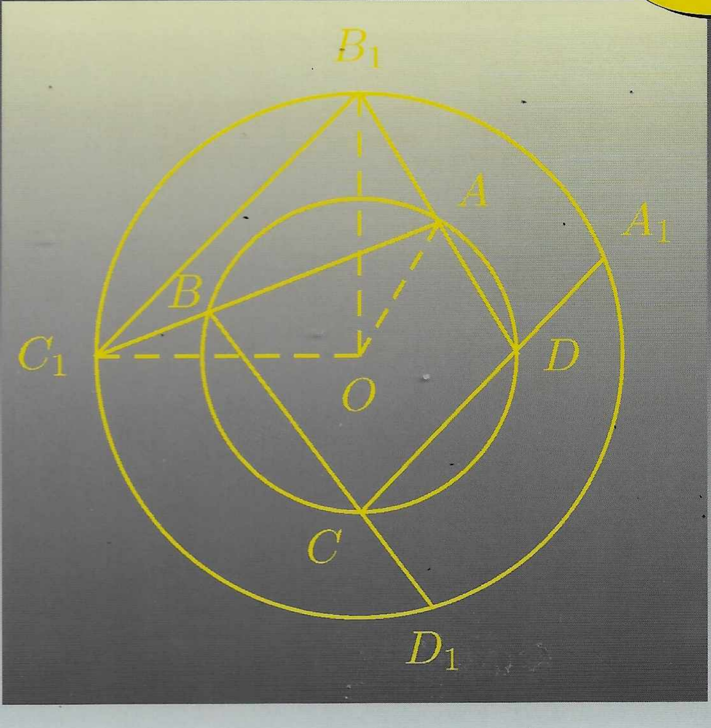
Tarik Belhaj Soulami

Les olympiades de mathématiques

Réflexes et stratégies

2e édition



ellipses

Tarik Belhaj Soulami

Les olympiades de mathématiques

Réflexes et stratégies

2e édition

ellipses

ISBN 978-2-7298-3661-0

www.editions-ellipses.fr

PRÉFACES

PRÉFACE DE LA SECONDE ÉDITION

Paru en 1999, cet ouvrage profondément original par sa forme et son organisation a connu un grand succès puisqu'il est aujourd'hui réédité à la demande de nombreux jeunes lecteurs.

J'ai fait la connaissance de Tarik en 1995 à l'occasion de la remise des prix de l'olympiade mathématique africaine, durant le congrès de l'union mathématique africaine à Ifrane au Maroc. Il y avait obtenu une médaille d'or, commençant ainsi avec beaucoup de modestie une longue série de succès aux olympiades internationales puis à l'école des mines de Paris et enfin dans sa vie professionnelle. Ce qui est tout à fait exceptionnel c'est qu'il entreprenait à vingt ans, dès son entrée dans cette école, la rédaction de ce livre dans l'objectif d'aider les futurs concurrents à se préparer en leur communiquant son plaisir et son enthousiasme et à franchir tous les obstacles auxquels il venait d'être confronté et qu'il avait lui même surmontés grâce à l'éducation patiente de ses réflexes et à l'élaboration minutieuse de sa stratégie.

En fait, ce recueil poursuit plusieurs buts :

- préparer, en particulier des candidats isolés aux compétitions internationales (olympiades internationales de mathématiques, tournoi des villes, rallyes sans frontières, Kangourou, ...) mais aussi nationales (concours général, olympiades de première, championnats des jeux mathématiques et logiques, rallyes régionaux des Irems, ...). Bien que la délégation française aux O.I.M. soit souvent dépassée par des pays structurant mieux leur préparation et la mettant en œuvre dès le début de la scolarité, l'analyse des résultats de ces trente dernières années montre que les lauréats de ces compétitions se retrouvent en tête à l'entrée des grandes écoles et que certains achèvent une carrière réussie de mathématicien.

- permettre de développer dans un grand nombre d'établissements des activités périscolaires et de mettre les élèves travaillant en équipes en situation de recherche sur des problèmes ouverts. Les animateurs de clubs et d'ateliers, comme par exemple ceux des maths en jeans, disposent ici d'une base de ressources parfaitement structurée.

- donner à tous les enseignants de mathématiques et plus généralement à tous les curieux de notre discipline l'occasion de chercher puis la joie de trouver la réponse à une question d'apparence anodine.

En conclusion lancez-vous vite dans la lecture et délectez-vous !

Paul-Louis Hennequin
Clermont-Ferrand, le 25 août 2007

PRÉFACE DE LA PREMIÈRE ÉDITION

Nul ne peut nous livrer le secret du raisonnement mathématique ; peut-être parce qu'il n'y a pas de secret ! Mais il y a tous les exposés qui, en disséquant les résultats du calcul, en créant des abstractions, en les analysant, en combinant et en variant les méthodes d'approche, réussissent à bien nous introduire dans l'édifice mathématique.

Ce livre en fait partie. Chaque problème est l'occasion pour quelques jeunes intelligences de goûter au plaisir de la recherche et aux jouissances abstraites. Face à des problèmes bruts où aucune méthode de recherche n'est suggérée, la liberté de création est totale. Il faut souvent plusieurs tentatives infructueuses pour se frayer un chemin vers la solution et parvenir à percer le mystère.

L'auteur nous propose ici d'exercer l'une des formes les plus captivantes du travail intellectuel. Il est clair que pour le novice, le paysage est tout autre. Ces mathématiques, si elles ne sont pas étrangères à celles que l'on enseigne au lycée, si elles ne sont pas en opposition, en contradiction avec celles que l'on dit scolaires, sont pourtant très différentes. Certains objecteront peut-être, et demanderont : à quoi bon ce genre de mathématiques ? Je suis tenté de leur répondre avec Lucas : « Il y eut toujours et toujours il y aura des savants pour dénigrer la fantaisie, des poètes pour répondre : à quoi bon la science ? des gens pratiques pour envelopper poètes et savants dans un inépuisable dédain d'abstrait et d'idéal. Et tout cela est bien heureux ».

Cet ouvrage est unique en son genre. C'est, à notre connaissance, le premier livre destiné à un vaste public francophone qui puisse servir de véritable outil de préparation aux olympiades internationales. Avec des exercices minutieusement corrigés, des exemples bien adaptés à leurs contextes et des illustrations parfaitement réalisées, nous pensons que ce livre rendra beaucoup de services à ses lecteurs. Nous ne pouvons qu'admirer cette œuvre et en remercier l'auteur.

Claude Deschamps
Paris, le 24 juin 1999

AVANT-PROPOS

Quand j'ai été candidat aux olympiades internationales, j'ai pu réaliser combien il était difficile de se procurer des documents en Français qui présentent les sujets traditionnellement abordés dans cette épreuve. Il fallait très souvent faire beaucoup d'exercices pour pouvoir apprécier une technique ou une méthode d'intérêt général. C'est ainsi qu'est née dans mon esprit l'idée d'écrire ce livre.

Tous les résultats qu'il est impératif de connaître pour réussir les épreuves d'olympiades y sont discutés. Loin d'être un garant de réussite, la connaissance de l'ensemble de ces résultats devrait au moins donner au candidat assez de confiance pour aborder sans trembler ce type d'exercices.

Cet ouvrage est divisé en six chapitres recouvrant l'ensemble des domaines explorés par les sujets des olympiades internationales suivant un consensus plus ou moins explicite ; certains points débordent largement les programmes des lycées français (équations diophantiennes, polynômes, inégalités, graphes) mais on n'y trouve généralement pas de géométrie dans l'espace ni de probabilités ni de statistiques.

Le contenu du livre est conçu pour être compréhensible par un élève courageux de terminale. J'ai donc supposé acquises certaines notions élémentaires d'analyse, ainsi que certains résultats très simples concernant les structures algébriques. Par contre, la plupart des notions enseignées au-delà de la classe terminale sont introduites avant d'être utilisées.

Les exercices proposés constituent un complément indispensable au cours : ce n'est qu'en les travaillant sérieusement que le lecteur pourra apprécier pleinement la portée des résultats obtenus et la manière de les mettre en œuvre. Les solutions fournies sont très détaillées, mais ne rendent pas compte du chemin souvent tortueux menant à la découverte des bons arguments ; c'est donc au lecteur de reconstituer toutes les étapes de la démonstration en reprenant si besoin est les calculs intermédiaires et en gardant toujours à l'esprit que la solution indiquée n'est pas forcément la seule possible.

Beaucoup d'exercices sont tirés des olympiades nationales et internationales. Bien qu'il soit assez délicat d'estimer la difficulté d'un exercice, je me suis efforcé de placer les plus difficiles en dernier. Dans le cas d'un exercice posé aux olympiades internationales, il m'a paru intéressant de mentionner son numéro d'ordre : rappelons en effet que la compétition consiste en deux épreuves de 4 heures et demie, comportant chacune trois exercices bien souvent ordonnés par difficulté croissante.

La bibliographie comporte 25 titres antérieurs à 1998 ; il sera facile au lecteur de la compléter en particulier par des énoncés de compétitions en consultant par exemple les sites `http://www.animath.fr/` et `http://publimath.irem.univ-mrs.fr/`.

Un livre comme celui-ci n'est jamais l'œuvre d'une seule personne. Il n'aurait jamais vu le jour sans l'aide de M. Mohammed Aassila, professeur de mathématiques à l'université de Strasbourg, et M. Francis Maisonneuve, professeur de mathématiques à l'école des Mines de Paris, qui ont bien voulu relire le texte en profondeur. Je tiens aussi à remercier Mme Brigitte d'Andréa-Novel qui m'a soutenu tout au long de la période de rédaction de ce livre. Je remercie également mes amis Eaman Eftekhary, Cyril Niboyet, Rachid Rabih et Hatim Marouane qui m'ont aidé en corrigeant certaines de mes erreurs et en me proposant des solutions alternatives.

Enfin, je tiens à exprimer ma gratitude à l'Association Mathématique des États-Unis qui m'a autorisé à utiliser les exercices des olympiades américaines et à Mme Corinne Baud des éditions Ellipses pour m'avoir si bien accueilli.

J'ai pris beaucoup de plaisir à écrire ce livre. Si, à travers les méthodes et techniques abordées j'arrive à faire partager au lecteur cette passion, si, à travers certaines remarques et questions profondes j'arrive à susciter la curiosité de quelques jeunes talents, si enfin, à travers des exercices passionnants j'arrive à prouver que l'on peut se faire plaisir tout en faisant des mathématiques, mon travail sera récompensé.

Je suis bien sûr attentif à toutes les remarques et critiques éventuelles que le lecteur voudra bien m'adresser aux bons soins des éditions Ellipses qui transmettront.

SOMMAIRE

1

LES STRATÉGIES DE BASE

On débute notre préparation par explorer un certain nombre de stratégies générales qui s'appliquent dans des contextes variés. Le but de ce chapitre est de montrer à quel point elles sont simples à comprendre, et cependant parfois si difficiles à utiliser.

1.1. Le principe des tiroirs

Ce principe est parfois appelé principe de Dirichlet[1] puisque c'est ce mathématicien qui fut le premier à réaliser qu'il pouvait servir pour montrer des résultats non triviaux.

Dans sa version la plus simple, ce principe peut être énoncé comme suit : « si $n+1$ balles sont placées dans n tiroirs, au moins un tiroir contiendra 2 balles ou plus ». Plus généralement :

1.1.1. Principe des tiroirs. *Si n balles sont placées dans k tiroirs, au moins un tiroir contiendra $\lceil n/k \rceil$ balles ou plus.*

♦ **Exemples.**

1. On se donne n entiers $a_1, a_2, \ldots, a_n$. Prouver qu'il existe un sous-ensemble de $\{a_1, a_2, \ldots, a_n\}$ dont la somme des éléments est divisible par n.

Considérons les sommes suivantes : $S_1 = a_1$, $S_2 = a_1 + a_2, \ldots, S_n = a_1 + a_2 + \cdots + a_n$. Si l'un des S_i, $i = 1, 2, \ldots, n$, est divisible par n, c'est fini. Sinon, considérons les restes de la division euclidienne des S_i par n. On dispose ainsi de n restes que l'on place dans les $n-1$ « tiroirs », les restes possibles modulo n. D'après le principe des tiroirs, il existe deux sommes S_i et S_j $(i < j)$ qui ont le même reste modulo n. Il est alors évident que $S_j - S_i = a_{i+1} + \cdots + a_j$ est divisible par n.

2. Un grand maître joue au moins une partie d'échecs par jour pour garder la

1. Johann Peter Gustav Lejeune Dirichlet (1805-1859), mathématicien allemand.

forme, mais pas plus de 10 par semaine pour ne pas se fatiguer. Prouver que s'il joue ainsi suffisamment longtemps, il y aura une période continue de jours pendant laquelle il aura joué exactement 21 parties.

Soit a_i le nombre de parties disputées jusqu'au jour i inclus. On a alors

$$1 \leqslant a_1 < a_2 < \cdots < a_k \leqslant 10 \times \lceil \frac{k}{7} \rceil, \quad k = 1, 2, \ldots$$

On en déduit que

$$22 \leqslant a_1 + 21 < a_2 + 21 < \cdots < a_k + 21 \leqslant 10 \times \lceil \frac{k}{7} \rceil + 21, \quad k = 1, 2, \ldots$$

Pour k suffisamment grand, l'inégalité $2k > 21 + 10 \times \lceil k/7 \rceil$ devient vraie. Il s'ensuit qu'il existe deux indices i et j tels que $a_j = a_i + 21$. Le grand maître aura alors disputé 21 rencontres pendant la période s'étalant entre le jour $i + 1$ et le jour j inclus.

EXERCICES

1. Soient $a_1, a_2, \ldots, a_{10}$ des entiers. Prouver qu'il existe des nombres $\alpha_1, \alpha_2, \ldots, \alpha_{10}$ non tous nuls et appartenant à l'ensemble $\{-1, 0, 1\}$ tels que $\sum_{i=1}^{10} \alpha_i a_i$ soit divisible par 1001.

(Proposé à l'OIM-1988)

2. Pour tout ensemble de dix naturels écrits à l'aide de deux chiffres (en système décimal), il existe au moins deux sous-ensembles disjoints dont les sommes des éléments sont égales.

(Olympiades internationales-1972/1)

3. On considère 13 nombres réels deux à deux distincts. Prouver que, parmi ces nombres, il existe deux réels a et b vérifiant :

$$0 < \frac{a - b}{1 + ab} \leqslant 2 - \sqrt{3}.$$

4. On colorie tous les points du plan en utilisant les deux couleurs rouge et vert. Démontrer qu'il existe un triangle équilatéral dont le côté mesure 1 ou $\sqrt{3}$ et les trois sommets sont de la même couleur.

(Olympiades chinoises-1986)

5. S est un ensemble convexe du plan. Les points de S sont coloriés à l'aide de p couleurs, et on suppose qu'il existe dans S trois points non alignés. Démontrer que pour tout entier naturel $n \geqslant 3$, il existe une infinité de polygones de n côtés, isométriques et dont les sommets sont de la même couleur.

(Olympiades roumaines-1995)

---

6. On fait une partition de l'ensemble des points du plan orienté en un nombre fini de parties représentées par autant de couleurs. On fixe deux points distincts O et A de ce plan. À tout point X du plan, distinct de O, on fait correspondre :

a) la mesure en radians $\alpha(X)$ de l'angle $(\widehat{OA, OX})$ prise dans $[0, 2\pi[$;

b) le cercle $\mathcal{C}(X)$ de centre O, de rayon $OX + \alpha(X)/OX$.

