'}$, alors $\overline{x+y} = \overline{x'+y'}$) : ceci découle immédiatement du fait que la relation de congruence est compatible avec les opérations.

La construction de $\mathbb{Z}/n\mathbb{Z}$ peut paraître conceptuellement difficile la première fois qu'on la voit, mais en fait, la manipulation de cet ensemble est très simple : écrire $\overline{x} + \overline{y} = \overline{z}$ est rigoureusement équivalent à écrire $x+y \equiv z \mod n$, par exemple. Pour passer d'une écriture à l'autre, on enlève les barres et on remplace l'égalité par une relation de congruence. Mais l'énorme avantage de l'utilisation de $\mathbb{Z}/n\mathbb{Z}$ est, dans le cas de $\mathbb{Z}/5\mathbb{Z}$ par exemple, le fait que $\overline{2}$ et $\overline{7}$ sont *un seul et même nombre*, et non plus simplement congrus. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n, et on a par exemple $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\} = \left\{\overline{-n}, ..., \overline{-2}, \overline{-1}\right\}$. De plus, $\mathbb{Z}/n\mathbb{Z}$ possède une certaine structure algébrique, celle d'*anneau*, ce qui permettra par exemple d'utiliser dans certains cas de façon très puissante les polynômes.

Définition 51. Un *anneau (commutatif unitaire)* $(A, +, \times)$ est un ensemble A muni de deux lois binaires $+$ et $\times$, toutes deux commutatives ($x+y = y+x$) et associatives ($x+(y+z) = (x+y)+z$), telles que :

– $\times$ est distributive sur $+$ ($(x+y)z = xz + yz$) ;
– La loi $+$ admet un élément neutre noté 0, tel que pour tout $x \in A$, $x + 0 = x$;
– La loi $\times$ admet un élément neutre noté 1, tel que pour tout $x \in A$, $x \times 1 = x$;
– Tout élément x de A admet un opposé noté $-x$, tel que $x + (-x) = 0$ (celui-ci est unique).

Si on a de plus $\forall x, y \in A$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$, on dit alors que A est *intègre*. On dit qu'un élément x de A est inversible s'il existe x^{-1} (appelé un *inverse* de x) tel que $xx^{-1} = 1$. On note A^* l'ensemble des inversibles de A. Si x est inversible, son inverse est unique. 0 n'admet jamais d'inverse. Si $A^* = A \setminus \{0\}$, on dit que A est un *corps*. Un corps est toujours intègre.

Exemple 52. $\mathbb{Z}$ est un anneau intègre, d'inversibles 1 et -1. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. Si A est un anneau, alors l'ensemble des polynômes à coefficients dans A, noté $A[X]$, est un anneau. Si A est intègre, alors $A[X]$ l'est aussi. Si A est un corps, alors les inversibles de $A[X]$ sont les polynômes constants non-nuls. Et enfin, $\mathbb{Z}/n\mathbb{Z}$ est un anneau !

De nombreuses propriétés de $\mathbb{Z}$ sont communes à tous les anneaux, et encore plus le sont à tous les anneaux intègres. De nombreuses propriétés de $\mathbb{Q}$, $\mathbb{R}$ où $\mathbb{C}$ sont communes à tous les corps, d'où l'intérêt de ces notions. On n'utilise en fait pour montrer ces propriétés que le fait que l'ensemble concerné soit un anneau (éventuellement intègre), ou un corps.

Proposition 53. Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{a}$, où a est un entier premier avec n. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier, et dans ce cas, c'est un corps.

Démonstration. On a les équivalences suivantes :

$\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$

$\Leftrightarrow$ il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \mod n$

$\Leftrightarrow$ il existe $b \in \mathbb{Z}$ et $k \in Z$ tels que $ab = kn + 1$

$\Leftrightarrow$ a est premier avec n (par Bézout).

Si n est premier, les éléments non-nuls de $\mathbb{Z}/n\mathbb{Z}$ étant $\overline{1}$, $\overline{2}$, ..., $\overline{n-1}$, il sont tous inversibles. Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps. Il ne reste plus qu'à montrer que si n est composé, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre ; mais si n est composé, on écrit $n = ab$ avec $1 \leqslant a,\ b \leqslant n$, et on a alors $\overline{a},\ \overline{b} \neq 0$ et $\overline{a}\overline{b} = \overline{n} = 0$.

□

- Ordre multiplicatif -

Soit $n \geqslant 2$. L'ensemble $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{x} | 1 \leqslant x \leqslant n-1, \mathrm{PGCD}(x, n) = 1\}$ est stable par produit, par passage à l'inverse, et contient $\overline{1}$ (on dit que c'est un *groupe*). Cet ensemble est de cardinal $\phi(n)$, et par le théorème d'Euler, pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $x^{\phi(n)} = \overline{1}$.

Définition 54. Soit $x \in \mathbb{Z}$. L'*ordre* de $\overline{x}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ (ou encore l'ordre de x modulo n) est le plus petit entier $\omega \geqslant 1$ tel que $\overline{x}^{\omega} = \overline{1}$ (ou encore $x^{\omega} \equiv 1 \mod n$). On le note $\omega_n(x)$ ou simplement $\omega(x)$ lorsqu'il n'y a pas d'ambiguité.

Le théorème d'Euler montre que l'ordre est bien défini. On remarquera qu'alors, $\overline{x}^{\omega-1}$ est l'inverse de $\overline{x}$. En particulier, si $\overline{x}$ n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$, il n'existe aucun entier $\omega \geqslant 1$ tel que $\overline{x}^{\omega} = \overline{1}$.

Exercice 1

Sans le théorème d'Euler, montrer que l'ordre est bien défini.

L'intérêt de l'ordre est la proposition suivante :

Proposition 55. Soit $x \in (\mathbb{Z}/n\mathbb{Z})^*$, et $n \in \mathbb{Z}$. Alors $x^n = \overline{1}$ si et seulement si $\omega(x)$ divise n.

Démonstration. Si $\omega(x) \mid n$, on pose $n = k\omega(x)$ et on a $x^n = (x^{\omega(x)})^k = \overline{1}^k = \overline{1}$. Réciproquement, si $x^n = \overline{1}$, alors on écrit $n = q\omega(x) + r$ avec $0 \leqslant r < \omega(x)$ et on a $x^r = x^r(x^{\omega(x)})^q = x^n = 1$. On ne peut pas avoir $1 \leqslant r < \omega(x)$, sinon ceci contredirait la minimalité de $\omega(x)$. Donc $r = 0$ et $\omega(x) \mid n$.

□

On en déduit, en particulier, que pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $\omega(x) \mid \phi(n)$ (et donc $\omega(x) \mid n-1$ si n est permier). Ceci est particulièrement pratique lorsque $\phi(n)$ a une forme particulière. Par exemple, si p est un nombre premier et $n \geqslant 1$, alors $\phi(p^n) = p^n(p-1)$. Pour $p = 2$ par exemple, $\phi(2^n) = 2^{n-1}$, et donc tout les éléments de $(\mathbb{Z}/2^n\mathbb{Z})^*$ ont pour ordre une puissance de 2.

Exercice 2

Soit n un entier naturel. Montrer que les diviseurs premiers du $n^{\text{ième}}$ nombre de Fermat $2^{2^n} + 1$ sont tous de la forme $k \cdot 2^{n+1} + 1$.

Exercice 3

Déterminer tous les entiers $n \geqslant 1$ tels que n divise $2^n - 1$.

- **Polynômes dans** $\mathbb{Z}/p\mathbb{Z}$ -

Sauf mention contraire, dans toute la suite, p désignera un nombre premier, et on travaillera dans le corps $\mathbb{Z}/p\mathbb{Z}$.

Si A est un anneau intègre, de nombreux résultats vrais dans $\mathbb{Z}[X]$ le restent dans $A[X]$. En particulier, on a l'existence d'une division euclidienne par les polynômes unitaires, si $r \in A$ est racine de $P \in A[X]$, alors $P(X)$ est divisible par $X-r$, et un polynôme de degré n possède au plus n racines, comptées avec multiplicités. En conséquence, si un polynôme P est de degré n, a pour coefficient dominant λ, a pour racines r_1, ..., r_k avec pour multiplicités respectives α_1, ..., α_k telles que $\alpha_1 + ... + \alpha_k = n$, alors $P(X) = \lambda(X-r_1)^{\alpha_1}...(X-r_k)^{\alpha_k}$. Si, de plus, A est un corps, alors on dispose d'une division euclidienne par n'importe quel polynôme non-nul, et dans $A[X]$ on a un PGCD, un PPCM, des théorèmes de Bézout et de Gauss, et existence et unicité de la décomposition en produit d'irréductibles. En particulier, toutes ces propriétés sont vraies dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 4

Résoudre dans $\mathbb{Z}/12\mathbb{Z}$ l'équation $x^2 + \overline{3}x + \overline{2} = 0$.

Exercice 5

Soit $p \geqslant 2$ un entier naturel. Montrer que p est premier si et seulement si $(p-1)! \equiv -1 \mod p$.

(Théorème de Wilson)

Exercice 6

Soit $p \geqslant 5$ un nombre premier. Soient a, $b \in \mathbb{Z}$ tels que $1 + \dfrac{1}{2} + ... + \dfrac{1}{p-1} = \dfrac{a}{b}$. Montrer que $p^2 \mid a$.

- **Résidus quadratiques** -

Définition 56. Soit $x \in \mathbb{Z}$. On dit que x est un résidu quadratique modulo p (ou encore que $\overline{x}$ est un résidu quadratique dans $\mathbb{Z}/p\mathbb{Z}$) si x n'est pas divisible par p et si $\overline{x}$ est le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$.

On note $\left(\dfrac{x}{p}\right) = 1$ si x est un résidu quadratique modulo p, $\left(\dfrac{x}{p}\right) = 0$ si $p \mid x$ et $\left(\dfrac{x}{p}\right) = -1$ sinon. Le symbole $\left(\dfrac{x}{p}\right)$ s'appelle le symbole de Legendre.

Théorème 57 (Critère d'Euler)**.** Soit p un nombre premier impair, et $x \in (\mathbb{Z}/p\mathbb{Z})^*$. Alors x est un résidu quadratique si et seulement si $x^{\frac{p-1}{2}} = \overline{1}$. Sinon, on a $x^{\frac{p-1}{2}} = -\overline{1}$.

Démonstration. Commençons par dénombrer les résidus quadratiques de $(\mathbb{Z}/p\mathbb{Z})^*$. Soit x un résidu quadratique, disons que $x = y^2$ avec $y \in (\mathbb{Z}/p\mathbb{Z})^*$. On a alors aussi $x = (-y)^2$, or $y \neq -y$ puisque p est impair, donc x est le carré d'au moins deux éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. En fait, c'est le carré d'exactement deux éléments, car le polynôme $X^2 - x$ est de degré 2, donc admet au plus deux racines dans $\mathbb{Z}/p\mathbb{Z}$. Puisque $(\mathbb{Z}/p\mathbb{Z})^*$ possède $p-1$ éléments, et puisque chaque résidu quadratique est le carré d'exactement deux de ces éléments, on en déduit qu'il y a exactement $\frac{p-1}{2}$ résidus quadratiques.

Tous ces résidus quadratiques vérifient $x^{\frac{p-1}{2}} = \overline{1}$, puisqu'en les écrivant $x = y^2$, on obtient $x^{\frac{p-1}{2}} = y^{p-1} = \overline{1}$, par petit Fermat. Il s'agit de montrer que c'est les seuls. Mais le polynôme $X^{\frac{p-1}{2}} - \overline{1}$ a au plus $\frac{p-1}{2}$ racines dans $\mathbb{Z}/p\mathbb{Z}$, et tous les résidus quadratiques, qui sont au nombre de $\frac{p-1}{2}$, en sont racines. Donc ce sont les seules, ce qui conclut la première affirmation du théorème.

Pour démontrer la seconde partie, il suffit de montrer que la fonction $f(x) = x^{\frac{p-1}{2}}$ ne prend que les valeurs $\overline{1}$ et $-\overline{1}$ lorsque x parcourt $(\mathbb{Z}/p\mathbb{Z})^*$. Mais $f(x)^2 = x^{p-1} = \overline{1}$, donc les valeurs prises par f sur $(\mathbb{Z}/p\mathbb{Z})^*$ sont des racines carrées de 1 : ce sont donc $\overline{1}$ et $-\overline{1}$.

$\square$

Cette preuve, ou du moins le premier paragraphe, est à connaître, car elle donne des informations sur la répartition des résidus quadratiques : leur nombre, et le fait que chacun soit le carré d'exactement deux éléments *opposés*. On peut en déduire, par exemple, que $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ forme un système complet de représentants des résidus quadratiques de $\mathbb{Z}/p\mathbb{Z}$, car ils sont au nombre de $\frac{p-1}{2}$ et sont deux-à-deux non-opposés.

Une autre remarque importante est que le critère d'Euler peut se reformuler de la façon suivante à l'aide du symbole de Legendre : pour tout nombre premier impair p et pour tout $x \in \mathbb{Z}$, on a $\left(\dfrac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \mod p$ (on remarquera que ceci marche *même* si $p \mid x$). On en déduit immédiatement que le symbole de Legendre est *complètement multiplicatif* par rapport à son argument supérieur, autrement dit, pour tous $x, y \in \mathbb{Z}$, on a $\left(\dfrac{x}{p}\right)\left(\dfrac{y}{p}\right) = \left(\dfrac{xy}{p}\right)$. En particulier, le produit de deux résidus quadratiques est un résidu quadratique, et l'inverse d'un résidu quadratique est un résidu quadratique (on dit que l'ensemble des résidus quadratiques est un *sous-groupe* de $(\mathbb{Z}/p\mathbb{Z})^*$), mais aussi, le produit de deux non-résidus quadratiques est un résidu quadratique, et le produit d'un résidu quadratique et d'un non-résidu quadratique n'est pas un résidu quadratique.

Exercice 7

(1) Trouver tous les nombres premiers p vérifiant la propriété suivante : pour tous entiers $a, b \in \mathbb{Z}$, si $p \mid (a^2 + b^2)$ alors $p \mid a$ et $p \mid b$.

(2) Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Voici un célèbre résultat dû à Gauss, que j'énoncerai sans preuve :

Théorème 58 (Loi de réciprocité quadratique)**.** Soient p et q deux nombres premiers impairs.

- Si au moins un des deux nombres p et q est congru à 1 modulo 4, alors q est un résidu quadratique modulo p si et seulement si p est un résidu quadratique modulo q ;
- Si les deux nombres p et q sont congrus à 3 modulo 4, alors q est un résidu quadratique modulo p si et seulement si p n'est pas un résidu quadratique modulo q.

À l'aide du symbole de Legendre, on peut reformuler ce résultat de la manière suivante : pour tous nombre premiers impairs p et q, on a $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$.

Ce théorème ne dit rien du cas où $p = 2$. Pour cela, on a la proposition suivante :

Proposition 59. Soit p un nombre premier impair. Alors 2 est un résidu quadratique modulo p si et seulement si p est congru à 1 où à -1 modulo 8. Autrement dit, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Avec la loi de réciprocité quadratique ainsi que la proposition précédente, on peut déterminer très rapidement si un entier est où non un résidu quadratique modulo un nombre premier p. On peut aussi, pour simplifier les calculs (même si ce n'est en réalité pas nécessaire), utiliser le fait que -1 est un résidu quadratique modulo p si et seulement si p est congru à 1 où 2 modulo 4, autrement dit $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Exercice 8

219 est-il un résidu quadratique modulo 383 ?

- Solution des exercices -

Solution de l'exercice 1

Soit $x \in (\mathbb{Z}/n\mathbb{Z})^*$; on cherche $\omega \geqslant 1$ tel que $x^\omega = \overline{1}$. Considérons la suite $x, x^2, x^3, \ldots$. Elle possède une infinité de termes et prend ses valeurs dans l'ensemble fini $\mathbb{Z}/n\mathbb{Z}$, donc par le principe des tiroirs, il existe des entiers s et t tels que $1 \leqslant s < t$ et $x^s = x^t$. En simplifiant par x^s, on obtient $x^{t-s} = \overline{1}$, donc $\omega = t - s$ convient.

Solution de l'exercice 2

Soit p un diviseur premier de $2^{2^n}+1$. Alors $2^{2^n} \equiv -1 \mod p$ et $2^{2^{n+1}} \equiv 1 \mod p$, donc l'ordre de 2 modulo p divise 2^{n+1} mais pas 2^n, donc c'est 2^{n+1}. Il s'ensuit que $2^{n+1} \mid (p-1)$, ce qui est le résultat voulu.

Solution de l'exercice 3

$n = 1$ convient, et on va montrer que c'est la seule solution. Soit $n \geqslant 2$, supposons que $n \mid 2^n - 1$. Déjà, il est clair que n est impair, puisque $2^n - 1$ l'est. Notons alors p le plus petit diviseur premier de n, et posons $n = kp$. On a $p \mid (2^n - 1)$ et par le petit théorème de Fermat, $2^n = (2^k)^p \equiv 2^k \mod p$, donc $2^k \equiv 1 \mod p$. Donc $\omega_p(2) \mid k$ et $\omega_p(2) \mid (p-1)$. De cette dernière relation de divisibilité, on tire que tous les diviseurs premiers de $\omega_p(2)$ sont strictement inférieurs á p. Or, $\omega_p(2) > 1$ puisque $p \geqslant 3$, et comme $\omega_p(2) \mid k$, on en déduit que k possède un diviseur premier strictement inférieur à p, donc n aussi. Ceci contredit la minimalité de k.

Solution de l'exercice 4

En factorisant, on obtient $(x+\overline{1})(x+\overline{2}) = 0$. Mais attention, on ne peut pas en déduire que $x = -\overline{1}$ ou $x = -\overline{2}$, car l'anneau $\mathbb{Z}/12\mathbb{Z}$ n'est pas intègre ! Dans un tel anneau, un polynôme de degré 2 peut avoir bien plus de deux racines. Il faut éviter d'essayer d'utiliser des résultats classiques sur les polynômes dans un anneau non intègre, car en général, très peu sont vrais. Ici, le seul moyen de résoudre l'équation est de tester tous les cas possibles, et de cette façon on obtient que l'ensemble des solutions est $\{\overline{2}, -\overline{5}, -\overline{2}, -\overline{1}\}$.

Solution de l'exercice 5

Si p est composé, on choisit $a \in [\![1, p-1]\!]$ divisant p. p et $(p-1)!$ ont alors a pour facteur commun, donc ne sont pas premiers entre eux. p n'est donc pas premier, sinon il diviserait $(p-1)!$ donc aussi un entier inférieur à $p-1$.

Réciproquement, supposons p premier. Il existe alors deux méthodes pour obtenir la congruence demandée.

Première méthode. On va partitionner $(\mathbb{Z}/p\mathbb{Z})^*$ en paires d'éléments deux à deux inverses. Pour cela, il faut connaître les $x \in (\mathbb{Z}/p\mathbb{Z})^*$ qui sont leur propre inverse ; ceux-là sont racines du polynôme $X^2 - \overline{1}$, de degré 2, donc il y en a au plus deux : ce sont donc $\overline{1}$ et $-\overline{1} = \overline{p-1}$. On regroupe les autres par paires d'inverses $\{x_i, x_i^{-1}\}$, de sorte que $\{\overline{1}\}$, $\{\overline{p-1}\}$ et les $\{x_i, x_i^{-1}\}$ forment une partition de $(\mathbb{Z}/p\mathbb{Z})^*$.

En réorganisant l'ordre des facteurs du produit, on a alors

$$\overline{(p-1)!} = \overline{1} \cdot \overline{p-1} \cdot (x_1 x_1^{-1}) \cdot \ldots \cdot (x_r x_r^{-1}) = \overline{p-1} = -\overline{1}.$$

Seconde méthode. Pour $p = 2$, le résultat est vrai. Supposons maintenant que $p \geqslant 3$. Considérons le polynôme $P(X) = X^{p-1} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Il est unitaire et de degré $p-1$, et par le petit théorème de Fermat, tous les $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ en sont racines. Par la remarque précédant l'exercice, on en déduit que $P(X) = (X-\overline{1})(X-\overline{2})\ldots(X-\overline{p-1})$. Le polynôme P étant de degré pair, son coefficient constant est produit de ses racines, autrement dit $\overline{(p-1)!} = -\overline{1}$.

Solution de l'exercice 6

L'égalité de l'énoncé se réécrit $(p-1)! \cdot a = bc_1$, où $c_1 = 2 \cdot 3 \cdot ... \cdot ... \cdot (p-1) + 1 \cdot 3 \cdot ... \cdot (p-1) + ... + 1 \cdot 2 \cdot ... \cdot (p-2)$ est le coefficient du terme en X du polynôme $P(X) = (X-1)...(X-(p-1))$. Pour résoudre le problème, il suffit de montrer que $p^2 \mid c_1$, car alors comme p^2 est premier avec $(p-1)!$, on en déduit par Gauss que $p^2 \mid a$.

Si on tente d'appliquer directement une méthode simillaire à la seconde méthode du problème précédent, on obtiendra, en réduisant P modulo p que $c_1 \equiv 0 \mod p$, ce qui n'est pas suffisant pour résoudre le problème. On va en fait utiliser une autre méthode : si on note $P(X) = \sum_{k=0}^{p-1} c_k X^k$, en évaluant P en p, on obtient $(p-1)! = \sum_{k=0}^{p-1} c_k p^k$, en remarquant que $c_0 = (p-1)!$ et simplifiant par p, on obtient $\sum_{k=1}^{p-1} c_k p^{k-1} = 0$. En réduisant modulo p^2, on obtient $c_2 p + c_1 \equiv 0 \mod p^2$. Il suffit donc de montrer que c_2 est divisible par p, mais ceci est clair en réduisant P modulo p.

<u>*Solution de l'exercice 7*</u>

(1) Il est clair que cette propriété n'est pas vérifiée par 2, en prenant par exemple $a = b = 1$. Soit maintenant p un nombre premier impair. On a $(-1)^{\frac{p-1}{2}} = 1$ si $p \equiv 1 \mod 4$ et -1 si $p \equiv 3 \mod 4$, donc par le critère d'Euler, -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1 \mod 4$. Ceci montre immédiatement qu'aucun nombre premier congru à 1 modulo 4 ne vérifie la propriété demandée, car un tel nombre premier divise un entier de la forme $n^2 + 1$ (prendre pour n un représentant de la classe dont le carré vaut $-\overline{1}$).

Montrons maintenant que tout nombre premier congru à 3 modulo 4 vérifie la propriété demandée. Supposons qu'il existe $a, b \in \mathbb{Z}$, avec a non divisible par p, tel que $p \mid (a^2 + b^2)$. Il est alors clair que p ne divise pas b non plus, donc $\overline{a}$ et $\overline{b}$ sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$. On a alors $\overline{a}^2 = -\overline{b}^2$, donc $(\overline{a}\overline{b}^{-1})^2 = -\overline{1}$, ce qui contredit le fait que -1 ne soit pas un résidu quadratique modulo p.

(2) Supposons que l'ensemble des nombres premiers congrus à 1 modulo 4 soit fini et notons-le $\{p_1, ..., p_n\}$. Posons alors $N = (2p_1...p_n)^2 + 1$. Il est clair que ni 2 ni aucun des p_i ne divise N, donc tous ses diviseurs premiers sont congrus à 3 modulo 4. Soit p un des diviseurs premiers de N ; comme p divise $(2p_1...p_n)^2 + 1^2$, alors par la question précédente il divise 1, absurde.

<u>*Solution de l'exercice 8*</u>

Par multiplicativité du symbole de Legendre, on a $\left(\frac{219}{384}\right) = \left(\frac{3}{383}\right)\left(\frac{7}{383}\right)$. Par deux applications de la loi de réciprocité quadratique, on en déduit que $\left(\frac{219}{383}\right) = -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right)$. Puis en réduisant modulo 3 et 73 respectivement, $\left(\frac{219}{383}\right) = -\left(\frac{-1}{3}\right)\left(\frac{18}{73}\right) = \left(\frac{18}{73}\right)$. Une nouvelle fois par multiplicativité, on a $\left(\frac{219}{383}\right) = \left(\frac{2}{73}\right)\left(\frac{3}{73}\right)^2 = \left(\frac{2}{73}\right)$, puis par la proposition 59, on finit par en déduire que $\left(\frac{2}{73}\right) = 1$, donc que 219 est un résidu quadratique modulo

383.

2 Deuxième cours/TD

- Racine primitive -

Soit $n > 1$ et a premier avec n. Dans le premier cours vous avez vu $\omega_n(a)$ l'ordre de a modulo n et vous savez que cet ordre est un diviseur de $\varphi(n)$. Ici nous chercherons des éléments dont l'ordre est pile $\varphi(n)$. Dans la suite de ce cours nous noterons $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ inversibles (c-à-d premiers avec n).

Définition 60. Soit n un entier et x premier avec n. On dit que x est une *racine primitive* modulo n si l'ordre de x est $\varphi(n)$.

Définition 61. Soit n un entier. On dit que $\mathbb{Z}/n\mathbb{Z}$ est *cyclique* s'il existe une racine primitive modulo n.

Essayons d'expliquer pourquoi nous utilisons le nom "cyclique". Soit x une racine primitive, considérons $x, x^2, x^3, \dots, x^{\varphi(n)}$. Tous ces points sont des éléments de $\mathbb{Z}/n\mathbb{Z}$ distincts deux à deux et premiers avec n, donc il s'agit de tous les éléments premiers avec n. De plus si on note $a = x^\alpha$, $b = x^\beta$, $c = x^\gamma$, on aura alors :

$$a \times b \equiv c[n] \iff \alpha + \beta \equiv \gamma[\varphi(n)].$$

Tous les éléments inversibles peuvent donc être placés sur un cycle de taille $\varphi(n)$, l'étude de $(\mathbb{Z}/n\mathbb{Z})^*$ revient juste à l'étude de $\mathbb{Z}/\varphi(n)\mathbb{Z}$, que vous connaissez bien.

Commençons par montrer une proposition sur les ordres.

Proposition 62. Soit $n > 1$, et a, b premiers avec n d'ordres respectifs u et v. Alors il existe un élément c d'ordre $\mathrm{ppcm}(u, v)$.

Démonstration. Intéressons nous d'abord au cas où u et v sont premiers entre eux et regardons w l'ordre de ab. Il est facile de vérifier que $(ab)^{uv} \equiv 1[n]$, donc $w|uv$. Montrons à présent que $u|w$:

$$(ab)^w \equiv 1[n] \implies a^w \equiv b^{-w}[n] \implies a^{wv} \equiv b^{-wv} \equiv 1[n] \implies u|wv \implies u|w$$

L'avant-dernière implication vient de la proposition $a^k \equiv 1[n] \iff \omega_n(a)|k$, et la dernière par l'hypothèse que u et v premiers entre eux. Donc $u|w$ et $v|w$, mais $w|uv$, donc $w = uv$, ce qui achève la démonstration.

Regardons maintenant le cas où u et v ne sont pas premiers entre eux, soit $d = \mathrm{pgcd}(u, v)$. Je vous laisse vérifier que a^d a pour ordre $\frac{u}{d}$, et que $\frac{u}{d}$ et v sont premiers entre eux. Par le paragraphe précédent, il existe un élément d'ordre $\frac{uv}{d} = \mathrm{ppcm}(u, v)$.

Revenons maintenant au problème qui nous intéresse. Pour $n > 1$, nous définissons l'ordre maximal modulo n

$$\Omega_n = \max_{a \text{ premier avec } n} \omega_n(a).$$

Proposition 63.

$$\Omega_n = \mathrm{ppcm}\{\omega_n(a) | a \text{ premier avec } n\}$$

Cette proposition découle facilement de la précédente.

On voit que si Ω_n est l'ordre maximal mod n, alors l'ordre de tous les éléments est un diviseur de Ω_n, ou encore que tous les éléments inversibles a vérifient

$$a^{\Omega_n} \equiv 1[n].$$

- Cyclicité de $\mathbb{Z}/p\mathbb{Z}$ -

Je vous renvoie au cours précédent pour montrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps (c'est-à-dire que tous les éléments sont inversibles) et que par conséquent on peut utiliser les polynômes comme si on était sur les réels. La propriété qui nous intéressera est qu'un polynôme de degré n a au plus n racines.

Remarque 64. Les polynômes ici ne sont pas sur des entiers mais sur des classes de congruences mod p. Ainsi k et $k+p$ ne comptent que pour une seule racine.

Théorème 65. Soit p un premier, $\mathbb{Z}/p\mathbb{Z}$ est cyclique.

Démonstration. Soit Ω_p l'ordre maximal modulo p. Tout d'abord, $\Omega_p|(p-1)$. Ensuite, d'après la section précédente, tous les entiers a premiers avec p vérifient $a^{\Omega_p} \equiv 1[p]$. Le polynôme $X^{\Omega_p}-1$ a donc $(p-1)$ racines. Ainsi $\Omega_p \geqslant (p-1)$, le seul cas possible est $\Omega_p = p-1$. Il existe donc un élément de $\mathbb{Z}/p\mathbb{Z}$ d'ordre $p-1$, $\mathbb{Z}/p\mathbb{Z}$ est cyclique.

Illustrons ce résultat par un exemple, avec $p = 7$. Un peu de tâtonnement permet de trouver que 3 est racine primitive modulo p et on trouve

$$3^0 \equiv 1 \;;\; 3^1 \equiv 3 \;;\; 3^2 \equiv 2 \;;\; 3^3 \equiv 6 \;;\; 3^4 \equiv 4 \;;\; 3^5 \equiv 5$$

Donc pour chaque élément a de $\mathbb{Z}/7\mathbb{Z}$ on associe α l'exposant tel que $a = 3^\alpha$. Ainsi nous pouvons traduire des égalités de produits par des égalités sur les exposants. Par exemple, avec a, b, c premiers avec p

$$4a^2b \equiv 6c^3[7] \iff 4 + 2\alpha + \beta \equiv 3 + 3\gamma[6].$$

Nous pouvons écrire le résultat de cette façon :

$$((\mathbb{Z}/p\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +).$$

Cette écriture signifie qu'il existe une bijection f de $(\mathbb{Z}/p\mathbb{Z})^*$ vers $\mathbb{Z}/((p-1))\mathbb{Z}$ qui transforme l'opération $\times$ en $+$, c-à-d pour tout a, b $f(a \times b) = f(a) + f(b)$ et $f(1) = 0$ (f conserve les neutres, 1 est le neutre pour $\times$ et 0 est le neutre pour $+$).

La ligne se lit de cette façon : "le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ muni de la multiplication est isomorphe au groupe $\mathbb{Z}/(p-1)\mathbb{Z}$ muni de l'addition".