Démontrer qu'il existe un point Y du plan avec $\alpha(Y) > 0$, tel qu'il existe un point de $\mathcal{C}(Y)$ de la même couleur que Y.

(Olympiades internationales-1984/3)

---

7. Soit ABC un triangle équilatéral. Soit $\mathcal{E}$ l'ensemble des points des segments fermés $[AB]$, $[BC]$, $[CA]$. Est-ce que, pour toute partition de E en deux sous-ensembles disjoints, il existe au moins un triangle rectangle dont les trois sommets appartiennent au même sous-ensemble ?

(Olympiades internationales-1983/4)

---

8. Soit n un entier $\geqslant 2$. Prouver que, dans une réunion de n personnes, il existe toujours deux personnes telles que, parmi les $n-2$ autres participants, il y ait au moins $\lfloor n/2 \rfloor - 1$ participants qui connaissent les deux personnes à la fois ou leur sont complètement étrangères.

(Olympiades des États-Unis-1985)

1.2. La récurrence

Dans l'axiomatique de Peano[2], le principe suivant est un axiome de construction de l'ensemble $\mathbb{N}$:

> **1.2.1. Le principe de récurrence.** *Soit m un entier naturel et P_m, $P_{m+1}, \ldots$ une suite de propositions. Si*
>
> *a) P_m est vraie, et si*
>
> *b) pour tout entier naturel $k \geqslant m$, $P_k \Longrightarrow P_{k+1}$ est vrai,*
>
> *alors toutes les propositions sont vraies.*

♦ **Remarques.**

1. Dans la preuve par récurrence, l'étape a) est appelée la base de la récurrence

2. Guissepe Peano (1858-1932), mathématicien italien.

et l'étape b) est appelée l'étape inductive.

2. Il ne faut surtout pas oublier la base de la récurrence : en effet, la condition b) est vraie pour toute suite de propositions fausses.

3. Il peut arriver que dans une preuve par récurrence, on ait besoin pour montrer P_{k+1} non seulement de P_k mais aussi des P_i pour $m \leqslant i \leqslant k$. En appliquant le principe de récurrence à la suite de propositions $(Q_n)_{n \geqslant m}$ définie par : $Q_n \iff (\forall k \in \{m, \ldots, n\}, P_k)$, on justifie le principe de récurrence suivant :

1.2.2. La récurrence forte. *Soit m un entier naturel et P_m, $P_{m+1}, \ldots$ une suite de propositions. Si*

a) P_m est vraie, et si

b) pour tout entier naturel $k \geqslant m$, (P_m et P_{m+1} et $\ldots$ et P_k) $\Longrightarrow P_{k+1}$ est vraie,

alors toutes les propositions sont vraies.

♦ **Exemples.**

1. Montrer que, pour tout $n \in \mathbb{N}^*$,

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2.$$

L'astuce est de prouver par récurrence une inégalité un peu plus forte. Soit P_n la propriété : « $\dfrac{1}{1^2} + \dfrac{1}{2^2} + \cdots + \dfrac{1}{n^2} \leqslant 2 - \dfrac{1}{n}$ ».

Il est alors clair que P_1 est vraie. Si P_n est vraie pour un certain $n \in \mathbb{N}^*$, alors

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} \leqslant 2 - \frac{1}{n} + \frac{1}{(n+1)^2} < 2 - \frac{1}{n+1},$$

d'où P_{n+1}.

2. Soit n un entier naturel, et soit $\mathcal{E}$ un ensemble constitué de $2n+1$ entiers naturels non nuls (non nécessairement distincts). On suppose que $\mathcal{E}$ vérifie la propriété (P) : « en enlevant à $\mathcal{E}$ un élément quelconque, il est toujours possible de partitionner les éléments restants en deux parties de n éléments, la somme des éléments constituant chaque partie étant la même ». Prouver que tous les éléments de $\mathcal{E}$ sont égaux.

On raisonne par récurrence à n fixé sur la valeur du plus grand élément de $\mathcal{E}$. Si le plus grand élément de $\mathcal{E}$ est égal à 1, alors tous les éléments de $\mathcal{E}$ sont égaux à 1 et on a le résultat souhaité.

Supposons donc le résultat vrai pour tout ensemble $\mathcal{E}$ à $2n+1$ éléments (non nécessairement distincts) vérifiant la propriété (P), et dont le plus grand élément est $\leqslant m$. Considérons alors un ensemble $\mathcal{E}$ dont le plus grand élément est égal à $m+1$, et soient $x_1, x_2, \ldots, x_{2n+1}$ ses éléments (on accepte toujours que les x_i ne soient pas tous distincts). Si $\mathcal{E}$ vérifie la propriété (P), alors tous les x_i, $i = 1, 2, \ldots, 2n+1$, sont de la même parité : en effet, pour tout $i, j \in \{1, 2, \ldots, 2n+1\}$, il existe des entiers naturels S_i et S_j tels que $x_i + 2S_i = x_j + 2S_j = x_1 + x_2 + \cdots + x_{2n+1}$.

Si tous les x_i, $i = 1, 2, \ldots, 2n+1$, sont pairs, alors l'ensemble $\mathcal{E}_1 = \{x_1/2, x_2/2, \ldots, x_{2n+1}/2\}$ vérifie la propriété (P). Comme le plus grand élément de $\mathcal{E}_1$ est $\leqslant m$, il s'ensuit que $x_1/2 = x_2/2 = \cdots = x_{2n+1}/2$, i.e., $x_1 = x_2 = \cdots = x_{2n+1}$.

Si tous les x_i, $i = 1, 2, \ldots, 2n+1$, sont impairs, alors l'ensemble $\mathcal{E}_2 = \{(x_1 + 1)/2, (x_2+1)/2, \ldots, (x_{2n+1}+1)/2\}$ vérifie la propriété (P), et comme le plus grand élément de $\mathcal{E}_2$ est $\leqslant m$, on a encore $x_1 = x_2 = \cdots = x_{2n+1}$, ce qui achève la récurrence.

3. Soient $x_1, x_2, \ldots, x_n$ et $y_1, y_2, \ldots, y_m$ des entiers naturels non nuls. On suppose que $x_1 + x_2 + \cdots + x_n = y_1 + y_2 + \cdots + y_m < mn$. Prouver qu'il est possible de supprimer certains termes (mais pas tous !) de part et d'autre de l'égalité $x_1 + x_2 + \cdots + x_n = y_1 + y_2 + \cdots + y_m$ tout en conservant une égalité.

On raisonne par récurrence sur $m+n$. Comme $m \leqslant x_1 + x_2 + \cdots + x_n < mn$, on a $n > 1$, et de même $m > 1$. Pour $m + n = 4$, on a donc $m = n = 2$ et les seuls cas possibles sont $1 + 1 = 1 + 1$ et $1 + 2 = 1 + 2$ (à l'ordre près), de sorte que le résultat est immédiat.

Supposons donc le résultat vrai pour un certain $k = m + n \geqslant 4$. Considérons

$$x_1 + x_2 + \cdots + x_n = y_1 + y_2 + \cdots + y_m < mn,$$

où $m + n = k + 1$. On peut supposer, sans nuire à la généralité, que x_1 est le plus grand des x_i, $i = 1, 2, \ldots, n$, et que y_1 est le plus grand des y_i, $i = 1, 2, \ldots, m$. On peut aussi supposer $x_1 > y_1$ car si $x_1 = y_1$, le problème est résolu. On a alors

$$(x_1 - y_1) + x_2 + \cdots + x_n = y_2 + \cdots + y_m,$$

avec $y_2 + \cdots + y_m < mn - \dfrac{mn}{m} = n(m-1)$. Comme $n + (m-1) = k$, on peut appliquer l'hypothèse de récurrence pour conclure.

EXERCICES

9. Soit n un entier strictement positif. Prouver que, pour tout entier strictement positif $a \leqslant n!$, il existe des entiers positifs $d_1, d_2, \ldots, d_k$, $k \leqslant n$, deux à deux distincts et divisant chacun $n!$, tels que : $a = d_1 + d_2 + \cdots + d_k$.

---

10. Soit n un entier de la forme 2^k, $k \geqslant 1$. Prouver que, dans tout ensemble de $2n - 1$ entiers strictement positifs, on peut trouver un sous-ensemble de n entiers dont la somme est divisible par n.

(Olympiades allemandes-1981)

---

11. On considère n points d'un même plan ($n \geqslant 5$). Démontrer qu'il est possible de relier ces points par des flèches de telle sorte que de chaque point on peut arriver à un autre point en suivant une ou deux flèches.

---

12. Soient $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{1989}$ des vecteurs dans le plan tels que $||\vec{v}_r|| \leqslant 1$ pour $1 \leqslant r \leqslant 1989$. Montrer qu'il est possible d'affecter à chaque vecteur $\vec{v}_r$ un nombre $\varepsilon_r = \pm 1$ de telle sorte que :

$$\Big|\Big|\sum_{r=1}^{1989} \varepsilon_r \vec{v}_r\Big|\Big| \leqslant \sqrt{2}.$$

(Proposé à l'OIM-1989)

---

13. On considère un ensemble de $2n$ points dans l'espace euclidien, $n > 1$, et on suppose construits $n^2 + 1$ segments entre ces points. Prouver que la configuration obtenue contient au moins un triangle.

---

14. Les sommets d'un polygone convexe ayant $2n + 1$ côtés sont coloriés de telle sorte que deux sommets consécutifs n'aient pas la même couleur. Prouver qu'il est possible de diviser ce polygone en triangles à l'aide de diagonales dont les extrémités sont de couleurs différentes et qui ne se recoupent pas entre elles.

(Olympiades hongroises-1978)

1.3. La descente infinie

Supposant le principe de récurrence acquis, il est facile de démontrer que « toute partie non vide de $\mathbb{N}$ admet un plus petit élément ». On dit que $\mathbb{N}$ est bien ordonné. Une conséquence de ce principe équivalent au principe de récurrence est la méthode de descente infinie découverte par Fermat[3].

1.3.1. La descente infinie. *Soit une suite de propositions $P_0, P_1, \ldots, P_n, \ldots$ Si pour tout $k \in \mathbb{N}$ tel que P_k est fausse, il existe $m \in \mathbb{N}$ tel que P_m soit fausse et $m < k$, alors toutes les propositions $P_0, P_1, \ldots, P_n, \ldots$ sont vraies.*

♦ **Preuve.** On démontre d'abord que toute partie non vide de $\mathbb{N}$ admet un plus petit élément : en effet, si S est une partie de $\mathbb{N}$ n'ayant pas de plus petit élément, considérons la suite de propositions $(P_n)_{n\in\mathbb{N}}$, où la proposition P_n est « $\forall k \leqslant n$, $k \notin S$ ». P_0 est alors vraie car autrement 0 serait le plus petit élément de S. De plus, si P_m est vraie pour un certain $m \in \mathbb{N}$, alors P_{m+1} est vraie : en effet, si P_{m+1} était fausse, alors $m + 1 \in S$ serait le plus petit élément de S puisque P_m est vraie.

Pour démontrer la validité de la méthode de descente infinie, on raisonne par l'absurde : l'ensemble des entiers k tels que P_k est fausse serait alors une partie non vide de $\mathbb{N}$ qui n'admet pas de plus petit élément.

□

3. Pierre de Fermat (1601-1665), mathématicien français.

♦ **Exemples.**

1. La suite des carrés parfaits contient-elle une progression arithmétique infinie ?

Si $(a_n^2)_{n\in\mathbb{N}^*}$ est une progression arithmétique infinie, alors

$$a_{m+1}^2 - a_m^2 = a_m^2 - a_{m-1}^2, \quad m = 2, 3, 4, \ldots$$

Comme $a_{m+1} + a_m > a_m + a_{m-1}$, on doit avoir $a_{m+1} - a_m < a_m - a_{m-1}$ pour $m \geqslant 2$, ce qui s'écrit encore :

$$a_2 - a_1 > a_3 - a_2 > a_4 - a_3 > \cdots$$

On a ainsi une suite strictement décroissante d'entiers positifs, ce qui est impossible.

2. Résoudre dans $\mathbb{Z}^3$ l'équation diophantienne :

$$x^3 + 2y^3 = 4z^3.$$

Montrons que $(0, 0, 0)$ est la seule solution à l'équation proposée. Si (x, y, z) est une solution non nulle, alors x est pair. Si on pose $x = 2w$ où $w \in \mathbb{Z}$, alors

$$(2w)^3 + 2y^3 = 4z^3,$$

c'est-à-dire

$$(-y)^3 + 2z^3 = 4w^3,$$

ce qui implique que $(-y, z, x/2)$ est aussi solution. D'une façon analogue, on trouve que $(-z, x/2, -y/2)$ est solution, puis que $(-x/2, -y/2, -z/2)$ est aussi solution, et ainsi de suite on arrivera à une solution contenant un entier impair, ce qui est impossible.

EXERCICES

15. Prouver qu'il n'existe pas de quadruplets (x, y, z, t) d'entiers strictement positifs tels que :

$$x^2 + y^2 = 3(z^2 + t^2).$$

---

16. 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 respectivement les nombres x, y, z avec $y < 0$, alors l'opération suivante est permise : « remplacer le triplet (x, y, z) par $(x + y, -y, y + z)$ ».

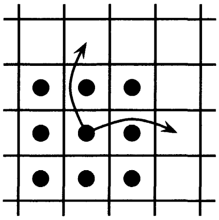
Cette opération est répétée tant qu'au moins un des cinq nombres est strictement négatif. Déterminer si ce processus prend nécessairement fin après un nombre fini d'opérations.

(Olympiades internationales-1986/3)

---

17. Il y a n^2 pièces occupant un carré de côté n sur un échiquier infini. Il est possible de déplacer une pièce par dessus une case occupée vers une case vide ; la pièce par dessus de laquelle le mouvement est effectué est alors immédiatement écartée de l'échiquier.

Pour quelles valeurs de n peut-on se retrouver avec une seule pièce sur l'échiquier ?



(Olympiades internationales-1993/3)

1.4. Maximums et minimums

L'un des réflexes qu'il faut avoir en présence de problèmes d'existence dans un ensemble fini est de considérer des objets de l'ensemble qui minimisent ou maximisent les valeurs prises par une certaine fonction. Il s'agit donc d'une méthode permettant de construire une solution ou de prouver qu'il n'existe aucune solution au problème. Les exemples et exercices qui suivent montreront à quel point il est facile de dérouler la démonstration une fois réussi le choix de la fonction.

♦ **Exemples.**

1. On se donne un ensemble fini $\mathcal{E}$ de points dans le plan. On suppose que pour toute paire $\{A, B\}$ de points dans $\mathcal{E}$, il existe un point $C \neq A, B$ dans $\mathcal{E}$ tel que les points A, B et C soient alignés. Prouver que tous les points de $\mathcal{E}$ sont alignés.

Si les points de $\mathcal{E}$ n'étaient pas tous alignés, l'ensemble des couples (A, Δ), où Δ est une droite passant par deux points de $\mathcal{E}$ et A est un point de $\mathcal{E}$ n'appartenant pas à Δ, serait non vide.

Considérons alors un couple (A, Δ) qui minimise la distance du point A à la droite Δ, et soit P le pied de la perpendiculaire issue du point A à la droite Δ. Il existe au moins trois points B, C et D de l'ensemble $\mathcal{E}$ sur la droite Δ.