- Cyclicité de $\mathbb{Z}/p^k\mathbb{Z}$ (p premier impair) -

Dans tout ce chapitre, p sera un nombre premier *impair*. Rappellons rapidement que $\varphi(p^k) = (p-1)p^{k-1}$.

Proposition 66. L'ordre de $(p+1)$ modulo p^k est p^{k-1}.

Démonstration. Regardons ce que vaut $(1+p)^{p^{k-1}}$:

$$\begin{aligned}(1+p)^{p^{k-1}} &= 1+\binom{p^{k-1}}{1}p+\binom{p^{k-1}}{2}p^2+\binom{p^{k-1}}{3}p^3+\dots\\ &= 1+p^k+p^{k+1}\cdot\frac{p-1}{2}+p^{k+2}\cdot\frac{(p-1)(p-2)}{6}+\dots\end{aligned}$$

Nous voyons que la puissance de p augmente de plus en plus lorsqu'on va vers la droite. Je vous laisse vous convaincre du résultat suivant :

$$(1+p)^{p^{k-1}} = 1+\lambda\cdot p^k \text{ avec } p \not| \lambda.$$

Ce résultat nous dit déjà que l'ordre de $(1+p)$ modulo p^k est un diviseur de p^{k-1}, c'est à dire une puissance de p. Si on suppose que l'ordre de $(1+p)$ est strictement plus petit que p^{k-1}, alors l'ordre serait un diviseur de p^{k-2} et on aurait

$$(1+p)^{p^{k-1}} = \left((1+p)^{p^{k-2}}\right)^p = (1+\mu\cdot p^k)^p = \dots = 1+\nu\cdot p^{k+1},$$

ce qui est en contradiction avec le résultat précédent. Donc l'ordre de $(p+1)$ modulo p^k est p^{k-1}.

Maintenant, pour obtenir $\varphi(p^k)$, il ne nous manque qu'un facteur $(p-1)$. Dans la section précédente nous avons montré qu'il est toujours possible de trouver une racine d'ordre $(p-1)$ modulo p. Donc prenons un entier a qui est une racine primitive modulo p et regardons ω son ordre modulo p^k :

$$a^\omega \equiv 1[p^k] \implies a^\omega \equiv 1[p] \implies (p-1)|\omega.$$

Théorème 67. Soit p un premier impair et $k \geqslant 1$ un entier, $\mathbb{Z}/p^k\mathbb{Z}$ est cyclique.

Démonstration. Regardons ce que nous avons : nous savons que tous les ordres modulo p^k divisent $\varphi(p^k) = (p-1)p^{k-1}$, et nous avons un élément d'ordre p^{k-1} et un élément dont l'ordre est un multiple de $p-1$. Par la première propriété du cours il existe un élément dont l'ordre est le ppcm des deux, qui sera exactement $(p-1)p^{k-1}$.

Comme pour la section précédente, écrivons ce résultat sous forme d'un isomorphisme de groupes :

$$((\mathbb{Z}/p^k\mathbb{Z})^*,\times) \simeq (\mathbb{Z}/((p-1)p^{k-1})\mathbb{Z},+).$$

- **Structure de** $(\mathbb{Z}/2^k\mathbb{Z})^*$ -

Commençons par regarder l'exemple de $\mathbb{Z}/8\mathbb{Z}$. Cherchons une racine primitive, c-à-d un élément d'ordre 4.

$$1^1 \equiv 1[8] \ ;\ 3^2 = 9 \equiv 1[8] \ ;\ 5^2 = 25 \equiv 1[8] \ ;\ 7^2 = 49 \equiv 1[8],$$

tous les éléments sont d'ordre 1 ou 2. Donc $\mathbb{Z}/8\mathbb{Z}$ n'est pas cyclique. La structure de $(\mathbb{Z}/2^k\mathbb{Z})^*$ est un peu plus compliquée.

Théorème 68. Soit $k \geqslant 3$,

$$((\mathbb{Z}/2^k\mathbb{Z})^*,\times) \simeq ((\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2^{k-2}\mathbb{Z}),+).$$

Expliquons ce qu'est $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z})$. Il s'agit de tous les couples $(\varepsilon; \alpha)$ avec $\varepsilon \in \mathbb{Z}/2\mathbb{Z}$ et $\alpha \in \mathbb{Z}/2^{k-2}\mathbb{Z}$. L'addition se fait de la manière suivante :

$$(\varepsilon; \alpha) + (\varepsilon'; \alpha') = \left(\varepsilon + \varepsilon'[2]; \alpha + \alpha'[2^{k-2}]\right).$$

Démonstration abrégée. Nous n'allons pas faire cette démonstration dans son intégralité, mais voici les points importants :

– Utiliser l'exemple de $\mathbb{Z}/8\mathbb{Z}$ pour prouver qu'il est impossible que $(\mathbb{Z}/2^k\mathbb{Z})$ soit cyclique
– Montrer que $5 = (1+4)$ est d'ordre 2^{k-2} de la même façon qu'on avait montré l'ordre de $(1+p)$ mod p^k
– Montrer que la fonction

$$\begin{array}{rccc} f: & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z}) & \to & (\mathbb{Z}/2^k\mathbb{Z})^* \\ & (\varepsilon, \alpha) & \mapsto & \epsilon \cdot 2^{k-1} + 5^{\alpha} \end{array}$$

est un isomorphisme de groupe (c-à-d que f est une bijection qui transform $+$ en $\times$).

- Exercices -

Certains des exercices sont sur les résultats du cours précédent. Au début de chaque sous-section j'ai mis le résultat dont vous avez besoin.

Cyclicité de $\mathbb{Z}/p\mathbb{Z}$

Théorème 69. Soit p un nombre premier impair et $k \geqslant 1$. Le groupe $\mathbb{Z}/p^k\mathbb{Z}$ est cyclique, c'est-à-dire qu'il existe une racine primitive x telle que la famille $(x^n)_{n\in\mathbb{N}}$ va passer par toutes les classes d'equivalence (premières avec p) modulo p^k. On peut considérer que

$$((\mathbb{Z}/p^k\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/((p-1)p^{k-1})\mathbb{Z}, +).$$

Pour les puissances de 2 c'est un peu plus compliqué : si $k \geqslant 3$,

$$((\mathbb{Z}/2^k\mathbb{Z})^*, \times) \simeq \left((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z}), +\right).$$

Exercice 1 Combien y a-t-il de classes a modulo 343 telles que $a^{70} \equiv 1[343]$? Même question modulo 128.

Exercice 2 Soit n divisible par deux premiers impairs distincts. Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas cyclique.

Exercice 3 Déterminer tous les entiers n tels qu'il existe un entier a vérifiant $a^{\frac{\varphi(n)}{2}} \equiv -1[n]$ (φ est l'indicatrice d'Euler).

Exercice 4 Trouver les entiers n tels que $37 | 2 \cdot 6^{4n+3} + 2^n$.

Exercice 5 Trouver tous les couples (a, b) solutions de $a^3 \equiv b^3[121]$. Même questions avec $[169]$.

Résidus quadratiques

Théorème 70. (Réciprocité quadratique) Soient p et q deux nombres premiers impairs distincts. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre. Vous pouvez utiliser les trois formules suivantes :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \ ; \ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1)}{2}} \ ; \ \left(\frac{2}{p}\right) = (-1)^{fracp^2-1)8}$$

Exercice 6 Quand 5 est-il un carré mod p ? Et 7 ? Et les deux ?

Exercice 7 Calculer $\left(\frac{37}{97}\right)$.

Exercice 8 Combien y a-t-il de “résidus quadratiques" mod pq ? Et mod p^n ?

Exercice 9 Trouver les solutions entières de $4x^2 + 77y^2 = 487z^2$.

Lemme LTE

Lemme 71. (Lifting The Exponent) Soit p un nombre premier impair et x, y deux entiers tels que $p|x-y$ mais $p \not| x$, $p \not| y$. Alors

$$\nu_p(x^n - y^n) = \nu_p(x-y) + \nu_p(n)$$

Exercice 10 Trouver les entiers n tels qu'il existe x, y, k avec $x$et y premiers entre eux et

$$3^n = x^k + y^k.$$

Exercice 11 Soit p un premier impair et m un entier tel qu'il existe des entiers $x, y > 1$ vérifiant

$$\frac{x^p + y^p}{2} = \left(\frac{x+y}{2}\right)^m.$$

Montrer que $m = p$.

Exercice 12 Trouver toutes les solutions entières de

$$x^{2009} + y^{2009} = 7^k$$

- Corrigé des exercices -

<u>*Solution de l'exercice 1*</u> Tout d'abord, $343 = 7^3$, le groupe $(\mathbb{Z}/343\mathbb{Z})^a st$ est donc cyclique et isomorphe à $\mathbb{Z}/294\mathbb{Z}$ ($294 = 6 \cdot 7^2$). Soit x une racine primitive et α tel que $a = x^\alpha$:

$$a^{70} \equiv 1[343] \iff 70\alpha \equiv 0[294] \iff 21|\alpha,$$

ce qui nous donne 14 classes d'équivalences mod 294 pour α qui correspondent à 14 classes d'équivalence modulo 343 pour a.

Maintenant, pour le modulo 128, c'est légèrement différent puisque

$$((\mathbb{Z}/128\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(32)\mathbb{Z}, +).$$

On cherche donc tous les couples (ε, k) avec $\varepsilon \in \mathbb{Z}/2\mathbb{Z}$ et $k \in \mathbb{Z}/32\mathbb{Z}$ qui vérifient $70\varepsilon \equiv 0[2]$ et $70k \equiv 0[32]$. On voit rapidement que l'on a deux choix pour ε et deux choix pour k, ce qui correspond à 4 classes d'équivalence mod 128.

<u>*Solution de l'exercice 2*</u> Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la décomposition en facteurs premiers de n. Je vous laisse utiliser le théorème chinois pour montrer que pour tout a, si on note $\omega_j(a)$ l'ordre de a mod j :

$$\omega_n(a) = ppcm\left(\omega_{p_1^{\alpha_1}}(a), p_2^{\alpha_2}(a), \dots, p_k^{\alpha_k}(a)\right).$$

Comme l'ordre d'un élément mod j divise $\varphi(j)$, on a que

$$\omega_n(a) \Big| \mathrm{ppcm}\left((p_1-1)p_1^{\alpha_1-1},(p_2-1)p_2^{\alpha_2-1},\dots,(p_k-1)p_k^{\alpha_k-1}\right)$$

Or on veut un élément dont l'ordre soir $\varphi(n)$, qui est le produit des termes de droite. Le ppcm de ces termes est égal à leur produit ssi ils sont tous premiers entre eux deux à deux, mais il est facile de voir que si n est divisible par deux premiers impairs distincts, deux de ces termes sont pairs. Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas cyclique.

Je vous laisse faire la généralisation suivante : $\mathbb{Z}/n\mathbb{Z}$ est cyclique ssi $n = 2, 4, p^k$ ou $2p^k$.

<u>*Solution de l'exercice 3*</u> On veut un entier a tel que $a^{\frac{\varphi(n)}{2}} \equiv -1[n]$, donc que $\omega_n(a) \not| \frac{\varphi(n)}{2}$. On utilise la même technique que précédemment pour calculer l'ordre maximal mod n en fonction de la décomposition en facteurs premiers de n, et on voit que les seuls n possibles sont 4, p^k et $2p^k$ (p premier impair).

<u>*Solution de l'exercice 4*</u> Ici il n'y a rien de sorcier, nous allons regarder les suites des 6^m et 2^n modulo 37 :

$$6 \to 36 = -1 \to -6 \to 1 \to 6 \to -1 \to \dots$$

donc $2 \cdot 6^{4n+3}$ est toujours congru à 12 mod 37.

$$2 \to 4 \to 8 \to 16 \to 32 \to 27 \to 17 \to 34 \to 31 \to 25 \to 13 \to 26 \to 15 \to 30 \to 23 \to 9 \to 18 \to -1$$

avec après la même suite mais avec des moins partout. Donc l'ordre de 2 est 36, et $2^n \equiv -12[37]$ ssi $n \equiv 10[36]$.

<u>*Solution de l'exercice 5*</u> Tout d'abord, on écarte les cas divisibles par 11 : si a et b sont divisibles par 11, l'équation est vérifiée. Maintenant on s'intéresse à ceux qui sont premiers avec 11. Comme 121 est une puissance de 11, on peut utiliser la cyclicité de $(\mathbb{Z}/p^k\mathbb{Z})^*$. Soit x une racine primitive et α, β tels que $a = x^\alpha$, $b = x^\beta$.

$$a^3 \equiv b^3[121] \iff 3\alpha \equiv 3\beta[110] \iff \alpha \equiv \beta[110]$$

la dernière équivalence puisque 3 est premier avec 110. Donc $a^3 \equiv b^3[121]$ ssi $a \equiv b[121]$ou a, b multiples de 11.

Pour 169, le cas a et b sont divisibles par 13 reste le même. Maintenant regardons la cyclicité avec les mêmes notations.

$$a^3 \equiv b^3[169] \iff 3\alpha \equiv 3\beta[156] \iff \alpha \equiv \beta[52]$$

il y a donc plus de solutions : $\alpha \equiv \beta[156]$, $\alpha \equiv \beta + 52[156]$ ou $\alpha \equiv \beta + 104[156]$. Pour voir à quoi cela correspond mod 169, il faut trouver une racine troisième de l'unité mod 169, 22 marche ($22^2 \equiv 146$, $22^3 \equiv 1$). Les solutions sont donc : a, b multiples de 13 ou $a \equiv b[169]$ ou $a \equiv 22 \cdot b[169]$ ou $a \equiv 146 \cdot b[169]$.

<u>*Solution de l'exercice 6*</u> Nous allons utiliser la réciprocité quadratique : $\left(\frac{p}{5}\right)\left(\frac{5}{p}\right) = 1$ puisque $5 \equiv 1[4]$, donc 5 est un carré mod p ssi p est un carré mod 5 ssi $p \equiv \pm 1[5]$.

Même topo pour 7 mais il faut faire une disjonction de cas :

– si $p \equiv 1[4]$, alors $\left(\frac{p}{7}\right)\left(\frac{7}{p}\right) = 1$ et 7 est un carré mod p ssi p est un carré mod 7 ssi $p \equiv 1, 2$ ou $4[7]$.

– si $p \equiv 3[4]$, alors $\left(\frac{p}{7}\right)\left(\frac{7}{p}\right) = -1$ et 7 est un carré mod p ssi p n'est pas un carré mod 7 ssi $p \equiv 3, 5$ ou $6[7]$.

Nous pouvons tout regrouper en disant que 7 est un carré mod p ssi $p \equiv 1, 3, 9, 19, 25$ ou $27[28]$.

Pour que 5 et 7 soient tous les deux des carré mod p, il faut que les deux conditions soient vérifiées. Je laisse au lecteur le soin de déterminer les 12 classes d'équivalences mod 140 que cela donnera en utilisant le théorème chinois.

Solution de l'exercice 7 Appliquons la réciprocité quadratique :

$$\begin{array}{rcll}
\left(\frac{37}{97}\right) & = & \left(\frac{97}{37}\right) & \text{puisque } \left(\frac{37}{97}\right)\left(\frac{97}{37}\right) = 1 \\
 & = & \left(\frac{23}{37}\right) & \text{puisque seule la classe de 97 mod 37 compte} \\
 & = & \left(\frac{37}{23}\right) = \left(\frac{14}{23}\right) & \text{puisque } \left(\frac{37}{23}\right)\left(\frac{23}{37}\right) = 1 \\
 & = & \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) & \text{puisque le symbole de Legendre est multiplicatif} \\
 & = & \left(\frac{2}{23}\right) \cdot -\left(\frac{23}{7}\right) & \text{puisque } \left(\frac{7}{23}\right)\left(\frac{23}{7}\right) = -1 \\
 & = & -1 & \text{puisque } \left(\frac{2}{23}\right) = 1 \text{ et } \left(\frac{2}{7}\right) = 1
\end{array}$$

Solution de l'exercice 8 Nous allons juste considérer que les "résidus quadratiques" mod n sont parmi les entier premiers avec n. La technique pour étudier $\mathbb{Z}/pq\mathbb{Z}$ est d'étudier séparément $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ et d'utiliser le théorème chinois. Je laisse au lecteur le soin de vérifier que a résidu quadratique mod pq ssi a résidu quadratique mod p et a résidu quadratique mod q. Modulo p il y a $\frac{p-1}{2}$ résidus quadratiques, et mod q il y en a $\frac{q-1}{2}$. Le nombre total de résidus quadratiques mod pq est donc $\frac{(p-1)(q-1)}{4}$.

Pour regarder mod p^k nous allons procéder autrement et profiter du fait que $(\mathbb{Z}/p^k\mathbb{Z})^*$ est cyclique. On écrit tous les élements comme les puissances x^n d'une racine primitive x. Il est facile de vérifier que x^n est un résidu quadratique ssi n est pair. Les résidus quadratiques correspondent donc à la moitié des éléments, c'est-à-dire $\frac{(p-1)p^{k-1}}{2}$.

Solution de l'exercice 9 Nous allons profiter que 487 est un carré. L'ésuation implique que $4x^2 = -77y^2[487]$, donc si -77 n'est pas un carré mod 487, l'équation n'a pas de solutions. Je laisse au lecteur le soin de vérifier que $\left(\frac{-77}{487}\right) = -1$.

Solution de l'exercice 10 Tout d'abord, k doit être impair. En effet si k était pair, x^k et y^k seraient des carrés et il est facile de vérifier $3|a^2 + b^2 \implies 3|a$ et $3|b$ (il suffit de vérifier toutes les congruences possibles mod 3 pour a et b). Supposons qu'il existe un premier impair p qui divise $x + y$, alors par le lemme LTE, on aurait

$$v_p(3^n) = v_p(x^k + y^k) = v_p(x + y) + v_p(k) \geqslant 1.$$

On en déduit donc que $p|3^n$, et donc $p = 3$. Cela signifie que $x+y = 3^m$, pour un entier positif m. On remarque que $n = v_3(k) + m$. Distinguons deux cas :

– si $m > 1$: Je vous laisse prouver que $3^a \geqslant a+2$ et donc $v_3(k) \leqslant k-2$. On peut supposer $x > y$ et comme $x + y = 3^m \geqslant 9$, on aura $x \geqslant 5$, mais aussi $x > \frac{3^m}{2}$. Nous utilisons maintenant quelques inégalités :

$$x^k + y^k \geqslant x^k \geqslant \frac{3^m}{2}5^{k-1} > 3^m 5^{k-2} \geqslant 3^{m+v_3(k)} = 3^n$$

ce qui est une contradiction.

– si $m = 1$, alors on a $x = 2$ et $y = 1$, et $3^{1+v_3(k)} = 1 + 2^k$. On remarque que $3^{1+v_3(k)}|k$, donc $3^{1+v_3(k)} \leqslant k$ et $2^k + 1 \leqslant 3k$, et donc $k \leqslant 3$. Il ne reste pas beaucoup de cas à vérifier et la seule solution est :

$$3^2 = 1^3 + 2^3.$$

<u>Solution de l'exercice 11</u> Par la convexité de $x \mapsto x^p$, $\frac{x^p+y^p}{2} \geqslant \left(\frac{x+y}{2}\right)^p$. Donc comme $\frac{x^p+y^p}{2} = \left(\frac{x+y}{2}\right)^m$ il s'ensuit que $m \geqslant p$. Soit $d = pgcd(x, y)$, $x = dx'$, $y = dy'$. L'équation se réécrit

$$2^{m-1}(x'^p + y'^p) = d^{m-p}(x' + y')^m.$$

Soit q un diviseur premier impair de $x'+y'$. Par le lemme LTE, $v_q(x'^p+y^p) = v_q(x+y)+v_q(p)$ et d'autre part $v_q(d^{m-p}(x' + y')^m) \geqslant mv_q(x + y)$. Donc $m \geqslant 2$ et $p \geqslant 2$, ce qui aboutit à une contradiction. À présent regardons v_2 : on obtient

$$m - 1 + v_2(x' + y') \geqslant mv_2(x' + y'),$$

donc $v_2(x' + y') \leqslant 1$, $x' + y' \leqslant 2$, donc $x' = y' = 1$ et $m = p$.

<u>Solution de l'exercice 12</u> Déjà, $2009 = 7^2 \times 41$. Comme $x + y$ divise $x^{2009} + y^{2009}$, $x + y$ est une puissance de 7. On remarque aussi que si x et y sont multiples de 7, on peut tout diviser par 7 et juste changer l'exposant k ; on peut donc supposer que x et y sont premiers avec 7. Le lemme LTE nous dit que $v_7(x^{2009} + y^{2009}) = v_7(x + y) + v_7(2009) = v_7(x + y) + 2$, donc $x^{2009} + y^{2009} = 49(x + y)$, donc

$$\frac{x^{2009} + y^{2009}}{x + y} = x^{2008} - x^{2007}y + x^{2006}y^2 - \cdots + y^{2008} = 49$$

Mais il estfacile de vérifier que ce terme est beaucoup plus grand que 49. Par exemple, si on suppose $x > y$, on aura toujours $(x^{2008} - x^{2007}y) \geqslant 1$; $(x^{2006}y^2 - x^{2005}y^3) \geqslant 1$ et ainsi de suite, la somme totale sera au moins égale à 1004. Il n'y a donc pas de solutions possibles.

3 Troisième cours/TD

- Polynômes cyclotomiques -

L'essentiel de ce cours provient de l'article *Elementary Properties of Cyclotomic Polynomials* de Yimin Ge.

Définition : Soit $n \in \mathbb{N}^*$. Une racine n-ième de l'unité est un nombre complexe ζ tel que $\zeta^n = 1$ (autrement dit, une racine complexe du polynôme $X^n - 1$). On dit que c'est une racine primitive n-ième si de plus $\zeta^k \neq 1$ pour $k = 1, \dots n - 1$. Le plus petit $k \geqslant 1$ tel que $\zeta^k = 1$ est appelé l'ordre de ζ, et noté $\mathrm{ord}(\zeta)$.

Les racines n-ièmes de l'unité sont exactement les nombres complexes $e^{\frac{2ik\pi}{n}}$, $k = 0, \dots, n - 1$. Les racines primitives sont celles de la forme $e^{\frac{2i\pi k}{n}}$, avec k premier avec n. En particulier, il y a exactement $\varphi(n)$ racines primitives n-ièmes.

Définition : Soit n un entier strictement positif. Alors le n-ième polynôme cyclotomique, noté Φ_n, est le polynôme unitaire qui a pour racines exactement les racines primitives n-ièmes, c'est-à-dire

$$\Phi_n(X) = \prod_{\substack{\zeta^n=1 \\ \mathrm{ord}(\zeta)=n}} (X - \zeta).$$

Remarque : Dans le cas particulier où $n = p$ est premier, toutes les racines p-ièmes différentes de 1 sont primitives, et donc

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + \ldots + X^{p-1}.$$

Proposition : Soit n un entier strictement positif. Alors

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{IV.1}$$

Démonstration. $X^n - 1$ n'a que des racines simples qui sont exactement les racines n-ièmes de l'unité. D'autre part, si ζ est une racine n-ième de l'unité et $d = \mathrm{ord}(\zeta)$, alors ζ est une racine de Φ_d, et comme $d|n$, ζ est une racine du côté droit. Ainsi le côté et le côté gauche ont les mêmes racines, qui sont simples des deux côtés. Puisqu'ils sont unitaires, ils sont égaux.

Remarque : Si on compare les degrés de ces polynômes, on retrouve l'identité bien connue

$$n = \sum_{d|n} \varphi(d).$$

Lemme : Soient f et g des polynômes unitaires à coefficients rationnels. Si fg a des coefficients entiers, alors f et g sont en fait à coefficients entiers.

Démonstration. On écrit $f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0$ et $g(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0$, et on note $M > 0$ le plus petit dénominateur commun des a_i, $N > 0$ le plus petit dénominateur commun des b_i. Alors

$$Mf(X) = A_m X^m + \ldots + A_1 X + A_0$$

avec des entiers A_i premiers entre eux dans leur ensemble, et

$$Ng(X) = B_n X^n + \ldots + B_1 X + B_0$$

avec des entiers B_j premiers entre eux dans leur ensemble. De plus,

$$MNfg(X) = A_m B_n X^{m+n} + \ldots + (A_1 B_0 + B_1 A_0)X + A_0 B_0$$

a des coefficients entiers divisibles par MN, en utilisant le fait que fg est à coefficients entiers. Supposons que $MN \neq 1$, et soit dans ce cas un diviseur premier p de MN. Il existe alors i, j tels que p ne divise pas A_i et p ne divise pas B_j. On note I, J les plus grands i et j vérifiant cela. Le coefficient devant X^{I+J} dans $MNf(X)g(X)$ est alors congru à $A_I B_J$ modulo p, ce qui contredit le fait qu'il soit divisible par MN.

Proposition : Soit n un entier strictement positif. Alors Φ_n est un polynôme à coefficients entiers.

Démonstration. On raisonne par récurrence forte sur n. Le cas $n = 1$ est clair puisque $\Phi_1 = X-1$. Supposons que Φ_k est à coefficients entiers pour tout $k < n$. Alors $X^n - 1 = \Phi_n(X) g_n(X)$ où $g_n(X) = \prod_{d|n,\, d<n} \Phi_d$ est à coefficients entiers par hypothèse de récurrence, donc $\Phi_n(X)$ est à coefficients rationnels, et le lemme précédent permet de conclure.

La formule (IV.1) peut, grâce à un outil appelé inversion de Möbius, nous donner une formule « explicite »pour les polynômes cyclotomiques.

- Inversion de Möbius -

Définition : Le fonction de Möbius $\mu : \mathbb{N} \longrightarrow \{-1, 0, 1\}$ est définie de la manière suivante :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n \text{ est sans carré et produit de } k \text{ diviseurs premiers distincts} \\ 0 & \text{sinon.} \end{cases}$$

Proposition Soit $n \in \mathbb{N}^*$. Alors

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geqslant 2 \end{cases}$$

Démonstration. Le cas $n = 1$ étant clair, supposons $n \geqslant 2$. On pose

$$m = \prod_{\substack{p \text{ premier} \\ p|n}} p$$

le produit de tous les nombres premiers distincts divisant n. Alors par définition de μ, on peut éliminer les diviseurs de n qui sont divisibles par un carré, et on a

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d).$$

Soit p un facteur premier de m (il y en a au moins un car $n \geqslant 2$). Alors

$$\sum_{d|m} \mu(d) = \sum_{d|\frac{m}{p}} (\mu(d) + \mu(pd)) = \sum_{d|\frac{m}{p}} (\mu(d) - \mu(d)) = 0.$$

Théorème : (Inversion de Möbius) Soient $F, f : \mathbb{N} \longrightarrow \mathbb{N}$ deux fonctions telles que

$$F(n) = \sum_{d|n} f(d).$$

Alors

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} F(d) \mu\left(\frac{n}{d}\right).$$

Démonstration. Il est clair que les deux formules proposées sont les mêmes, donc il suffit de montrer la première. Or on a, en remplaçant F par son expression en fonction de f,

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{t|\frac{n}{d}} f(t) = \sum_{t|n} f(t) \sum_{d|\frac{n}{t}} \mu(d).$$

La proposition précédente nous dit que $\sum_{d|\frac{n}{t}} \mu(d)$ est non-nul si et seulement si $n = t$, et égal à 1 dans ce cas-là, d'où le résultat.

L'inversion de Möbius existe aussi sous forme multiplicative, la preuve étant la même en remplaçant les sommes par des produits.

Théorème : (Inversion de Möbius multiplicative) Soient $F, f : \mathbb{N} \longrightarrow \mathbb{N}$ deux fonctions telles que

$$F(n) = \prod_{d|n} f(d).$$

Alors

$$f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} F(d)^{\mu\left(\frac{n}{d}\right)}.$$

Exemple Appliquant l'inversion de Möbius à $F = \mathrm{id}$ et $f = \varphi$ la fonction indicatrice d'Euler, reliées par la relation

$$n = \sum_{d|n} \varphi(d),$$

on obtient

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{d|n} d\mu\left(\frac{n}{d}\right).$$

Si par exemple $n = p^k$, on retrouve bien $\varphi(p^k) = p^k - p^{k-1}$.

De même, appliquant l'inversion de Möbius multiplicative à la formule (IV.1) prise pour $\varphi(n) + 1$ valeurs entières distinctes de X et en utilisant un polynôme interpolateur de Lagrange, on trouve la formule suivante pour les polynômes cyclotomiques :

Théorème : Soit n un entier strictement positif. Alors

$$\Phi_n(X) = \prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

Grâce à cette expression, on peut prouver le résultat suivant, qui permet de relier deux polynômes cyclotomiques dont les indices se divisent l'un l'autre :

Proposition : Soit $n \in \mathbb{N}^*$ et p un nombre premier. Alors

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & \text{si } p|n \\ \frac{\Phi_n(X^p)}{\Phi_n(X)} & \text{sinon.} \end{cases}$$

Démonstration. On a

$$\begin{aligned}\Phi_{pn}(X) &= \prod_{d|pn}\left(X^{\frac{pn}{d}}-1\right)^{\mu(d)}\\ &= \prod_{d|n}\left(X^{\frac{pn}{d}}-1\right)^{\mu(d)}\prod_{\substack{d|pn\\ d\nmid n}}\left(X^{\frac{pn}{d}}-1\right)^{\mu(d)}\end{aligned}$$

.

Si $p|n$, alors $d|pn$ et $d \nmid n$ impliquent que $p^2|d$, donc $\mu(d)=0$ et on a bien $\Phi_{pn}(X)=\Phi_n(X^p)$ dans ce cas. Si maintenant $p \nmid n$, alors

$$\begin{aligned}\Phi_n(X) &= \prod_{d|n}\left(X^{\frac{pn}{d}}-1\right)^{\mu(d)}\prod_{d|n}\left(X^{\frac{pn}{pd}}-1\right)^{\mu(pd)}\\ &= \prod_{d|n}\left(X^{\frac{pn}{d}}-1\right)^{\mu(d)}\prod_{d|n}\left(X^{\frac{n}{d}}-1\right)^{-\mu(d)}\\ &= \frac{\Phi_n(X^p)}{\Phi_n(X)}.\end{aligned}$$

Remarque : En particulier, on retrouve bien, pour p premier, $\Phi_p(X)=\frac{\Phi_1(X^p)}{\Phi_1(X)}=\frac{X^p-1}{X-1}$.