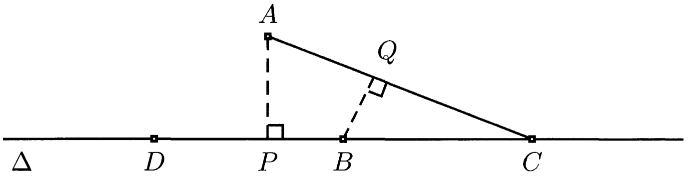


FIG. 1.1.

Sans nuire à la généralité, on peut supposer que B et C se trouvent du même côté du point P et que B est plus proche de P que C. Ceci étant, on obtient une contradiction en considérant le pied de la perpendiculaire issue de B à la droite (AC) puisque $BQ < AP$.

2. Le raisonnement précédent peut être appliqué pour résoudre des exercices du même type. Considérons par exemple le problème suivant : soit $\mathcal{E}$ un ensemble fini de droites dont deux quelconques ne sont pas parallèles. On suppose de plus que toute intersection de deux droites de $\mathcal{E}$ appartient à au moins une autre droite dans $\mathcal{E}$. On va prouver que toutes les droites ont un point commun.

Si les droites de $\mathcal{E}$ ne passaient pas toutes par un même point, l'ensemble des couples (A, Δ), où Δ est une droite dans $\mathcal{E}$ et A est un point d'intersection de deux droites dans $\mathcal{E}$ n'appartenant pas à Δ, serait non vide.

Considérons donc un couple (A, Δ) qui minimise la distance du point A à la droite Δ, et soit P le pied de la perpendiculaire issue du point A à la droite Δ. Par hypothèse, il existe trois droites $\Delta_1, \Delta_2, \Delta_3 \in \mathcal{E}$ qui passent par le point A. On se retrouve alors avec la même contradiction que dans le premier exemple :

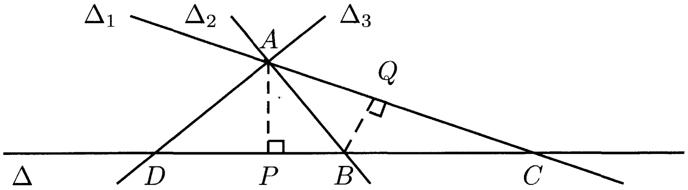


FIG. 1.2.

EXERCICES

18. Dans le plan on se donne un disque fermé de rayon 1, et on suppose qu'il contient sept points dont les distances mutuelles sont toutes $\geqslant 1$. Prouver que le centre du disque est l'un de ces points.

(Olympiades britanniques-1975)

---

19. On considère un pentagone convexe $ABCDE$ tel que parmi ses côtés et ses diagonales, il n'existe pas de segments parallèles. Les droites (AD) et (BC) se coupent en un point X, et on dessine une flèche sur le segment $[BC]$ dans le sens de ce point. De manière analogue, on dessine des flèches sur les autres côtés du pentagone. Prouver qu'il existe deux flèches dirigées vers un même sommet du pentagone.

---

20. On se donne un ensemble S de $2n+3$ points dans le plan dont trois quelconques ne sont pas alignés, et quatre quelconques ne sont pas cocycliques. Prouver qu'il est toujours possible de trouver un cercle passant par exactement 3 points de S et séparant les autres points en n points à l'intérieur du cercle et n points à l'extérieur du cercle.

---

21. Soit X un ensemble fini et $E(X)$ la collection des sous-ensembles de X possédant un nombre pair d'éléments. Soit f une fonction à valeurs réelles définie sur $E(X)$ telle que $f(D) > 1990$ pour un certain D dans $E(X)$ et $f(A \cup B) = f(A) + f(B) - 1990$ pour tous éléments disjoints A et B dans $E(X)$.

Prouver que X peut être partitionné en deux sous-ensembles disjoints P et Q tels que $f(S) > 1990$ pour tout élément non vide S dans $E(P)$ et $f(T) \leqslant 1990$ pour tout élément T dans $E(Q)$.

(Olympiades chinoises-1990)

---

22. On considère l'opération suivante : « passer du point $P(x, y)$ à l'un des points $P_1(x, y+2x)$, $P_2(x, y-2x)$, $P_3(x-2y, y)$ ou $P_4(x+2y, y)$ ». On suppose encore qu'il est interdit de parcourir un segment que l'on a déjà décrit. Prouver que, si l'on part du point $(1, \sqrt{2})$, il n'est pas possible d'y revenir.

(Olympiades hongroises-1990)

1.5. Les invariants

Il peut arriver que, dans un problème donné, on ait un ensemble d'états possibles $\mathcal{E}_0$, $\mathcal{E}_1, \ldots$, le passage d'un état à l'état suivant étant régi par un ensemble de règles bien définies. On se pose alors la question suivante : « peut-on atteindre un état final $\mathcal{E}_f$ en partant de l'état initial $\mathcal{E}_0$? ».

Une stratégie souvent efficace pour s'attaquer à ce type de problèmes est de considérer une fonction f, définie sur l'ensemble des états du système, telle que si on peut passer d'un état $\mathcal{E}$ à un état $\mathcal{E}'$, on ait nécessairement $f(\mathcal{E}) = f(\mathcal{E}')$. Si $f(\mathcal{E}_f) \neq f(\mathcal{E}_0)$, la conclusion est immédiate : partant de l'état $\mathcal{E}_0$, on ne peut jamais atteindre l'état $\mathcal{E}_f$. La fonction f est alors appelée *invariant*. Elle peut être par exemple la parité d'une variable, le nombre d'éléments d'un ensemble, ...

♦ **Exemples.**

1. On écrit sur un tableau les nombres 1, 2, ..., 1998. On choisit deux nombres arbitraires que l'on efface pour les remplacer par leur différence. Cette opération est répétée tant que le tableau contient au moins deux nombres. Le dernier nombre qui reste sur le tableau peut-il être égal à 2 ?

La réponse est non : en effet, la somme des éléments inscrits sur le tableau conserve sa parité au cours du processus décrit dans l'énoncé. Celle-ci étant celle de la somme initiale

$$1 + 2 + \cdots + 1998 = \frac{1}{2} \times 1998 \times 1999 = 999 \times 1999,$$

qui est impaire, le dernier nombre qui reste ne peut pas être égal à 2.

2. Dans la suite

$$1, 0, 1, 0, 1, 0, 3, 5, 0, \ldots$$

chaque terme après le sixième est égal au dernier chiffre de la somme des six termes qui le précèdent. Prouver qu'il est impossible de trouver la succession :

$$0, 1, 0, 1, 0, 1,$$

dans la suite ainsi définie.

(Olympiades russes-1984)

On désigne par $(x_n)_{n \geqslant 1}$ la suite définie dans l'énoncé, et on considère la fonction :

$$f(x, y, z, t, u, v) = 2x + 4y + 6z + 8t + 10u + 12v.$$

On a alors :

$$\begin{aligned}
&f(x_{n+1}, x_{n+2}, \ldots, x_{n+6}) - f(x_n, x_{n+1}, \ldots, x_{n+5}) \\
&= (2x_{n+1} + 4x_{n+2} + \cdots + 12x_{n+6}) - (2x_n + 4x_{n+1} + \cdots + 12x_{n+5}) \\
&= 12x_{n+6} - 2x_n - 2x_{n+1} - 2x_{n+2} - 2x_{n+3} - 2x_{n+4} - 2x_{n+5} \\
&\equiv 12(x_n + x_{n+1} + \cdots + x_{n+5}) - 2(x_n + x_{n+1} + \cdots + x_{n+5}) \\
&\equiv 0 \pmod{10}.
\end{aligned}$$

Il s'ensuit que le dernier chiffre de $f(x_n, x_{n+1}, \ldots, x_{n+5})$ est un invariant. Mais $f(1, 0, 1, 0, 1, 0) = 18$ et $f(0, 1, 0, 1, 0, 1) = 24$, d'où la conclusion que la succession 0, 1, 0, 1, 0, 1 ne peut se produire.

EXERCICES

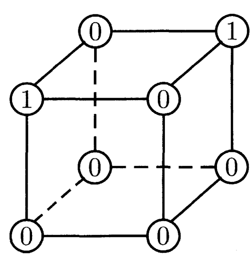
23. On considère le tableau suivant où seul l'élément à l'intersection de la première ligne et de la troisième colonne est un signe « − », les autres éléments étant des signes « + » :

+	+	−	+
+	+	+	+
+	+	+	+
+	+	+	+

Est-il possible qu'à l'issue d'un processus où, à chaque étape, on peut changer les signes d'une ligne, d'une colonne ou d'une diagonale quelconque, on se retrouve avec un tableau où tous les éléments sont des signes « + » ?

---

24. On affecte à chaque sommet d'un cube donné un entier naturel. Il est alors possible de choisir une arête et augmenter de 1 les nombres correspondant à ses deux extrémités.



Partant de la situation représentée ci-dessus, prouver qu'il est impossible de rendre les nombres dans les huit sommets égaux.

(Olympiades russes-1981)

---

25. On affecte arbitrairement à chaque élément d'un tableau 9×9 la valeur 1 ou -1. On calcule pour chaque élément du tableau le produit des éléments adjacents (deux éléments sont dits adjacents si leurs cases respectives ont exactement un côté en commun) puis, simultanément, on remplace tous les éléments par les produits correspondants.

Est-il possible qu'après un nombre fini de telles opérations on aboutisse à un tableau constitué uniquement d'éléments égaux à 1 ?

(Olympiades chinoises-1992)

---

26. On se donne quatre triangles rectangles isométriques. On prend l'un d'entre eux et on le coupe en deux à l'aide de l'altitude issue de l'angle droit puis on recommence avec l'ensemble de tous les triangles rectangles résultants. Prouver qu'il est impossible de se débarrasser des triangles isométriques.

(Olympiades russes-1995)

SOLUTIONS

1. On considère l'ensemble E formé par les vecteurs $(y_1, y_2, \ldots, y_{10})$ tels que $y_i = \pm 1$ pour $i = 1, 2, \ldots, 10$. On affecte à chaque somme $\sum_{i=1}^{10} y_i a_i$ sa classe modulo 1001. Comme $|E| = 2^{10} = 1024$, il existe deux vecteurs $(u_1, u_2, \ldots, u_{10})$ et $(v_1, v_2, \ldots, v_{10})$ tels que :

$$\sum_{i=1}^{10} u_i a_i - \sum_{i=1}^{10} v_i a_i = \sum_{i=1}^{10} (u_i - v_i) a_i$$

soit divisible par 1001. Mais $u_i - v_i \in \{-2, 0, 2\}$ et $u_j - v_j \neq 0$ pour un certain j. Il s'ensuit que

$$\sum_{i=1}^{10} \frac{1}{2}(u_i - v_i) a_i$$

est divisible par 1001 et $(u_i - v_i)/2 \in \{-1, 0, 1\}$, d'où le résultat.

---

2. Soit X un ensemble $\subseteq \{11, 12, \ldots, 99\}$ tel que $|X| = 10$. Cet ensemble possède $2^{10} - 2 = 1022$ parties non vides strictes. D'un autre côté, si A est un sous-ensemble de X ($A \neq \varnothing$, X), alors :

$$1 \leqslant \sum (x \mid x \in A) \leqslant 91 + 92 + \cdots + 99 = 855.$$

Puisque le nombre d'« objets » (sous-ensembles non vides strictes de X) est supérieur au nombre de « tiroirs » (les sommes distinctes des éléments d'un tel sous-ensemble), il s'ensuit qu'il existe deux parties B, C de l'ensemble X dont la somme des éléments est la même, i.e.,

$$\sum (y \mid y \in B) = \sum (z \mid z \in C).$$

Il est alors clair que $B \not\subseteq C$ et $C \not\subseteq B$. Posons $X = B \backslash (B \cap C)$ et $Y = C \backslash (B \cap C)$. On a donc

$$\sum (x \mid x \in X) = \sum (y \mid y \in Y),$$

d'où le résultat.

---

3. Soient a_i, $i = 1, 2, \ldots, 13$, les réels considérés. Pour tout $i \in \{1, 2, \ldots, 13\}$, il existe un unique réel x_i dans $]-\pi/2, \pi/2[$ tel que $a_i = \tan x_i$, et le principe des tiroirs prouve l'existence de deux indices i, $j \in \{1, 2, \ldots, 13\}$ tels que :

$$0 < x_i - x_j \leqslant \frac{\pi}{12}.$$

On a alors

$$\tan 0 < \tan(x_i - x_j) \leqslant \tan \frac{\pi}{12},$$

et comme $\tan \pi/12 = 2 - \sqrt{3}$, le résultat est acquis.

---

4. Si tous les points du plan sont de la même couleur, le problème est résolu. Supposons donc que les points du plan ne sont pas tous de la même couleur ; démontrons alors qu'il existe deux points dont la distance vaut 2 et qui sont de couleurs différentes : en effet, on suppose que lorsque la distance entre deux points vaut 2 alors ces deux points sont de la même couleur. Soient alors A et B deux points distincts du plan. On place les points A_1, $A_2, \dots, A_k$ sur le segment $[AB]$ de telle sorte que $AA_1 = A_1A_2 = \cdots = A_{k-1}A_k = 2$ et $A_kB \leqslant 2$. Si $A_kB = 2$, alors B a la même couleur que A et si $A_kB < 2$, on considère un point C tel que $A_kC = CB = 2$. Les points A, B et C sont de la même couleur.

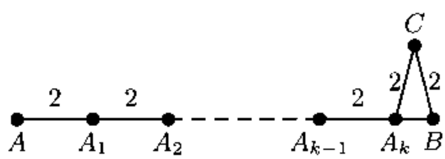


FIG. 1.3.

Ainsi, on démontre que tous les points du plan sont de la même couleur, ce qui est en contradiction avec l'hypothèse.

Soient alors A et B deux points de couleurs différentes et tels que $AB = 2$. Soit O le milieu du segment $[AB]$. Le point O a la même couleur que A ou que B. Supposons qu'il a la même couleur que A. On construit alors les deux triangles équilatéraux AOD et AOC.

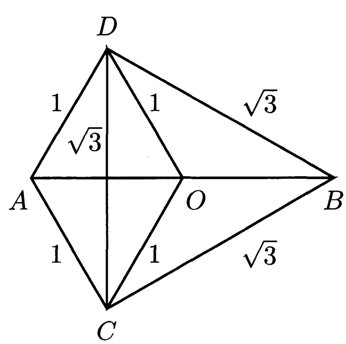


FIG. 1.4.

Si l'un des points C ou D a la même couleur que A, alors l'un des triangles AOD ou AOC est une solution. Sinon le triangle BCD sera une solution.

---

5. Soit C un cercle à l'intérieur d'un triangle formé par trois points non alignés de S, et posons $m = np + 1$. Considérons un polygone régulier $A_1, A_2, \dots, A_m$

inscrit dans $\mathcal{C}$. D'après le principe des tiroirs, il existe au moins n points de la même couleur qui forment un polygone de n côtés dont les sommets sont de la même couleur.

Soit α un angle de $]0, 2\pi/m[$. Par des rotations d'angle α, on obtient une infinité de polygones de n côtés inscrits dans le cercle $\mathcal{C}$ et ayant des sommets de la même couleur. Comme le nombre de couleurs est fini, il s'ensuit qu'il existe une couleur commune à une infinité de ces polygones (qui ne sont pas nécessairement isométriques). Mais comme il n'y a qu'un nombre fini de façons de choisir un polygone de n côtés (à une isométrie près) dont les sommets appartiennent à l'ensemble $\{A_1, A_2, \ldots, A_m\}$, il s'ensuit qu'il existe une infinité de polygones convexes de n côtés qui sont isométriques et dont les sommets sont de la même couleur.