Le corollaire suivant est alors immédiat :

Corollaire Soit p premier et $n,k\in\mathbb{N}^*$. Alors

$$\Phi_{p^k n}(X)=\begin{cases}\Phi_n(X^{p^k}) & \text{si } p|n\\ \frac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})} & \text{sinon.}\end{cases}$$

- Diviseurs premiers des valeurs entières prises par un polynôme cyclotomique -

Nous savons que les polynômes cyclotomiques sont à coefficients entiers, donc nous allons pouvoir les étudier modulo des entiers. En particulier, nous allons classifier les diviseurs premiers de $\Phi_n(x)$ pour $n\geqslant 1$ et x entiers.

Lemme : Soit p un nombre premier. Si X^n-1 a une racine double modulo p, alors $p|n$.

Démonstration. Par hypothèse, $X^n-1 \pmod p$ a un pgcd de degré supérieur à 1 avec sa dérivée nX^{n-1}, ce qui est possible seulement si cette dernière est nulle, c'est-à-dire si $p|n$.

Proposition : Soit $n\in\mathbb{N}^*$, d un diviseur strict de n et x un entier. Si $\Phi_n(x)$ et $\Phi_d(x)$ ont un diviseur premier commun p, alors $p|n$.

Démonstration On a $x^n-1=\prod_{t|n}\Phi_t(x)$ d'après la formule (IV.1). Ainsi, X^n-1 a une racine double modulo p en $X=x$, et par le lemme précédent, $p|n$.

Nous arrivons à un résultat clé du cours, qui est celui qui va servir dans la plupart des applications :

Théorème : (Résultat fondamental) Soit $n \in \mathbb{N}^*$, $x \in \mathbb{Z}$. Alors tout diviseur premier p de $\Phi_n(x)$ vérifie

– $p \equiv 1 \pmod n$ si x est d'ordre n modulo p

– $p|n$ sinon.

Démonstration. Soit p un diviseur premier de $\Phi_n(x)$. x est premier avec p car $p|\Phi_n(x)|x^n-1$, et on peut donc poser $k = \mathrm{ord}_p(a)$ (qui divise n).

Si $k = n$, alors $p \equiv 1 \pmod n$ par le petit théorème de Fermat.

Sinon, $0 \equiv x^k - 1 \equiv \prod_{d|k} \Phi_d(x) \pmod p$, donc il existe un diviseur d de k tel que $p|\Phi_d(x)$. Mais $d|k|n$ et $d < n$, donc donc d'après la proposition précédente, $p|n$.

Un autre résultat qui peut être utile est le suivant :

Proposition : Soient a et b des entiers positifs. S'il existe un entier x tel que

$$\mathrm{pgcd}(\Phi_a(x), \Phi_b(x)) > 1$$

alors $\frac{a}{b}$ est une puissance de p.

Démonstration. Supposons que p est un diviseur premier commun de $\Phi_a(x)$ et de $\Phi_b(x)$. Nous allons montrer que $\frac{a}{b}$ est une puissance de p. Pour cela, écrivons $a = p^\alpha A$, $b = p^\beta B$ avec A, B non divisibles par p et montrons que $A = B$.

Première étape : Nous allons montrer que $p|\Phi_A(x)$. C'est évident pour $\alpha = 0$. Si $\alpha > 1$, on a vu que, A étant premier avec p,

$$\Phi_a(X) = \frac{\Phi_A(X^{p^\alpha})}{\Phi_A(X^{p^{\alpha-1}})},$$

et donc

$$0 \equiv \Phi_a(x) \equiv \frac{\Phi_A(x^{p^\alpha})}{\Phi_A(x^{p^{\alpha-1}})} \pmod p,$$

ce qui implique que $\Phi_A(x^{p^\alpha}) \equiv 0 \pmod p$. D'autre part, si on itère $x^p \equiv x \pmod p$, on obtient que $x^{p^\alpha} \equiv x \pmod p$, d'où $\Phi_A(x) \equiv \Phi_A(x^{p^\alpha}) \equiv 0 \pmod p$. De même, on a $p|\Phi_B(x)$.

Deuxième étape : Puisque p divise $\Phi_a(x)$ et $\Phi_b(x)$, il divise $x^a - 1$ et $x^b - 1$, donc il divise $\mathrm{pgcd}(x^a - 1, x^b - 1) = |x^{\mathrm{pgcd}(a,b)} - 1|$. Posons $k = \mathrm{pgcd}(A, B)$ et supposons que $A \neq B$. Alors k est strictement inférieur à au moins l'un des entiers A et B, disons A. On a

$$0 \equiv x^k - 1 \equiv \prod_{d|k} \Phi_d(x) \pmod p,$$

donc il existe un diviseur d de k, qui est un diviseur strict de A, tel que $p|\Phi_d(x)$. Par la propriété précédant le résultat fondamental, on en conclut $p|A$, qui est une contradiction. Donc $A = B$.

- Applications et exercices -

Le résultat que nous venons de voir permet de prouver un cas particulier du théorème de Dirichlet sur les nombres premiers dans les progressions arithmétiques :

Théorème : (Dirichlet) Soit $n \in \mathbb{N}^*$. Alors il existe une infinité de nombres premiers p congrus à 1 modulo n.

Démonstration Le cas $n = 1$ correspond à l'infinité des nombres premiers tout court, donc est clair. Nous pouvons cependant nous en inspirer pour la preuve du cas $n \geqslant 2$. En effet, la preuve de l'infinité des nombres premiers consiste à supposer qu'il n'y a qu'un nombre fini $p_1, \dots, p_k$ de nombres premiers, et d'évaluer le polynôme $X + 1$ en $p_1 \dots p_k$ pour obtenir une contradiction. L'idée ici est la même : supposons qu'il n'y a qu'un nombre fini $p_1 \dots p_k$ de nombres premiers congrus à 1 modulo n. On pose

$$m = p_1 \dots p_k \prod_{\substack{p|n \\ p \text{ premier}}} p.$$

Le produit à utiliser est un peu plus complexe car il faut aussi éliminer les facteurs premiers de n. Etant donné que $n \geqslant 2$, on a $m > 1$. Le polynôme à utiliser va être Φ_n : puisque c'est un polynôme unitaire non-constant, il existe un entier k tel que $\Phi_n(m^k) > 1$. Soit alors q un diviseur premier de $\Phi_n(m^k)$. q divise $m^{kn} - 1$, donc q est premier avec m. Ainsi, q n'est pas parmi les p_i, donc n'est pas congru à 1 modulo n, et ne divise pas n. Ceci est une contradiction avec notre résultat fondamental.

Exercice 1 (IMO Shortlist 2006) Trouver toutes les solutions entières de l'équation

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

Exercice 2 Soit $a > 1$ un entier fixé. Montrer que $\frac{p-1}{\text{ord}_p(a)}$ est non borné lorsque p parcourt l'ensemble des nombres premiers.

Exercice 3 (IMO Shortlist 2002, généralisation) Soient $p_1, \dots, p_n$ des nombres premiers impairs. Montrer que $2^{p_1 p_2 \cdots p_n} + 1$ a au moins $2^{2^{n-1}}$ diviseurs.

- Solution des exercices -

<u>*Solution de l'exercice 1*</u> L'équation équivaut à

$$\Phi_7(x) = (y - 1)(1 + \ldots + y^4).$$

Remarquons que le côté gauche est toujours strictement positif, et que donc y doit être supérieur à 2. Le résultat fondamental nous dit que tout diviseur premier du côté gauche soit est égal à 7, soit est congru à 1 modulo 7. Ainsi, tout diviseur positif du côté gauche est soit divisible par 7, soit congru à 1 modulo 7. $y - 1$ étant un tel diviseur, on a $y \equiv 1$ ou $2 \pmod 7$. Dans ce cas, $1 + y + \ldots + y^4 \equiv 5$ ou $3 \pmod 7$, ce qui est une contradiction car il devrait aussi être congru à 0 ou 1 modulo 7. L'équation n'a donc pas de solutions.

<u>*Solution de l'exercice 2*</u> La solution utilise le lemme suivant, qui a déjà un intérêt en soi :

Lemme Soit $n \in \mathbb{N}^*$. Il existe un nombre premier $p > a$ tel que les n entiers

$$p+1, 2p+1, \dots, np+1$$

ne sont pas premiers.

Démonstration. Choisissons $p_1, \dots, p_n$ des nombres premiers distincts strictement plus grands que n, et considérons le système de congruences

$$\begin{cases} x+1 & \equiv & 0 & \pmod{p_1^2} \\ 2x+1 & \equiv & 0 & \pmod{p_2^2} \\ & \vdots & & \\ nx+1 & \equiv & 0 & \pmod{p_n^2}, \end{cases}$$

qui, puisque $2, \dots, n$, étant plus petits que les p_i, sont inversibles modulo les p_i, est equivalent au système

$$\begin{cases} x & \equiv & -1 & \pmod{p_1^2} \\ x & \equiv & -\frac{1}{2} & \pmod{p_2^2} \\ & \vdots & & \\ x & \equiv & -\frac{1}{n} & \pmod{p_n^2}. \end{cases}$$

Soit x_0 une solution de ce système, obtenue grâce au lemme chinois. Alors tout nombre de la forme $x_0 + kp_1^2 \dots p_n^2$ est aussi solution de ce système. D'après le théorème de Dirichlet, il existe un nombre premier $p > a$ de cette forme-là. Alors $p+1, \dots, np+1$ ne sont pas premiers, étant chacun divisible par un carré.

Revenons maintenant à l'exercice. Soit p comme dans le lemme, et q un diviseur premier de $\Phi_p(a)$. Si on avait $q|p$, on aurait $q = p$, donc $a^q \equiv 1 \pmod{q}$, donc $a \equiv 1 \pmod{q}$, ce qui est impossible car $a < p = q$. Donc par le résultat fondamental, $q \equiv 1 \pmod{p}$ et $\text{ord}_q(a) = p$. Or, $p+1, \dots, np+1$ étant composés, $q \geqslant (n+1)p+1$, donc $\frac{q-1}{\text{ord}_q(a)} \geqslant n+1$, ce qui conclut, puisque n était arbitraire.

Solution de l'exercice 3 Il suffit de montrer que $2^{p_1 \cdots p_n} + 1$ a au moins 2^{n-1} diviseurs premiers deux à deux. On écrit

$$\begin{aligned} (2^{p_1 \cdots p_n} - 1)(2^{p_1 \cdots p_n} + 1) &= 2^{2p_1 \cdots p_n} - 1 \\ &= \prod_{d|2p_1 \cdots p_n} \Phi_d(2) \\ &= \left(\prod_{d|p_1 \cdots p_n} \Phi_d(2) \right) \left(\prod_{d|p_1 \cdots p_n} \Phi_{2d}(2) \right) \\ &= (2^{p_1 \cdots p_n} - 1) \left(\prod_{d|p_1 \cdots p_n} \Phi_{2d}(2) \right), \end{aligned}$$

d'où

$$2^{p_1 \cdots p_n} + 1 = \prod_{d|p_1 \cdots p_n} \Phi_{2d}(2).$$

Par la proposition qui suit le résultat fondamental, nous savons que si $\Phi_a(2)$ et $\Phi_b(2)$ ne sont pas premiers entre eux, alors $\frac{a}{b}$ doit être une puissance d'un nombre premier. Il suffit donc que nous prouvions que nous pouvons choisir 2^{n-1} diviseurs de $p_1 \dots p_n$ tels que deux d'entre eux ne diffèrent jamais d'un seul nombre premier. On effectue cela en choisissant les diviseurs qui sont produit d'exactement un nombre pair de facteurs premiers : il y en a bien 2^{n-1}, d'où le résultat.

4 Quatrième cours/TD

François

5 Test

- Énoncés -

Exercice 1 Calculer le nombre de classes x modulo 225 telles que $x^{30} \equiv 1 \pmod{225}$.

Exercice 2 Trouver toutes les fonction $f : \mathbb{Z} \longrightarrow \mathbb{R}$ p-périodiques pour p un nombre premier impair et multiplicatives, c'est-à-dire telles que

$$f(m+p) = f(m)$$

pour tout entier m et

$$f(mn) = f(m)f(n)$$

pour tous les entiers m, n.

Exercice 3 Trouver tous les entiers naturels n tels que $2^n | 3^n - 1$.

Exercice 4 Trouver tous les nombres premiers p et q tels que

$$p^2 + 1 \mid 2003^q + 1 \quad \text{et} \quad q^2 + 1 \mid 2003^p + 1.$$

- Corrigé -

<u>*Solution de l'exercice 1*</u> Commençons par décomposer 675 en facteurs premiers : $675 = 3^3 \times 5^2$. Nous allons d'abord raisonner modulo 27. Nous avons vu en cours que $(\mathbb{Z}/27\mathbb{Z})^*$ est cyclique et isomorphe à $\mathbb{Z}/18\mathbb{Z}$. Soient x une racine primitive et α tel que $a = x^\alpha$.

$$a^{30} \equiv 1[27] \iff 30\alpha \equiv 0[18] \iff 18|30\alpha \iff 3|\alpha$$

Donc $\alpha = 0, 3, 6, 9, 12$ ou $15[18]$, ce qui fait 6 possibilités. Si on regarde modulo 25 que l'on va déplacer dans $\mathbb{Z}/20\mathbb{Z}$: soit y une racine primitive modulo 25 et β tel que $a = y^\beta$ et on trouve

$$a^{30} \equiv 1[25] \iff \beta \equiv 0[20] \iff 2|\beta$$

Il y a donc 6 possiblités pour α (qui correspondent à 6 classes d'équivalence mod 27) et 10 possibilités pour β. Par le théorème chinois, cela nous donne 60 classes d'équivalence modulo 675 qui vérifient l'équation.

<u>*Solution de l'exercice 2*</u> Tout d'abord on remarque que $f(k^n) = f(k)^n$, et comme la fonction est périodique $f(k)^n$ ne peut pas avoir plus de p valeurs différentes, donc $f(k) \in \{-1, 0, 1\}$. En suite écartons pour le moment les k multiples de p et regardons uniquement les k qui sont premiers avec p. Nous savons que $\mathbb{Z}/p\mathbb{Z}$ est cyclique, prenons donc x une racine primitive et regardons $f(x)$:

1. si $f(x) = 0$, alors $f(x^n) = 0$ pour tout n entier, et comme on va recouvrir toutes les classes d'equivalence mod p. Donc pour tout k non divisible par p, $f(k) = 0$. Regardons maintenant les multiples de p : $f(np) = f(np \cdot 1) = f(np) \cdot f(1) = 0$. Donc la fonction est nulle partout.
2. si $f(x) = 1$, alors par le même raisonnement $f(k) = 1$ pour tout k premier avec p. Pour les multiples de p, $f(p^2) = f(p)^2$, il y a donc deux solutions : la fonction constante égale à 1 et la fonction qui vaut 0 sur $p\mathbb{Z}$ et 1 ailleurs.
3. si $f(x) = -1$, alors $f(x^n) = f(x)^n$. On vérifie facilement $f(k) = 1$ ssi k est un carré modulo p. Ensuite pour les multiples de p, on voit que $f(xp) = -f(p)$, donc $f(p) = 0$. La seule solution est le symbole de Legendre $f(k) = \left(\frac{k}{p}\right)$.

<u>*Solution de l'exercice 3*</u> Notons E l'ensemble des entiers recherchés. Il est clair que $0 \in E$, dans toute la suite on supposera donc $n \geqslant 1$. Si $n \in E$, on a $3^n \equiv 1 \mod 2^n$. Notons k l'ordre de 3 modulo 2^n ; on a alors que $k \mid n$, et de plus il est clair que $k \in E$. De plus, $k \mid \phi(2^n)$, et comme $\phi(2^n) = 2^{n-1}$, on en déduit que k est une puissance de 2. On est donc naturellement amené a rechercher dans un premier temps quelles puissances de 2 appartiennent à E.

Notons $a_l = 3^{2^l} - 1$. On cherche donc les entiers $l \geqslant 0$ tels que $v_2(a_l) \geqslant 2^l$. On a $v_2(a_0) = 1$ et $v_2(a_1) = 3$. De plus, comme $a_{l+1} = a_l(a_l + 2)$, on en déduit que si $v_2(a_l) \geqslant 2$, alors $v_2(a_{l+1}) = v_2(a_l) + 1$. Donc, par une récurrence immédiate, pour tout $l \geqslant 1$, $v_2(a_l) = l + 2$. En particulier, $v_2(a_l) \geqslant 2^l$ si et seulement si $n \leqslant 2$. Les puissances de 2 appartenant à E sont donc exactement 1, 2 et 4.

Considérons maintenant $n \in E$. Comme on l'a vu, l'ordre k de 3 modulo 2^n est une puissance de 2 appartenant à E, donc 1, 2 où 4. 2^n est donc un diviseur de $3^1 - 1$, de $3^2 - 1$ ou de $3^4 - 1$, ce qui nous donne que $n \leqslant 4$. En testant au cas par cas, on en déduit finalement que $E = \{0, 1, 2, 4\}$.

<u>*Solution de l'exercice 4*</u> Par symétrie, on peut supposer que $p \leqslant q$. Nous allons tout d'abord traiter le cas $p = 2$. Dans, ce cas, puisque $2003 \equiv 3 \pmod 5$, l'ordre de 2003 modulo 5 est 4, et q est nécessairement divisible par 2, donc égal à 2. D'autre part, on voit que le couple $(2, 2)$ convient bien.

Supposons maintenant $p > 2$. Soit r un facteur premier de $p^2 + 1$. Remarquons que r peut être soit 2, soit congru à 1 modulo 4. En effet, l'ordre de p modulo r est clairement 4, donc 4 divise $r - 1$ (Une manière plus rapide mais équivalente de le dire est de remarquer que -1 est résidu quadratique modulo r). Par hypothèse, nous avons

$$2003^q \equiv -1 \pmod r,$$

ce qui nous laisse deux possibilités pour l'ordre de 2003 modulo r, à savoir 2 et $2q$.

Montrons que l'ordre peut être 2 seulement si $r = 2$. Supposant que l'ordre est 2, r divise

$$2003^2 - 1 = 2002 \times 2004 = 2^3 \times 3 \times 7 \times 11 \times 13 \times 167.$$

Si r est impair, il est congru à 1 modulo 4, donc la seule possibilité est $r = 13$. Or nous devons aussi avoir $r | 2003^q + 1$, qui est impossible car $2003 \equiv 1 \pmod{13}$. Ainsi, r est bien égal à 2 dans ce cas.

Ainsi, pour tout facteur premier impair r de $p^2 + 1$, l'ordre de 2003 modulo r est $2q$, et en particulier pour chaque tel r, nous obtenons la relation de congruence $r \equiv 1 \pmod{q}$. Or, puisqu'un carré impair est congru à 1 modulo 4, $p^2 + 1 \equiv 2 \pmod{4}$, donc la valuation 2-adique de $p^2 + 1$ est 1. Puisque $p^2 + 1$ est égal à 2 multiplié par un produit de facteurs impairs congrus à 1 modulo q, nous avons

$$p^2 + 1 \equiv 2 \pmod{q},$$

et donc, q divise $p^2 - 1 = (p-1)(p+1)$. Nous avions supposé $p \leqslant q$ au début, donc q est un facteur premier impair de $p + 1$. Puisque $p + 1$ est pair, ses facteurs premiers sont tous strictement inférieurs à p, ce qui contredit $p \leqslant q$. Ainsi, la seule solution est le couple $(2, 2)$.

V. La Muraille

Une muraille de 126 exercices était affichée dans la salle commune. Une fois qu'un exercice était résolu par un élève, ou un groupe d'élèves, la solution devait être rédigée et apportée aux animateurs. Si la solution était correcte, l'exercice était barré, et celle-ci incorporée dans le poly. Les exercices sont classés par ordre de difficulté :

- Les exercices 1 à 35 sont destinés aux 4èmes et 3èmes.
- Les exercices 36 à 80 sont destinés aux 2ndes et 1ères.
- Les exercices au delà de 81 sont d'un niveau "olympique".

Exercice 1

Si, en étant à jeun au départ, le loup mange 3 cochons et 7 lièvres, il a encore faim après. Si en revanche, en étant à jeun, il mange 7 cochons et 1 lièvre, alors il a mal au ventre parce qu'il a trop mangé. Que se passe-t-il s'il mange 11 lièvres?

Exercice 2

p filles et q garçons se mettent en cercle. On note a le nombre de paires de filles se tenant côte à côté, b le nombre de paires de garçons se tenant côte à côte. Montrer que $a - b = p - q$.

Exercice 3

De combien de manières peut-on mettre 10 pièces de monnaie dont 5 sont identiques et 5 autres différentes dans 5 poches numérotées de 1 à 5?

Exercice 4

Soient a, b, et c trois nombres réels tels que $a^2 + b^2 + c^2 = ab + bc + ca$. Montrer que $a = b = c$.

Exercice 5

On considère 2013 nombres et chaque nombre est égal à 1 ou à -1. Montrer que si leur produit est égal à 1, alors leur somme ne peut pas être égale à 0.

Exercice 6

Cinq pirates veulent partager 100 pièces d'or selon les règles suivantes :

Ils ont une hiérarchie stricte - premier officier, seconde officier, etc.

Le commandant actuel propose une distribution. Après, ils votent tous sur cette distribution. Si une majorité (c'est-à-dire plus que 50%) accepte, l'or est distribué. Sinon, le commandant est jeté en pâture aux requins et le prochain devient commandant.

On répète cette procédure jusqu'au moment où offre de distribution est acceptée.

On suppose : 1)Les pirates sont des excellents logiciens. 2)Leur priorité est de survivre, après maximiser le montant d'or. 3) Entre deux possibilités avec le même montant d'or, ils préfèrent de voir quelqu'un se faire dévorer par les requins. 4)Ils savent que les autres partagent ces points de vue.

Qu'est-ce que la stratégie optimale pour le premier officier ?

Exercice 7

Montrer que pour tout entier $n \geq 1$, $3^{6n} - 2^{6n}$ est divisible par 35.

Exercice 8

Soit k un entier supérieur ou égal à 2. Trouver tous les entiers x et y tels que:

$$y^k = x^2 + x.$$

Exercice 9

Soit $[EF]$ un segment inclus dans le segment $[BC]$ tel que le demi-cercle de diamètre $[EF]$ est tangent à $[AB]$ en Q et à $[AC]$ en P. Prouver que le point d'intersection K des droites (EP) et (FQ) appartient à la hauteur issue de A du triangle ABC.

Exercice 10

Tous les points du plan sont coloriés soit en rouge, soit en bleu, soit en vert. Montrer qu'il y a deux points à distance 1 qui ont la même couleur.

Exercice 11

En n'utilisant que $+$,-,$\times$,/ et parenthèses, est-il possible d'obtenir 21 à partir des quatre entiers 1,5,6,7 ?

Exercice 12

On considère un nombre fini de segments sur la droite réelle tels que, quels que soient deux de ces segments, ils aient un point commun. Montrer qu'il existe un point appartenant à tous ces segments.

Exercice 13 $\star$

Si a, b, c sont les longueurs des côtés d'un triangle rectangle dont le plus long côté est c, montrer que $c^n > a^n + b^n$ pour tout entier $n > 2$.

Exercice 14

Un L est la forme obtenue en enlevant un coin d'un échiquier 2×2. Prouver que l'on peut paver un échiquier $2^n \times 2^n$ privé d'un coin par des L.

Exercice 15

On a un polyèdre convexe, dont les faces sont des triangles. Les sommets du polyèdre sont coloriés avec trois couleurs.
Montrer que le nombre de triangles dont les sommets ont trois couleurs distinctes est pair.

Exercice 16

Considérons deux droites d et d' se coupant en A. Les points A, B, C, D, et E sont alignés dans cet ordre sur d, et les points A, B', C', D', E' sont alignés dans cet ordre sur d'. On suppose que $AB = BC' = C'D = DE' = E'E = ED' = D'C = CB' = B'A$. Déterminer la mesure de l'angle $\widehat{BAB'}$.

Exercice 17

Soit n un entier naturel. À un stage de mathématiques, $2n + 1$ élèves se réunissent, chacun étant muni d'un pistolet à eau. On suppose que les distances entre élèves sont deux à deux distinctes. À midi précises, chaque élève tire sur son plus proche voisin. Montrer qu'il existe au moins un élève qui restera sec.

Exercice 18

Soit $ABCD$ un carré, et E un point intérieur à $ABCD$ tel que le triangle AEB soit isocèle en E, avec $\widehat{AEB} = 150°$. Déterminer la mesure de l'angle $\widehat{CED}$.

Exercice 19

Les nombres naturels n_1, n_2, …, n_{2012} satisfont l'équation
$$n_1^2 + \ldots + n_{2011}^2 = n_{2012}^2.$$
Montrer qu'au moins deux nombres sont pairs.

Exercice 20 *

Montrer que:
$$\frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \cdots - \frac{1}{999} + \frac{1}{1000} < \frac{2}{5}.$$

Exercice 21

Le dernier chiffre du carré d'un nombre naturel est égal à 6. Démontrez que son avant-dernier chiffre est impair.

Exercice 22

Soit $u_0, u_1, \ldots$ une suite de nombres vérifiant $u_0 = 1$ et pour $n \geq 0$:
$$u_{n+1} = u_0 + \cdots + u_n.$$
Calculer u_n.

Exercice 23

Chaque jour, un de 100 prisonniers est convoqué dans une salle avec une ampoule avec un interrupteur et il peut allumer ou éteindre l'ampoule, s'il veut. Le même prisonnier peut être convoqué plusieurs fois, mais ils savent que tous vont être convoqués un nombre arbitrairement grand de fois, s'ils sont suffisamment patients.

Chaque prisonnier peut déclarer à tout moment que tous les prisonniers ont visité la salle. Si la déclaration est correcte, ils sont tous libérés, sinon, ils sont tous exécutés.

Après une discussion initiale de stratégie au debut de premier jour, les prisonniers sont séparés et ils ne peuvent pas communiquer que par la manipulation de l'ampoule.

Peuvent-ils assurer leur succès ?

Exercice 24

Trouver tous les entiers naturels n tels que l'écriture décimale de n^2 se termine par n.

Exercice 25

Soit $x_0, x_1, x_2, \ldots$ une suite de nombres réels. On dit que la suite $x_0, x_1, \ldots$ est convexe si :

$$\text{pour tout entier } n \geq 0, \frac{x_{n-1} + x_{n+1}}{2} \geq x_n$$

et qu'elle est log-convexe si :

$$\text{pour tout entier } n \geq 0, x_{n+1}x_{n-1} \geq x_n^2$$

On suppose que pour tout nombre réel $a > 0$, la suite $x_0, ax_1, a^2x_2^2, a^3, x_3^3, \ldots$ est convexe. Prouver que la suite $x_0, x_1, \ldots$ est log-convexe.

Exercice 26

Trouver tous les entiers $x, y \geq 0$ tels que $xy = x + y + 3$.

Exercice 27

Soit ABC un triangle isocèle en C. On considère un point P sur le cercle circonscrit au triangle ABC situé entre A et B (et P n'est pas dû même côté que C par rapport à la droite (AB)). Soit D un point de la droite (PB) tel que les droites (CD) et (PB) soient perpendiculaires. Prouver que $PA + PB = 2 \cdot PD$.

Exercice 28

Soient $x, y > 0$, et soit $s = min(x, y + 1/x, 1/y)$. Quelle est la valeur maximale possible de s ? Pour quels x, y est-elle atteinte ?

Exercice 29

Trouver les nombres premiers p pour lesquels il existe des entiers positifs x et y tels que:

$$x(y^2 - p) + y(x^2 - p) = 5p.$$

Exercice 30 ⋆

On place $2n$ points dans le plans et on trace $n^2 + 1$ segments entre ces points.

Montrer que l'on peut trouver 3 points reliés deux à deux.

Exercice 31

Soit $\mathcal{P} = A_1 \dots A_{2n}$ un $2n-$gone convexe dans le plan. Soit P un point intérieur à $\mathcal{P}$, non situé sur une diagonale. Prouver que P est contenu dans un nombre pair de triangles à sommets parmi les A_i.

Exercice 32

Soit $n > 0$ un entier. On considère un entier A constitué de $2n$ chiffres qui sont tous des 4, et un entier B constitué de n chiffres, qui sont tous des 8. Prouver que l'entier $A + 2B + 4$ est un carré parfait.

Exercice 33

Soit ABC un triangle isocèle en A tel que $\widehat{BAC} < 60°$. Les points D et E sont des points du côté $[AC]$ tels que $EB = ED$ et $\widehat{ABD} = \widehat{CBE}$. Soit O le point d'intersection des bissectrices des angles $\widehat{BDC}$ and $\widehat{ACB}$. Trouver la valeur de l'angle $\widehat{COD}$.

Exercice 34

Trouver tous les entiers positifs a, b, c tels que

$$2^a 3^b + 9 = c^2.$$

Exercice 35

Soit ABC un triangle dont tous les angles sont aigus. On note Γ son cercle circonscrit. On suppose que La tangente en A à Γ coupe la droite (BC) en un point P. Soit M le milieu de $[AP]$ et soit R le deuxième point d'intersection de la droite (BM) avec le cercle Γ. La droite (PR) recoupe le cercle Γ en S.

Prouver que les droites (AP) et (CS) sont parallèles.

Exercice 36

Trouver tous les nombres naturels n tels que $n2^{n+1}+1$ soit un carré parfait.

Exercice 37

Soit ABC un triangle isocèle en A tel que $\widehat{BAC} = 20°$. Soit X le point sur le segment $[AB]$ avec $\widehat{XCA} = 20°$ et soit Y le point sur le segment $[AC]$ avec $\widehat{ABY} = 30°$.

Déterminer la valeur de l'angle $\widehat{CXY}$.

Exercice 38

Considérons un polynôme :

$$f(x) = x^{2012} + a_{2011}x^{2011} + ... + a_1x + a_0.$$

Albert Einstein et Homer Simpson jouent au jeu suivant. Tour à tour, ils choisissent un des coefficients a_0, a_1, ..., a_{2011}, et lui assignent une valeur réelle. Une fois qu'une valeur est assignée à un coefficient, elle ne peut plus être changée. C'est Albert qui commence. Le but d'Homer est de rendre $f(x)$ divisible par un polynôme $m(x)$, fixé à l'avance, et le but d'Albert est de l'en empêcher. Quel joueur à une stratégie gagnante si :

a) $m(x) = x - 2012$?

b) $m(x) = x^2 + 1$?

(On rappelle que le polynôme $m(x)$ *divise* le polynôme $f(x)$ s'il existe un polynôme $g(x)$ tel que $f(x) = m(x) \cdot g(x)$).

Exercice 39 ⋆

Six cercles sont concourants en un point A. Montre que l'un de ces cercles contient le centre d'un autre.