---

6. On suppose les points du plan orienté coloriés à l'aide de n couleurs différentes. Affectons à chaque ensemble de points dans le plan l'ensemble des couleurs qui le colorient. Il y a alors

$$\sum_{k=1}^{n} \binom{n}{k} = 2^n - 1$$

ensembles possibles.

Si on considère un ensemble de 2^n cercles concentriques de centre O et de rayons $< \sqrt{2\pi}$, alors il existe forcément deux de ces cercles, $\mathcal{C}_1$ et $\mathcal{C}_2$, avec le même ensemble de couleurs. Si $R_1 < R_2$ sont les rayons respectifs de $\mathcal{C}_1$ et $\mathcal{C}_2$, alors il existe un point Y du cercle $\mathcal{C}_1$ tel que :

$$\alpha(Y) > 0, \quad R_2 = R_1 + \frac{\alpha(Y)}{R_1}.$$

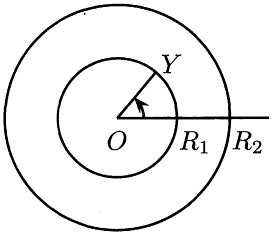


FIG. 1.5.

En effet, puisque $0 < R_1(R_2 - R_1) < 2\pi$, le point Y est parfaitement déterminé sur le cercle $\mathcal{C}_1$. Mais alors Y a la même couleur qu'un certain point du cercle $\mathcal{C}_2 = \mathcal{C}(Y)$, d'où le résultat.

---

7. L'idée est de partager le triangle ABC en quatre triangles, dont trois sont rectangles. Pour ce faire, considérons un point D de $[BC]$, et soient F son projeté orthogonal sur $[AB]$ et E le projeté orthogonal de F sur $[AC]$. On souhaiterait que D soit le projeté orthogonal de E sur $[BC]$.

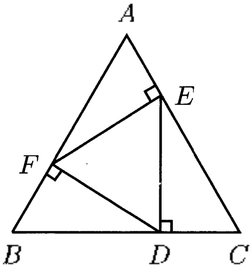


FIG. 1.6.

Si tel était le cas, on aurait $\widehat{BDF} = \widehat{CED} = \widehat{AFE} = 30°$, ce qui impliquerait que

$$\frac{AF}{FB} = \frac{BD}{DC} = \frac{CE}{EA} = 2.$$

Réciproquement, si D, E et F sont choisis sur les segments $[BC]$, $[AC]$ et $[AB]$ respectivement, de telle sorte que la dernière égalité soit vérifiée, alors :

$$EF^2 = AE^2 + AF^2 - 2AE \cdot AF \cdot \cos \widehat{EAF} = \frac{1}{3}AB^2,$$

ce qui donne $EF^2 + AE^2 = AF^2$, i.e., $\widehat{AEF} = 90°$. De même, on montre que $\widehat{BFD} = \widehat{EDC} = 90°$.

Supposons maintenant qu'il existe une partition de $\mathcal{E} = [AB] \cup [BC] \cup [CA]$ en deux sous-ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$ telle qu'aucun triangle rectangle dont les sommets sont situés dans $\mathcal{E}$ n'a tous ses sommets dans un même sous-ensemble. Sans perte de généralité, on peut supposer que D, $F \in \mathcal{E}_1$. Il s'ensuit qu'aucun point situé sur $[AB] \setminus \{F\}$ n'appartient à $\mathcal{E}_1$, ce qui implique encore que C, $E \in \mathcal{E}_1$. On a donc $\{C, E, D\} \subseteq \mathcal{E}_1$, et le triangle CED étant rectangle, on a une contradiction.

---

8. On désigne par $\mathcal{S}$ l'ensemble de tous les participants et par $\mathcal{A}$ l'ensemble des triplets $(A, B, C) \in \mathcal{S}^3$ tels que C soit une connaissance commune de A et B ou une personne étrangère à A et B à la fois.

Si $C \in \mathcal{S}$ connaît k participants à la réunion, alors il existe $k(n-1-k)$ paires où C connaît exactement un seul élément. On en déduit que :

$$|\mathcal{A}| \geqslant 2n\left[\binom{n-1}{2} - \left(\frac{n-1}{2}\right)^2\right] = \frac{n(n-1)(n-3)}{2}.$$

Si on prend pour « tiroirs » l'ensemble de tous les couples $(A, B) \in \mathcal{S}^2$, et l'on pose l'« objet » $(A, B, C) \in \mathcal{A}$ dans le tiroir (A, B) pour tout $C \in \mathcal{S}$ tel que $(A, B, C) \in \mathcal{A}$, alors on aura au moins $n(n-1)(n-3)/2$ objets à distribuer entre $n(n-1)$ tiroirs. On en déduit qu'il existe au moins un tiroir contenant au minimum

$$\left\lceil \frac{n(n-1)(n-3)/2}{n(n-1)} \right\rceil = \left\lceil \frac{n-3}{2} \right\rceil = \left\lfloor \frac{n}{2} \right\rfloor - 1$$

objets, ce qui permet de conclure.

---

9. La propriété est vraie pour $n = 1$. Supposons qu'elle est vraie pour un entier $n \geqslant 1$, et soit a un entier $\leqslant (n+1)!$. Divisons a par $n+1$: il existe $(d, r) \in \mathbb{N} \times \mathbb{N}$ tel que

$$a = d(n+1) + r,$$

où $d \leqslant n!$ et $r < n+1$. Par hypothèse de récurrence, il existe des nombres $d_1, d_2, \ldots, d_l$ ($l \leqslant n$), deux à deux distincts et divisant chacun $n!$, tels que : $d = d_1 + d_2 + \cdots + d_l$, soit

$$a = d_1(n+1) + d_2(n+1) + \cdots + d_l(n+1) + r,$$

d'où le résultat.

---

10. Le résultat est vrai pour $n = 2$: en effet, tout ensemble de trois entiers strictement positifs possède deux éléments de même parité ; leur somme est alors divisible par 2.

Supposons donc la propriété vérifiée pour $n = 2^{k-1}$, $k \geqslant 2$, et soit S un ensemble de $2 \times 2^k - 1$ entiers strictement positifs. Soit alors un sous-ensemble quelconque de S ayant $2 \times 2^{k-1} - 1$ éléments. Par hypothèse de récurrence, ce sous-ensemble contient 2^{k-1} entiers dont la somme Σ_1 est divisible par 2^{k-1} : $\Sigma_1 = 2^{k-1}x$ ($x \in \mathbb{N}$). L'ensemble obtenu en enlevant à S les 2^{k-1} entiers précédemment sélectionnés possède $2 \times 2^k - 1 - 2^{k-1} = 3 \times 2^{k-1} - 1$ éléments. On peut donc trouver parmi ces éléments 2^{k-1} entiers dont la somme Σ_2 est divisible par 2^{k-1} : $\Sigma_2 = 2^{k-1}y$ ($y \in \mathbb{N}$). En ignorant de nouveau ces 2^{k-1} entiers, on se retrouve avec un ensemble ayant $2 \times 2^{k-1} - 1$ éléments et il est donc possible d'en sélectionner 2^{k-1} dont la somme Σ_3 est divisible par 2^{k-1} : $\Sigma_3 = 2^{k-1}z$ ($z \in \mathbb{N}$).

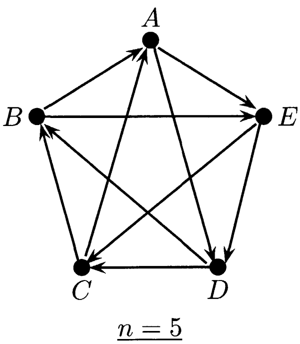
Parmi les entiers x, y et z, deux au moins sont de même parité ; disons x et y. On a alors :

$$\Sigma_1 + \Sigma_2 = 2^{k-1}(x+y) = 2^k t \quad (t \in \mathbb{N}),$$

ce qui montre que la propriété est vraie pour 2^k.

---

11. Le résultat est vrai pour $n = 5$ et $n = 6$.



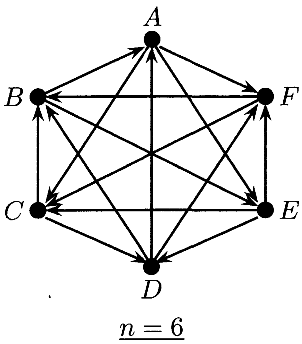


FIG. 1.7.

Supposons qu'un système de n points $A_1, A_2, \ldots, A_n$ vérifie la propriété et ajoutons à ce système deux points A_{n+1} et A_{n+2}. Relions A_{n+1} à tous les points

A_i, $i = 1, 2, \ldots, n$, puis relions les points A_i, $i = 1, 2, \ldots, n$, au point A_{n+2}. Relions enfin le point A_{n+2} au point A_{n+1}.

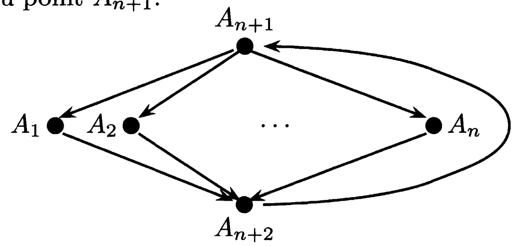


FIG. 1.8.

Il est alors immédiat que la propriété est vérifiée par le nouveau système. Il s'ensuit qu'elle est vérifiée pour tout entier $n \geqslant 5$.

---

12. On considère des vecteurs $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ ($n \geqslant 1$) tels que $||\vec{v}_r|| \leqslant 1$ pour $1 \leqslant r \leqslant n$, et on démontre le résultat demandé par récurrence sur l'entier n :

- Le résultat est évident pour $n = 1$ ou 2.

- On suppose alors qu'il est vrai pour $n - 1$, où $n \geqslant 3$, et on considère un ensemble de n vecteurs $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ tels que $||\vec{v}_r|| \leqslant 1$ pour $1 \leqslant r \leqslant n$. Parmi les vecteurs $\vec{v}_1, \vec{v}_2, \vec{v}_3$, il existe toujours une paire $\{\vec{v}_i, \vec{v}_j\}$ telle que l'un au moins des vecteurs $\vec{v}_i \pm \vec{v}_j$ ait une norme $\leqslant 1$: en effet, les six vecteurs $\pm\vec{v}_1, \pm\vec{v}_2, \pm\vec{v}_3$, construits à partir de l'origine, divisent le plan en 6 domaines anguleux dont un au moins a une ouverture $\leqslant 60°$. Sans perte de généralité, on peut supposer que $||\vec{v}_1 + \eta\vec{v}_2|| \leqslant 1$ où $\eta = \pm 1$. On considère alors le vecteur $\vec{\omega} = \vec{v}_1 + \eta\vec{v}_2$ et on applique l'hypothèse de récurrence à l'ensemble de vecteurs

$$\{\vec{\omega}, \vec{v}_3, \vec{v}_4, \ldots, \vec{v}_n\};$$

il existe donc $n - 1$ réels $\lambda, \varepsilon_3, \varepsilon_4, \ldots, \varepsilon_n$, égaux à ± 1, tels que :

$$\left|\left|\lambda\vec{\omega} + \sum_{r=3}^{n} \varepsilon_r \vec{v}_r\right|\right| \leqslant \sqrt{2}.$$

Mais $\lambda\vec{\omega} = \lambda\vec{v}_1 + \lambda\eta\vec{v}_2$, d'où le résultat.

---

13. On considère d'abord le cas $n = 2$. Si 4 points sont reliés à l'aide de 5 segments, alors il y a un seul segment qui manque aux $\binom{4}{2} = 6$ segments déterminés par ces points. Si $[AB]$ est ce segment, alors tout triplet formé de 3 parmi les 4 points et ne contenant pas les deux points A et B à la fois forme un triangle.

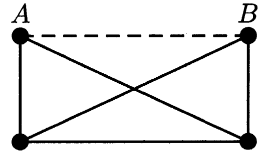


FIG. 1.9.

Supposons donc que pour tout ensemble de $2(n-1)$ points reliés à l'aide de $(n-1)^2+1$ segments, il y ait toujours un triangle formé, et prenons $2n$ points quelconques dans l'espace euclidien. Relions ensuite ces points à l'aide de n^2+1 segments et soit $[AB]$ l'un de ces segments. S'il existe un triangle de la forme ABC dans la configuration obtenue, alors il n'y a plus rien à prouver. Dans le cas contraire, les points A et B sont les extrémités d'au plus $2n-2$ segments. Il s'ensuit que, après suppression des points A et B et des segments dont A ou B est extrémité, la configuration obtenue consiste en $2(n-1)$ points reliés à l'aide d'au moins $(n^2+1)-(2n-1)=(n-1)^2+1$. Par l'hypothèse de récurrence, cette configuration contient au moins un triangle, d'où le résultat.

---

14. Le cas $n=1$ est trivial. Supposons le résultat valable pour tout polygone convexe ayant $2n-1$ côtés, $n \geqslant 1$, et dont les sommets sont coloriés conformément aux exigences de l'énoncé. On considère alors un polygone $A_1A_2\ldots A_{2n+1}$ dont les sommets sont coloriés de telle sorte que deux sommets consécutifs n'aient pas la même couleur. Une diagonale de ce polygone sera dite « bonne » si elle est de la forme A_iA_{i+2}, où A_i et A_{i+2} sont de couleurs différentes. On se propose de démontrer qu'il existe deux « bonnes » diagonales qui ne se recoupent pas entre elles.

On considère les diagonales A_1A_3, A_3A_5 ,..., $A_{2n-1}A_{2n+1}$. Comme A_1 et A_{2n+1} sont de couleurs différentes, il existe forcément une de ces diagonales, d_1 par exemple, qui est « bonne », et on peut supposer que toutes les autres ne le sont pas (dans le cas contraire, le problème serait résolu). Si $A_{2k-1}A_{2k+1}$ est cette diagonale, alors les points A_1, $A_3, \ldots, A_{2k-1}$, d'une part, et $A_{2k+1}, \ldots, A_{2n+1}$ d'autre part sont de même couleur. Il s'ensuit que A_{2k} et A_1 d'une part, et A_{2k} et A_{2n+1} d'autre part sont de couleurs différentes.

On considère alors les diagonales A_1A_{2n}, $A_{2n}A_{2n-2}, \ldots, A_4A_2$. Comme A_1 et A_2 sont de couleurs différentes, il existe forcément une de ces diagonales, d_2 par exemple, qui est « bonne », et on peut encore supposer que toutes les autres ne le sont pas. Il s'ensuit que A_{2k} et A_2 sont de même couleur, ce qui implique que A_2A_{2n+1} est « bonne ».

Si $d_1=A_1A_3$ et $d_2=A_1A_{2n}$, il n'y a plus rien à prouver. Supposons donc $d_1 \neq A_1A_3$ ou $d_2 \neq A_1A_{2n}$. En considérant la « bonne » diagonale A_2A_{2n+1}, on trouve dans chacun des deux derniers cas une paire de « bonnes » diagonales, A_iA_{i+2} et A_jA_{j+2} $(i<j)$, qui ne se recoupent pas entre elles. Il suffit alors d'appliquer l'hypothèse de récurrence au polygone $A_1A_2\ldots A_iA_{i+2}\ldots A_jA_{j+2}\ldots A_{2n+1}$.