Exercice 40

Soit $n > 2$ un entier naturel, T la transformation $\mathbb{R}^n \to \mathbb{R}^n, (x_1, \ldots, x_n) \mapsto (\frac{x_1+x_2}{2}, \frac{x_2+x_3}{2}, \ldots, \frac{x_{n-1}+x_n}{2}, \frac{x_n+x_1}{2})$. On part d'un $n-uplet$ $(a_1, \ldots, a_n)$ d'entiers deux à deux distincts. Prouver que pour $k \in \mathbb{N}$ assez grand, $T^k(a_1, \ldots, a_n) \notin \mathbb{N}^n$.

Exercice 41 ⋆

(a) Pour quelles valeurs de n l'entier $2^n - 1$ est-il une puissance de 3?

(b) Pour quelles valeurs de n l'entier $2^n + 1$ est-il une puissance de 3 ?

Exercice 42

Chaque sous-ensemble à k éléments de $\{1, 2, \ldots n\}$ possède un plus petit élément. Calculer la moyenne de ces plus petits éléments.

Exercice 43 ⋆

Soit f une fonction qui à deux entiers strictement positifs associe un entier strictement positif, définie par $f(1,1) = 2$, $f(m+1,n) = f(m,n) + m$, et $f(m,n+1) = f(m,n) - n$.
Quels sont les couples (p,q) tels que $f(p,q) = 2011$?

Exercice 44

Soit P un point à l'intérieur d'un polygone régulier à n côtés tel que quel que soit un côté du polygone, P se projette orthogonalement sur l'intérieur du côté. Ces n projections orthogonales partagent les n côtés du polygône en $2n$ segments. On numérote ces segments de 1 à $2n$, en commençant par un segment arbitraire, puis en tournant dans le sens direct le long du polygone. Prouver que la somme des longueurs des segments de numéros pairs est égale à la somme des longueurs des segments de numéros impairs.

Exercice 45 ⋆

Une compagnie internationale possède 70 employés. Si X et Y sont deux quelconques d'entre eux, il y a une langue parlée par X et non parlée par Y, et une langue parlée par Y mais pas par X.
Quel est le nombre minimum total de langues parlées par les employés?

Exercice 46 ⋆

Soit $n > 0$ un entier. Prouver qu'un carré de $2^n \times 2^n$ cases unité, privé d'une case, peut être pavé par des coins (un coin est un carré 2×2 dont on a enlevé une case).

Exercice 47 ⋆

Trouver toutes les fonctions f allant de $\mathbb{Q}$ dans $\mathbb{Q}$ telles que $f(1) = 2$ et pour tout couple (x,y) on ait :

$$f(xy) = f(x)f(y) - f(x+y) + 1.$$

Exercice 48 ⋆

On place des nombres entiers dans un tableau carré. Au dessus de chaque colonne, on écrit le plus grand entier de cette colonne. On appelle a le plus petit élément parmi ceux écrits au dessus d'une colonne. À gauche de chaque ligne, on écrit le plus petit entier de cette ligne. On appelle b le le grand élément parmi ceux écrits à gauche d'une ligne.
Comparer les deux entiers a et b.

Exercice 49

Si A est un ensemble d'entiers naturels non vide, on note $PGCD(A)$ le plus grand diviseur commun à tous les éléments de A.
Trouver le plus petit entier naturel non nul n vérifiant la propriété suivante : pour toute partie A de $\{1, 2, ..., 2012\}$, il existe une partie B de A de cardinal inférieur ou égal à n telle que $PGCD(B) = PGCD(A)$.

Exercice 50 *

De combien de manières différentes peut-on écrire 2^n comme somme de quatre carrés de nombres strictement positifs?

Exercice 51 *

Soit A le point d'intersection de deux cercles Γ_1 et Γ_2 de rayons p et q. Soient respectivement B et C deux points de Γ_1 et Γ_2 tels que (BC) est tangente aux deux cercles.
Prouver que $pq = R^2$, où R est le rayon du cercle circonscrit au triangle ABC.

Exercice 52 *

Montrer que parmi les réels positifs $a, 2a, \ldots, (n-1)a$, l'un au moins est à distance au plus $1/n$ d'un entier positif, pour tout $a > 0$.

Exercice 53

Résoudre dans $\mathbb{N}$ l'équation:

$$3^x - 5^y = z^2.$$

Exercice 54 *

Soit n un entier divisible ni par 2, ni par 5.
Montrer qu'il existe un multiple de n ne comportant que des 1.

Exercice 55

Il y a n clés sur un porte-clé, il est impossible de les identifier à l'œil nu. On veut accrocher une étiquette de couleur sur certaines clés, de façon à pouvoir les identifier. Combien de couleurs sont nécessaires au minimum?

Exercice 56 *

Considérons les $2^n - 1$ sous-ensembles non vides de $\{1, 2, \dots, n\}$. Pour chacun de ces sous-ensembles, on calcule le produit des inverses de ses éléments. Trouver la somme de tous ces produits.

Exercice 57 *

On choisit un point sur chaque côté d'un carré de côté 1. On considère alors a, b, c et d les longueurs du quadrilatère ainsi formé.

Montrer que

$$2 \leq a^2 + b^2 + c^2 + d^2 \leq 4 \quad \text{et} \quad 2\sqrt{2} \leq a + b + c + d \leq 4.$$

Exercice 58

On a communiqué à deux animateurs du stage un nombre naturel; on leur a dit que ces nombres différaient d'une unité. Après ceci, les animateurs se posent la même question: "Est-ce que tu connais mon nombre? ". Prouvez que, tôt ou tard, l'un d'eux répondra positivement.

Exercice 59 *

Montrer que:

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

Exercice 60

Soient ABC un triangle, H le pied de la hauteur issue de B, M le milieu de $[AB]$ et N le milieu de $[BC]$. Les cercles circonscrits aux triangles AHN et CHM se recoupent au point P. Prouver que la droite (PH) coupe le segment $[MN]$ en son milieu.

Exercice 61

On a deux dés truquées. Sur le premier dé, les nombres $1, 2, \ldots, 6$ ont les probabilités $p_1, p_2, \ldots, p_6$ d'apparaître, respectivement, et sur le deuxième $q_1, q_2, \ldots, q_6$, respectivement.

Est-il possible de choisir $p_1, \ldots, p_6, q_1, \ldots, q_6$ tel que la somme des résultats des deux dés prend les valeurs $2, 3, \ldots, 12$ avec la même probabilité ?

Exercice 62 *

On place les entiers $1, \ldots, 2n$ dans n'importe quel ordre à des places numérotées $1, \ldots, 2n$. On ajoute la valeur de sa place à chaque entier.

Montrer qu'il y a deux sommes qui ont le même reste modulo $2n$.

Exercice 63 *

On a des pièces de 1, 2, 5, 10, 20, 50 centimes et 1 euro.

Prouver que si avec N de ces pièces on peut payer une facture de M centimes, alors il est possible de payer une facture de N euros avec M pièces.

Exercice 64

Soit ABC un triangle, E_A, E_B, E_C les points de contacts des cercles exinscrits tangents aux segments BC, AC et AB respectivement. Prouver

- Les droites (AE_A), (BE_B) et (CE_C) sont concourantes (leur point d'intersection est appelé *point de Nagel* du triangle ABC).
- Les perpendiculaires à (BC), (AC), (AB) passant par E_A, E_B, E_C respectivement sont concourantes.

Exercice 65 *

Un cercle passant par les sommets A et C d'un triangle ABC coupe le côté $[AB]$ en son milieu D et le côté $[BC]$ en E. Le cercle tangent à (AC) en C et passant par E recoupe la droite (DE) en F. Soit K le point d'intersection des droites (DE) et (AC).

Prouver que les droites (CF), (AE) et (BK) sont concourantes.

Exercice 66

Une ampoule est placée sur chaque case d'un échiquier 2011×2012. Initialement, 4042111 ampoules sont allumées. On a le droit d'éteindre une ampoule si elle appartient à un bloc 2×2 dont les trois autres ampoules sont éteintes. Peut-on éteindre toutes les ampoules?

Exercice 67 ⋆

On place m jetons ($m > n$) sur les sommets d'un n-gone convexe. À chaque étape, deux jetons se trouvant sur un même sommet sont déplacés sur un voisin différent de ce sommet.

Montrer que si l'on retrouve la distribution initiale après un certain nombre de mouvements, ce nombre de mouvements est un multiple de n.

Exercice 68

Soit p un nombre premier congru à 2 modulo 3 et a et b des entiers tels que p divise $a^2 + ab + b^2$. Montrer que p divise a et b.

Exercice 69 ⋆

Considérons n sièges en ligne. Un enfant est assis sur chaque siège. Chaque enfant peut se déplacer d'au plus un siège. Trouver le nombre a_n de façons dont ils peuvent se déplacer.

Exercice 70

Soit n un entier non nul. Montrer que

$$\lfloor\sqrt{n}\rfloor + \lfloor\sqrt[3]{n}\rfloor + \ldots + \lfloor\sqrt[n]{n}\rfloor = \lfloor\log_2 n\rfloor + \lfloor\log_3 n\rfloor + \ldots + \lfloor\log_n n\rfloor.$$

On rappelle que $\lfloor x\rfloor$ désigne le plus grand entier inférieur ou égal à x, et que $\lfloor\log_k n\rfloor$ est égal au plus grand exposant a tel que $k^a \leq n$.

Exercice 71 ⋆

Soit ABC un triangle isocèle en A, avec $\widehat{BAC} = 100\,°$. Soit D le point de la droite (AB) tel que $AD = BC$, et B est entre A et D. Montrer que $\widehat{ADC} = 30\,°$.

Exercice 72

Soit $ABCD$ un carré, E un point sur $[BC]$ et F un point sur $[DC]$, tels que le périmètre de ECF soit égal au double du côté du carré. Trouver l'angle $\widehat{EAF}$.

Exercice 73 ⋆

Soit ABC un triangle isocèle en A, les points M et N sont pris sur les côtés AB et AC respectivement. Les droites (BN) et (CM) se coupent en P.

Montrer que les droites (MN) et (BC) sont parallèles si, et seulement si, $\widehat{APM} = \widehat{APN}$.

Exercice 74

Soit $n \geq 6$ un entier naturel et $\mathcal{P}$ un $n-$gone régulier. Pour quels valeurs de n existe-t-il un coloriage en noir et blanc des sommets de $\mathcal{P}$ tel qu'il n'existe pas de triangle isocéle monochrome ?

Exercice 75

On met un pion sur chaque case d'un quadrillage 57×57, puis on enlève tous les pions, et on en remet de nouveau un sur chaque case. Est-il possible que chaque pion se retrouve sur une case adjacente à celle où il était lors de la première disposition?

Exercice 76

Soit ABC un triangle. On note comme d'habitude $a = BC$, $b = AC$, $c = AB$ et R le rayon du cercle circonscrit. Montrer que :

$$\frac{1}{R^2} \leq \frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2}$$

avec égalité si et seulement si ABC est équilatéral.

Exercice 77

Quatre fourmis sont placés sur les sommets d'un carré de côté 1 mètre. Chaque fourmi tourne vers le prochain fourmi dans le sens d'aiguille d'une montre. Ils commencent à marcher avec la même vitesse, toujours dans la direction de voisin choisi. Apres un certain temps, ils arrive tous au centre de carre original.

Quelle est la distance traversée par chaque fourmi ?

Exercice 78 ⋆

Soit ABC un triangle quelconque et H son orthocentre. Soient deux points M et N pris respectivement sur les côtés AB et AC. Les cercles des diamètres BN et CM se coupent en P et Q.

Montrer que les points P, Q, H sont alignés.

Exercice 79

Soit $n \geq 0$ un entier naturel. Montrer qu'il existe un disque dans le plan contenant exactement n points à coordonnées entiéres.

Exercice 80 *

Montrer que si n points du plan ne sont pas tous colinéaires, il y a au moins n droites distinctes passant par deux d'entre eux.

Exercice 81

Étant donné un polygone convexe dans le plan, prouver qu'il existe deux droites perpendiculaires qui le divisent en quatre morceaux de même aire.

Exercice 82

Un nombre est dit "varié" s'il a 9 chiffres, tous distincts et non nuls (par exemple, 782319564 ou 678123954). Montrer que le nombre de paires de nombres variés dont la somme est 987654321 est impair.

Exercice 83

Le polynôme $P = ax^3 + bx^2 + cx + d$ est à coefficients entiers avec ad impair et bc pair. Prouver qu'au moins une racine de P est irrationnelle.

Exercice 84 *

Soit ABC un triangle et d une droite passant par le centre du cercle inscrit γ de ABC. Soient A_1 (resp. B_1, C_1) le projeté orthogonal de A (resp. B, C) sur d et A_2 (resp. B_2, C_2) le point de γ diamétralement opposé au point de tangence entre γ et $[BC]$ (resp. $[CA], [AB]$).

Prouver que les droites $(A_1A_2), (B_1B_2), (C_1C_2)$ sont concourantes en un point appartenant à γ.

Exercice 85

Une magicienne effectue le tour de magie suivant : au début du tour, n pièces de monnaie sont placées en ligne sur une table, en position pile. La magicienne a les yeux bandés. Une spectatrice est sélectionnée dans le public, et elle commence par retourner autant de pièces qu'elle le désire. Puis, elle choisit un nombre entre 1 et n, qu'elle annonce à l'assistante de la magicienne. Pour finir, l'assistante détourne l'attention de l'audience et en profite pour retourner discrètement une des n pièces. La magicienne enlève son bandeau, regarde la disposition des pièces sur la table, et devine le nombre choisi par la spectatrice. Pour quelles valeurs de n un tel tour est-il possible?

Exercice 86

Il y a $n > 1$ clous et $\binom{n}{2}$ ficelles relient deux à deux les clous. Chaque ficelle a une couleur et, pour tout triplet de couleurs, il y a un triangle ayant précisément ces trois couleurs. Est-ce que n peut être égal à 6 ? À 7 ?

Exercice 87 ⋆⋆

Les points D et E appartiennent respectivement aux segments $[AB]$ et $[AC]$, de sorte que les droites (DE) et (BC) soient parallèles. Soit P un point arbitraire intérieur au triangle ABC. Les droites (PB) et (PC) rencontrent (DE) respectivement en F et G. On appelle O_1 (resp. O_2) le centre du cercle circonscrit à PDG (resp. PFE).

Prouver que (AP) et (O_1O_2) sont perpendiculaires.

Exercice 88

Soient A', B' et C' des point appartenant respectivement aux côtés BC, CA et AB d'un triangle ABC, tels que AA', BB' et CC' soient concourantes, et tels que

$$\overrightarrow{AA'} + \overrightarrow{BB'} + \overrightarrow{CC'} = \overrightarrow{0}.$$

Prouver que A', B' et C' sont les milieux de leurs côtés respectifs.

Exercice 89 ⋆

Alice et Bob jouent sur un échiquier plan infini. Alice commence par choisir une case et la colorie en rouge, puis Bob choisit une case non encore coloriée et la colorie en vert, et ainsi de suite. Alice gagne la partie si elle réussi à colorier en rouge quatre cases qui dont les centre forment les sommets d'un carré de côtés parallèles à ceux des cases.

a) Prouver qu'Alice possède une stratégie gagnante.

b) Qu'en est-il si Bob a, lui, le droit de colorier deux cases en vert à chaque coup?

Exercice 90

On place n points dans un carré de côté 1. Prouver qu'il existe un triangle dont les sommets sont parmi ces points et d'aire $\leq \frac{1}{n-2}$.

Exercice 91

Soit $\alpha_0, \alpha_1, \alpha_2, \ldots$ une suite de chiffres de 0 à 8. On construit à partir de cette dernière les nombres

$$a_n = \overline{\alpha_0\alpha_1\ldots\alpha_n} = 10^n\alpha_0 + 10^{n-1}\alpha_1 + \ldots + 10\alpha_{n-1} + \alpha_n.$$

Montrer que dans la suite a_n il y a une infinité de nombres composés (c'est-à-dire non premiers).

Exercice 92

Trouver toutes les fonctions $f : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ pour lesquelles il existe un entier $a \in \mathbb{N}^*$ tel que $f(f(n)) = an$ pour tout $n \in \mathbb{N}^*$.

Exercice 93 ⋆

On considère l'ensemble des mots constitués des lettres a, b et c. On définit les deux familles d'ensembles suivantes :

- $A_n = \{$ mots de longueur n qui ne contiennent ni aa ni bb $\}$.
- $B_n = \{$ mots de longueur n tels que trois lettres consécutives ne sont jamais toutes distinctes $\}$.

Montrer que $\#B_{n+1} = 3\#A_n$.

Exercice 94

Soient a, b, c, d des réels positifs tels que $a + b + c + d = 2$. Montrer que:

$$\frac{a^2}{(a^2+1)^2} + \frac{b^2}{(b^2+1)^2} + \frac{c^2}{(c^2+1)^2} + \frac{d^2}{(d^2+1)^2} \leq \frac{16}{25}.$$

Exercice 95 ⋆

L'ensemble $\{1, 2, \ldots, 3n\}$ est partitionné en trois ensembles A, B et C de n éléments chacun.

Montrer qu'il est possible de choisir un élément dans chacun de ces trois ensembles, tels que la somme de deux d'entre eux soit égale au troisième.

Exercice 96

Existe-t-il un nombre fini ou une infinité d'entiers n tels que $\lfloor n\sqrt{2} \rfloor$ soit une puissance de 3 ?

($\lfloor x \rfloor$ désigne la partie entière de x.)

Exercice 97 ⋆⋆

Les élèves d'une classe sont allés se chercher des glaces par groupe d'au moins deux personnes. Il y a eu $k > 1$ groupes en tout. Deux élèves quelconques sont partis ensemble exactement une fois

Prouver qu'il n'y a pas plus de k élèves dans la classe.

Exercice 98 ⋆

Soient a, b, c, d les longueurs des côtés consécutifs d'un quadrilatère convexe $ABCD$. Soient m et n les longueurs de ses diagonales.

Prouver que:

$$m^2n^2 = a^2c^2 + b^2d^2 - 2abcd\cos(\widehat{A} + \widehat{C}).$$

Exercice 99 ⋆

Montrer que pour tout entier $n \geq 1$, 2 est racine primitive modulo 3^n.

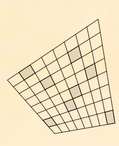
Un entier a est dit racine primitive modulo b si, pour tout entier n, il existe un entier $k \geq 0$ tel que $a^k \equiv n \mod b$.

Exercice 100 ⋆

On veut paver un rectangle $m \times n$ $(m, n > 1)$ par des **L** (pensez Tetris). Montrer que ce pavage est possible si et seulement si mn est multiple de 8.

Exercice 101

On prend un quadrilatère convexe $ABCD$, et on divise chacun de ses côtés en N portions égales. On relie ensuite ces différentes portions de façon à former un quadrillage $N \times N$, comme sur la figure. On sélectionne ensuite N quadrilatères de ce quadrillage, de telle sorte qu'il n'y en ait pas deux sur la même ligne ou sur la même colonne du quadrillage. Calculer l'aire totale de tous ces quadrilatères.



Exercice 102 ⋆

Une suite croissante $(s_n)_{n\geq 0}$ est dite super-additive si pour tout couple (i, j) d'entiers on a $s_{i+j} \geq s_i + s_j$. Soient (s_n) et (t_n) deux telles suites super-additives. Soit (u_n) la suite croissante d'entiers vérifiant qu'un nombre apparaît autant de fois dans (u_n) que dans (s_n) et (t_n) combinées.

Montrer que (u_n) est elle aussi super-additive.

Exercice 103 ⋆

Soit ABC un triangle, soit $A'B'C'$ un triangle directement semblable à ABC de telle sorte que A appartienne au côté $B'C'$, B au côté $C'A'$ et C au côté $A'B'$. Soit O le centre du cercle circonscrit à ABC, H son orthocentre et H' celui de $A'B'C'$.
Montrer qu'on a $OH = OH'$.

Exercice 104

On considère un nombre fini de segments sur la droite réelle tels que, pour tout sous-ensemble de k segments, on puisse trouver deux segments de ce sous-ensemble ayant un point commun. Montrer qu'il existe un ensemble de $k-1$ points tel que tout segment contienne l'un de ces points.

Exercice 105

Soient a, b, c les longueurs des côtés d'un triangle. Prouver que

$$\frac{c^2}{(a-b)^2} + \frac{a^2}{(b-c)^2} + \frac{b^2}{(c-a)^2} > 3.$$

Exercice 106 ⋆

Pour un entier $n \geq 1$, on note $\sigma(n)$ la somme des diviseurs positifs de n. Montrer que $\sigma(N)/N < 2$, où $N = 2^{2^n} + 1$.

Exercice 107

Soit $n, k \in \mathbb{N}$. Déterminer le nombre de $k-$uplets $(T_1, \ldots, T_k)$ de parties de l'ensemble $\{1, \ldots, n\}$ tel que $T_1 \subseteq T_2 \supseteq T_3 \subseteq T_4 \supseteq T_5 \subseteq \cdots T_k$.

Exercice 108 ⋆

Alice et Bob disposent d'un nombre fini d'ampoules, chacune pouvant être soit allumée soit éteinte. Alice décide alors de placer à sa guise des guirlandes entre certaines paires d'ampoules. Puis, Bob installe un système d'interrupteurs qui, si l'on change l'état d'une ampoule L quelconque change alors aussi, et simultanément, l'état de toutes les autres ampoules reliées à L par une guirlande.
Initialement, toutes les ampoules sont éteintes. Peut-on, à l'aide de ces interrupteurs, allumer simultanément toutes les ampoules?

Exercice 109

On dit qu'un nombre est intéressant si, dans sa décomposition en produit de nombres premiers, tous les nombres premiers qui apparaissent ont un exposant au moins 2 (par exemple, $72 = 2^3 \cdot 3^2$). Combien existe-t-il de paires de nombres intéressants consécutifs?

Exercice 110 ⋆

On considère un ensemble de $2n+1$ droites du plan, deux jamais parallèles ni perpendiculaires et trois jamais concourantes. Trois droites forment donc toujours un triangle non-rectangle.
Déterminer le nombre maximal de triangles aigus qui puissent ainsi être formés.

Exercice 111

Soient $a, b, c > 1$ des nombres réels tels que $a + b + c = 9$. Prouver que

$$\sqrt{ab + ac + bc} \leq \sqrt{a} + \sqrt{b} + \sqrt{c} \leq \sqrt{a^2 + b^2 + c^2}.$$

Exercice 112 ⋆

Soient A, B, C_2, C_1 des points d'un cercle Γ dans cet ordre. Soit γ un cercle tangent à $[AC_2]$, $[BC_1]$ et Γ. On note M_2 le point de contact entre γ et $[AC_2]$ et par N_1 le point de contact entre γ et $[BC_1]$.
Prouver que le centres des cercles inscrits à ABC_1 et ABC_2 sont sur $[M_2N_1]$

Exercice 113

Soit ABC un triangle, et M un point intérieur à ABC. On note J, K et L les projetés orthogonaux de M sur les cotés (BC), (AC), et (AB) respectivement. Pour quel(s) point(s) M le produit $MJ \cdot MK \cdot ML$ est-il maximal ?

Exercice 114

Soit ABC un triangle, et O un point à l'intérieur de ce triangle. Quel est le point M minimisant la quantité $AM + BM + CM + OM$?

Exercice 115

Les deux nombres A et B sont pairs, et s'écrivent avec les mêmes chiffres (par exemple, $A = 15652$ et $B = 55216$). Prouver que la somme des chiffres de $A/2$ est égale à la somme des chiffres de $B/2$.

Exercice 116 **

Soit E un ensemble de $n \geq 2$ points du plan. On désigne respectivement par D et d la plus grande et la plus petite distance entre deux points distincts de E.

Prouver que:

$$D \geq \frac{\sqrt{3}}{2}(\sqrt{n}-1)d.$$

Exercice 117

Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que :

$$\forall x, y \in \mathbb{R}, (x+y)(f(x)-f(y)) = (x-y)f(x+y).$$

Exercice 118 *

Soit S un ensemble infini de points du plan tel que si A, B et C sont trois points quelconques dans S, la distance de A à la droite (BC) soit un entier.

Prouver que les points de S sont tous alignés.

Exercice 119

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 120 **

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 121

Trouver tous les polynômes P à deux variables tels que :

$$\forall x, y \in \mathbb{R}, P(x+y, x-y) = 2P(x, y).$$

Exercice 122 *

Soit n un nombre pouvant s'écrire de deux façons différentes comme somme de deux carrés d'entiers. Montrer que n est composé.

Exercice 123

Soient P et Q deux polynômes à coefficients entiers, premiers entre eux. Pour tout entier n, posons $u_n = PGCD(P(n), Q(n))$. Montrer que la suite (u_n) est périodique.

Exercice 124

Soit ABC un triangle dont les angles sont notés α, β, γ. Soit S son aire et R le rayon de son cercle circonscrit. Montrer que:

$$\tan\frac{\alpha}{2} + \tan\frac{\beta}{2} + \tan\frac{\gamma}{2} \leq \frac{9R^2}{4A}.$$

Exercice 125 *

On veut colorier certains des points de l'ensemble $E_n = \{(a, b)/a, b \text{ entiers et } 0 \leq a, b \leq n\}$ de sorte que tout carré $k \times k$ dont les sommets sont dans E_n contienne au moins un point colorié sur son bord. On note $m(n)$ le nombre minimum de points à colorier pour que la condition désirée soit satisfaite.

Prouver que

$$\lim_{n \to +\infty} \frac{m(n)}{n^2} = \frac{2}{7}.$$

Exercice 126 **

Soit $E = \{M_1, M_2, \ldots, M_n\}$ un ensemble de $n \geq 3$ points appartenant à un même cercle Γ. Pour $i = 1, \ldots n$, on désigne par G_i l'isobarycentre des $n-1$ points de $E \backslash \{M_i\}$, et par Δ_i la droite passant par G_i et perpendiculaire à la tangente à Γ en M_i.

Prouver que les droites $\Delta_1, \Delta_2, \ldots, \Delta_n$ sont concourantes.

VI. Solutions de la Muraille

Solution de l'exercice 1 (résolu par Khalil Besrour) On note c pour cochon et l pour lapin. D'apres l'énoncé,

$$\begin{aligned} 7c + 1l &> 3c + 7l \\ 4c &> 6l \\ c &> 1.5l \end{aligned}$$

Un repas de 3 cochons et 7 lapins correspond à plus de 11.5 lapins, et il avait encore faim après ça. Donc s'il ne manque que 11 lapins il aura encore faim.

Solution de l'exercice 4 (Résolu par Alexandre Thiault) On remarque que

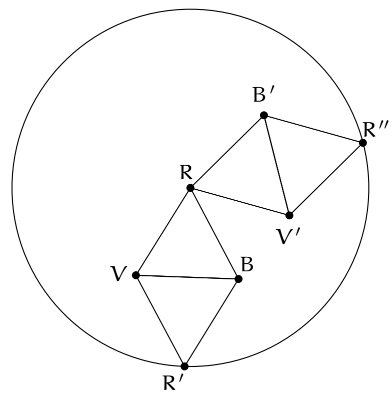
$$(a-b)^2 + (a-c)^2 + (b-c)^2 = 2(ab + bc + ca - (a^2 + b^2 + c^2)) = 0.$$

Ainsi, on doit avoir $(a-b)^2 = (a-c)^2 = (b-c)^2 = 0$, donc $a = b = c$.

Solution de l'exercice 5 (résolu par Titouan Poquillon) Le produit de tous ces nombres est 1, donc il y a un nombre pair de -1. Mais s'il y a un nombre pair de -1, il y a un nombre impair de 1 et leur somme ne peut pas être égale à 0.

Solution de l'exercice 6 (résolu par Timothée Defourné) Pour résoudre ce problème il faut d'abord trouver ce que le plus gradé doit faire avec 2, 3, 4 puis 5 pirates (pour des raisons de styles, je parlerai des grades dans l'ordre suivant : le capitaine, le second, le quartier-maitre, le matelot et le mousse) :
- Avec 2 pirates : Aucun partage ne pourra être accepté car il faudrait convaincre le mousse (le pirate le moins gradé), alors qu'il pourrait voter contre, tuer le matelot et garder tout le trésor pour lui.
- Avec 3 pirates : le quartier-maitre garde tout pour lui ! Comme le matelot ne veut pas être tué par le mousse il acceptera n'importe quel partage. Le partage est donc 100-0-0.
- Avec 4 pirates : le second doit convaincre deux personnes d'accepter son partage. Pour cela il suffit de donner une pièce au matelot et au mousse, et s'ils refusaient ils se retrouveraient sans le sou. Le partage est donc 98-0-1-1.
- Avec 5 pirates : le capitaine doit aussi convaincre deux personnes. Pour cela il doit donner à deux personnes plus de pièces qu'ils n'en ont dans le partage précédent : le partage est soit 97-0-1-0-2, soit 97-0-1-2-0.

Solution de l'exercice 10 (résolu par Alexandre Thiault) Nous allons considérer des losanges de côté 1 comme dans la figure suivante :



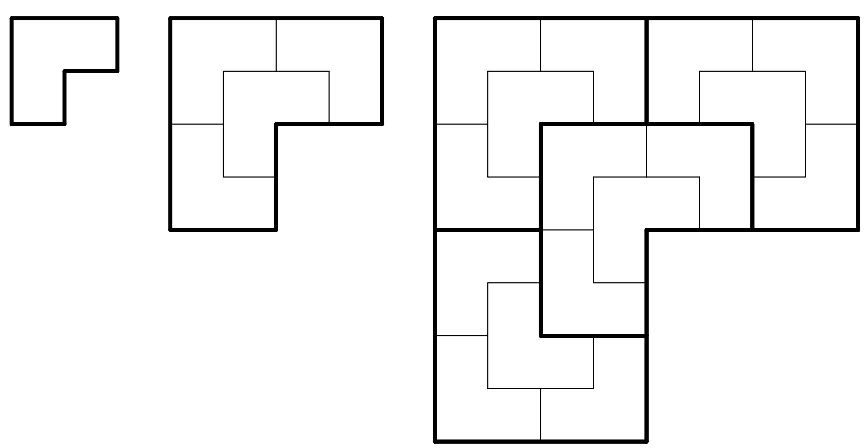
Si le point R est colorié en rouge, alors il faut que les points V et B soient vert et bleu sinon on a fini, et le point R' est rouge également. Il est facile de calculer la distance RR' : c'est deux fois la hauteur d'un triangle équilatéral de côté 1, donc $RR' = \sqrt{3}$. En faisant tourner le losange, on prouve que tous les points du cercle de centre R et de rayon $\sqrt{3}$ sont rouges, et il est facile de trouver deux points du cercle distants de 1.

Solution de l'exercice 11 (Résolu par Adrien Lemercier) On a

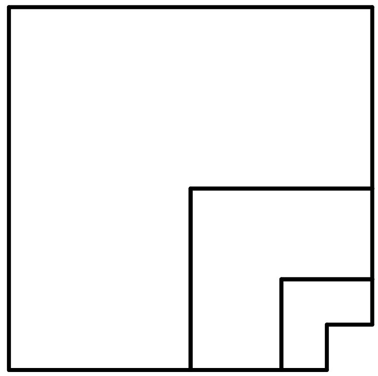
$$\frac{6}{1-\frac{5}{7}} = \frac{6}{\frac{2}{7}} = 21.$$

Solution de l'exercice 13 (Résolu par Adrien Lemercier) Par le théorème de Pythagore, on a $c^2 = a^2+b^2$. Montrons le résultat de l'énoncé par récurrence. Initialisation : $c^3 = c\cdot c^2 = c(a^2+b^2) = c\cdot a^2 + c\cdot b^2$. Or par hypothèse $c > a$ et $c > b$, et donc $c\cdot a^2 + c\cdot b^2 > a^3 + b^3$. Propagation : supposons que $c^n > a^n + b^n$. Alors $c^{n+1} = c\cdot c^n > c(a^n + b^n) > c\cdot a^n + c\cdot b^n > a^{n+1} + b^{n+1}$, ce qui clôt la récurrence.

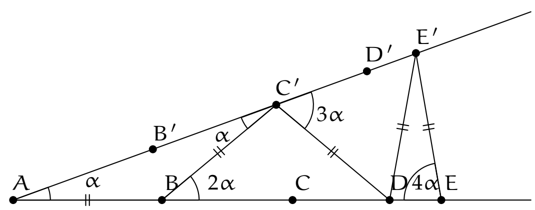
Solution de l'exercice 14 (résolu par Moïse Blanchard et Marc Michaux simultanément) Tout d'abord on remarque qu'on peut construire des coins de côté 2, 4, 8, etc de la manière suivante :



Ensuite il est facile de recouvrir le carré de côté 2^n où il manque un carré comme ceci :

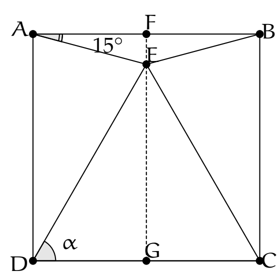


Solution de l'exercice 16 (résolu par Adrien Lemercier) On note α l'angle $\widehat{BAB'}$:



Nous avons beaucoup de triangles isocèles, donc la chasse aux angles n'est pas très dure. On trouve facilement $\widehat{AEE'} = 4\alpha$. De même, $\widehat{AE'E} = 4\alpha$, et en faisont la somme des angles dans le triangle AEE', on trouve $9\alpha = 180°$, et $\alpha = 20°$.

Solution de l'exercice 18 (résolu par Alexandre Thiault) Commençons par faire une figure :



Le triangle AEB est isocèle en E, donc CDE l'est aussi. On considère $AB = 1$. Dans ce cas $EF = \frac{1}{2}\tan(15°)$ et $EF = \frac{1}{2}\tan(\alpha)$, mais on a aussi $AG = 1 - EF$, donc $\tan(\alpha) = 2 - \tan(15°)$. Or

$$\tan\left(\frac{x}{2}\right) = \frac{1-\cos(x)}{\sin(x)} \implies \tan(15°) = \frac{1-\cos(30°))}{\sin(30°))} = \frac{1-\sqrt{3}/2}{1/2} = 2-\sqrt{3}.$$

Donc $\tan(\alpha) = \sqrt{3}$, $\alpha = 60°$, le triangle CED est equilatéral et $\widehat{CED} = 60°$.

Solution de l'exercice 20 (Résolu par Tobias Parker) On découpe la somme de la manière suivante :

$$\frac{1}{2}-\frac{1}{3}+\frac{1}{4}-\frac{1}{5}+\frac{1}{6}+\left(-\frac{1}{7}+\frac{1}{8}\right)+\left(-\frac{1}{9}+\frac{1}{10}\right)+\ldots+\left(-\frac{1}{999}+\frac{1}{1000}\right).$$

Chaque terme entre parenthèses est négatif. Ainsi, la somme totale est inférieure à $\frac{1}{2}-\frac{1}{3}+\frac{1}{4}-\frac{1}{5}+\frac{1}{6}=\frac{23}{60}<\frac{2}{5}$.

Solution de l'exercice 21 (résolu par Moïse Blanchardet Marc Michaux simultanément) Soient ab les deux derniers chiffres du nombre de départ. Comme son carré se finit par un 6, on peut vérifier que $b=4$ ou 6. Si $b=4$, $b^2=16$, donc lorsqu'on fait le carré on a une retenue de 1. En posant la multiplicatin, on voit que le chiffre des dizaines du carré correspond au dernier chiffre de $2ab+1$, qui est un nombre impair. Pour $b=6$, comme $b^2=36$, c'est le même principe avec une retenue de 3.

Solution de l'exercice 22 (résolu par Maxence Seymat) Calculons les premiers termes :

$$\begin{aligned}
&u_0=u_1=1\\
&u_2=u_0+u_1=2\\
&u_3=u_0+u_1+u_2=4\\
&u_4=u_0+u_1+u_2+u_3=8\\
&\ldots\\
&u_{n+1}=(u_0+\cdots+u_{n-1})+u_n=u_n+u_n=2u_n
\end{aligned}$$

La suite u_n est une suite qui multiplie par 2 à chaque étape, donc $u_n=2^{n-1}$.

Solution de l'exercice 23 (résolu par Khalil Besrour) Pendant la réunion les 100 prisonniers décident d'un stratégie commune dont le personnage principal "x" est celui qui entrera en premier dans la salle de l'ampoule. Celui-ci doit être sûr que l'ampoule est éteinte sinon c'est à lui de l'éteindre. Le prochain prisonnier qui visitera la salle allumera l'ampoule et si un autre prisonnier entre après et voit l'ampoule allumée il ne fait rien, sauf x qui éteindra l'ampoule.

Pour la suite les autres prisonniers vont allumer la lampe à tour de rôle et x l'éteindra (si un prisonnier a déjà allumé l'ampoule une fois il ne fait plus rien). Pendant ce temps, x comptera combien de fois il a dû éteindre l'ampoule. Dès qu'il arrive à 99 il sait que tous les autres prisonniers sont passés et il peut l'annoncer.

Solution de l'exercice 26 (résolu par Aymeric Jacquin) On cherche des entiers positifs tels que $xy=x+y+3$:

$$\begin{aligned}
xy-x-y &= 3\\
x(y-1)-y &= 3\\
x(y-1)-y+1 &= 4\\
(x-1)(y-1) &= 4
\end{aligned}$$

On décompose 4 en produit de 2 facteurs entiers :

$$4=1\times 4=2\times 2=-1\times -4=-2\times -2$$

Comme x et y sont positifs, $x-1$ et $y-1$ sont supérieurs ou égaux à -1 et ne peuvent pas valoir -2 ou -4. L'ensemble des solutions est donc :

$$S = \{(3,3);(2,5);(5,2)\}.$$

Solution de l'exercice 39 (résolu par Aymeric Jacquin) Considérons deux cercles de centres A et B qui se coupent en P et tels que chaque centre est à l'extérieur de l'autre cercle (ie $AB > AP$ et $AB > BP$). Il faut alors que l'angle $\widehat{APB} > 60°$ (si $AP = BP$, c'est évident

Maintenant revenons à nos six cercles et supposons par l'absurde qu'aucun des centres ne soit inclus dans un autre cercle. Appelons les centre $A, B; C, D, E$ et F (lus dans l'ordre autour de P) et $\alpha_1 = \widehat{APB}$, $\alpha_2 = \widehat{BPC}$, ..., $\alpha_6 = \widehat{FPA}$. Par la propriété ci-dessus, $\alpha_i > 60°$ pour $i = 1, \dots, 6$ mais leur somme doit faire 360°, ce qui est impossible. Un des six cercles contient forcément le centre d'un autre.

Solution de l'exercice 41 (résolu par Noémie Cartier) Soit $n \in \mathbb{N}$

– supposons que le reste de la division euclidienne de 2^n par 3 est 1. alors

$$2^{n+1} = 2(3k+1) = 3 \times 2k + 2,$$

donc le reste de la division euclidenne de 2^{n+1} par 3 est 2.

– supposons que le reste de la division euclidienne de 2^n par 3 est 2. alors

$$2^{n+1} = 2(3k+2) = 3 \times (2k+1) + 1,$$

donc le reste de la division euclidenne de 2^{n+1} par 3 est 1.

Donc la suite des restes de division euclidienne de 2^n par 3 est 1,2,1,2,1,2, etc.

1. $2^n - 1$ est divisible par 3 ssi le reste de la division euclidienne de 2^n par 3 est 1, ssi n est pair.
2. $2^n + 1$ est divisible par 3 ssi le reste de la division euclidienne de 2^n par 3 est 2, ssi n est impair.

Solution de l'exercice 42 (résolu par Florent Noisette) Si un élément i est le plus petit d'un sous-ensemble, c'est que les autres éléments de ce sous-ensemble ont été choisis dans les $n-i$ éléments supérieurs à i. Donc la moyenne vaut

$$M = \frac{\sum_{i=1}^{n-k+1} i\binom{n-i}{k-1}}{\binom{n}{k}}.$$

Grace à l'identité

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

on obtient

$$M = \frac{1}{\binom{n}{k}} \times \left(\begin{array}{l} \binom{k-1}{k-1} + \binom{k}{k-1} + \dots + \binom{n-3}{k-1} + \binom{n-2}{k-1} + \binom{n-1}{k-1} + \\ \binom{k-1}{k-1} + \binom{k}{k-1} + \dots + \binom{n-3}{k-1} + \binom{n-2}{k-1} + \\ \binom{k-1}{k-1} + \binom{k}{k-1} + \dots + \binom{n-3}{k-1} \\ \dots \\ \binom{k-1}{k-1} \end{array} \right) = \frac{\sum_{i=1}^{n-k+1} \binom{n-i+1}{k}}{\binom{n}{k}}$$

On réutilise l'identité et on trouve

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

Solution de l'exercice 43 (résolu par Étienne Duclos) Il est facile de vérifier par récurrence que la fonction a pour formule

$$f(m,n) = 2 + \sum_{i=1}^{m-1} i - \sum_{i=1}^{n-1} i$$

On veut $f(p,q) = 2011$

$$2 + \sum_{i=1}^{p-1} i - \sum_{i=1}^{q-1} i = 2011 \iff \sum_{i=q}^{p-1} i = 2009.$$

On cherche des suites d'entiers consécutifs dont la somme est 2009.

– Pour tout nombre impair $2n+1$

$$\sum_{i=q}^{q+2n} = q + (q+1) + \cdots + (q+2n) = q(2n+1) + \frac{2n(2n+1)}{2} \equiv 0[2n+1].$$

– Pour tout nombre pair $2n$

$$\sum_{i=q}^{q+2n-1} = q + (q+1) + \cdots + (q+2n-1) = q(2n) + \frac{(2n-1)2n}{2} \equiv n[2n].$$

Pour être la somme de n nombres comsécutifs, un entier doit donc être un multiple de n si n est impair, et de $\frac{n}{2}$ si n est pair.

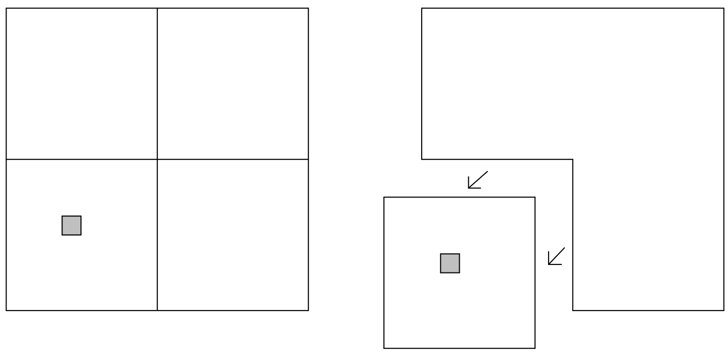
Étant donné que les diviseurs de 2009 sont 1, 7, 41, 49, 287 et 2009, seules des suites de 1, 2, 7, 14, 41, 49, 82, 98, 287, 574, 2009 et 4018 peuvent exister. La somme des nombres de 0 à 81 est supérieure à 2009, donc les sommes de plus de 82 entiers sont exclues. Les seules suites d'entiers consécutifs dont la somme fait 2009 sont l'entier 2009, le couple $(1004, 1005)$, les entiers de 284 à 290, de 137 à 150, de 29 à 69 et de 17 à 65. L'ensemble des solutions cherchées est donc :

$$\{(2010, 2009); (1006, 1004); (291, 284); (151, 137); (70, 29); (66, 17)\}.$$

Solution de l'exercice 45 (Résolu par Florent Noisette et Marc Ganet) C'est possible avec 8 langues, par exemple si chaque employé parle 4 langues, car il y a $\binom{8}{4} = 70$ ensembles de 4 langues distincts. Montrons par l'absurde que c'est impossible avec 7 langues. On code par un nombre binaire l'ensemble des langues parlées par chaque employé. Par exemple, si un employé parle les langues 1, 3 et 6, on lui associe le nombre 1010010. Si les codes de deux employés diffèrent d'un seul chiffre, alors l'ensemble des langues parlées par un de ces employés est inclut dans l'ensemble des langues parlées par l'autre. On groupe les 128 nombres binaires en 64 paires en disant que deux nombres sont dans la même paire si leurs 6 premiers chiffres sont les mêmes.

Si notre entreprise comporte 70 employés, par principe des tiroirs il y en a 2 dans la même paire, ce qui conclut.

Solution de l'exercice 46 (résolu par Tobias Parker et Colin Davalo simultanément) Tout d'abord je vous renvoie à la correction de l'exercice 14 pour voir comment construire un coin de taille 2^n. Ensuite pour gérer le carré manquant, on fait comme suit :



et on pave le petit carré par récurrence.

Solution de l'exercice 47 (résolu par Yasir Akram) Écrivons l'hypothèse sous la forme

$$f(x+y) = f(x)f(y) - f(xy) + 1.$$

On sait que $f(1) = 2$, prenons $y = 1$:

$$f(x+1) = 2f(x) - f(x) + 1 = f(x) + 1.$$

Il est facile de montrer par récurrence sue pour les entiers $f(n) = n+1$, et pour tout $x \in \mathbb{Q}$ et $n \in \mathbb{Z}$, $f(x+n) = f(x) + n$. Prenons $x = \frac{a}{b}$ et $y = b$.

$$\begin{aligned} f\left(\frac{a}{b} \cdot b\right) &= f\left(\frac{a}{b}\right) f(b) - f\left(\frac{a}{b} + b\right) + 1 \\ a + 1 &= (b+1) f\left(\frac{a}{b}\right) - f\left(\frac{a}{b}\right) - b + 1 \\ \frac{a+b}{b} &= f\left(\frac{a}{b}\right) \end{aligned}$$

donc pour tout $x \in \mathbb{Q}$, $f(x) = x + 1$.

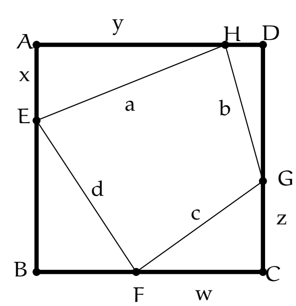
Solution de l'exercice 48 (résolu par Etienne Duclos et Sébastien Baumert simultanément) Soit A la colonne à laquelle appartient a et B la ligne à laquelle appartient b. On considère x l'intersection de A et B. On a alors $a \geqslant x$ et $b \leqslant x$ d'où $a \geqslant b$.

Solution de l'exercice 54 (Résolu par étienne Duclos) On note 1_a le nombre entier composé de a fois le chiffre 1. Par principe des tiroirs, il existe $a > b$ tels que 1_a et 1_b aient le même reste modulo n. Alors, leur différence est divisible par n, donc n divise $10^b \cdot 1_{a-b}$. Or n n'est divisible ni par 2 ni par 5, donc n est premier avec 10^b, donc n divise 1_{a-b}, ce qui termine.

Solution de l'exercice 55 (résolu par Paul Laubie) Si $n = 1$, aucune couleur n'est nécessaire. Si $n = 2$, il faut différencier les deux clés, donc il faut une couleur. Ensuite pour $n > 2$, il faut pouvoir savoir dans quel sens tenir le trousseau. S'il y a assez de clés un couleur suffit : on colorie BNBBNN puis que des blancs. Ainsi on sait que pour tenir le trousseau dans le bon sens, on doit voir le groupe de 1 N, puis le goupe de 2 N. pour faire ceci il faut au moins 6 clés. Ensuite il faut vérifier qu'avec 3, 4 ou 5 clés, toutes les dispositions à deux couleurs sont symétriques, donc il faut une troisième couleur.

<u>*Solution de l'exercice 56*</u> (Résolu par Ewen Goisot) On prend la convention usuelle disant qu'un produit vide vaut 1, et on va calculer la somme des produits de tous les sous-ensembles, ensemble vide compris (ce qui rajoute 1 à la somme), par récurrence sur n. On note cette somme S_n. Pour $n = 1$, les deux sous-ensembles sont $\emptyset$ et $\{1\}$, donc $S_1 = 2$. Supposons que que $S_n = n+1$. Il y a deux sortes de sous-ensembles de $\{1, 2, \dots, n+1\}$: ceux qui ne contiennent pas $n+1$, leur contribution à la somme est S_n, et ceux qui contiennent $n+1$, qui contribuent $\frac{S_n}{n+1}$. Donc $S_{n+1} = S_n(1 + \frac{1}{n+1}) = n+2$. Cela clôt la récurrence. Ainsi, le nombre cherché vaut $S_n - 1 = n$.

<u>*Solution de l'exercice 57*</u> (résolu par Sébastien Baumert) On place les points dans la configuration suivante :



Par Pythagore, $a^2 = x^2 + y^2$, $b^2 = (1-y)^2 + (1-z)^2$, etc pour c et d

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &= x^2 + (1-x)^2 + y^2 + (1-y)^2 + z^2 + (1-z)^2 + w^2 + (1-w)^2 \\ &= 2x^2 - 2x + 2y^2 - 2y + 2z^2 - 2z + 2w^2 - 2w + 4 \\ &= 2 + 2\left[(x-0.5)^2 + (y-0.5)^2 + (y-0.5)^2 + (y-0.5)^2\right] \\ &\geqslant 2 \end{aligned}$$

ce qui permet de montrer la première inégalité. Pour la seconde remontons un peu :

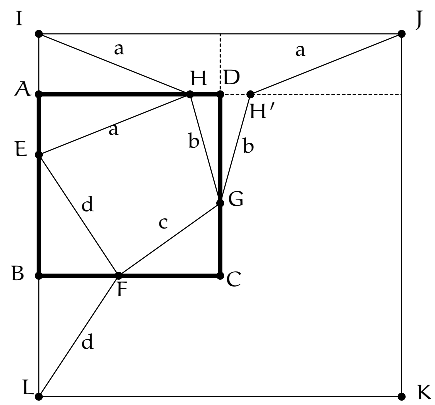
$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &= 2x^2 - 2x + 2y^2 - 2y + 2z^2 - 2z + 2w^2 - 2w + 4 \\ &= 4 + 2\left[x(1-x) + y(1-y) + z(1-z) + w(1-w)\right] \\ &\leqslant 4 \end{aligned}$$

puisque $x(1-x)$ est toujours négatif.

Passons à la somme des longueurs. D'après l'inégalité triangulaire, $a \leqslant x + y$, $b \leqslant (1-y) + (1-z)$, etc. En sommant les quatres on trouve

$$a + b + c + d \leqslant 4$$

Pour la dernière inégalité, faisons quelques symétries comme dans la figure suivante :



Il est facile e se rendre compte que IJKL est un carré de côté 1, donc la diagonale JL mesure $2\sqrt{2}$ et par l'inégalité triangulaire

$$2\sqrt{2} \leqslant a + b + c + d.$$

<u>*Solution de l'exercice 58*</u> (résolu par Paul Laubie) Le nombre attribué à chaque animateur est un entier naturel donc compris entre 0 et ∞. Appelons les animateurs A et B (la première question est posée à A).

1. si l'animateur A a le nombre 0, il peut répondre "oui" à la première question puisque 0 a un seul voisin ; par conséquent s'il dit "non" c'est qu'il n'a pas le nombre 0.
2. si l'animateur B a le nombre 1, il peut répondre "oui" à la deuxième question, puisqu'il sait que l'animateur A n'a pas le nombre 0, le seul voisin restant est 2 ; s'il répond "non" c'est qu'il n'a ni 0, ni 1.
3. si l'animateur A a le nombre 2, il peut répondre "oui" à la troisième question, s'il répond "non" c'est qu'il n'a ni 0, ni 1, ni 2.
4. etc

Par récurrence on peut montrer que si n est le plus petit des entiers donnés, l'animateur qui l'a reçu pourra répondre "oui" avant la $n+2$ème question.

<u>*Solution de l'exercice 59*</u> (résolu par Florent Noisette) Nous considérons l'expérience suivante : lançons des pièces à pile ou face et arrêtons-nous dès que nous avons $(n+1)$ piles ou $(n+1)$ faces. Il est évident que l'expérience s'arrêtera au plus tard après le $(2n+1)$-ème lancer.

Soit $k \leqslant n$, calculons la probabilité $\mathbb{P}[n+k+1]$ que l'expérience s'arrête après le $(n+k+1)$-ème lancer. Pour cela si le dernier lancer était Pile, il fallait qu'il y ait n Pile et k Face parmi les $n+k$ lancers précédents.

$$\mathbb{P}[n+k+1] = \frac{1}{2}\binom{n+k}{n}\frac{1}{2^{k+n}} + \frac{1}{2}\binom{n+k}{k}\frac{1}{2^{k+n}}$$

(le premier terme correspond au dernier lancer Pile, et le deuxième terme au dernier lancer Face. Comme l'expérience se finit entre le $(n+1)$-ème et le $(2n+1)$-ème lancer, on a

$$\sum_{k=0}^{n} \mathbb{P}[n+k+1] = 1 \implies \sum_{k=0}^{n} \binom{n+k}{k}\frac{1}{2^{k+n}} = 1$$

Solution de l'exercice 61 (résolu par Théo Guillaumot et Quentin Woinet) On veut que les probabilités $P(n)$ de sorties des nombres $2 \leqslant n \leqslant 12$ soient égales, à $\frac{1}{11}$. On remarque que 2 ne sort que si les deux dés tombent sur 1 et que 12 ne sort que lorsqu'on fait un double 6, donc

$$p_1q_1 = p_6q_6 = \frac{1}{11} \implies q_1 = \frac{1}{11p_1} \text{ et } q_2 = \frac{1}{11p_2}.$$

Intéressons nous maintenant à la probabilité que 7 sorte :

$$\frac{1}{11} = P(7) = p_1q_6 + p_2q_5 + p_3q_4 + p_4q_3 + p_5q_2 + p_6q_1 \geqslant p_1q_6 + p_6q_1$$

$$\begin{aligned} p_1q_6 + p_6q_1 &\leqslant \frac{1}{11} \\ \frac{p_1}{11p_6} + \frac{p_6}{11p_1} &\leqslant \frac{1}{11} \\ p_1^2 + p_6^2 &\leqslant p_1p_6 \end{aligned}$$

ce qui est en contradiction avec l'inégalité $a^2 + b^2 \geqslant 2ab$. Il est donc impossible de truquer les dés de manière à ce que les entiers de 2 à 12 aient la même probabilité.

Solution de l'exercice 62 (résolu par Etienne Duclos) Soient $(a_1, a_2, \dots, a_{2n})$ l'ensemble des entiers de 1 à $2n$, et $(b_1, b_2, \dots, b_{2n})$ le même ensemble dans un ordre différent. On note $(c_1, c_2, \dots, c_{2n})$ l'ensemble des restes des $a_i + b_i$ modulo $2n$. Alors on a

$$\sum a_i + b_i \equiv \sum c_i [2n].$$

De plus, supposons que tous les c_i ont des valeurs différentes, comme il y a $2n$ termes qui sont tous des entiers entre 0 et $2n - 1$, chaque entier correspond à un c_i. Montrons que dans ce cas l'equivalence modulo 2N au dessus n'est pas vérifiée.

$$\sum_{i=1}^{n} a_i + b_i = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = 2 \times \frac{2n(2n+1)}{2} = 2n(2n+1) \equiv 0 \ [2n]$$

$$\sum_{i=1}^{n} c_i = \frac{2n(2n-1)}{2} = n(2n+1) \equiv n \ [2n]$$

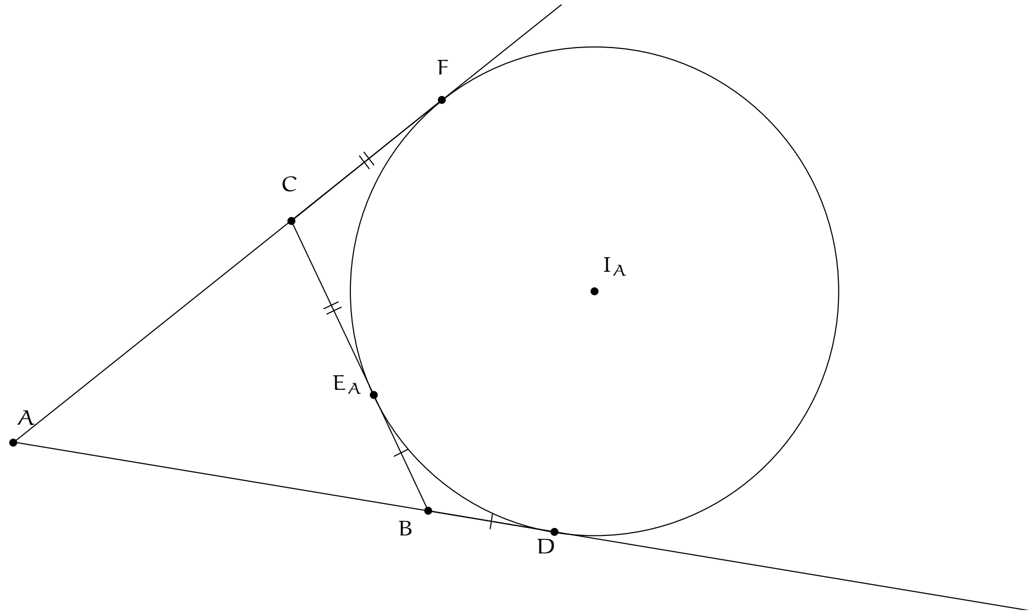
Nous avons notre contradiction, il y a deux restes qui sont égaux.

Solution de l'exercice 63 (résolu par Alexander Semenov) Notons x_1 le nombre de pièces de 1 centime, x_2 2 centimes, x_5 5 centimes, etc pour x_{10}, x_{20}, x_{50} et x_{100}. Donc

$$x_1 + 2x_2 + 5x_5 + 10x_{10} + 20x_{20} + 50x_{50} + 100x_{100} = M$$

Si on prend x_1 pièces de 1 euro, $2x_2$ pièces de 50c, $5x_5$ pièces de 20c, $10x_{10}$ pièces de 10c, ...et $100x_{100}$ pièces de 1c, on aura exactement M pièces pour une somme de N euros.

Solution de l'exercice 64 (résolu par Yassine Hamdi) Pour la première question nous allons vouloir utiliser le théorème de Ceva. Il faut donc calculer les rapports du type $\frac{BE_A}{CE_A}$. Faisons une figure avec un seul cercle exinscrit :



On introduit D et F les points où le cercle est tangent avec (AB) et (AC) respectivement. Les deux tangentes du cercle issues de B sont BD et BE_A ; donc les longueurs sont égales : $BD = BE_A$. De même $CF = CE_A$, et $AD = AF$. $AD = AB + BD = AB + BE_A$ et $AF = AC + CF = AC + CE_A$, et

$$AD = AF = \frac{AD + AF}{2} = \frac{AB + BE_A + AC + CE_A}{2} = \frac{AB + AC + BC}{2}$$

Si on note $p = \frac{AB+AC+BC}{2}$ le demi-perimètre, alors on a $BE_A = p - AB$ et $CE_A = p - AC$. On fait le même calcul pour E_B et E_C et on applique Ceva :

$$\frac{BE_A}{CE_A} \cdot \frac{CE_B}{AE_B} \cdot \frac{AE_C}{BE_C} = \frac{p - AB}{p - AC} \cdot \frac{p - BC}{p - AB} \cdot \frac{p - AC}{p - BC} = 1$$

donc les trois droites sont concourantes.

Attaquons nous à la deuxième question. Le théorème de Carnot dit que trois droites perpendiculaires aux coôtés d'un triangle en E_A, E_B et E_C sont concourantes ssi :

$$BE_A^2 - E_A C^2 + CE_B^2 - E_B A^2 + AE_C^2 - E_C B^2 = 0,$$

or $BE_A = AE_B = p - AB$, $AE_C = CE_A = p - AC$ et $CE_B = BE_C = p - BC$ d'où la conclusion.

Solution de l'exercice 67 (Résolu par étienne Duclos) On numérote les sommets de 1 à n. On appelle a_k le nombre d'étapes où l'on a enlevé deux pions du sommet a_k. Pour revenir à la configuration initiale, il faut avoir enlevé autant de jetons du sommet k que l'on en a rajouté, et donc il faut $2a_k = a_{k-1} + a_{k+1}$ (avec la convention $a_{n+1} = a_1$. Cela permet de montrer par récurrence que $b_k = kb_1 - (k-1)b_n$. En appliquant cela en $k = n+1$, cela donne $b_1 = (n+1)b_1 - nb_n$, et donc $b_1 = b_n$. Par symétrie, tous les b_i sont égaux.

Solution de l'exercice 69 (résolu par Aymeric Jacquin) On commence par chercher les premiers termes de la suite. Lorsqu'il y a un seul siège, l'enfant est obligé de rester sur place, $u_0 = 1$.

Lorsqu'il y a deux personnes, elles peuvent soit rester sur place, soit échanger de place, $u_2 = 2$. Avec trois personnes, soit les deux de droite switchent, soit les deux de gauche, soit personne ne bouge, $u_3 = 3$. On vérifie facilement que $u_4 = 5$.

Cas général : à chaque fois que l'on rajoute un siège, il y a deux cas :

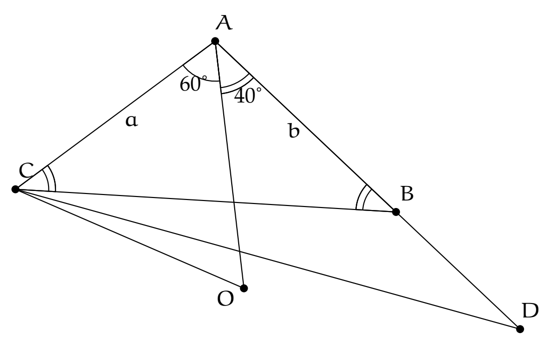
– soit la personne tout au bout ne bouge pas, et les $n-1$ autres choisissent un déplacement parmi les u_{n-1} possibles,
– soit la personne tout au bout change de place avec son voisin, et les $n-2$ autres choisissent un déplacement parmi les u_{n-2} possibles.