---

15. Si $(x,y,z,t) \in \left(\mathbb{Z}^*\right)^4$ est tel que : $x^2+y^2=3(z^2+t^2)$, alors 3 divise x^2+y^2. Comme tout carré est congru à 0 ou 1 modulo 3, il s'ensuit que $x^2 \equiv y^2 \equiv 0 \pmod 3$, i.e., $x \equiv y \equiv 0 \pmod 3$. Si on pose $x=3u$, $y=3v$, où $(u,v) \in \left(\mathbb{Z}^*\right)^2$, alors on obtient

$$3(u^2+v^2)=z^2+t^2.$$

Ainsi, $(z,t,u,v) \in \left(\mathbb{Z}^*\right)^4$ est une solution telle que $z^2+t^2+u^2+v^2 < x^2+y^2+z^2+t^2$. En réitérant ce procédé, on aboutit à une suite strictement décroissante d'entiers positifs, d'où la contradiction.

---

16. Soit x_i l'entier relatif associé au sommet A_i du pentagone, $i = 1, 2, 3, 4, 5$. On définit alors la fonction f par :

$$f(x_1, x_2, x_3, x_4, x_5) = \sum_{i=1}^{5} (x_{i+1} - x_{i-1})^2,$$

où $x_5 = x_0$ et $x_6 = x_1$.

Étudions l'influence du processus décrit dans l'énoncé sur les valeurs prises par f. Quitte à réindexer les sommets, on peut supposer $x_3 < 0$. Le processus consiste alors à remplacer le vecteur $X_1 = (x_1, x_2, x_3, x_4, x_5)$ par le vecteur $X_2 = (x_1, x_2 + x_3, -x_3, x_4 + x_3, x_5)$. Il s'ensuit que :

$$\begin{aligned} f(X_2) - f(X_1) &= (x_2 + x_3 - x_5)^2 + (x_1 + x_3)^2 + (x_4 - x_2)^2 \\ &\quad + (x_3 + x_5)^2 + (x_1 - x_3 - x_4)^2 - (x_2 - x_5)^2 \\ &\quad - (x_3 - x_1)^2 - (x_4 - x_2)^2 - (x_5 - x_3)^2 - (x_1 - x_4)^2 \\ &= 2x_3(x_1 + x_2 + x_3 + x_4 + x_5) < 0. \end{aligned}$$

Les valeurs successives prises par f constituent donc une suite d'entiers positifs strictement décroissante. Il en résulte que cette suite est finie.

Note. On peut se demander s'il existe un moyen qui permette de prédire le nombre d'opérations nécessaires avant la fin du processus connaissant les valeurs initiales affectées aux sommets du pentagone. La réponse est affirmative : considérons l'ensemble S de toutes les sommes $s(i, j) = x_i + x_{i+1} + \cdots + x_{i+j}$, où $1 \leqslant i \leqslant 5$, $j \geqslant 0$ et où les indices sont considérés modulo 5. Le remplacement du vecteur $X_1 = (x_1, x_2, x_3, x_4, x_5)$ par le vecteur $X_2 = (x_1, x_2 + x_3, -x_3, x_3 + x_4, x_5)$ ne fait que remplacer l'élément x_3 de S par l'élément $-x_3$. Le processus prend nécessairement fin lorsque tous les éléments de S deviennent positifs, ce qui implique que le nombre d'opérations nécessaires avant la fin du processus est égal au nombre d'éléments strictement négatifs de S (en considérant que S peut contenir des éléments égaux). Ce nombre est fini car $x_1 + x_2 + x_3 + x_4 + x_5 > 0$, et on voit que les nombres affectés aux sommets du pentagone peuvent être choisis dans $\mathbb{R}$, et pas seulement dans $\mathbb{Z}$.

---

17. Signalons que cet énoncé a été proposé aux olympiades russes en 1992 et que, idéalement, il n'aurait pas dû figurer aux olympiades internationales.

On suppose chaque pièce repérée par un point $(x, y) \in \mathbb{Z}^2$, où $1 \leqslant x, y \leqslant n$, et on désigne par $s(k, j)$ le nombre de points tels que $x + y = k$ après j mouvements. On pose alors pour $i = 0, 1, 2$,

$$S_i(j) = \sum_{k \equiv i \pmod 3} s(k, j).$$

Si $n = 3p$ ($p \in \mathbb{N}^*$), alors $S_0(0) = S_1(0) = S_2(0) = 3p^2$. Ainsi, les $S_i(0)$, $i = 0, 1, 2$, sont de même parité. Par ailleurs, chaque mouvement modifie la valeur de $s(k,j)$ pour trois valeurs consécutives de k de ± 1 et modifie donc la parité de tous les S_i. On ne peut donc se retrouver avec une seule pièce sur l'échiquier puisqu'alors, un des $S_i(n^2 - 1)$ sera égal à 1 et les autres à 0, ce qui contredit le fait que tous les S_i doivent avoir la même parité.

On suppose maintenant $n \equiv 1$ ou $2 \pmod 3$. Si $n = 2$, les mouvements $(1,1) \to (3,1)$, $(1,2) \to (3,2)$ et $(3,2) \to (3,0)$ permettent d'effectuer la tâche requise. Si $n \geqslant 3$, on applique la procédure suivante :

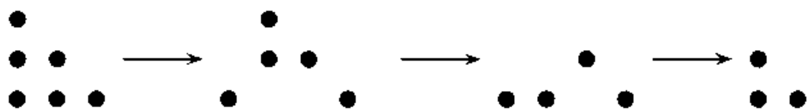


Fig. 1.10.

dont l'application répétée permet de passer d'un carré $n \times n$ à un carré $(n-3) \times (n-3)$:

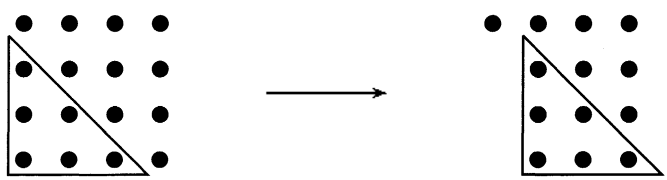


Fig. 1.11.

Ce processus permet donc d'arriver à un carré 2×2 ou à une seule pièce restant sur l'échiquier, ce qui montre que la tâche requise peut être effectuée si et seulement si $n \equiv 1$ ou $2 \pmod 3$.

---

18. On désigne par O le centre du disque et par $A_1, A_2, \ldots, A_7$ les points en question. Si aucun de ces sept points n'est le centre du disque, alors le plus petit parmi les angles $\widehat{A_iOA_j}$ est strictement inférieur à 60°. Soient alors A et B les points correspondant à cet angle. Comme

$$AB^2 = OA^2 + OB^2 - 2OA \cdot OB \cdot \cos \widehat{AOB},$$

il s'ensuit que $AB < 1$, d'où la contradiction.

---

19. Parmi les cinq triangles formés par trois sommets consécutifs du pentagone, on choisit le triangle de surface minimale. Sans perte de généralité, on peut supposer que c'est le triangle ABC. Montrons que la flèche sur le côté $[BC]$ est dirigée vers le sommet B.

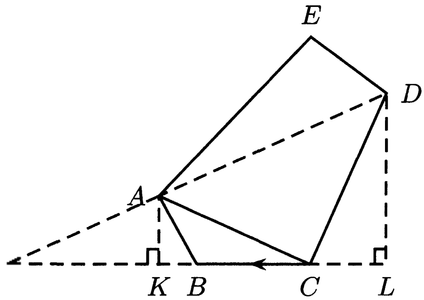


FIG. 1.12.

Soient K et L les projections orthogonales de A et D sur (BC) respectivement. On a $\mathcal{A}(ABC) < \mathcal{A}(BCD)$, et par conséquent $AK < DL$, ce qui signifie que le point d'intersection de (AD) et (BC) se trouve du côté de B. On démontre de la même façon que la flèche sur $[AB]$ est aussi dirigée vers le point B.

---

20. On considère une droite Δ dans le plan des points en question. Si nous déplaçons cette droite, sans en modifier la direction, en commençant loin de tous les points, tous les points sont d'abord d'un côté de cette droite ; puis la droite atteindra le premier point de S que l'on désigne par A. Si nous faisons ensuite tourner cette droite autour du point A, alors elle passera par un second point de S que l'on désigne par B (en termes plus savants, la droite (AB) est une frontière de l'enveloppe convexe de S). Ainsi, tous les points de S, autres que A et B, se trouvent du même côté de la droite (AB).

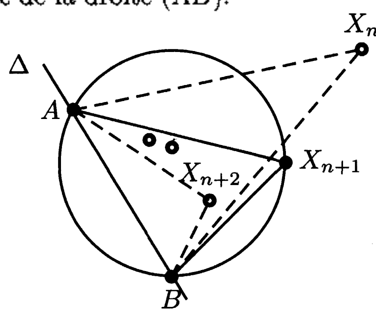


FIG. 1.13.

Si on ordonne ces points suivant les valeurs de l'angle $\widehat{AXB}$, on peut les noter $X_1, X_2, \ldots, X_{2n+1}$, de telle sorte que $\widehat{AX_1B} \leqslant \widehat{AX_2B} \leqslant \cdots \leqslant \widehat{AX_{2n+1}B}$. Il est alors immédiat que le cercle passant par les points A, B et X_{n+1} fournit une solution. En effet, les angles $\widehat{AX_iB}$, $i = 1, 2, \ldots, 2n+1$, sont deux à deux distincts puisque l'égalité $\widehat{AX_iB} = \widehat{AX_jB}$ implique que les quatre points A, B, X_i et X_j sont cocycliques, ce qui est exclu.

---

21. Parmi les éléments de $E(X)$, choisissons un sous-ensemble P de X tel que $f(P)$ soit maximal. S'il y en a plusieurs, on choisit l'un quelconque de ceux d'entre eux ayant le plus petit nombre d'éléments. Posons enfin $Q = X \setminus P$.

On a ainsi $f(P) \geqslant f(D) > 1990$, et si $S \neq P$ est non vide inclus dans $E(P)$, alors

$$f(S) = 1990 + \underbrace{(f(P) - f(P \setminus S))}_{>0} > 1990.$$

Si, d'un autre côté, T est un sous-ensemble de Q appartenant à $E(Q)$, alors

$$f(T) = 1990 + (f(P \cup T) - f(P)) \leqslant 1990.$$

---

22. On commence d'abord par étudier l'influence du processus décrit dans l'énoncé sur la distance séparant l'origine O du point $P(x, y)$. On remarque alors que si P n'est situé sur aucune des droites $\Delta_1 : x = 0$, $\Delta_2 : y = 0$, $\Delta_3 : x = y$ ou $\Delta_4 : x = -y$, alors la distance OP diminue dans une seule des quatre possibilités autorisées par le processus, et augmente dans le reste des cas.

Si l'on part du point $P_0(1, \sqrt{2})$, alors le processus décrit dans l'énoncé ne nous mènera jamais sur l'une des droites Δ_i, $i = 1, 2, 3, 4$: en effet, comme $\sqrt{2}$ est irrationnel, les points décrits par applications successives de l'opération décrite dans l'énoncé sont toujours tels que le rapport des coordonnées soit irrationnel. Supposons alors qu'il existe une suite $(P_0, P_1, \ldots, P_n)$ telle que $P_n = P_0$, et considérons le point le plus éloigné de l'origine. Si P_i est ce point, alors nécessairement $0 < i < n$, et on a de plus $OP_{i+1} < OP_i$. La seule façon pour que cette dernière inégalité se réalise lors du passage du point P_i au point P_{i+1} est de revenir au point P_{i-1}. Cependant, ceci est impossible car il est interdit de retracer un segment que l'on a déjà parcouru.

---

23. La parité du nombre de signes « $-$ » dans les cases ci-dessous coloriées reste la même au cours du processus.

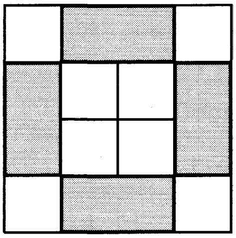


Fig. 1.14.

La conclusion en découle immédiatement.

---

24. Considérons les tétraèdres $ABCD$ et $A_1B_1C_1D_1$. La somme des nombres dans les sommets de $ABCD$ après n applications de la procédure décrite dans l'énoncé sera notée S_n, et celle des nombres dans les sommets de $A_1B_1C_1D_1$ sera notée S_n'.

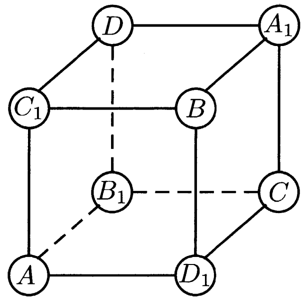


FIG. 1.15.

Il est alors clair que la différence $S_n - S_n^{'}$ se conserve au cours du processus. Par conséquent, $S_n - S_n^{'} = S_0 - S_0^{'} = -2$, $\forall n \in \mathbb{N}$, d'où le résultat.

---

25. On commence par étudier ce qui se passe dans un tableau 4×4 quand on part de la situation suivante :

-1	1	1	1
1	1	1	1
1	1	1	1
1	1	1	1

FIG. 1.16.

On s'aperçoit qu'on aboutit très vite à deux configurations qui se reproduisent en alternance indéfiniment. En superposant les deux configurations on obtient une configuration invariante par le processus décrit dans l'énoncé :

1	-1	-1	-1
-1	1	-1	1
-1	-1	1	1
-1	1	1	1

FIG. 1.17.

À partir de cette configuration, on construit une configuration qui correspond au tableau 9×9, et qui reste invariante au cours du processus :

1	−1	−1	−1	1	−1	−1	−1	1
−1	1	−1	1	1	1	−1	1	−1
−1	−1	1	1	1	1	1	−1	−1
1	1	1	1	1	1	1	1	−1
1	1	1	1	1	1	1	1	1
−1	1	1	1	1	1	1	1	−1
−1	−1	1	1	1	1	1	−1	−1
−1	1	−1	1	1	1	−1	1	−1
1	−1	−1	−1	1	−1	−1	−1	1

FIG. 1.18.

On en déduit qu'il n'est pas toujours possible d'obtenir un tableau constitué uniquement d'éléments égaux à 1.

---

26. On peut supposer, sans nuire à la généralité, que les triangles de départ sont d'hypoténuse 1 et de côtés p et q ($p, q < 1$). Le processus décrit dans l'énoncé fait apparaître des triangles homothétiques aux triangles de départ avec des rapports $p^m q^n$, $(m, n) \in \mathbb{N}^2$.

À chaque étape, on remplace un triangle de type (m, n) par deux triangles de types $(m+1, n)$ et $(m, n+1)$. Si on affecte à un triangle de type (m, n) le poids $1/2^{m+n}$, la somme de tous les poids reste alors invariante au cours du processus.

Si au bout d'un nombre fini d'étapes on aboutit à des triangles non isométriques, alors chaque classe (m, n) contiendra au plus un triangle. Le poids total est alors strictement inférieur à (il faut un nombre infini d'opérations pour avoir l'égalité)

$$\sum_{m,\, n=0}^{+\infty} \frac{1}{2^{m+n}} = 4.$$

Comme par ailleurs le poids total dans la configuration initiale valait 4, on a une contradiction.

2

ARITHMÉTIQUE

L'arithmétique a toujours eu une place de choix dans les olympiades internationales. Avec des énoncés simples et familiers, elle est sans doute la discipline la mieux adaptée à un enseignement élémentaire des mathématiques.