On obtient donc la formule récurrente suivante :

$$u_n = u_{n-1} + u_{n-2}.$$

La suite fait 1,2,3,5,8,11,19, etc (pour les connaisseurs, il s'agit de la suite de Fibonacci).

Solution de l'exercice 71 (résolu par Florent Noisette) Commençons par faire un dessin :



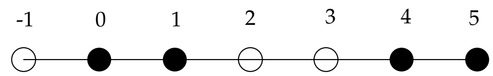
Soit O le point crée en faisant faire une rotation de 60° de centre A à C. Le triangle OAC a un angle de 60° et deux côtés égaux, c'est fonc un triangle equilatéral.

Regardons maintenant le triangle AOD : l'angle $\widehat{OAD}$ fait 40^circ comme les angles de base du triangle ABC, $OA = AC$ et $AD = BC$, donc le triangle OAD est identique au triangle ABC, $OD = OA$, O est le centre du cercle passant par A, C et D. L'angle $\widehat{ADC}$ vaut la moitié de l'angle au centre, c'est-à-dire 30°.

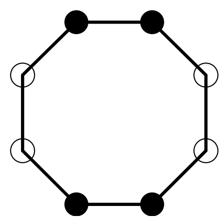
Solution de l'exercice 74 (résolu par Étienne Duclos) Lorsque nous regarderons des polygones, nous numéroterons les sommets $1, 2, \ldots, n$ dans l'ordre (parfoiis nous appellerons n le sommet 0). Essayons de construire un polygone sans triangle isocèle monochrome.

Supposons qu'il n'y ait jamais deux sommets de même couleur côte à côte. Dans ce cas les sommets sont colorés alternativement noir, blanc, noir, blanc. Si on prend les sommets 1, 3 et 5 on aura un triangle isocèle monochrome. Il existe donc deux sommets voisins de même couleur, disons noirs.

Prenons ces deux sommets noirs et mettons les en 0 et 1. Du coup, les points -1 et 3 sont plancs, sinon en prenant 3 points consécutifs noirs on aurait un triangle isocèle noir. Ensuite, 5 doit être noir sinon $(-1, 2, 5)$ serait un triangle blanc. Le sommet 3 doit être blanc à cause du triangle $(1, 3, 5)$ et 4 doit être noir à cause de $(2, 3, 4)$.



Donc les points 4 et 5 sont aussi deux points consécutifs noirs, on peut les mettre en 0 et 1 et recommencer le raisonnement. Donc si un polygone n'a aucun triangle isocèle monochrome, alors ses sommets sont coloriés noir, noir, blanc, blanc, noir, noir, blanc, blanc, etc. Cela signifie entre autres que n est divisible par 4. De plus si le motif est répété trois fois de suite, on prend le premier sommet de chaque motif et on obtient un triangle isocèle noir. Donc $n < 12$. Le seul multiple de 4 compris entre 6 et 11 est 8, $n = 8$ est la seule solution.



Solution de l'exercice 75 (résolu par Ewen Goisot) On colorie le quadrillage 57×57 avec des cases noires et blanches comme un échiquier. On aura alors 1625 cases noires et 1624 cases blanches. Si on veut déplacer chaque pion sur une case adjacente il faut que chaque pion sur une case blanche aille sur une case noire et vice-versa. Comme il y a plus de cases noires que de blanches, c'est impossible.

Solution de l'exercice 76 (Résolu par Antoine Dupuis) On commence par montrer que la fonction $f : [0, \pi] \to \mathbb{R}$ définie par $f(x) = \frac{1}{\sin^2 x}$ est convexe. Pour cela, on dérive deux fois, on trouve $f'(x) = \frac{-2\cos x}{\sin^3 x}$, puis $f''(x) = 2\frac{\sin^2 x + 3\cos^2 x}{\sin^4 x}$ qui est bien strictement positif. Ensuite, on transforme l'inégalité de départ en

$$\frac{a^2b^2c^2}{R^2} \leqslant b^2c^2 + a^2c^2 + a^2b^2.$$

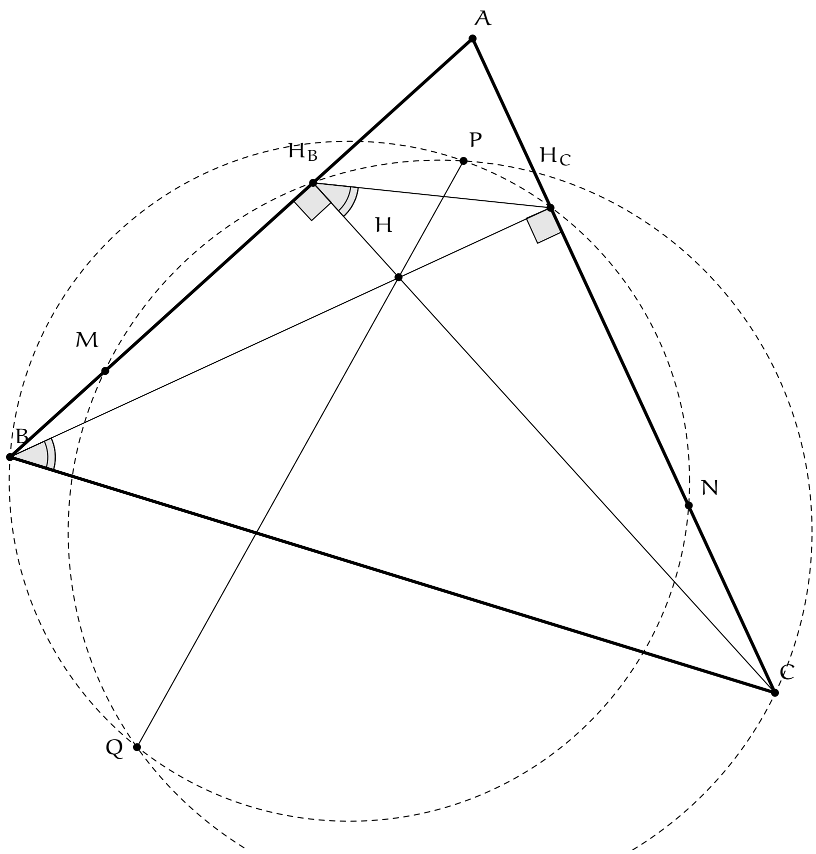
En notant S l'aire du triangle et en utilisant les formules $4RS = abc$ et $2S = bc\sin\alpha = ca\sin\beta = ab\sin\gamma$, où α, β et γ sont les angles du triangle placés à l'opposé des côtés BC, CA et AB. l'inégalité devient

$$4 \leqslant f(\alpha) + f(\beta) + f(\gamma).$$

Comme $\alpha + \beta + \gamma = \pi$, et comme $f\left(\frac{\pi}{3}\right) = \frac{4}{3}$, l'inégalité cherchée est l'inégalité de Jensen appliquée à la fonction f.

Solution de l'exercice 77 (résolu par Alexander Semenov) Soit v la vitesse des fourmis. Dans l'exercice on observe le mouvement des fourmis par rapport au carré. Nous, nous allons regarder le mouvement par rapport à une des fourmis F_1. Cette fourmi fait toujours face à la fourmi F_2. À sa droite elle verra toujours la fourmi F_4 qui s'approche d'elle en "ligne droite" (cela semblera être une ligne droite pour F_1) avec une vitesse relative v (le fait que cette vitesse soit la même que celle de départ est lié au fait que l'on est sur un carré et que les angles sont droits). Ainsi la fourmi F_4 rejoindra sa cible après avoir parcouru $1m$. Toutes les fourmis auront parcouru $1m$.

Solution de l'exercice 78 (résolu par Antoine Dupuis et Mehdi Trense) Tout d'abord faisons une figure :



Les points P, q et h sont alignés ssi H appartient à l'axe radical de Γ_1 et Γ_2. Or H_c appartient à $Gamma_1$ puisque $\widehat{NH_CC} = 90°$ et que NC est le diamètre de Γ_1, idem pour H_B et Γ_2. Donc

$$H \in [PQ] \Leftrightarrow HH_B \cdot HB = HH_C \cdot HC \Leftrightarrow \frac{HH_B}{HC} = \frac{HH_C}{HC}.$$

Donc si on arrive à prouver que les triangles HBC et HH_CH_B sont semblables on aura gagné. Ces deux triangles ont déjÌangle $\widehat{H}$ en commun, il nous en faut un deuxième. On sait également que B, C, H_B, H_C sont cocycliques (tous sur le cercle de diamètre BC), donc les angles inscrits sont égaux : $H_B\widehat{H_C}C = \widehat{H_BB}C$, ce qui achève la démonstration.

Solution de l'exercice 81 (résolu par Nathanaël Courant et Lucas Flammant simultanément) On place le polygone dans un plan muni d'un repère orthonormé. Il est facile de prouver par continuité qu'il existe une unique droite horizontale qui coupe le polygone en deux parties de même aire, et de même pour une droite verticale. Par contre il n'est pas sûr que les deux droites coupent le polygone en 4 parties de même aire (on peut juste vérifier que l'aire en haut à gauche est égale à l'aire en bas à droite). Ce que nous allons faire c'est faire pivoter continuement par un angle α le polygone et à chaque fois considérer la droite horizontale qui coupe le polygone pivoté en deux parties de même aire. On considère $A(\alpha)$ l'aire de la partie en haut à droite et $B(\alpha)$ celle de la partie en bas à gauche. La fonction $f(\alpha) = A(\alpha) - B(\alpha)$

change de signe entre 0° et 90°, et est continue (*Note du correcteur :* il n'est pas si facile de vérifier que la fonction est continue), donc elle s'annule pour un α. En cet α le polygone est coupé en 4 parties de même aire.

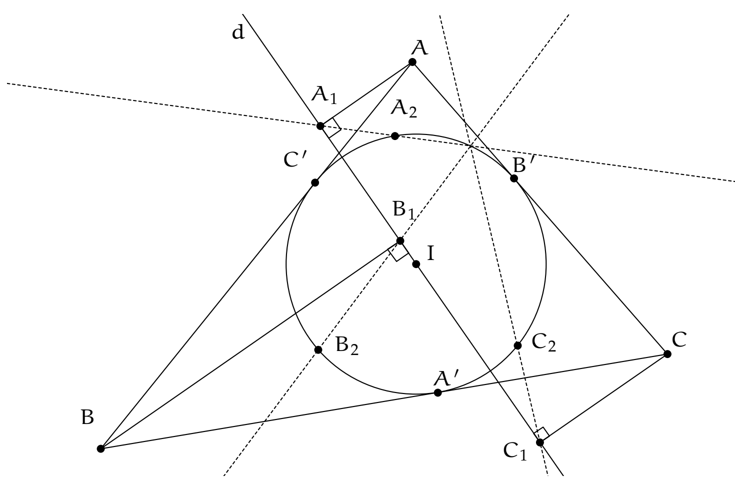
Solution de l'exercice 83 (Résolu par Lucas Flammant) Supposons par l'absurde que les trois racines de P soient rationnelles, on les met au même dénominateur et on les note $\frac{p_1}{q}$, $\frac{p_2}{q}$ et $\frac{p_3}{q}$. Alors

$$\begin{aligned} P(X) &= a\left(X-\frac{p_1}{q}\right)\left(X-\frac{p_2}{q}\right)\left(X-\frac{p_3}{q}\right) \\ &= aX^3 - a\left(\frac{p_1+p_2+p_3}{q}\right)X^2 + a\left(\frac{p_1p_2+p_2p_3+p_3p_1}{q^2}\right)X - a\left(\frac{p_1p_2p_3}{q^3}\right) \\ &= aX^3+bX^2+cX+d. \end{aligned}$$

On peut donc identifier les termes : on a $b = -a\left(\frac{p_1+p_2+p_3}{q}\right)$, $c = a\left(\frac{p_1p_2+p_2p_3+p_3p_1}{q^2}\right)$ et $d = -a\left(\frac{p_1p_2p_3}{q^3}\right)$. Supposons q impair. Comme a et d sont impairs par hypothèse, $p_1p_2p_3$ doit aussi être impair, donc les trois p_i sont impairs, donc leur somme est impaire, donc b est impair. Comme bc est pair par hypothèse, c est pair, donc $p_1p_2+p_2p_3+p_3p_1$ doit aussi être pair, c'est absurde.

On sait donc que p est pair. Ainsi $p_1p_2p_3$ est divisible par 8. Si un seul des p_i est pair, alors $p_1p_2+p_2p_3+p_3p_1$ est impair, or le nombre impair $a(p_1p_2+p_2p_3+p_3p_1)$ doit être divisible par le nombre pair q, c'est absurde. Donc au moins deux des p_i sont pairs. Comme $p_1+p_2+p_3$ doit être divisible par q, la somme est paire, donc en fait les 3 nombres p_i sont pairs, et les trois fractions sont simplifiables par 2. On conclut donc par descente infinie.

Solution de l'exercice 84 (résolu par Arthur Blanc-Renaudie et Cyril Letrouit) Commençons par une figure



Nous allons raisonner en complexe. On considère que le cercle inscrit est le cercle unité et la droite d est la droite déelle. On pose A', B' et C' les points de tangence du cercle inscrit avec les trois côtés, qui auront pour affixes respectives p, q et r, donc $p\overline{p} = q\overline{q} = r\overline{r} = 1$. De plus d'après des relations connues (cf cours d'imomaths sur les nombres complexes) les affixes de A, B et C seront :

$$a = \frac{2qr}{q+r},\ b = \frac{2pr}{p+r}\ \text{ et }\ c = \frac{2pq}{p+q}.$$

Donc l'affixe de A_1 qui est sur la droite réelle est $a_1 = \mathcal{R}](a)$:

$$a_1 = \frac{a+\overline{a}}{2} = \frac{\frac{2qr}{q+r} + \frac{2\overline{qr}}{\overline{q+r}}}{2} = \frac{q+r+\overline{q}+\overline{r}}{(q+r)(\overline{q}+\overline{r})}$$

$$b_1 = \frac{p+r+\overline{p}+\overline{r}}{(p+r)(\overline{p}+\overline{r})} \text{ et } c_1 = \frac{p+q+\overline{p}+\overline{q}}{(p+q)(\overline{p}+\overline{q})}.$$

Nous devons montrer que A_1A_2 intersecte γ en un point qui a une affixe symétrique en p, q, r car ce point sera aussi sur B_1B_2 et C_1C_2. Cherchons donc le point d'affixe ω tel que

$$\frac{a_2-\omega}{\overline{a_2}-\overline{\omega}} = \frac{a_1-a_2}{\overline{a_1}-\overline{a_1}}.$$

Comme $a_2 = -p$, on a

$$\frac{a_2-\omega}{\overline{a_2}-\overline{\omega}} = \frac{p+\omega}{\overline{p}+\overline{\omega}} = \omega p,$$

$$\frac{a_1-a_2}{\overline{a_1}-\overline{a_1}} = \frac{a_1+p}{\overline{a_1}+\overline{p}} = \frac{q+r+\overline{q}+\overline{r}+p(q+r)(\overline{q}+\overline{r})}{q+r+\overline{q}+\overline{r}+\overline{p}(q+r)(\overline{q}+\overline{r})}$$

$$\text{Donc } \omega = \frac{q+r+\overline{q}+\overline{r}+p(q+r)(\overline{q}+\overline{r})}{pq+pr+p\overline{q}+p\overline{r}+(q+r)(\overline{q}+\overline{r})}.$$

On multiplie en haut et en bas par qr pour se débarasser des conjugués et on trouve

$$\omega(p,q,r) = \frac{q^2r+qr^2+r+q+pq^2+pr^2+2pqr}{pq^2r+pqr^2+pr+pq+q^2+r^2+2qr}.$$

Cette expression est symétrique en q et r, il nous suffit donc de vérifier que $\omega(p,q,r) = \omega(q,r,p)$ et on aura fini. Je laisse au lecteur le soin de vérifier que :

$$(q^2r+qr^2+q+r+pq^2+pr^2+2pqr)(qr^2p+qrp^2+qp+qr+r^2+p^2+2rp)$$

$$= (r^2p+rp^2+r+p+qr^2+qp^2+2qrp)(pq^2r+pqr^2+pr+pq+q^2+r^2+2qr),$$

après tout il n'y a que 98 termes à distribuer (je vous promet que ça marche).

<u>*Solution de l'exercice 85*</u> (résolu par Lucas Flammant) Commençons par associer à chacune configuration de n pièces un suite binaire (disons que pile correspond à 0 et face à 1). Nous dirons que deux configurations (ou deux suites) sont voisines lorsqu'elles ne diffèrent que d'un seul chiffre.

Pour réussir son tour, la magicienne doit répartir les 2^n configurations en n ensembles $E_1, \dots, E_n$ (si la configuration de pièces qu'elle voit à la fin est dans l'ensemble E_i, elle annonce le chiffre i). De plus, les ensembles $E_1, \dots, E_n$ doivent vérifier la condition suivante : pour toute configuration X, l'ensemble des voisins de X doit se répartir parfaitement dans les ensembles $E_1, \dots, E_n$ (un voisin par ensemble). En effet, si X est la configuration choisie par la spectatrice et i l'entier choisi, l'assistante doit pouvoir choisir une configuration voisine de X qui appartienne à E_i. Le problème est donc de trouver les entiers n pour lesquels une telle répartition est possible.

Soit n tel que le tour soit possible. On répartit les configurations en n ensembles. Nous allons dénombrer les couples (X, Y) de suites binaires telles que X et Y soient voisines et $Y \in E_i$.

Si on choisit Y d'abord, on a $|E_i|$ choix pour Y et n choix pour X (Y a n voisins). Si on commence par choisir X, on a 2^n choix pour X et un seul pour Y (X a un seul voisin dans E_i). donc

$$n|E_i| = 2^n,$$

donc n est une puissance de 2.

Réciproquement, montrer que si $n = 2^k$ le tour est faisable. Pour chaque entier $i \in [[1, n]]$, on associe la suite binaire B_i de longueur k qui correspond à son écriture en binaire. Faisons la répartition suivante : pour chaque configuration X on garde toutes les B_i qui correspondent à des pièces face et on fait leur addition chiffre à chiffre sans faire de retenue (on fait XOR pour les informaticiens). Le résultat est une suite binaire de longueur k, donc correspond à un entier entre 1 et n et permet de savoir dans quel ensemble E_i on place X. Je laisse au lecteur le soin de se persuader que cette répartition satisfait les conditions que l'on cherchait.

Ainsi le tour de magie est possible si et seulement si n est une puissance de 2.

Solution de l'exercice 86 (résolu par Arthur Blanc-Renaudie)

Premier cas : Pour $n = 6$. Comme il y a 6 clous, il y a $\binom{6}{3}$ triangles, et comme il y a 6 couleurs il y a $\binom{6}{3}$ triplets de couleurs différents. Comme il y a au moins un triangle pour chaque triplet, il y a exactement un triangle pour chaque triplet de couleurs. Chaque ficelle fait partie de exactement 4 triangles et chaque couleur doit faire partie de exactement 10 triangles. Le nombre de ficelles d'une couleur donnée est donc $\frac{10}{4} = 2.5$, ce qui est impossible.

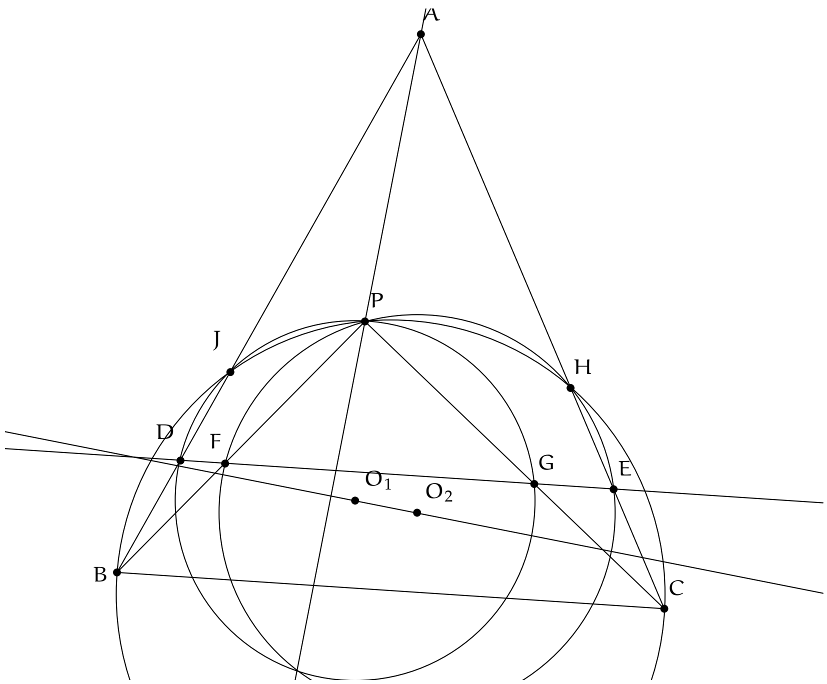
Deuxième cas : Pour $n = 7$. Nous allons construire une configuration sui vérifie les conditions de l'énoncé. On va numéroter les clous et les couleurs de 1 à 7, et on va relier les clous i et j par une ficelle de couleur k ssi $i + j \equiv k[7]$. Maitenant, prouvons que cette coloration est adéquate : soient a, b et c trois couleurs différentes, il faut trouver trois clous x, y et z tels que :

$$\begin{cases} x + y \equiv a[7] \\ x + z \equiv b[7] \\ y + z \equiv c[7] \end{cases} \Longrightarrow \begin{cases} x \equiv \frac{a+b-c}{2}[7] \\ y \equiv \frac{a+c-b}{2}[7] \\ z \equiv \frac{b+c-a}{2}[7] \end{cases}$$

Comme 2 est inversible modulo 7 (d'inverse 4), de tels clous existent. Il suffit ensuite de vérifier que x, y et z sont distincts : $x - y \equiv b - c \not\equiv 0[7]$ puisque les trois couleurs sont distinctes.

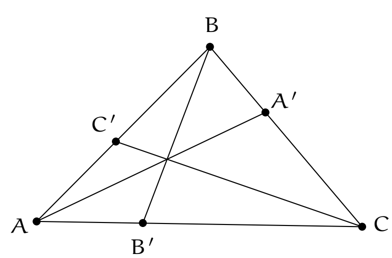
Solution de l'exercice 87 (Résolu par Yassir Akram et Arthur Blanc-Renaudie)

Soit J (resp. H) le deuxième point d'intersection du cercle circonscrit à DGP (resp. EPF) et de (AB) (resp. (AC)). On a $\widehat{BPH} = \widehat{FPH} = 180° - \widehat{DEH} = 180° - \widehat{BCH}$, donc B, C, H et P sont cocycliques. Un raisonnement symétrique montre que B, C, J et P sont eux aussi cocycliques, donc ces 5 points sont sur le même cercle.



Maintenant, $\widehat{AHJ} = 180° - \widehat{JHC} = \widehat{JBC} = \widehat{ABC}$. Un raisonnement symétrique donne que $\widehat{AJH} = \widehat{ACB}$. Donc ABC et AHJ sont semblables, donc $AJ \cdot AB = AH \cdot AC$ (NDLR : on pouvait obtenir cela plus tôt en regardant la puissance de A par rapport au cercle contenant B, C, J et H). Donc, d'après le théorème de Thalès, $AJ \cdot AD = AH \cdot AE$. Donc A appartient à l'axe radical des deux cercles circonscrits, et P aussi. Donc $(AP) \perp (O_1O_2)$.

Solution de l'exercice 88 (résolu par Cyril Letrouit) Faisons une figure pour se fixer les idées.



$$\begin{aligned} \overrightarrow{AA'} + \overrightarrow{BB'} + \overrightarrow{CC'} &= \overrightarrow{0} \\ \overrightarrow{AB} + \overrightarrow{BA'} + \overrightarrow{BC} + \overrightarrow{CB'} + \overrightarrow{CA} + \overrightarrow{AC'} &= \overrightarrow{0} \\ \overrightarrow{BA'} + \overrightarrow{CB'} + \overrightarrow{AC'} &= \overrightarrow{0} \end{aligned}$$

Comme A' est sur le segment $[BC]$, il existe $j \in (0, 1)$ tel que $\overrightarrow{BA'} = j\overrightarrow{BC}$. De même $\overrightarrow{CB'} = k\overrightarrow{CA}$ et $\overrightarrow{AC'} = l\overrightarrow{AB}$.

$$\begin{aligned} j\overrightarrow{BC} + k\overrightarrow{CA} + l\overrightarrow{AB} &= \overrightarrow{0} \\ (k - j)\overrightarrow{CA} + (l - j)\overrightarrow{AB} &= \overrightarrow{0} \end{aligned}$$

Mais les vecteurs $\overrightarrow{CA}$ et $\overrightarrow{AB}$ ne sont pas colinéaires, donc $k - j = l - j = 0$, donc $j = k = l$.

À présent nous allons utiliser le fait que AA', BB' et CC' sont concourantes, donc par Céva :

$$\frac{AB'}{B'C} \cdot \frac{CA'}{A'B} \cdot \frac{BC'}{C'A} = 1 \implies \left(\frac{1-j}{j}\right)^3 = 1 \Longrightarrow j = \frac{1}{2}.$$

Les points A', B' et C' sont les milieux de leurs segments respectifs.

<u>*Solution de l'exercice 90*</u> (résolu par Nathanaël Courant) On considère un polygone non croisé qui passe par les n points et on le triangule. On aura $n-2$ triangles qui recouvrent un polygone d'aire $\leqslant 1$, par le principe des tiroirs il y aura donc un triangle d'aire plus petite que $1/(n-2)$.

<u>*Solution de l'exercice 91*</u> (résolu par Arthur Blanc-Renaudie) Supposons par l'absurde que la suite a_n ne contienne qu'un nombre fini de nombres somposés., c'est-à-dire qu'à partir d'un certain rang tous les a_n seront premiers. On peut déterminer plusieurs conditions sur la suite des chiffres α_n :

- α_n ne peut pas être égal à 0, 2, 4, 6 ou 8, sinon le nombre a_n serait divisible par 2
- α_n ne peut pas être égal à 5, sinon le nombre a_n serait divisible par 5
- à partir d'un certain rang, α_n vaut donc 1, 3 ou 7 (9 est exclu par les conditions). Mais si il il y a trois rangs où α_n vaut 1 ou 7, alors il y aura un des nombres qui sera divisible par 3.

Donc à partir d'un certain rang, tous les α_n seront des 3, et donc tous les nombres de la suite seront de la forme $\overline{n33\dots3}$. $\overline{n3}$ est un nombre premier plus grand que 3, donc $10^{\overline{n3}-1} - 1$ est divisible par $\overline{n3}$ et 3 est inversible modulo $\overline{n3}$ et donc :

$$\overline{n3}\underbrace{\overline{33\dots3}}_{\overline{n3}\text{ fois}} = \overline{n3} \times 10^{\overline{n3}} + \frac{10^{\overline{n3}} - 1}{3}$$

qui est divisible par $\overline{n3}$, et donc non premier.

<u>*Solution de l'exercice 92*</u> (résolu par Arthur Blanc-Renaudie) Tout d'abord, pour vérifier la condition $f(f(x)) = ax$, la fonction f doit être injective. Choisissons $a \in \mathbb{N}^*$.

Premier cas : $a = 1$. On va générer la fonction. On classe tous les entiers en paires (x, y) et on fera $f(x) = y$ et $f(y) = x$. On vérifie facilement que cette fonction marche.

Deuxième cas : $a > 1$. On va classer tous les entiers *non divisibles par a* en couples (x, y). Ensuite on définit

$$f(x) = y,\ f(y) = ax,\ f(ax) = ay,\ f(ay) = a^2x,\ \dots,\ f(a^n x) = a^n y,\ f(a^n y) = a^{n+1}x$$

Il est facile de vérifier qu'on définit la fonction pour tous les entiers et que cette fonction vérifie la condition.

<u>*Solution de l'exercice 93*</u> (résolu par Arthur Blanc-Renaudie) On va diviser l'ensemble $A(n)$ en $A_1(n) = \{$ mots de $A(n)$ se finissant par $c\}$ et $A_2(n) = \{$ mots de $A(n)$ se finissant par a ou $b\}$. De la même manière, on répartit l'ensemble $B(n)$ en $B_1(n) = \{$ mots de $B(n)$ se finissant par deux lettres identiques $\}$ et $B_1(n) = \{$ mots de $B(n)$ se finissant par deux lettres différentes $\}$.

On a les relations de récurrence suivantes :

$$\begin{aligned} A_1(n+1) &= A_1(n) + A_2(n), \\ A_2(n+1) &= 2 \times A_1(n) + A_2(n), \\ B_1(n+1) &= B_1(n) + B_2(n), \\ B_1(n+1) &= 2 \times B_1(n) + B_2(n). \end{aligned}$$

Il faut ensuite démontrer par récurrence que $B_1(n+1) = 3A_1(n)$ et $B_2(n+1) = 3A_2(n)$, ce qui conclut l'exercice. Il est facile de vérifier $A_1(1) = 1$, $A_2(1) = 2)$, $B_1(2) = 3$, $B_2(2) = 6$. Je laisse la récurrence au lecteur.

Solution de l'exercice 96 (résolu par Arthur Blanc-Renaudie et Lucas Flammant) Nous allons montrer par l'absurde qu'il existe une infinité d'entiers n tels que $\lfloor n\sqrt{2} \rfloor$ soit une puissance de 3. Supposons qu'il existe seulement un nombre fini de n tels que ce soit vérifié, autrement dit, il existe un entier k tel qu'aucune puissance de 3 supérieure à k ne peut s'écrire sous la forme $\lfloor n\sqrt{2} \rfloor$. Nous allons montrer le résultat suivant :

Pour tout $\alpha \in]0, 0.45]$, pour tout entier i tel que $3^i > k$, si $3^i - 1 \leqslant n\sqrt{2} < 3^i + 1$, alors $3^i - \alpha \leqslant n\sqrt{2} < 3^i$.

Montrons le résultat pour $\alpha = 0.45$: comme $\lfloor n\sqrt{2} \rfloor \neq 3^i$, $n\sqrt{2} < 3^i$ et comme $\lfloor (n+1)\sqrt{2} \rfloor \neq 3^i$, $n\sqrt{2} \geqslant 3^i + 1 - \sqrt{2} > 3^i - 0.45$ (je rappele que $\sqrt{2} \approx 1.414$).