Avec la matière discutée dans ce chapitre, le lecteur pourra aborder, avec confiance, la plupart des compétitions mathématiques. Cependant, on ne saurait assez recommander au lecteur de ne pas lire trop rapidement la solution d'un exercice : ce n'est qu'ainsi qu'il parviendra à apprécier pleinement les techniques de l'arithmétique.

2.1. La division euclidienne

2.1.1. Définition. *On considère deux entiers a et b. On dit que a divise b, et on note $a \mid b$ s'il existe un entier $q \in \mathbb{Z}$ tel que $b = aq$.*

♦ **Remarques.**

1. Tout entier $a \in \mathbb{Z}$ divise 0 et est divisible par 1 et a.

2. Si $a \mid b$ et $b \mid c$ alors $a \mid c$.

3. Soit m un entier non nul. $a \mid b$ si et seulement si $ma \mid mb$.

4. Si $a \mid b$ et $a \mid c$, alors $a \mid bx + cy$ pour tous entiers x, y. En particulier, $a \mid b - c$ et $a \mid b + c$.

2.1.2. Théorème. *(Division euclidienne) Soit b un entier strictement positif. Tout entier a s'écrit, de manière unique, sous la forme $a = bq + r$, où $q \in \mathbb{Z}$ et $0 \leqslant r < b$. q et r sont respectivement appelés quotient et reste de la division euclidienne de a par b.*

♦ **Preuve.** On considère la progression arithmétique $\ldots$, $a - 2b$, $a - b$, a, $a + b$, $\ldots$ Cette progression contient 0 parmi ses termes si et seulement si $a = qb$ pour un certain $q \in \mathbb{Z}$. Supposons donc que a ne divise pas b. Soit $r = a - qb$ le plus petit terme strictement positif dans la progression précédemment considérée. On a alors

$0 \leqslant r < b$: en effet, si $r \geqslant b$, $r - b = a - (q+1)b$ serait un terme strictement positif de la progression qui est $< r$, ce qui est impossible.

L'unicité du couple (q, r) est facile à démontrer. Si (q_1, r_1) et (q_2, r_2) sont deux tels couples et si l'on suppose, ce qui ne nuit pas à la généralité, que $r_1 \geqslant r_2$, alors $0 \leqslant r_1 - r_2 = (q_1 - q_2)b < b$, ce qui impose $q_1 = q_2$, puis $r_1 = r_2$.

□

♦ **Exemples.**

1. Soit n un entier quelconque. Le reste de la division euclidienne de n^2 par 4 est 0 ou 1.

En effet, si n est pair, $n = 2k$, alors $n^2 = 4k^2 = 4 \cdot k^2 + 0$, et si n est impair, $n = 2k + 1$, $n^2 = 4k^2 + 4k + 1 = 4 \cdot (k^2 + k) + 1$.

2. Soit n un entier naturel > 1. Montrer que tout entier naturel N peut être représenté, de manière unique sous la forme

$$N = a_0 + a_1 n + a_2 n^2 + \cdots + a_k n^k.$$

où les coefficients a_i sont tels que $0 \leqslant a_i < n$ $(i = 0, 1, \ldots, k)$. Une telle écriture est *la représentation en base n du nombre N*.

Le résultat est évident si $N < n$, cas exclu par la suite. On divise N par n, $N = q_1 n + r_0$ et on pose $a_0 = r_0$. Si $q_1 < n$, on a obtenu la représentation désirée. Sinon, on divise q_1 par n, $q_1 = q_2 n + r_1$ et on pose $a_1 = r_1$, et ainsi de suite. On construit ainsi une suite finie $q_1 > q_2 > \cdots > q_k$ d'entiers naturels telle que $q_{k-1} \geqslant n > q_k \geqslant 1$, et on obtient la forme désirée en posant $a_k = q_k$.

Cette représentation est unique : en effet, si N admet deux représentations différentes : $N = a_0 + a_1 n + \cdots + a_k n^k$ et $N = b_0 + b_1 n + \cdots + b_m n^m$, soit i le plus petit indice tel que $a_i \neq b_i$. On a alors $n \mid a_i - b_i$, ce qui est impossible puisque $0 < |a_i - b_i| < n$, d'où la contradiction.

2.1.3. Définition. *Un entier naturel $p > 1$ est dit premier s'il possède exactement deux diviseurs naturels, à savoir 1 et p.*

♦ **Remarques.**

1. Les nombres 2, 3 et 5 sont par exemple premiers. 1 et 12 ne le sont pas.

2. Tout entier $n > 1$ peut être exprimé comme le produit de nombres premiers. Ceci justifie l'importance de cette classe particulière de nombres qui permet en quelque sorte de construire tous les entiers naturels.

2.2. Plus grand commun diviseur, plus petit commun multiple

2.2.1. Définition. *Un entier divisant à la fois l'entier a et l'entier b, non tous les deux nuls, est appelé diviseur commun de a et b. Le plus grand nombre strictement positif parmi ces diviseurs communs est appelé plus grand commun diviseur de a et b, et on le note (a, b).*

2.2.2. Théorème. *(Identité de Bézout[1]) Soient a et b deux entiers, non tous les deux nuls. L'ensemble $\{ax + by \mid x, y \in \mathbb{Z}\}$ est l'ensemble de tous les multiples de (a, b), i.e.,*

$$a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}. \tag{2.1}$$

En particulier, tout diviseur commun de a et b est un diviseur de (a, b).

♦ **Preuve.** L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ contient des nombres strictement positifs ; soit d le plus petit de ces nombres. Tout élément de $a\mathbb{Z} + b\mathbb{Z}$ est alors un multiple de d : en effet, si $n = ax + by$, effectuons sa division euclidienne par d, $n = qd + r$ avec $0 \leqslant r < d$. Le nombre $r = n - qd$ est un élément de $a\mathbb{Z} + b\mathbb{Z}$, ce qui impose $r = 0$.

Or, comme $d = ax_0 + by_0$, il s'ensuit que tout diviseur de a et de b divise aussi d. Comme par ailleurs d est un diviseur commun de a et de b (a, $b \in a\mathbb{Z} + b\mathbb{Z}$), on voit bien que $d = (a, b)$.

□

♦ **Remarques.**

1. On a $(a, b) = 1$ si et seulement s'il existe u, $v \in \mathbb{Z}$ tels que $au + bv = 1$.

2. L'identité de Bézout se généralise facilement au cas de n entiers $a_1, a_2, \dots, a_n$, non tous nuls :

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = (a_1, a_2, \dots, a_n)\mathbb{Z},$$

où $(a_1, a_2, \dots, a_n)$ désigne le plus grand commun diviseur des entiers a_1, a_2, $\dots$, a_n.

On est maintenant en mesure d'énoncer quelques propriétés concernant le plus grand commun diviseur :

2.2.3. Propriétés. *On a les deux propriétés suivantes :*
(P1) *pour tout entier c, $(a, b) = (a, b + ac) = (a + bc, b)$;*
(P2) *si $d \mid a$ et $d \mid b$, alors*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{|d|}.$$

♦ **Preuve.** Si $c \in \mathbb{Z}$, l'ensemble des diviseurs communs de a et b est le même que l'ensemble des diviseurs communs de a et $b + ac$, d'où $(a, b) = (a, b + ac)$.

Passons à la deuxième propriété. Comme $\frac{a}{d}\mathbb{Z} + \frac{b}{d}\mathbb{Z} = \frac{1}{|d|}(a\mathbb{Z} + b\mathbb{Z})$, il s'ensuit que $\left(\frac{a}{d}, \frac{b}{d}\right)$, qui est le plus petit élément strictement positif de $\frac{a}{d}\mathbb{Z} + \frac{b}{d}\mathbb{Z}$ est égal à $\frac{(a, b)}{|d|}$.

□

1. Étienne Bézout (1730-1783), mathématicien français.

♦ **Exemples.**

1. prouver que la fraction $\dfrac{21n+4}{14n+3}$ est irréductible pour tout entier naturel n.

(Olympiades internationales-1959/1)

En appliquant la propriété (P1), on obtient :

$$(21n+4, 14n+3) = (7n+1, 14n+3) = (7n+1, 1) = 1.$$

2. Soient a et m des nombres naturels tels que $a > 1$. Démontrer que

$$\Big(\Big(\frac{a^m - 1}{a-1}\Big), a-1\Big) = (a-1, m).$$

On écrit :

$$\frac{a^m - 1}{a-1} = \big(a^{m-1} - 1\big) + \big(a^{m-2} - 1\big) + \cdots + \big(a - 1\big) + m.$$

Tout diviseur commun de $a-1$ et de $\dfrac{a^m - 1}{a-1}$ est donc aussi un diviseur commun de $a-1$ et de m, et réciproquement. Le résultat en découle immédiatement.

2.2.4. Définition. *Deux entiers non nuls a et b sont dits premiers entre eux si $(a, b) = 1$. De même, des entiers non nuls a_1, $a_2, \ldots$, a_n sont dits premiers entre eux dans leur ensemble si $(a_1, a_2, \ldots, a_n) = 1$; ils sont dits premiers entre eux deux à deux si $(a_i, a_j) = 1$ pour toute paire d'indices $\{i, j\} \in \{1, 2, \ldots, n\}^2$ telle que $i \neq j$.*

2.2.5. Théorème. *(Théorème de Gauss[2]) Si $a \mid bc$ et $(a, b) = 1$, alors $a \mid c$.*

♦ **Preuve.** Puisque $(a, b) = 1$, il existe des entiers u et v tels que $au + bv = 1$ (identité de Bézout). Il s'ensuit que $c = a(uc) + (bc)v$ est divisible par a.

□

♦ **Exemples.**

1. Soit p un nombre premier. Montrer que p divise $\dbinom{p}{k}$ pour tout k, $1 \leqslant k \leqslant p-1$, où[3] : $\dbinom{p}{k} = \dfrac{p!}{k!(p-k)!}$.

On écrit

$$p! = \binom{p}{k} k!(p-k)!$$

si bien que p divise $\dbinom{p}{k} k!(p-k)!$. Or, pour tout k, $1 \leqslant k \leqslant p-1$,

$$\big(p, k!(p-k)!\big) = 1.$$

2. Carl Friedrich Gauss (1777-1855), mathématicien allemand.

3. Se reporter au chapitre consacré à la combinatoire pour comprendre pourquoi ce nombre est entier.

D'après le théorème de Gauss, il s'ensuit que p divise $\binom{p}{k}$.

On présente maintenant un algorithme permettant de calculer le plus grand commun diviseur de deux nombres a, $b \in \mathbb{N}^*$:

2.2.6. Théorème. *(Algorithme d'Euclide[4]) Soit $a \geqslant b > 0$ des entiers. La procédure suivante permet d'obtenir, au bout d'un nombre fini d'opérations, le plus grand commun diviseur des nombres a et b :*

1. *on effectue la division euclidienne de a par b, $a = bq + r$, avec $0 \leqslant r < b$;*
2. *si $r = 0$, alors $(a, b) = b$. Sinon, on remplace a par b et b par r, et on recommence 1.*

♦ **Preuve.** L'algorithme s'arrête au bout d'un nombre fini d'opérations : en effet, la suite des restes obtenus est une suite d'entiers positifs strictement décroissante.

D'un autre côté, si $a = bq + r$, alors $(a, b) = (b, r)$. L'algorithme permet donc bien d'obtenir (a, b).

□

♦ **Exemples.**

1. On trouve en appliquant l'algorithme d'Euclide :

$$(125, 60) = (60, 5) = 5;$$
$$(937, 215) = (215, 77) = (77, 61) = (61, 16) = (16, 13) = (13, 3) = (3, 1) = 1.$$

2. On considère deux nombres naturels non nuls a et b. Prouver que :

$$\left(2^a - 1, 2^b - 1\right) = 2^{(a,b)} - 1.$$

Supposons $a \geqslant b$; on effectue la division euclidienne de a par b, $a = bq + r$, où $0 \leqslant r < b$. On a alors :

$$2^a - 1 = \left(2^{bq}2^r - 2^r\right) + \left(2^r - 1\right) = A \cdot \left(2^b - 1\right) + \left(2^r - 1\right),$$

avec $A = 2^r\left(2^{b(q-1)} + 2^{b(q-2)} + \cdots + 1\right)$. Il s'ensuit que

$$\left(2^a - 1, 2^b - 1\right) = \left(2^b - 1, 2^r - 1\right),$$

avec $0 \leqslant 2^r - 1 < 2^b - 1$, et en suivant la procédure de l'algorithme d'Euclide, on obtient :

$$\left(2^a - 1, 2^b - 1\right) = \left(2^b - 1, 2^r - 1\right) = \cdots = \left(2^{(a,b)} - 1, 0\right) = 2^{(a,b)} - 1.$$

2.2.7. Définition. *Un entier divisible à la fois par l'entier non nul a et l'entier non nul b est appelé multiple commun de a et b. Le plus petit nombre strictement positif parmi ces multiples communs est appelé plus petit commun multiple de a et b, et on le note $[a, b]$.*

4. Euclide d'Alexandrie (325 av. J.-C.-265 av. J.-C.), mathématicien grec.

2.2.8. Théorème. *Tout multiple commun de a et b est un multiple de $[a,b]$, autrement dit,*

$$a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}. \tag{2.2}$$

♦ **Preuve.** Il est clair que $[a,b]\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$. Par ailleurs, considérons un multiple commun n de a et b. Effectuons la division euclidienne de n par $[a,b]$, $n = q[a,b]+r$, où $0 \leqslant r < [a,b]$; r est alors un multiple commun de a et b, ce qui impose $r = 0$, d'où le résultat.

□

On établit maintenant une relation directe entre le plus grand commun diviseur et le plus petit commun multiple que l'on érige en :

2.2.9. Théorème. *Soient a et b deux éléments de $\mathbb{N}^*$. On a alors :*

$$(a,b)[a,b] = ab. \tag{2.3}$$

♦ **Preuve.** Comme ab est un multiple commun de a et b, il s'ensuit que $d = \dfrac{ab}{[a,b]}$ est un entier. De plus, puisque $a = \dfrac{[a,b]}{b} \cdot d$ et $b = \dfrac{[a,b]}{a} \cdot d$, il s'ensuit que $d \mid a$ et $d \mid b$, d'où $d \mid (a,b)$, i.e., $(a,b) = kd$, $k \in \mathbb{N}^*$.

Or, $\dfrac{[a,b]}{k} = \dfrac{[a,b]\cdot d}{(a,b)} = \dfrac{ab}{(a,b)}$ est un entier. De plus, c'est un multiple commun de a et b. Il s'ensuit que :

$$[a,b] \leqslant \frac{[a,b]}{k},$$

ce qui implique que $k = 1$, d'où le résultat.

□

2.3. L'ensemble des nombres premiers

2.3.1. Théorème. *Tout entier naturel > 1 possède un diviseur premier.*

♦ **Preuve.** En effet, le plus petit diviseur $p > 1$ de tout entier $n > 1$ est premier, puisque sinon il posséderait un diviseur m, $1 < m < p$ qui diviserait aussi n.

□

♦ **Remarque.** Si n est un nombre naturel composé > 1, alors il possède un diviseur premier $\leqslant \sqrt{n}$ (pourquoi ?).

2.3.2. Théorème. *(Théorème d'Euclide) L'ensemble des nombres premiers est infini.*

♦ **Preuve.** L'idée de la preuve d'Euclide est de raisonner par l'absurde en supposant que l'ensemble $\mathcal{P}$ des nombres premiers est fini :

$$\mathcal{P} = \{p_1, p_2, \ldots, p_n\}.$$

Le nombre $N = p_1 p_2 \cdots p_n + 1$ est alors un nombre composé, mais il n'admet aucun diviseur premier puisque $p_i \nmid N$ pour $i = 1, 2, \ldots, n$, ce qui contredit le théorème précédent.

□

♦ **Exemples.**

1. Prouver que la progression arithmétique $4k - 1$, $k \in \mathbb{N}^*$, contient une infinité de nombres premiers.

On utilise l'idée de la preuve du théorème d'Euclide. Si on suppose que l'ensemble des nombres premiers de la forme $4k - 1$ est fini, et que l'on note ces nombres p_1, $p_2, \ldots, p_n$, le nombre

$$N = 4p_1 p_2 \cdots p_n - 1$$

doit être composé. tout diviseur premier de N est de la forme $4k + 1$ ou $4k - 1$. Comme ils ne sont pas tous de la forme $4k + 1$ (pourquoi ?), il s'ensuit que N est divisible par l'un des p_i, ce qui est absurde.

2. Soit n un nombre naturel. Construire une suite de n nombres composés consécutifs.

Les nombres $(n+1)! + 2$, $(n+1)! + 3, \ldots, (n+1)! + (n+1)$ sont tous composés (pourquoi ?).

3. Montrer que dans la suite $2^n - 1$, $n \in \mathbb{N}^*$, il existe un segment de longueur arbitraire dont les termes sont tous composés.

Soit m un entier arbitraire, $m > 1$. On sait (exemple précédent) que les nombres $n_k = m! + k$, où $k \in \{2, 3, \ldots, m\}$, sont tous composés. De manière plus précise, $\forall k \in \{2, 3, \ldots, m\}$, $k \mid n_k$, donc

$$2^k - 1 \mid 2^{n_k} - 1,$$

ce qui montre que les entiers $2^{n_k} - 1$, $k \in \{2, 3, \ldots, m\}$, sont composés. On a ainsi obtenu un segment de la suite $2^n - 1$, $n \in \mathbb{N}^*$, de longueur $m - 1$ et ne contenant que des nombres composés.

2.4. Le théorème fondamental de l'arithmétique

2.4.1. Théorème. *(Théorème fondamental de l'arithmétique) Tout entier naturel $n > 1$ se met, de manière unique à l'ordre des facteurs près, sous la forme*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \tag{2.4}$$

où les p_i sont des nombres premiers distincts, et les α_i sont des entiers $\geqslant 1$.

♦ **Preuve.** L'existence d'une telle décomposition se démontre par récurrence sur n en utilisant le théorème 2.3.1.

L'unicité résulte du lemme suivant, conséquence du théorème de Gauss :

Lemme. *Si p est un nombre premier divisant le produit $a_1a_2\cdots a_n$ de n entiers $a_1, a_2, \ldots, a_n$, alors p divise au moins un de ces entiers.*

□

♦ **Exercice.** Soit $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ et $m = p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$ les décompositions en produit de nombres premiers de n et de m (ici, on autorise à certains exposants d'être nuls).

a) Prouver que $n \mid m$ si et seulement si $\alpha_i \leqslant \beta_i$ pour $i = 1, 2, \ldots, k$.

b) On pose $\gamma_i = \min(\alpha_i, \beta_i)$, $\delta_i = \max(\alpha_i, \beta_i)$, $i = 1, 2, \ldots, k$. Montrer que :

$$(m, n) = p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}, \qquad [m, n] = p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}.$$

On se pose à présent le problème suivant : quel est l'exposant d'un nombre premier p dans la décomposition en produit de nombres premiers de n ! ?

Il y a $\lfloor n/p \rfloor$ multiples de p qui sont compris entre 1 et n. Chacun de ces nombres introduit un facteur p, mais, parmi ces nombres, il y a $\lfloor n/p^2 \rfloor$ multiples de p^2 qui introduisent chacun un nouveau facteur p. En continuant sur cette voie, on arrive à compter toutes les contributions amenant des facteurs p dans la décomposition en produit de nombres premiers de $n!$:

2.4.2. Théorème. *(Formule de Legendre[5]) L'exposant du nombre premier p dans la décomposition en produit de nombres premiers de $n!$ est donné par*

$$\sum_{r \geqslant 1} \left\lfloor \frac{n}{p^r} \right\rfloor. \tag{2.5}$$

♦ **Exemples.**

1. Par combien de zéros se termine le nombre 100! ?

Le nombre recherché est l'exposant de 5 dans la décomposition de 100! en produit de nombres premiers (pourquoi ?). Ce nombre se calcule à l'aide de la formule de Legendre :

$$\left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 24.$$

2. Montrer que le nombre

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

est un entier, quels que soient les nombres naturels m et n.

(Olympiades internationales-1972/3)

compte tenu de la formule de Legendre, il suffit de montrer que :

$$\left\lfloor \frac{2m}{p^k} \right\rfloor + \left\lfloor \frac{2n}{p^k} \right\rfloor \geqslant \left\lfloor \frac{m}{p^k} \right\rfloor + \left\lfloor \frac{n}{p^k} \right\rfloor + \left\lfloor \frac{m+n}{p^k} \right\rfloor$$

5. Adrien Marie Legendre (1752-1833), mathématicien français.

pour tout p premier et $k \in \mathbb{N}^*$.

Or, l'inégalité $\lfloor 2a \rfloor + \lfloor 2b \rfloor \geqslant \lfloor a \rfloor + \lfloor b \rfloor + \lfloor a+b \rfloor$ est vraie pour tous réels a et b, d'où le résultat.

On termine ce paragraphe par l'étude d'une fonction qui joue un rôle important en arithmétique, appelée indicatrice d'Euler[6].

2.4.3. Définition. *Soit n un entier naturel > 1. On appelle indicatrice d'Euler de n que l'on note $\varphi(n)$, le nombre d'entiers naturels non nuls $\leqslant n$ et premiers avec n.*

♦ **Exemples.**

1. Si p est un nombre premier, alors $\varphi(p) = p - 1$.

2. Si $n = p^r$, où p est un nombre premier, alors $\varphi(n) = p^r - p^{r-1}$: en effet, parmi $\{1, 2, \ldots, p^r\}$, p^{r-1} nombres sont des multiples de p, donc non premier avec p. On en déduit que :

$$\varphi(p^r) = p^r - p^{r-1}.$$

2.4.4. Théorème. *La fonction φ est multiplicative, i.e., pour tout couple d'entiers naturels m et n premiers entre eux, on a :*

$$\varphi(mn) = \varphi(m)\varphi(n). \tag{2.6}$$

♦ **Preuve.** Si n est un nombre naturel > 1, on note

$$\mathcal{A}(n) = \{k \leqslant n \mid (k, n) = 1\}.$$

On considère l'application f :

$$\begin{array}{rcl} \mathcal{A}(mn) & \longrightarrow & \mathcal{A}(m) \times \mathcal{A}(n) \\ x & \longmapsto & (x_1, x_2), \end{array}$$

où x_1 est le reste de la division euclidienne de x par m et x_2 est le reste de la division euclidienne de x par n.

L'application f est bien définie puisque $(m, x_1) = 1$ et $(n, x_2) = 1$. De plus, comme $(m, n) = 1$, il est facile de voir qu'elle est injective. Finalement, on montre grâce à l'identité de Bézout que f est surjective (c'est un cas particulier du théorème chinois, démontré au paragraphe 2.8 de ce chapitre). f est donc bijective et $\varphi(mn) = \varphi(m)\varphi(n)$.

□

2.4.5. Corollaire. *Soit n un entier naturel > 1 et $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ sa décom-*

6. Leonhard Euler (1707-1783), éminent mathématicien suisse.

position en produit de facteurs premiers. On a alors :

$$\begin{aligned}\varphi(n) &= \left(p_1^{\alpha_1}-p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2}-p_2^{\alpha_2-1}\right)\cdots\left(p_k^{\alpha_k}-p_k^{\alpha_k-1}\right)\\ &= n\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdots\Big(1-\frac{1}{p_k}\Big).\end{aligned} \tag{2.7}$$

2.5. La relation de congruence

On dit que a et b sont congrus modulo $n \geqslant 2$, et on note $a \equiv b \pmod n$ si n divise $a-b$. Ainsi, l'utilisation de la congruence est simplement une autre façon de parler de la divisibilité. La notation $a \equiv b \pmod n$ a été introduite par Gauss. On peut donc reformuler les propriétés de la relation de divisibilité à l'aide de cette notation, par exemple :

- si $a \equiv b \pmod n$ et $c \equiv d \pmod n$, alors $a+c \equiv b+d \pmod n$;
- si $a \equiv b \pmod n$ et $c \equiv d \pmod n$, alors $ac \equiv bd \pmod n$;
- si $ab \equiv ac \pmod n$ et $(a,n)=1$, alors $b \equiv c \pmod n$ (théorème de Gauss).

D'un autre côté, la congruence modulo n, $n \geqslant 2$, est une relation d'équivalence (elle est réflexive, symétrique et transitive). L'ensemble constitué de ses classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$; il est fini et de cardinal n : en effet, si on note $\overline{k}$ la classe d'équivalence contenant k, $0 \leqslant k \leqslant n-1$, on a $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

♦ **Exemples.**

1. Soit n un nombre naturel et $s(n)$ la somme des chiffres de n. Montrer que

$$n \equiv s(n) \pmod 9.$$

Si on écrit $n = 10^k a_k + 10^{k-1}a_{k-1} + \cdots + a_0$, comme $10^i \equiv 1^i \equiv 1 \pmod 9$, $i = 0, 1, \ldots, k$, on obtient :

$$n \equiv a_k + a_{k-1} + \cdots + a_0 = s(n) \pmod 9.$$

2. Montrer que le dernier chiffre dans la représentation décimale d'un carré parfait ne peut pas appartenir à l'ensemble $\{2, 3, 7, 8\}$.

Si $n = m^2$ est un carré parfait, et si d est le dernier chiffre dans la représentation décimale de m, alors $m \equiv d \pmod{10}$, et donc $n \equiv d^2 \pmod{10}$. Il suffit donc d'étudier l'ensemble des restes de d^2, $d = 0, 1, \ldots, 9$, modulo 10. Cet ensemble est égal à l'ensemble $\{0, 1, 4, 5, 6, 9\}$, d'où le résultat.

3. Soient a et b deux entiers tels que $7 \mid a^2+b^2$. Montrer que $7 \mid a$ et $7 \mid b$.

Soit $x \in \mathbb{Z}$ tel que $x \not\equiv 0 \pmod 7$. On a alors $x^2 \equiv 1, 2$ ou $4 \pmod 7$. Ainsi, en étudiant toutes les possibilités, on trouve :

$$\big(a \not\equiv 0 \pmod 7 \ \text{ ou } \ b \not\equiv 0 \pmod 7\big) \Longrightarrow \big(a^2+b^2 \equiv 1, 2, 3, 4, 5 \text{ ou } 6 \pmod 7\big),$$

d'où le résultat.

2.6. Les systèmes de résidus

Soit n un nombre naturel $\geqslant 1$. L'ensemble $\{0, 1, \dots, n-1\}$ est l'ensemble de tous les restes possibles modulo n, i.e., tout entier est congru modulo n à un et un seul élément de cet ensemble. Les ensembles $\{1, 2, \dots, n\}$, $\{-1, 0, \dots, n-2\}$ possèdent la même propriété, ce qui motive la définition suivante :

2.6.1. Définition. *Un ensemble de n entiers $x_1, x_2, \dots, x_n$ est dit système complet de résidus modulo n si, pour tout entier y, il existe exactement un élément x_i tel que $y \equiv x_i \pmod{n}$.*

On remarque tout de suite qu'un ensemble de n entiers est un système complet de résidus modulo n si et seulement si deux quelconques d'entre eux n'ont pas le même reste modulo n.

2.6.2. Théorème. *Si $\{x_1, x_2, \dots, x_n\}$ est un système complet de résidus modulo n, et si k est un entier premier avec n, alors $\{kx_1, kx_2, \dots, kx_n\}$ est aussi un système complet de résidus modulo n.*

♦ **Preuve.** Si $kx_i \equiv kx_j \pmod{n}$, alors $n \mid k(x_i - x_j)$, et il s'ensuit que $n \mid x_i - x_j$ (théorème de Gauss), ce qui est absurde si $i \neq j$.

□

♦ **Exemples.**

1. Soit n un entier naturel, k un entier premier avec n, $1 \leqslant k \leqslant n-1$ et M l'ensemble $\{1, 2, \dots, n-1\}$. Chaque élément de M est coloré avec l'une des couleurs blanche ou bleue. On suppose que :

a) pour tout i dans M, i et $n-i$ ont la même couleur ;

b) pour tout i dans M tel que $i \neq k$, i et $|i-k|$ ont la même couleur.

Montrer que tous les éléments de M ont la même couleur.

(Olympiades internationales-1985/2)

D'après le dernier théorème, l'ensemble $\{0, k\times 1, \dots, k\times(n-1)\}$ est un système complet de résidus modulo n. En réduisant ses éléments sauf 0 modulo n :

$$m_i \equiv ik \pmod{n}, \quad i = 1, 2, \dots, n-1,$$

on obtient une permutation $(m_1, m_2, \dots, m_{n-1})$ de M.

Or, $m_1 = k$ et pour $2 \leqslant r \leqslant n-1$,

$$m_r = \begin{cases} m_{r-1} + k & \text{si } m_{r-1} + k < n, \\ m_{r-1} + k - n & \text{si } m_{r-1} + k \geqslant n. \end{cases}$$

Dans le premier cas, m_r est de la même couleur que $|m_r - k| = m_{r-1}$. Dans le second cas, m_r est de la même couleur que $|m_r - k| = n - m_{r-1}$, qui est à son tour de même couleur que m_{r-1}.

2. (*Théorème de Wilson*[7]) Démontrer que p divise $(p-1)! + 1$ si, et seulement si,

[7] John Wilson (1741-1793), mathématicien anglais.

p est premier.

Si p est composé, alors il existe des entiers p_1, p_2 tels que $1 < p_1, p_2 < p$ et $p = p_1 p_2$. Si $p_1 \neq p_2$, alors $p_1 p_2 \mid (p-1)!$, ce qui implique que $(p-1)! \equiv 0 \pmod{p}$. Si $p_1 = p_2$, alors $2p_1 = 2\sqrt{p} \leqslant p$ ($p \geqslant 4$), et si $p > 4$, alors $p_1 \times 2p_1 \mid (p-1)!$, et de nouveau $(p-1)! \equiv 0 \pmod{p}$. Si enfin $p = 4$, alors $(p-1)! + 1 = 7$ n'est pas divisible par 4.