Maintenant, supposons le résultat vrai pour $\alpha \in]0, 0.45]$ et nous montrerons qu'il est vrai pour $\alpha/3$, et donc pour tout le segment $[\alpha, \alpha/3]$. Ainsi par récurrence le résultat sera vrai pour tout $\alpha \in]0, 0.45]$. Soit n et i tels que $3^i - 1 \geqslant \lfloor n\sqrt{2} \rfloor < 3^i + 1$. Par hypothèse de récurrence, $3^i - \alpha \leqslant n\sqrt{2} < 3^i$, On va tout multiplier par 3 : $3^{i+1} - 3\alpha \leqslant 3n\sqrt{2} < 3^{i+1}$, et comme $\alpha \leqslant 0.45$, $3\alpha \leqslant 1.35$. Si on avait $3^{i+1} - 1.35 \leqslant 3n\sqrt{2} < 3^{i+1} - 1$, on aurait $3^{i+1} \leqslant (3n+1)\sqrt{2} < 3^{i+1} + 1$, ce qui est en contradiction avec notre hypothèse de départ. On a donc $3^{i+1} - 1 \leqslant 3n\sqrt{2} < 3^{i+1} + 1$, et par hypothèse de rećurrence, cela implique que

$$3^{i+1} - \alpha \leqslant 3n\sqrt{2} < 3^{i+1} \iff 3^i - \frac{\alpha}{3} \leqslant n\sqrt{2} < 3^i + 1.$$

Ceci achève la récurrence et la démonstration de la propriété.

Maintenant prenons un i quelconque tel que $3^i > k$. Il est facile de voir qu'il existe un n tel que $3^i - 1 \leqslant n\sqrt{2} < 3^i + 1$. Dans ce cas, par la propriété $n\sqrt{2}$ est aussi près qu'on veut de 3^i, et donc $n\sqrt{2} = 3^i$, ce qui est impossible car $\sqrt{2}$ est irrationnel. L'hypothèse de départ est donc absurde.

Solution de l'exercice 99 (résolu par Lucas Flammant) Soit ω l'ordre de 2 modulo 3^n. D'après le petit théorème de Fermat, ω divise $\varphi(3^n) = 2 \cdot 3^{n-1}$. $2^\omega \equiv 1[3^n]$ donc $4^\omega \equiv 1[3^n]$, c'est-à-dire $v_3(4^\omega - 1) \geqslant n$. Nous allons utiliser le LTE (3 divise 4-1 mais ne divise ni 4 ni 1) ainsi

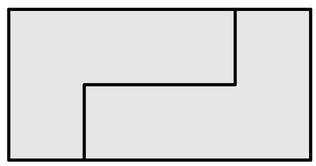
$$v_3(4^\omega - 1) = v_3(4 - 1) + v_3(\omega) = 1 + v_3(\omega).$$

Donc $v_3(\omega) \geqslant n-1$, or $\omega | 2 \cdot 3^{n-1}$, donc $omega = 3^{n-1}$ ou $omega = 2 \cdot 3^{n-1}$. Ensuite regardons mod 3 : si ω était impair, alors $2^\omega \equiv 2[3]$, donc il faut que ω soit pair. Donc $\omega = \varphi(3^n)$ et 2 est une racine primitive modulo 3^n.

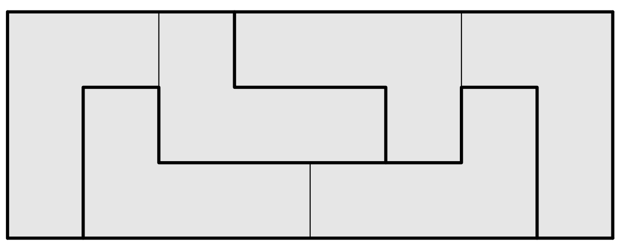
Solution de l'exercice 100 (résolu par Nathanaël Courant) Tout d'abord on remarque qu'un L de Tetris recouvre 4 cases, donc si on veut paver un damier $m \times n$ par des L, il faut que mn soit divisible par 4.

Supposons que mn est divisible par 4 mais pas par 8, cela signifie que la surface représente un nombre impair de L. On peut supposer qu'il y a un nombre pair de lignes. Nous allons colorier les cases de la manière suivante : une ligne en noir, un ligne en blanc. Ainsi il y a autant de cases blanche que de cases noires, et il est facil de vérifier que chaque L recouvre soit trois cases noires et un blanche, soit trois cases blanches et une noire. Avec un nombre impair de L il est donc impossible de recouvrir autant de cases noires que de cases blanches.

Supposons maintenant que m est divisible par 2 et n divisible par 4. Dans ce cas on pave avec des rectangles comme ceci :



Supposons maintenant que m est impair $\geqslant 3$ et n divisible par 8. Dans ce cas on pave les trois premières lignes avec des rectangles comme cela :



et on finit le pavage comme dans le cas précédent. Ainsi un rectangle $m \times n$ est pavable par des L ssi mn est divisible par 8 (à part bien sûr le cas où il n'y a qu'une seule ligne).

Solution de l'exercice 105 (résolu par Loïc Pujet) Tout d'abord on suppose que les côtés ont des longueurs distinctes, sinon on divise par 0. Par l'inégalité triangulaire, $c \geqslant |a-b| > 0$, donc $\frac{c^2}{(a-b)^2} \geqslant 1$, donc la somme est supérieure ou égale à 3. Montrons maintenant que l'égalité est impossible. L'égalité $c = |a-b|$ ssi $\hat{A}$ ou $\hat{B}$ est plat. Pour que les trois termes soient égaux à 1, il faut qu'au moins deux angles soient plats, ce qui est impossible.

Solution de l'exercice 106 (résolu par Arthur Blanc-Renaudie) Montrons d'abord un premier résultat : si p est un premier divisant N, alors $p \equiv 1[2^{n+1}]$. En effet

$$2^{2^n} \equiv -1[p] \text{ et } 2^{2^{n+1}} \equiv 1[p]$$

donc l'ordre de 2 modulo p est 2^{n+1}, et $2^{n+1}|(p-1)$. En particulier, $p > 2^{n+1}$.

Si on note $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la décomposition de N en facteurs premiers, comme tous les p_i sont supérieurs à 2^{n+1}, il s'en suit que

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k < 2^n.$$

Notons d le nombre de diviseurs de N,

$$\begin{array}{rcl} d & = & (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1) \\ \ln(d) & = & \ln(\alpha_1+1)+\ln(\alpha_2+1)+\cdots+\ln(\alpha_k+1) \\ \ln(d) & \leqslant & k\ln\left(1+\dfrac{\alpha_1+\alpha_2+\cdots+\alpha_k}{k}\right) \text{ puisque } \ln(1+x) \text{ est concave} \\ \ln(d) & \leqslant & k\cdot\dfrac{\alpha_1+\alpha_2+\cdots+\alpha_k}{k} \text{ puisque } \ln(1+x)\leqslant x, \text{ consésuence de la concavité} \\ \ln(d) & \leqslant & \alpha_1+\alpha_2+\cdots+\alpha_k < 2^n \end{array}$$

Le nombre N a d diviseurs distincts $m_1,\dots,m_d$, qui sont tous $\equiv 1[2^{n+1}]$, on a donc les relations suivantes (si on place les m_i dans le bon sens) :

$$m_1 = 1\ ;\ m_2 \geqslant (2^{n+1}+1)\ ;\ m_3 \geqslant (2\cdot 2^{n+1}+1)\ ;\dots;\ m_d \geqslant ((d-1)\cdot 2^{n+1}+1).$$

$$\begin{array}{rcl} \dfrac{\sigma(N)}{N} & = & \dfrac{1}{m_1}+\dfrac{1}{m_2}+\dfrac{1}{m_3}+\cdots+\dfrac{1}{m_d} \\ & \leqslant & 1+\dfrac{1}{2^{n+1}+1}+\dfrac{1}{2\cdot 2^{n+1}+1}+\cdots+\dfrac{1}{(d-1)\cdot 2^{n+1}+1} \\ & < & 1+\dfrac{1}{2^{n+1}}\left(1+\dfrac{1}{2}+\dfrac{1}{3}+\cdots+\dfrac{1}{d-1}\right) \end{array}$$

Pour conclure nous avons besoin du résultat sur la série harmonique suivant :

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{d-1} \leqslant \ln(d)+1.$$

En réinjectant, on trouve

$$\frac{\sigma(N)}{N} < 1+\frac{\ln(d)+1}{2^{n+1}} \leqslant 1+\frac{2^n+1}{2^{n+1}} \leqslant 1.$$

Solution de l'exercice 108 (résolu par Lucas Flammant) Nous allons montrer par récurrence qu'il est toujours possible d'allumer toutes les ampoules, quels que soient le nombre d'ampoules et la configuration des guirlandes. Pour $n = 1$ c'est évident. À présent supposonsque pour toute configuration à n ampoules, il est possible de toutes les allumer et prenons une une configuration à $n+1$ ampoules, que nous allons numéroter $1, 2,\dots, n+1$.

Soit i une des ampoules, si on retire l'ampoule i il rest n ampoules et par récurrence il existe une manipulation (appelons-la Γ_i) qui allume toutes les autres ampoules. Il y a deux cas possibles : soit Γ_i allume l'ampoule i, soit elle la laisse éteinte. Si l'une des Γ_i allume l'ampoule i on a terminé, et le cas qui reste à étudier est si toutes les manipulations Γ_i laissent l'ampoule i éteinte.

Si $n+1$ est pair : Dans ce cas il suffit de faire successivement toutes les manipulations Γ_i. Ainsi, toutes les ampoules auront changé détat n fois et seront donc allumées.

Si $n+1$ **est impair :** Commençons par montrer un premier résultat : il existe une ampoule qui a un nombre pair de voisins. Pour démontrer ce résultat, on additione le nombre de voisins de chaque ampoule. Si elles avaient toutes un nombre impair de voisin, la somme serait un nombre impair, mais cette somme consiste à compter deux fois chaque guirlande, et est donc un nombre pair. Choisissons i une ampoule qui a un nombre pair de voisines notées x_1, x_2, ..., x_{2k}. On actionne une fois l'interrupteur i (qui allume i et toutes ses voisines), et on fait les manipulations Γ_i, Γ_{x_1}, Γ_{x_2},...,$\Gamma_{x_{2k}}$. Ainsi i et ses voisines ont été changées $2k$ fois et restent allumés, et les autres ampoules ont été changées $2k+1$ fois et s'allument.

Ceci achève la récurrence et notre démonstration.

<u>*Solution de l'exercice 109*</u> (résolu par Arthur Blanc-Renaudie) Il existe au moins une paire : $8 = 2^3$ et $9 = 3^2$. Supposons par l'absurde qu'il n'existe qu'un nombre fini de paires consécutives de nombres intéressants. Prenons $(n, n+1)$ la paire maximale. Nous allons montrer que la paire $(4n(n+1), (2n+1)^2)$ est aussi intéressante. Tout d'abord il est facile de vérifier que les deux nombres sont consécutifs et que $(2n+1)^2$ est intéressant. Intéressons nous au terme $2n(2n+2)$ et soit p un de ses diviseurs premier.

1. si $p = 2$ c'est facile
2. si $p|n$ alors $p^2|n$ puisque n est intéressant
3. si $p|(n+1)$ alors $p^2|(n+1)$ puisque $n+1$ est intéressant

<u>*Solution de l'exercice 111*</u> (résolu Par Mehdi Trense) Commençons par le côté $\sqrt{a}+\sqrt{b}+\sqrt{c} \leqslant \sqrt{a^2+b^2+c^2}$. Par l'inégalité de Cauchy-Schwarz,

$$1 \cdot \sqrt{a} + 1 \cdot \sqrt{b} + 1 \cdot \sqrt{c} \leqslant \sqrt{3(a+b+c)} = \sqrt{27}.$$

Par la convexité de $x \mapsto x^2$

$$a^2+b^2+c^2 \geqslant 3\left(\frac{a+b+c}{3}\right)^2 = 27.$$

$$\sqrt{a}+\sqrt{b}+\sqrt{c} \leqslant \sqrt{27} \leqslant \sqrt{a^2+b^2+c^2}$$

Nous allons maintenant démontrer $\sqrt{ab+bc+ca} \leqslant \sqrt{a}+\sqrt{b}+\sqrt{c}$ par la technique des multiplicateurs de Lagrange. Nous allons démontrer le résultat sur le domaine fermé $a+b+c = 9$ et $a, b, c \geqslant 1$. Nous voulons minimiser la fonction $f(a,b,c) = \sqrt{a}+\sqrt{b}+\sqrt{c} - \sqrt{ab+bc+ca}$, lorsque $a, b, c > 1$ et $g(a,b,c) = a+b+c = 9$. Un extremum est atteint lorsque les deux vecteurs

$$\left(\frac{\partial f}{\partial a}, \frac{\partial f}{\partial b}, \frac{\partial f}{\partial c}\right) \text{ et } \left(\frac{\partial g}{\partial a}, \frac{\partial g}{\partial b}, \frac{\partial g}{\partial c}\right)$$

sont colinéaires. Calculons toutes ces dérivées

$$\frac{\partial f}{\partial a} = \frac{1}{2\sqrt{a}} - \frac{b+c}{2\sqrt{ab+bc+ca}} = \frac{1}{2\sqrt{a}} - \frac{9-a}{2\sqrt{ab+bc+ca}}.$$

Pour alléger les notations, nous noterons

$$k = \sqrt{ab+bc+ca}.$$

Nous voulons que les deux vecteurs suivants soient colinéaires :

$$\left(\frac{1}{2\sqrt{a}}-\frac{9-a}{2k},\frac{1}{2\sqrt{b}}-\frac{9-b}{2k},\frac{1}{2\sqrt{c}}-\frac{9-c}{2k}\right)\ \text{ et }\ (1,1,1)$$

ce qui est équivalent à $\frac{1}{2\sqrt{a}}-\frac{9-a}{2k}=\frac{1}{2\sqrt{b}}-\frac{9-b}{2k}=\frac{1}{2\sqrt{c}}-\frac{9-c}{2k}$.

$$\frac{1}{2\sqrt{a}}-\frac{9-a}{2k}=\frac{1}{2\sqrt{b}}-\frac{9-b}{2k}\iff\frac{1}{2\sqrt{a}}-\frac{1}{2\sqrt{b}}=\frac{(9-a)-(9-b)}{2k}=\frac{b-a}{2k}\iff k=(\sqrt{a}+\sqrt{b})\sqrt{ab}.$$

Donc en particulier on veut

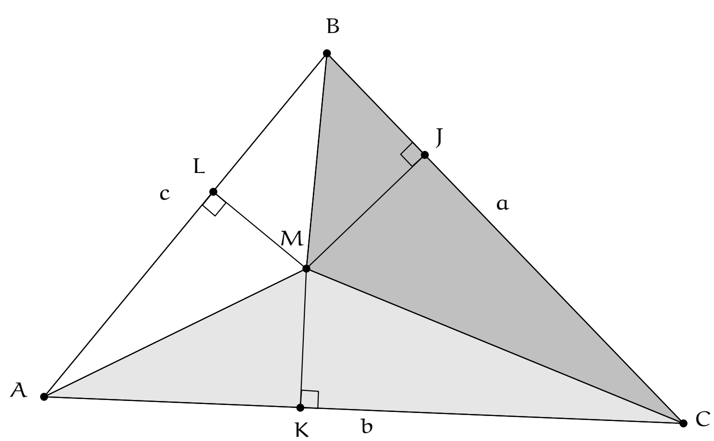
$$(\sqrt{a}+\sqrt{b})\sqrt{ab}=(\sqrt{b}+\sqrt{c})\sqrt{bc}=(\sqrt{a}+\sqrt{c})\sqrt{ac}$$

et on voit facilement que ceci n'est possible que si $a=b=c=3$ (si $a\geqslant b>c$, le terme de droite est plus petit que le terme de gauche). Calculons $f(3,3,3)=3\sqrt{3}-\sqrt{27}=0$.

Nous avons trouvé tous les extrema à l'intérieur du domaine. Comme dans toute preuve avec les multiplicateurs de Lagrange il faut maintenant chercher les extrema sur les bords du domaine, les trois segments de la forme $a=1, b+c=8, b,c\geqslant 1$. On réutilise les multiplicateurs de Lagrange sur ce segment (ou plutôt vous le faites) et vous trouvez un seul extremum en $(1,4,4)$: $f(1,4,4)=3-\sqrt{8}>0$. Mais il reste le bord de ce segment, les sommets $(1,1,7)$ et $(1,7,1)$. Calculons $f(1,1,7)=2+\sqrt{7}-\sqrt{15}>0$.

Nous avons cherché tous les extrema de f et ils sont tous $\geqslant 0$, donc la fonction f est positive sur tout le domaine.

Solution de l'exercice 113 (résolu par Yassine Hamdi) On note a, b et c les longueurs du triangle, en nous noterons dans le reste de l'exo A_{XYZ} l'aire du triangle XYZ :



Par l'inégalité arithmético-géométrique :

$$\begin{aligned}a\cdot MJ\times b\cdot MK\times c\cdot ML &\leqslant \left(\frac{a\cdot MJ+b\cdot MK+c\cdot ML}{3}\right)^3\\ &= \left(\frac{2A_{BMC}+2A_{CMA}+2A_{AMB}}{3}\right)^3\\ &= \frac{8}{27}A_{ABC}^3\end{aligned}$$

$$MJ \cdot MK \cdot ML \leqslant \frac{3A_{ABC}^3}{27abc}.$$

Il y a égalité ssi $A_{BMC} = A_{CMA} = A_{AMB} = \frac{1}{3}A_{ABC}$. Pour réaliser ceci il faut que M soit sur la droite parallèle à BC qui coupe la hauteur AH_A en $1/3 - 2/3$, pareil pour B et C, donc M est unique. On voit ensuite que le centre de gravité G vérifie les conditions (rappelez-vous que G est au tiers de la médiane).

Solution de l'exercice 115 (résolu par Nathanaël Courant) Regardons ce qui se passe pour chaque chiffre lorsque l'on fait la division par 2 en deux étapes :

- on remplace chaque chiffre par la partie entière de sa moitié
- pour chaque chiffre est impair, on rajoute 5 au chiffre de rang inférieur.

On voit facilement qu'il n'y a pas de retenue puisque après la première étape, tous les chiffres sont inférieurs ou égaux à 4.

Regardons maintenant la contribution de chaque chiffre c de départ à la somme des chiffres de sa moitié. Si c est pair, il contribue $\frac{c}{2}$, et si c est impair, il contribue $\left[\frac{c}{2}\right] + 5$. Donc la somme des chiffres de la moitié est indépendante de l'ordre des chiffres du nombre de départ.

Solution de l'exercice 117 (résolu par Arthur Blanc-Renaudie) Nous allons utiliser l'expression de définition avec $(x, 1)$, $(x + 1, 1)$ et $(x, 2)$.

$$\begin{aligned}
(x+1)(f(x) - f(1)) &= (x-1)f(x+1) \\
(x+2)(f(x+1) - f(1)) &= xf(x+2) \\
(x+2)(f(x) - f(2)) &= (x-2)f(x+2)
\end{aligned}$$

En utilisant les deux dernières égalités, on peut trouver

$$(x-2)(x+2)(f(x+1) - f(1)) = x(x+2)(f(x) - f(2)).$$

À présent on prend $x \neq -2$ pour simplifier les $(x + 2)$ et on remplace $f(x + 1)$ grace à la première égalité.

$$(x-2)\left(\frac{(x+1)(f(x) - f(1))}{x-1} - f(1)\right) = x(x+2)(f(x) - f(2))$$

$$2f(x) = x(x-1)f(2) - 2x(x-2)f(1).$$

Le dernière ligne implique que pour $x \neq -2$, $f(x)$ est de la forme $ax^2 + bx + c$. Avec $x = 1$ et $y = 0$, on trouve $f(1) - f(0) = f(1)$, donc $f(0) = c = 0$. Maintenant essayons de prouver que toutes les fonctions de la forme $f(x) = ax^2 + bx$ marchent.

$$(x+y)(f(x) - f(y)) = (x+y)(ax^2 - ay^2 + bx - by) = (x+y)(x-y)(ax + ay + b),$$

$$(x-y)f(x+y) = (x-y)(a(x+y)^2 + b(x+y)) = (x-y)(x+y)(ax + ay + b).$$

L'égalité est donc vérifiée. Il faut maintenant regarder la valeur de $f(-2)$ quand $f(x) = ax^2+bx$ partout ailleurs. En prenant $x = -2$ et $y = 0$, il est facile de vérifier que $f(-2) = a(-2)^2+b(-2)$.

Les solutions sont donc toutes les fonctions de la forme $f(x) = ax^2 + bx$.

Solution de l'exercice 121 (résolu par Arthur Blanc-Renaudie)

$$\begin{aligned}
2P(x, y) &= P(x+y, x-y) \\
2P(x+y, x-y) &= P(2x, 2y) \\
\implies 4P(x, y) &= P(2x, 2y)
\end{aligned}$$

On peut aussi vérifier par récurrence que $P(2^n x, 2^n y) = 4^n P(x,y)$. Prenons M le maximum de $P(x,y)$ lorsque le point (x,y) est dans le disque origine de rayon 1. Soit (x,y) un point quelconque et nl'entier tel que $2^{n-1} < \sqrt{x^2+y^2} \leqslant 2^n$, donc $\left(\frac{x}{2^n}, \frac{y}{2^n}\right)$ est dans le disque de rayon 1 et $P(x,y) \leqslant 4^n M \leqslant 2(x^2+y^2)M$. Donc le polynôme P est de degré au plus 2. On écrit

$$P(x,y) = a + bx + cy + dx^2 + exy + fy^2.$$

On rentre cette formule dans $4P(x,y) = P(2x,2y)$ et on trouve $a = b = c = 0$, puis dans $2P(x,y) = P(x+y, x-y)$ et on trouve que $e = d - f$. On vérifie que toutes ces solutions marchent. Les solutions sont tous les polynômes de la forme

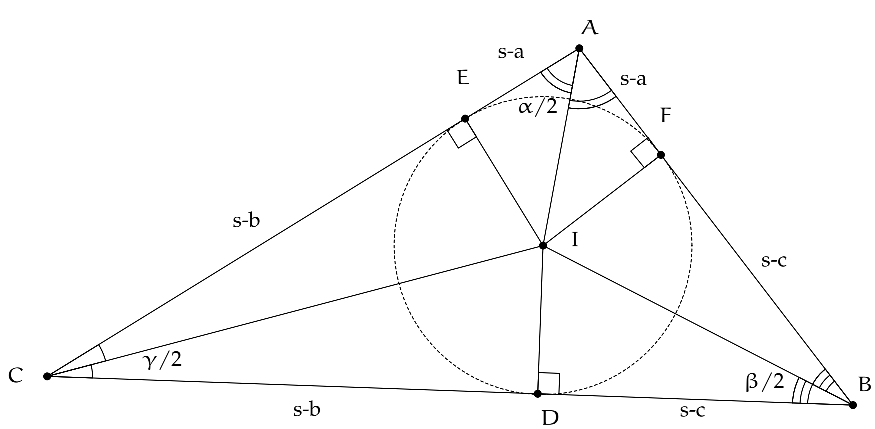
$$P(x,y) = dx^2 + (d-f)xy + fy^2 \quad ;f \in \mathbb{R}.$$

<u>*Solution de l'exercice 122*</u> (Résolu par Séginus Mowlavi) Soient p un nombre premier différent de 2, et a, b, c et d dans $\mathbb{N}$ tels que $p = a^2 + b^2 = c^2 + d^2$, on veut montrer que $\{a,b\} = \{c,d\}$. Alors $p^2 = (a^2+b^2)(c^2+d^2)$, et donc on a les deux écritures suivantes : $p^2 = (ac-bd)^2 + (ad+bc)^2$ et $p^2 = (ac+bd)^2 + (ad-bc)^2$. On a de plus $(ac-bd)(ac+bd) = a^2c^2 - b^2d^2 \equiv 0 \pmod{p}$. Donc p divise $ac+bd$ ou $ac-bd$. Quitte à changer d en $-d$ (attention, on perd une hypothèse de positivité), on suppose que p divise $ac-bd$.

Un raisonnement similaire nous dit que p divise $ad+bc$ ou $ad-bc$. Montrons en fait que p divise forcément $ad+bc$. Sinon, on aurait $ac - bd \equiv 0 \equiv ad - bc \pmod{p}$, donc $(a+b)(c-d) \equiv 0 \pmod{p}$, donc p divise $a+b$ ou $c-d$, donc soit $a^2 \equiv b^2 \pmod{p}$, soit $c^2 \equiv d^2 \pmod{p}$. Si on est dans le premier cas, alors $0 \equiv p \equiv a^2 + a^2 \pmod{p}$, donc p divise $2a^2$, donc a^2 (par imparité), donc p divise a (et de même pour b), donc p^2 divise $p = a^2 + b^2$, c'est absurde.

On peut donc écrire $1 = \left(\frac{ac-bd}{p}\right)^2 + \left(\frac{ad+bc}{p}\right)^2$, et les deux termes dans les carrés sont des entiers. Si d est positif, cela impose $ac - bd = 0$ et $ad + bc = p$, donc $pb = abd + b^2c = c(a^2+b^2) = cp$, et enfin $b = c$ et $a = d$. Si d est négatif, on prouve de la même manière que $a = c$ et $b = -d$.

<u>*Solution de l'exercice 124*</u> (résolu par Yassine Hamdi) On place I le centre du cercle inscrit à ABC et D, E, F les points de tangence du cercle. On notera r le rayon du cercle inscrit et s le demi-périmètre :



Dans le triangle AFI on voit

$$\tan\left(\frac{\alpha}{2}\right) = \frac{r}{s-a}, \text{ de même } \tan\left(\frac{\beta}{2}\right) = \frac{r}{s-b} \text{ et } \tan\left(\frac{\gamma}{2}\right) = \frac{r}{s-c}.$$

Si on note $\mathcal{A}$ l'aire du triangle

$$\begin{aligned} \mathcal{A} \cdot \left(\tan\left(\frac{\alpha}{2}\right) + \tan\left(\frac{\beta}{2}\right) + \tan\left(\frac{\gamma}{2}\right)\right) &= r \cdot \left(\frac{\mathcal{A}}{s-a} + \frac{\mathcal{A}}{s-b} + \frac{\mathcal{A}}{s-c}\right) \\ &= r \cdot (r_a + r_b + r_c) \end{aligned}$$

où r_a est le rayon du cercle exinscrit opposé au sommet A. Or d'après l'égalité de Feuerbach

$$r_a + r_b + r_c = r + 4R$$

et d'après l'inégalité d'Euler $r \leqslant \frac{R}{2}$. On a

$$\tan\left(\frac{\alpha}{2}\right) + \tan\left(\frac{\beta}{2}\right) + \tan\left(\frac{\gamma}{2}\right) = \frac{r(r+4R)}{\mathcal{A}} \leqslant \frac{R/2(R/2+4R)}{\mathcal{A}} = \frac{9R}{4\mathcal{A}}.$$

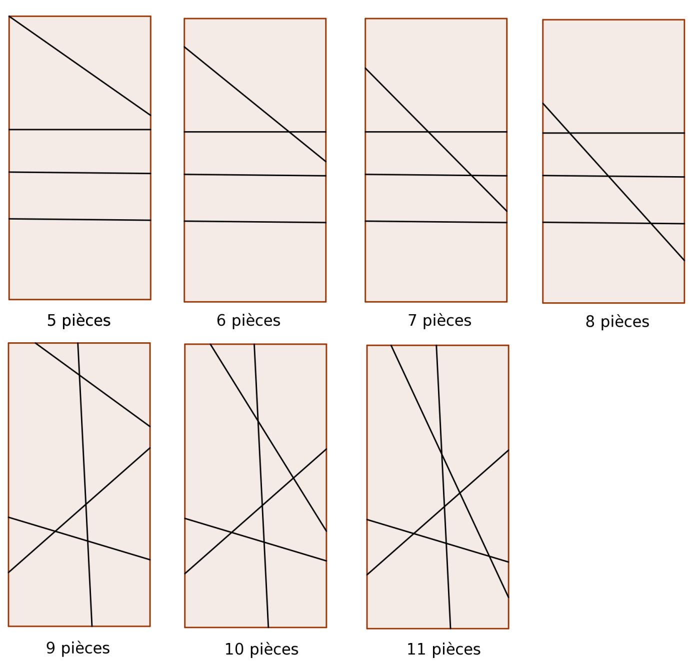
VII. Test de sélection

Nous incluons dans ce polycopié les énoncés et solutions du test de sélection pour le stage de Montpellier, auquel ont participé près de 350 élèves de 177 établissements différents.

Exercice 1. Mathieu prend une feuille de papier rectangle et y trace à la règle quatre lignes droites distinctes, dont chacune va d'un côté à un autre côté (aucune de ces droites ne peut être un bord du rectangle). Ensuite, il coupe sa feuille de papier le long de chaque droite tracée. Combien de pièces peut-il obtenir ? Esquisser un exemple pour chaque nombre de pièces possible, et expliquez pourquoi il n'y a pas d'autre possibilité.

Solution

On va placer les 4 droites les unes après les autres. La première droite coupe nécessairement le rectangle en deux parties. La seconde peut traverser l'une de ces deux parties, ou chacune des deux : il faut pour cela qu'elle coupe la première. De même la troisième droite peut couper 0, 1 ou 2 des deux premières, donc traverser 1, 2 ou 3 des parties déjà présentes, créant 1, 2 ou 3 nouvelles parties. Et la quatrième crée 1, 2, 3 ou 4 nouvelles parties. En définitive, après découpage, nous aurons 2 + (1 ou 2) + (1 ou 2 ou 3) + (1 ou 2 ou 3 ou 4) pièces, soit toutes les possibilités entre 5 et 11. Plus précisément, le nombre de pièces est égal à 5 + nombre de points d'intersection (si des points d'intersection appartiennent à plus de deux droites, ils doivent être comptés plusieurs fois, mais on ne demandait pas de se préoccuper de ce cas particulier). La figure de la page suivante illustre chacun des cas.



Exercice 2. Un prisonnier est au centre d'un cercle de rayon 10 mètres. Chaque minute, il annonce une direction qu'il veut prendre, et c'est au gardien de choisir entre cette direction et la direction opposée. Le prisonnier avance alors d'un mètre dans la direction choisie par le gardien. Le prisonnier a-t-il une stratégie garantissant qu'il sortira finalement du cercle, même si le gardien veut l'en empêcher ?

Solution

Nous allons montrer que le prisonnier possède une stratégie gagnante lui permettant de sortir du cercle. Notons O le centre du cercle et P_n la position du prisonnier après la $n^{\text{ième}}$ minute. Toutes les distances seront exprimées en mètres.

La stratégie que le prisonnier doit adopter est la suivante. À la première minute, il indique une direction quelconque, ce qui l'amènera à un point P_1 tel que $OP_1 = 1$. Puis à la $(n+1)^{\text{ième}}$ minute, le prisonnier, alors en P_n, va indiquer au gardien une direction perpendiculaire à la droite OP_n ; quel que soit le choix du gardien, le prisonnier se retrouvera alors en un point P_{n+1} tel que $P_nP_{n+1} = 1$ et tel que le triangle OP_nP_{n+1} soit rectangle en P_n ; en particulier, la distance OP_{n+1} ne dépendra pas du choix du gardien et sera strictement supérieure à OP_n.

On a donc trouvé une stratégie permettant au prisonnier, à chaque minute, d'augmenter strictement sa distance au centre du cercle. **Ceci ne suffit pas à conclure qu'il pourra en sortir** ; en effet, ce n'est pas parce que la distance OP_n est strictement croissante qu'elle dépassera forcément 10. (De façon analogue, la suite $u_n = 2 - \frac{1}{n}$ est strictement croissante, mais aucun de ses termes n'est supérieur à 10). Pour conclure, il faut calculer explicitement la distance OP_n ; comme $OP_1^2 = 1$ et comme, par le théorème de Pythagore, $OP_{n+1}^2 = OP_n^2 + 1$, on en déduit que pour tout n, $OP_n^2 = n$ et donc $OP_n = \sqrt{n}$. En particulier, $OP_{100} = 10$; le prisonnier sort donc du cercle au bout de la $100^{\text{ième}}$ minute.

Quelques remarques après correction. À chaque minute, le prisonnier doit annoncer une direction au gardien. Par *direction*, on entend n'importe quelle demi-droite d'origine la position actuelle P_n du prisonnier. En particulier, il n'y a pas que quatre, ni même huit directions possibles (haut, bas, gauche, droite, et les quatre directions inclinées de 45° par rapport aux précédentes), mais une infinité. D'ailleurs, il est possible de démontrer qu'aucune stratégie comprenant uniquement des mouvements dans les huit directions précédemment citées ne permet au prisonnier de sortir du cercle.

D'autre part, si vous annoncez qu'une stratégie permet au prisonnier de sortir du cercle quels que soient les choix du gardien, il faut le démontrer rigoureusement, et il ne suffit pas qu'elle *ait l'air* de marcher. Plusieurs d'entre vous ont ainsi proposé des stratégies et ont montré que les premières étapes de celles-ci permettaient au prisonnier de s'éloigner du centre du cercle ; puis ils ont dit (sans le démontrer) qu'en répétant les mêmes mouvements, le prisonnier allait continuer à progressivement s'éloigner du centre jusqu'à sortir du cercle. En fait, dans presque tous les cas, ces stratégies ne fonctionnaient pas. N'oubliez donc pas de démontrer rigoureusement tout ce que vous affirmez. Et si vous n'êtes vous-même pas convaincus que ce que vous dites est vrai, vous ne risquez pas de convaincre le correcteur.

Exercice 3. Monsieur et Madame Mathon se partagent un plateau de sept fromages. Ils désirent en prendre chacun trois en entier, et partager le septième de sorte que chacun reçoive le même poids total de fromage. Est-il possible, quels que soient les poids des sept fromages, de choisir les trois fromages de l'un, les trois fromages de l'autre et comment découper le septième fromage de sorte que leur désir soit satisfait ?

Solution

Soient $0 < a_1 \leqslant a_2 \leqslant \cdots \leqslant a_7$ les poids de fromages dans l'ordre croissant.

On donne les fromages de poids a_1, a_3 et a_5 à Monsieur Mathon et les fromages de poids a_2, a_4 et a_6 Màdame Mathon.

On a $a_1 \leqslant a_2$, $a_3 \leqslant a_4$ et $a_5 \leqslant a_6$, donc on a

$$a_1 + a_3 + a_5 \leqslant a_2 + a_4 + a_6.$$

Mais, on a $a_2 \leqslant a_3$, $a_4 \leqslant a_5$ et $a_6 \leqslant a_7$, donc on a

$$a_2 + a_4 + a_6 \leqslant a_3 + a_5 + a_7 < a_1 + a_3 + a_5 + a_7.$$

Donc, la différence de poids des fromages de deux personnes est

$$(a_2 + a_4 + a_6) - (a_1 + a_3 + a_5) < a_7.$$

Donc, le septième poids est suffisament lourd pour combler la différence, et une fois cette différence comblée, ce qui reste du septième fromage est distribué équitablement.

Remarque

On peut construire plusieurs autres solutions, mais c'est toujours le fromage le plus lourd qui sera découpé pour rétablir l'équilibre, car il se peut qu'à lui tout seul il pèse plus de la moitié du poids total P. Par exemple, on peut donner à Madame l'un quelconque des fromages a_1 ou a_2, l'un quelconque de a_3 et a_4, l'un quelconque de a_5 ou a_6 : si celui qui a la plus petite part prend tout le gros fromage, il a nécessairement plus que l'autre, donc on peut partager a_7 pour rétablir l'équilibre. Ou encore, les quatre nombres $p_1 = a_1 + a_2 + a_3$, $p_2 = a_1 + a_2 + a_6$, $p_3 = a_1 + a_5 + a_6$ et $p_4 = a_4 + a_5 + a_6$ vérifient : $p_1 \leqslant p_2 \leqslant p_3 \leqslant p_4$, $p_{i+1} < p_i + a_7$, et $p_1 < \frac{P}{2} < p_4 + a_7$ car $p_1 + p_4 + a_7 = P$. Si $p_i + a_7 \leqslant \frac{P}{2}$, $p_{i+1} < \frac{P}{2}$, ce qui permet d'en trouver un tel que $p_i < \frac{P}{2} < p_i + a_7$. Autre raisonnement : on distribue le plus équitablement possible les six fromages $a_1 \ldots a_6$: si la différence entre les deux portions était supérieure à a_7, la distribution ne serait pas la plus équitable possible, car en échangeant le plus lourd fromage de celui qui a la plus grosse portion avec un fromage quelconque de l'autre, on obtiendrait une distribution plus équitable. Nous ne détaillerons pas davantage ces différentes variantes.

Exercice 4. Soient b et d des nombres réels non nuls tels que $b+d$ soit lui aussi non nul. Mathias affirme que l'identité $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$ est vraie pour tous les nombres réels a et c : elle s'appelle "additivité des fractions". Mathilde pense que cette additivité des fractions est correcte si et seulement s'il existe un nombre réel m tel que $a = mb^2$ et $c = -md^2$. Leur professeur rappelle que l'on peut additionner des fractions comme Mathias le propose si et seulement si elles ont le même dénominateur, c'est-à-dire $b = d$. Un inspecteur affirme que cette "additivité des fractions" est toujours fausse. Qui a raison : Mathias, Mathilde, le professeur, l'inspecteur, ou aucun des quatre ? Justifiez soigneusement votre réponse.

Solution

Examinons successivement les affirmations des uns et des autres.

- celle de Mathias :

Il suffit de trouver un contre-exemple pour mettre en défaut une affirmation générale.

Pour $a = b = c = d = 1$, on a $\frac{a}{b} + \frac{c}{d} = 2$ alors que $\frac{a+c}{b+d} = 1$. Il n'y a pas égalité, donc l'affirmation de Mathias est fausse.

- celle du Professeur :

Celui-ci fait également une affirmation générale, et le même contre-exemple (puisque $b = d$) montre qu'il a tort lui aussi.

- celle de l'Inspecteur :

Cette fois, pour mettre en défaut l'affirmation de l'Inspecteur, il suffit de trouver des valeurs pour lesquelles l'additivité des fractions est vraie. Par exemple, on peut choisir $a = c = 0$ et $b = d = 1$, puisqu'alors $\frac{a}{b} + \frac{c}{d} = 0 = \frac{a+c}{b+d}$. Ainsi, l'Inspecteur a tort.

- celle de Mathilde :

C'est la seule des quatre qui puisse être juste, encore faut-il le prouver.

Dans un premier temps, considérons des nombres a, b, c, d, m tels que b, d et $b + d$ soient non nuls, et avec $a = mb^2$ et $c = -md^2$.

On a d'une part : $\frac{a}{b} + \frac{c}{d} = mb - md = m(b - d)$.

d'autre part : $\frac{a+c}{b+d} = \frac{mb^2-md^2}{b+d} = \frac{m(b^2-d^2)}{b+d} = \frac{m(b-d)(b+d)}{b+d} = m(b - d)$.

On constate donc que, dans ces conditions, l'additivité des fractions est vraie.

Mais, attention, cela ne suffit pas encore pour pouvoir conclure que Mathilde a raison. En effet, Mathilde affirme non seulement que l'additivité des fractions est vraie si l'on choisit les nombres de la façon indiquée, mais aussi qu'elle n'est vraie que dans ce cas là. Il nous faut maintenant prouver la réciproque du résultat ci-dessus, à savoir que si a, b, c, d sont des nombres pour lesquels b, d et $b + d$ ne sont pas nuls et $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$ alors il existe un réel m tel que $a = mb^2$ et $c = -md^2$.

Si quatre nombres a, b, c, d (avec b, d et $b + d$ non nuls) vérifient $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$ (1), multiplions tout par $bd(b + d)$ afin d'éliminer les dénominateurs : l'égalité (1) devient $ad(b + d) + cb(b + d) = (a + c)bd$, soit : $ad^2 + cb^2 = 0$, qui s'écrit aussi $\frac{a}{b^2} = -\frac{c}{d^2}$.

Posons alors $m = \frac{a}{b^2}$. On a clairement $a = mb^2$. Mais aussi, d'après (2), $m = -\frac{c}{d^2}$, donc $c = -md^2$.

Nous avons atteint notre objectif et nous pouvons maintenant affirmer que Mathilde a effectivement raison.

Exercice 5. En région parisienne, les numéros de téléphone fixe se composent des chiffres 01 suivis de huit autres chiffres (par exemple 01.99.98.10.00 ou 01.00.00.35.77 etc.). Pour limiter les appels par erreur, on a décidé que si l'on compose un numéro de téléphone en ne se trompant que d'un seul chiffre, on tombe toujours sur un numéro non attribué : par exemple si 01.99.98.10.00 est attribué, alors 01.89.98.10.00 et 01.99.98.10.30 sont non attribués. Combien de numéros de téléphone différents peut-on attribuer au maximum en région parisienne ? Justifiez soigneusement votre réponse.

Remarques préliminaires

Lorsque l'on pose une question du type "quelle est la plus grande quantité de...", la démonstration comporte *deux étapes* : il faut montrer d'une part qu'il est possible d'en obtenir un certain nombre (la plupart du temps en donnant un exemple), et d'autre part qu'il est impossible d'en obtenir plus. Peut-être certains ont-ils pensé que les mots "au maximum" voulaient dire qu'il fallait juste trouver une borne supérieure. Cette interprétation ne tient pas la route : il aurait alors suffi de dire 10^8 pour résoudre l'exercice !

La première partie valait 3 points et la deuxième partie, 4 points. Mais certaines erreurs grossières justifiaient à elles seules un 0 : réponse non-entière ou supérieure à la quantité totale de numéros disponibles, erreurs de manipulation des opérations arithmétiques de base... Les idées sont parfois si confuses que localiser précisément l'erreur s'avère très difficile, d'autant plus qu'il y en a souvent plusieurs !

En revanche, dès lors qu'une copie ne contenait pas d'erreur grossière de ce genre et contenait au moins une affirmation juste (sans compter la remarque qu'il y a 10^8 numéros au total), elle méritait un point. Beaucoup ont cru que comme il existait 72 façons de se tromper sur un numéro, on ne pouvait pas attribuer plus d'un numéro sur 73. Ce n'est là qu'un des résultats, parmi plus de trente différents, trouvés dans les copies, et c'est faux car un numéro erroné peut correspondre à plusieurs numéros attribués. Toutefois, ceux qui ont fait ce raisonnement, mais qui ont remarqué et expliqué leur erreur (et qui n'en ont pas fait d'autre), ont gagné un point supplémentaire.

Quelques conseils

Soyez précis et détaillés dans votre rédaction. Faites clairement apparaître la structure logique, pour qu'on sache quels arguments servent à démontrer quelles affirmations. Définissez toujours clairement les objets que vous manipulez. Evitez les périphrases, introduisez plutôt des notations et des définitions. Attention aux pronoms, aux "ce", "cela" et autres mots ambigus de ce genre. Attention aux "de la même façon", "de même", "par analogie"... A chaque fois que vous écrivez de telles formulations vagues ou elliptiques, posez-vous deux questions. La plus importante : "suis-je bien certain que j'ai une idée claire de ce que je suis en train d'écrire ?" Et ensuite "le correcteur va-t-il comprendre la même chose ?" Mais n'oubliez pas : *ce qui se conçoit bien s'énonce clairement*.

Lorsque la réponse est "non", essayez de détailler. Dites-vous que plus vous détaillez, plus vous avez de chances d'attraper une erreur que vous n'aviez pas vue et donc d'obtenir un résultat juste à la fin. Dans le corrigé ci-dessous, volontairement très détaillé, *absolument chaque phrase*, et *presque chaque mot*, sert à quelque chose. Quand vous rédigez vous-même, vous pouvez vous permettre de sauter certaines étapes dans votre copie, mais certainement pas dans votre pensée.

Solution

Le 01 n'a aucune importance ici ; on va donc le laisser tomber, et traiter les numéros comme s'ils ne contenaient que 8 chiffres. On dira que deux numéros sont *adjacents* s'ils ne diffèrent qu'en une seule position, en appelant "position" l'une des 8 positions où sont situés les chiffres d'un numéro.

Montrons d'abord qu'il est effectivement possible d'attribuer 10 000 000 numéros.

Choisissons arbitrairement les 7 premiers chiffres du numéro, ce qui représente bien 10^7, soit dix millions de possibilités distinctes. A chacune d'elles, associons un huitième chiffre de sorte que la somme des huit chiffres soit divisible par 10. Par exemple, à 44 27 66 7, qui vérifie : $4+4+2+7+6+6+7=36$ on associe 4 de sorte que $(4+4+2+7+6+6+7)+4=40$ soit divisible par 10, et on décide que parmi les numéros commençant par 44 27 66 7 c'est 44 27 66 74 qui sera attribué : c'est bien toujours possible quels que soient les sept premiers chiffres. Or si l'on change un et un seul des huit chiffres, on augmente ou diminue la somme d'une différence de deux chiffres distincts, nécessairement comprise entre 1 et 9. La nouvelle somme ne peut pas être divisible par 10, donc le numéro obtenu ne peut pas être attribué. Cet exemple montre à lui seul qu'il est possible d'attribuer 10 000 000 numéros distincts vérifiant la condition de l'énoncé. Et ce n'est pas le seul exemple !

Montrons maintenant qu'il n'est jamais possible d'attribuer plus de 10 000 000 numéros.

Variante A

Considérons un ensemble de numéros attribués conforme aux conditions de l'énoncé. Deux d'entre eux ne peuvent jamais avoir les mêmes chiffres dans les 7 premières positions (qui suivent le 01), car alors ces numéros seraient adjacents (ils ne différeraient que par la dernière position). Donc, pour chaque suite de 7 chiffres, il y a au plus un numéro attribué qui commence par cette suite-là. Il y a donc au plus 10 000 000 numéros attribués.

Variante B

On remarque d'abord que chaque numéro est adjacent à exactement 72 autres numéros. En effet, considérons un numéro X. Si X' est un autre numéro adjacent à X, X' est entièrement déterminé par le choix de la position i par laquelle il diffère de X, et du chiffre qui occupe cette i-ième position, à condition que celui-ci soit différent du i-ième chiffre de X (sinon on aurait $X' = X$) ; réciproquement, chacun de ces choix fournit un numéro adjacent à X. Etant donné qu'il y a 8 positions, et que quelle que soit la position choisie, 9 chiffres peuvent l'occuper, il y a donc $8 \times 9 = 72$ possibilités au total.

Considérons un ensemble de numéros attribués conforme aux conditions de l'énoncé. Soit a le nombre de numéros attribués, $n = 10^8$ le nombre de numéros total. On appelle m le nombre de couples (A, B) où A est un numéro attribué et B un numéro qui lui est adjacent (donc qui n'est pas attribué). Estimons m de deux façons différentes :

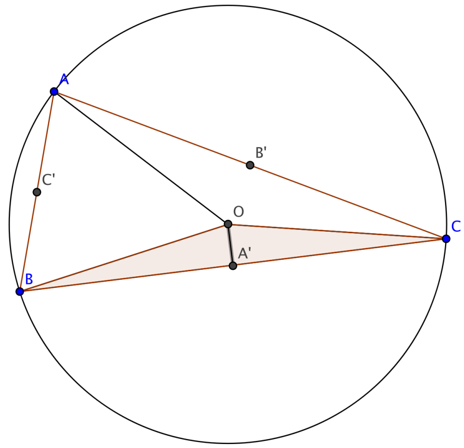
- Il y a a façons de choisir A. D'après ce qui précède, pour chaque valeur de A, il y a 72 façons de choisir B. Donc $m = 72a$.
- Il y a $n - a$ façons de choisir B. Fixons la valeur de B, et choisissons une position i. Alors parmi les numéros qui sont adjacents à B par la position i, au plus un est attribué (car ces 9 numéros sont tous adjacents entre eux). Il y a donc au plus 8 numéros attribués adjacents à B. Attention ! rien ne permet d'affirmer a priori qu'il y en a exactement 8. Mais on a $m \leqslant 8(n - a)$. En rassemblant les deux conditions, il vient : $72a \leqslant 8(n - a)$, soit $80a \leqslant 8n$, donc $a \leqslant \frac{n}{10} = 10\,000\,000$.

Exercice 6. Soit ABC un triangle d'aire S. On note $a = BC$, $b = CA$, $c = AB$ les longueurs de ses côtés, et $a' = AA'$, $b' = BB'$, $c' = CC'$ les longueurs de ses médianes, où A', B',C' sont les milieux respectifs de BC, CA, AB. Soit R le rayon du cercle circonscrit de ABC. Montrer que $aa' + bb' + cc' \leqslant 2S + R(a + b + c)$ si ABC est acutangle (c'est-à-dire si tous les angles de ABC sont inférieurs à 90°). Est-ce que cette inégalité est également vraie pour tous les triangles obtusangles (dont un angle est supérieur à 90°) ?

Solution

Notons O le centre du cercle circonscrit. Commençons par traiter le cas du triangle acutangle. Dans ce cas O est à l'intérieur du triangle ABC. Pour le voir on peut appliquer la loi de l'angle inscrit/l'angle au centre : par exemple $\widehat{BOC} = 2\widehat{BAC}$. Or, comme ABC est acutangle, $\widehat{BAC} < 90°$, donc $\widehat{BOC} < 180°$, ce qui signifie que O se trouve du même côté de la droite (BC) que A. On procède de même pour les côtés AB et AC et on conclut que O est à l'intérieur de

ABC.



On peut donc écrire que : $S = |AOB| + |BOC| + |COA|$ en notant $|XYZ|$ l'aire du triangle XYZ. Par ailleurs, en appliquant la formule *aire du triangle* $= \frac{1}{2} \times$ *base* $\times$ *hauteur* dans chacun des triangles AOB, BOC et COA, on obtient : $|AOB| = \frac{1}{2}AB \times OC'$, $|BOC| = \frac{1}{2}BC \times OA'$, $|COA| = \frac{1}{2}AC \times OB'$. D'où $2S = aOA' + bOB' + cOC'$. L'inégalité à démontrer est donc équivalente à

$$aa' + bb' + cc' \leqslant aOA' + bOB' + cOC' + R(a + b + c)$$

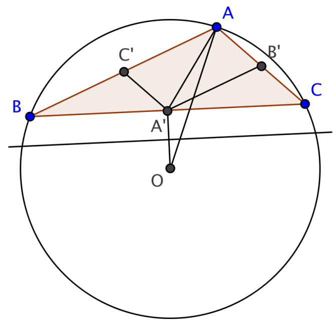
Pour démontrer cette dernière inégalité, remarquons que dans le triangle AOA', l'inégalité triangulaire donne $AA' \leqslant AO + OA'$, soit $a' \leqslant OA' + R$. En multipliant cette inégalité par a, on obtient

$$aa' \leqslant aOA' + Ra$$

De même : $bb' \leqslant bOB' + Rb$, et $cc' \leqslant cOC' + Rc$. On obtient le résultat en sommant ces trois inégalités.

Contrairement à ce que beaucoup ont imaginé, le cas d'égalité ne correspond pas aux triangles rectangles mais au triangle équilatéral. Pour le prouver (même si ce n'était pas demandé), on remarque que l'on a égalité si et seulement si $AA' = OA + OA'$, $BB' = OB + OB'$ et $CC' = OC + OC'$, ou encore si et seulement si A', O, A sont alignés dans cet ordre, ainsi que B', O, B et C', O, C. Si ces trois conditions sont satisfaites, alors A est sur la médiatrice (OA') du segment [BC], donc ABC est isocèle en A. De même ABC est isocèle en B (et en C), donc ABC est équilatéral. Réciproquement, le triangle équilatéral vérifie ces trois conditions.

La démonstration ci-dessus reste valable lorsque ABC est rectangle, mais plus lorsqu'il est obtusangle, car O ne se trouve plus à l'intérieur du triangle ABC et on ne peut plus écrire que $S = |AOB| + |BOC| + |COA|$. Néanmoins, l'inégalité reste vraie. Quitte à renommer les points, on peut supposer que c'est l'angle $\widehat{A}$ qui est obtus. Alors O est dans le demi-plan délimité par la droite (BC) et qui ne contient pas A. On a donc : $a' = AA' < R$ (pour bien justifier cette inégalité, on peut par exemple évoquer la position de A par rapport à la médiatrice du segment $[OA']$, ou écrire la loi des sinus ou le théorème d'Al Kashi dans le triangle OAA' qui est obtus en A').



Par ailleurs : $BB' < BA' + A'B' = \frac{a+c}{2}$, et : $CC' < CA' + A'C' = \frac{a+b}{2}$. Il suffit donc de montrer que

$$aR + (b+c)\frac{a}{2} + bc \leqslant 2S + R(a+b+c)$$

Or $2S = bc.\sin\widehat{A}$ et $\frac{a}{2} = R.\sin\widehat{A}$ par la loi des sinus dans le triangle ABC. L'inégalité équivaut donc à

$$bc(1-\sin\widehat{A}) \leqslant R(b+c)(1-\sin\widehat{A})$$

ou encore, après division par $1-\sin\widehat{A}$ (qui est un nombre strictement positif)

$$bc \leqslant R(b+c)$$

Pour conclure, on remarque que les inégalités $b \leqslant 2R$ et $c \leqslant 2R$ entraînent $\frac{1}{2}bc \leqslant Rc$ et $\frac{1}{2}bc \leqslant Rb$. On obtient le résultat en sommant ces deux dernières inégalités.

Remarques

Personne n'a résolu la deuxième question. c'est pourquoi il suffisait de traiter parfaitement le cas acutangle et de remarquer que la même preuve ne marchait plus dans le cas obtusangle pour avoir 7/7.

VIII. Citations mémorables

- Arthur qui joue à la coinche : "Rha, y'a deux [*censuré*] dans mon équipe !"
- Noémie : "Une droite, c'est une ligne, mais longue..."
- Au cours d'une tentative de résolution de l'exercice 77 :
  "La vitesse de la fourmi tend vers 0 donc elles ne bougent pas. Donc elles sont paraplégiques."
  "Bah oui, il n'y a qu'un seul centre."
  "Infini, c'est bien une sorte de paire de lunettes."
  "Oh, des cobayes ! (en voyant des fourmis)"
  "Si on conditionnait les fourmis..."
  "Les chiffres de la théorie sont en contradiction avec les résultats de l'expérience. On garde lesquels ?"
  "Ou alors, on trouve celui qui a fait le problème et on le frappe."

- Arthur, revenant des WC : "Voilà, j'espère que j'ai rien raté de compréhensible ?"
  Bodo : "Non".
- Bodo : "Le chef n'est pas content car son problème n'a pas de solution, mais il est content car vous avez bien travaillé."
  Arthur N : "Mais il n'est pas content car il doit vous payer".
- Bodo : "Tchiof tchiof teuteuteuteuteu, et le chef est convaincu."
- Bodo : "Quelqu'un passe au tableau pour montrer l'interprétation combinatoire de cette égalité, maintenant." (Longue attente)
  Félix : "Le père Noël ?"
- Félix, après avoir montré l'impossibilité d'un problème d'embauche : "Mais F. Hollande permet de créer un nouvel emploi, et tout le monde est content !" (en rajoutant une arête au graphe)
- Longtemps après le début d'une partie de mao :
  Julien, en donnant une carte à un autre joueur : "Pour ne pas avoir frotté tes cartes."
  L'autre joueur : "Merci !"
  Julien : "De rien !" (Il donne une autre carte.) "Pour ne pas avoir dit : "P[*censuré*]n de m[*censuré*]e, fait c[*censuré*]r !"
  Les deux dernières répliques se sont répétées en boucle très longtemps, sur une voix stupide.
- "Il m'a perdu Bodo, là ! !"
- Noémie : "La descente infinie ? C'est ce qui arrive à nos cerveaux depuis le début du stage..."
- Noémie : "J'viens de me rendre compte que troublant c'est l'inverse de trou noir !"
- Paul, en parlant du tableau interactif : "C'est pas pratique, c'est comme un tableau blanc

sauf que c'est mieux parce que c'est plus cher."

- Igor, en simplifiant une fraction : "Et là, y a le k du haut et le k du bas qui se tuent entre eux."
- Igor : "Qui connaît les dérivées ? Bon, les autres, vous fermez grands vos yeux et vos oreilles."
- Igor : "L'ensemble vide, bah, le malheureux, il est vide."
- Anne Onyme : "Rah, attendez, j'ai trop de cerveau..."
- Théorème de Noémie : "Soit un triangle ABC, soit une droite (Δ) coupant $(AB), (AC)$ et (BC) en M, N et P, alors les points M, N, P sont alignés." (dérivé du théorème de Ménélaüs)
- Paul : "Je torture une bouteille. N'entends-tu pas son cri d'agonie ?"
- Marc : "Paul, Paul ! On a confirmé, topologiquement, ta bouteille, c'est une souris !"
- Igor, en faisant irruption dans une salle de classe : "Qui meurt de soif ?"
  "Pas plus de trois, par contre, parce que j'ai que trois bouteilles..."
- Cécile : J'ai trouvé pourquoi ils s'appelaient X et Y, c'est parce que c'était les inconnues.
- Alice, venant de trouver un exercice de la muraille à étoile avec Cécile et Noémie : "Eh, à trois, on est intelligentes."
- Igor : "Et là, il suffit d'utiliser le Binôme de Pascal."
- "Oh, des chtites lumières de merde."
- Augustin : "Si $a = b$, alors $f(f(f(a))) = f(f(f(b)))$.
- Pendant un cours de Bodo, 17h.
  Cyril : "En fait, de 17h à 19h, nous avons prévu de résoudre des exos de la muraille."
  Bodo : "Mais vous savez, la muraille c'est pour les débutants !"
- Bodo : "[...] vaudrait mieux résoudre cet exercice normalement, car tout le monde n'est pas aussi brillant que Lucas et ses droites magiques."
  Cyril : "Il a quand même eu 8 sur 49..."
- Pierre : "Et il y a des triangles de Pascal sur les trente dernières pages de mon cahier de philo."
- Pierre : "Il faut montrer qu'il y a 2 trucs qui bidulent."
- Paul : "C'est un exercice de CP."
  Non, ça peut aussi être posé au bac."
- Pierre : "Donc je vais faire une parenthèse sur un truc qui m'a été très utile quand je m'ennuyais en philo..."
- Paul, à propos du triangle de Sierpinski : "C'est une triforce fractale !"
- Igor : "Dans le Nord-Pas de Calais, y a pas de villes, y a que des villages, on vous a enlevé des points quand vous vous êtes trompés."
- Antoine : "13+3, ça fait 14..."
- Igor : "Donc là, c'est vraiment diabolique..."
- Augustin : "Eh, mais c'est ce que j'ai fait tout à l'heure !
  Margaret : "Oui, mais c'était moins bien."
- Marc : "Moi, ce qui me fait rire, c'est que le tableau s'appelle "Smart". Moi, je l'aurais appelé "StupideTM"."
- Augustin, dans une copie du test : "Ne tenez pas comte des erreurs qu'il y a dans ma copie."
- Igor, le premier jour : "Oui, le poly est déjà tout tapé !"
- Nathanaël : "Arthur, arrête de complexer à faire des preuves complexes de géométrie en

complexes !"

- François Lo Jacomo, à la cérémonie d'ouverture : "Il faut faire des groupes équilibrés pour les cours."
  Arthur : "On a qu'à couper chaque personne en 4."
- Arthur, en regardant Dimension : "ça doit être bien des hyper-repas, on a beau les manger, on en a toujours."
  Plus tard : "OH, des hyper-donuts ! ! ! Quel goût ils ont ?"
  Arthur : "Ouais ouais ouais" (pour la au moins 500ème fois du stage...)
- Arthur, après avoir fini le test de combinatoire, fait une blague sur des oeufs (? ?) pourris : "Pour acheter un réseau de trafic de drogue, je regarde LDLC, pour acheter un réseau de trafic de drogue, je regarde ça ! !"
- Pendant la projection du film dimension : "Et donc -1 fois -1 égale $+1$" (applaudissements)
- Pierre : "C'est une très bonne question... Non, c'est pas une bonne question... Si, c'est une bonne question... Non, c'est une question...". Sur un ton décidé : "C'est une question".
- Cyril : "Et le théorème des restes chinois s'applique sans sushis."
- François : "C'est une équation connue... Enfin, de ceux qui la connaissent"
- Vincent : "Non mais t'as le droit de jouer aux cartes... en plus tu perdrais"
- Vincent : "Bonjour Igor,pour toi ? tu veux suivre un cours d'arithmétique 1ère ? Il y a une place isolée pour toi, en plus tu ne pourras pas papoter."
- Maxime "J'vais pas faire la preuve, je vais vous donner des éléments, et puis vous compléterez" Aymeric : "- Il est bien, il a le sens de l'humour"
- Loïc rentre dans la chambre où Nathanaël dort ; ce dernier se réveille
  - Il faut que je me lève !
  - Pourquoi ?
  - Ben, j'ai faim !
  - Tu veux un biscuit ?
  - Non, je vais prendre le petit déjeuner-déjeuner.
  - Mais il est onze heure du soir...
  - Ha !
  Et il se rendort.