Réciproquement, si p est premier, montrons que

$$(p-1)! \equiv -1 \pmod{p}.$$

Le résultat est vérifié lorsque $p = 2$ ou 3. On suppose dans la suite $p \geqslant 5$. Soit k un entier compris entre 2 et $p-2$. L'ensemble $\{0, k, \ldots, (p-1)k\}$ est alors un système complet de résidus modulo p ; il s'ensuit qu'il existe un unique élément m de l'ensemble $\{0, 1, \ldots, p-1\}$ tel que $km \equiv 1 \pmod{p}$ (on peut aussi le voir à l'aide de l'identité de Bézout ou en se rappelant que $\mathbb{Z}/p\mathbb{Z}$ est un corps). De plus, m ne peut pas être égal à 0, 1 ou $p-1$. En outre, si k_1 et k_2 sont deux éléments distincts de l'ensemble $\{2, 3, \ldots, p-2\}$, alors $mk_1 \not\equiv mk_2 \pmod{p}$ si $1 \leqslant m \leqslant p-1$: en effet, dans le cas contraire, on aurait $p \mid m(k_1 - k_2)$, ce qui est impossible car $(m, p) = 1$. Ainsi, les nombres $2, 3, \ldots, p-2$ peuvent être regroupés en paires $\{k, m\}$ telles que $km \equiv 1 \pmod{p}$. On a donc

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p},$$

soit enfin,

$$(p-1)! \equiv -1 \pmod{p}.$$

2.7. Le petit théorème de Fermat, le théorème d'Euler

2.7.1. Théorème. *(Petit théorème de Fermat[8]) Soit p un nombre premier et a un entier naturel. On a alors :*

$$a^p \equiv a \pmod{p}. \tag{2.8}$$

De plus, si a n'est pas un multiple de p, alors :

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.9}$$

♦ **Preuve.** On peut démontrer le théorème par récurrence sur a. Le cas $a = 1$ est trivial. Par ailleurs, en utilisant la formule du binôme de Newton :

$$(a+1)^p - (a+1) = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i - a.$$

8. Pierre de Fermat (1601-1665), mathématicien français.

Ainsi, si $a^p \equiv a \pmod p$, il s'ensuit que $(a+1)^p \equiv a+1 \pmod p$ car on a déjà vu que p divise $\binom{p}{i}$ pour $i = 1, 2, \ldots, p-1$, ce qui conclut la récurrence.

Si a n'est pas un multiple de p, alors $(a,p) = 1$, et donc $p \mid a^{p-1} - 1$ en appliquant le théorème de Gauss.

□

♦ **Remarques.**

1. La réciproque du petit théorème de Fermat est fausse. En particulier, on a le contre-exemple suivant dû à Euler : 341 divise $2^{341} - 2$, mais $341 = 31 \times 11$ n'est pas premier. En effet,

$$2^{340} - 1 = (2^{10})^{34} - 1$$

est divisible par $2^{10} - 1 = 3 \times 341$.

2. Le théorème de Fermat est un cas particulier du théorème d'Euler que l'on énonce ci-dessous :

2.7.2. Théorème. *(Théorème d'Euler) Si a est premier avec n, alors :*

$$a^{\varphi(n)} \equiv 1 \pmod n, \tag{2.10}$$

φ étant la fonction indicatrice d'Euler définie au paragraphe 2.4 de ce chapitre.

♦ **Preuve.** On pose $k = \varphi(n)$ et on considère l'ensemble $\{r_1, r_2, \ldots, r_k\}$ des nombres naturels $r \leqslant n$ tels que $(r,n) = 1$.

L'ensemble $\{ar_1, ar_2, \ldots, ar_k\}$ est une permutation des nombres $r_1, r_2, \ldots, r_k$ modulo n : en effet, comme $(ar_i, n) = 1$, le reste de ar_i modulo n est l'un des nombres $r_1, r_2, \ldots, r_k$. Par ailleurs, $ar_i \equiv ar_j \pmod n$ implique $r_i \equiv r_j \pmod n$ (théorème de Gauss), donc $r_i = r_j$.

Il s'ensuit donc que :

$$(ar_1) \cdot (ar_2) \cdots (ar_k) \equiv r_1 r_2 \cdots r_k \pmod n,$$

et comme $(n, r_1 r_2 \cdots r_k) = 1$, il s'ensuit que $a^k \equiv 1 \pmod n$, d'où le théorème.

□

♦ **Exemples.**

1. Soit n un nombre naturel impair. Montrer que

$$n \mid 2^{n!} - 1.$$

D'après le théorème d'Euler $n \mid 2^{\varphi(n)} - 1$ $\big((n,2) = 1\big)$. Or, $\varphi(n)$ représente le nombre des entiers a tels que $a \leqslant n$ et $(a,n) = 1$; par conséquent, $\varphi(n) < n$ et donc $\varphi(n) \mid n!$. Il s'ensuit que $2^{\varphi(n)} - 1 \mid 2^{n!} - 1$, d'où le résultat.

2. Quel est le chiffre des dizaines de milliers du nombre $5^{5^{5^{5^5}}}$?

On s'intéresse au reste de la division euclidienne de $5^{5^{5^{5^5}}}$ par $10^5 = 2^5 \times 5^5$. Comme $\varphi(2^5) = 16$, il suffit de déterminer le reste de la division euclidienne de

$5^{5^{5^5}}$ par 16. Comme $\varphi(16) = 8$, il suffit de nouveau de déterminer le reste de la division euclidienne de 5^{5^5} par 8. Or,

$$5^{5^5} \equiv 5^5 \equiv 5 \pmod 8.$$

En prenant le chemin inverse et en appliquant le théorème d'Euler, on obtient

$$5^{5^{5^5}} \equiv 5^5 \equiv 3125 \equiv 5 \pmod{16},$$

puis

$$5^{5^{5^{5^5}}} \equiv 5^5 \pmod{2^5}, \quad 5^{5^{5^{5^5}}} \equiv 5^5 \pmod{2^5 \times 5^5}.$$

Or, $5^5 = 3125$, ce qui implique que le chiffre des dizaines de milliers du nombre en question est 0.

3. Trouver le plus petit terme dans la suite définie par : $a_1 = 1993^{1994^{1995}}$, et

$$a_{n+1} = \begin{cases} a_n/2 & \text{si } a_n \text{ est pair,} \\ a_n + 7 & \text{si } a_n \text{ est impair.} \end{cases}$$

(Olympiades roumaines-1994)

On commence par calculer le reste de a_1 modulo 7. D'après les règles de congruence, on a

$$1994^{1995} \equiv 2^{1995} \equiv 2 \pmod 6,$$

puis, d'après le petit théorème de Fermat,

$$1993^{1994^{1995}} \equiv 1993^2 \equiv (-2)^2 \equiv 4 \pmod 7.$$

Si $a_n = x$ alors $a_{n+1} = x + 7 \equiv x \pmod 7$ si x est impair et $a_{n+1} = \dfrac{x}{2} \equiv 4x \pmod 7$ si x est pair.

Mais puisque $a_1 \equiv 4 \pmod 7$, il s'ensuit que tous les termes de la suite en question sont $\equiv 1, 2$ ou $4 \pmod 7$.

Finalement, si m est le plus petit terme de la suite, alors m doit être impair, et on a $\dfrac{m+7}{2} \geqslant m$, i.e., $m \leqslant 7$; par conséquent $m = 1$.

2.7.3. Théorème. *Si a est premier avec n, alors il existe un plus petit entier strictement positif k tel que :*

$$a^k \equiv 1 \pmod n.$$

De plus, tout nombre naturel m tel que $a^m \equiv 1 \pmod n$ est un multiple de k.

♦ **Preuve.** L'ensemble des entiers strictement positifs k tels que $a^k \equiv 1 \pmod n$ est une partie non vide de $\mathbb{N}^*$ puisqu'elle contient $\varphi(n)$. Elle admet donc un plus petit élément que l'on note k.

Si m est tel que $a^m \equiv 1 \pmod{n}$, on effectue la division euclidienne de m par k, $m = qk + r$, avec $0 \leqslant r < k$. On a donc :

$$1 \equiv a^{qk+r} \equiv (a^k)^q a^r \equiv a^r \pmod{n},$$

ce qui impose $r = 0$, vu l'hypothèse vérifiée par k.

$\square$

♦ **Exemples.**

1. Déterminer tous les entiers impairs n tels que $n \mid 3^n + 1$.

Il n'existe qu'un entier impair n tel que $n \mid 3^n + 1$: c'est $n = 1$.

Si $n > 1$ est un entier impair, on considère le plus petit diviseur premier p de n. Comme n est impair, on a $p \neq 2$, et puisque $p \neq 3$ car 3 ne divise pas $3^n + 1$, il s'ensuit que $p > 3$.

Soit k le plus petit entier tel que $3^k \equiv 1 \pmod{p}$. D'après le théorème de Fermat, $3^{p-1} \equiv 1 \pmod{p}$. Par ailleurs, $p \mid n \mid 3^n + 1$, ce qui donne $3^{2n} \equiv 1 \pmod{p}$. D'après le théorème précédent, on a

$$k \mid p - 1, \quad k \mid 2n.$$

Si k est impair, alors $k \mid n$ et $k \leqslant p - 1$ (car $k \mid p - 1$), ce qui impose $k = 1$, mais alors $3 \equiv 1 \pmod{p}$, ce qui est impossible puisque $p \neq 2$.

Si k est pair, $k = 2k'$, alors $k' \mid n$ et $k' < k \leqslant p - 1$, ce qui impose $k' = 1$. Or, ceci donne $k = 2$, valeur inacceptable puisque $p \neq 2$.

2.8. Le théorème chinois

2.8.1. Théorème. *(Théorème chinois) On considère des nombres naturels $m_1, m_2, \ldots, m_k$, premiers entre eux deux à deux, et des entiers $b_1, b_2, \ldots, b_k$. Le système de congruences :*

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \quad \cdots \\ x \equiv b_k \pmod{m_k}, \end{cases} \tag{2.11}$$

admet une unique solution modulo $M = m_1 m_2 \cdots m_k$.

♦ **Preuve.** On commence par construire une solution entière du système en question. Pour ce faire, on pose $M_i = \dfrac{M}{m_i}$ pour $i = 1, 2, \ldots, k$. On a ainsi $(m_i, M_i) = 1$ si bien qu'il existe un entier u_i tel que $u_i M_i \equiv 1 \pmod{m_i}$ (identité de Bézout).

Ainsi,

$$u_1 M_1 b_1 + u_2 M_2 b_2 + \cdots + u_k M_k b_k \equiv b_i \pmod{m_i}, \quad i = 1, 2, \ldots, k,$$

ce qui montre que $x = u_1M_1b_1 + u_2M_2b_2 + \cdots + u_kM_kb_k$ est solution du système (2.11).

Si y est une autre solution du système (2.11), alors m_i divise $x - y$ pour $i = 1, 2, \ldots, k$, et donc $x - y$ est divisible par M.

□

♦ **Remarques.**

1. Les Chinois savaient déjà résoudre de tels systèmes il y a vingt siècles, sans utiliser bien sûr le langage des congruences.

2. La preuve ci-dessus fournit une méthode de résolution du système étudié.

♦ **Exemples.**

1. Toutes les solutions du système de congruences :

$$\begin{cases} x \equiv 0 \pmod 3, \\ x \equiv 1 \pmod 5, \\ x \equiv 7 \pmod 8, \end{cases}$$

sont congrus à 111 modulo 120.

2. Montrer que pour tout nombre naturel n, on peut extraire de toute progression arithmétique n termes consécutifs qui soient des entiers composés.

On considère une progression arithmétique a, $a+r$, $a+2r, \ldots$, où a et r sont des nombres naturels. Soient $p_1, p_2, \ldots, p_n$ des nombres premiers tels que $r < p_1 < p_2 < \cdots < p_n$. On a donc $(r, p_i^2) = 1$ pour $i = 1, 2, \ldots, n$, et chaque congruence $rx \equiv -a - ri \pmod{p_i^2}$ admet donc une unique solution x_i modulo p_i^2 (l'ensemble $\{r, 2r, \ldots, p_i^2 r\}$ est un système complet de résidus modulo p_i^2). Ainsi, le système de congruences

$$\begin{cases} rx \equiv -a - r \pmod{p_1^2}, \\ rx \equiv -a - 2r \pmod{p_2^2}, \\ \qquad \cdots \\ rx \equiv -a - nr \pmod{p_n^2}, \end{cases}$$

est équivalent au système :

$$\begin{cases} x \equiv x_1 \pmod{p_1^2}, \\ x \equiv x_2 \pmod{p_2^2}, \\ \qquad \cdots \\ x \equiv x_n \pmod{p_n^2}, \end{cases}$$

qui possède une solution d'après le théorème chinois. On a donc n termes consécutifs de la progression $rk + a$, à savoir $r(x + i) + a$, où $i \in \{1, 2, \ldots, n\}$, qui sont composés.

2.9. Les équations diophantiennes

On appelle équation diophantienne une équation dont les inconnues sont des entiers. Un exemple célèbre de telle équation est donné par le grand théorème de

Fermat, à savoir, pour tout entier $n \geqslant 3$, l'équation diophantienne

$$x^n + y^n = z^n$$

n'admet aucun triplet (x, y, z) de solutions, où x, y et z sont des entiers naturels non nuls. Cette assertion a pu être démontrée en 1994 par Andrew Wiles[9], qui a mis fin à 300 ans de vaines tentatives.

Dans le cas $n = 2$, l'équation $x^2 + y^2 = z^2$ possède une infinité de solutions dans $(\mathbb{N}^*)^3$. On peut évidemment se restreindre au cas où $(x, y, z) = 1$; une telle solution sera alors dite *primitive*. D'un autre côté, x et y ne peuvent pas être tous les deux impairs puisqu'alors modulo 4, $z^2 \equiv 2 \pmod 4$, ce qui est impossible.

2.9.1. Théorème. *Toute solution primitive de l'équation $x^2 + y^2 = z^2$, où y est supposé pair, est de la forme*

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2, \tag{2.12}$$

où u et v sont des entiers naturels non nuls, de parités différentes et tels que $(u, v) = 1$ et $u > v > 0$.

♦ **Preuve.** On commence par écrire l'équation sous la forme :

$$(z + x)(z - x) = y^2,$$

ce qui montre que $z + x$ et $z - x$ sont pairs. On a alors

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

et comme $(z, x) = 1$ (car $y^2 = z^2 - x^2$), il s'ensuit que $(z + x)/2$ et $(z - x)/2$ sont premiers entre eux ; si bien que du fait de l'équation précédente

$$\frac{z + x}{2} = u^2, \quad \frac{z - x}{2} = v^2,$$

où $u > v > 0$ et $(u, v) = 1$. On en déduit que $x = u^2 - v^2$, $y = 2uv$ et $z = u^2 + v^2$. Comme z est impair, u et v sont de parités différentes.

□

On illustre maintenant une notion utile dans la résolution des équations diophantiennes : il s'agit de la recherche d'une *solution particulière* qui joue le rôle de « solution de base ». L'exemple choisi est l'équation dite de Pell[10]-Fermat :

$$x^2 - y^2 d = 1,$$

où d est un entier naturel non nul et qui n'est pas un carré parfait.

2.9.2. Théorème. *Si l'équation $x^2 - y^2 d = 1$ possède au moins une solution dans $(\mathbb{N}^*)^2$, alors l'ensemble des solutions dans $(\mathbb{N}^*)^2$ de l'équation est formé des*

9. Andrew John Wiles (né en 1953), mathématicien anglais.

10. John Pell (1611-1685), mathématicien anglais.

couples (x_n, y_n), $n \in \mathbb{N}^*$, *donnés par la formule :*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,$$

où (x_1, y_1) *est une solution pour laquelle la quantité* $x + y\sqrt{d}$ *est minimale.*

♦ **Preuve.** Si $(x_n, y_n) \in (\mathbb{N}^*)^2$ est défini par

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,$$

alors

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n,$$

ce qui donne

$$x_n^2 - y_n^2 d = (x_n - y_n\sqrt{d})(x_n + y_n\sqrt{d}) = (x_1^2 - y_1^2 d)^n = 1.$$

Supposons maintenant qu'il existe une autre solution $(u, v) \subset (\mathbb{N}^*)^2$ telle que $u + v\sqrt{d}$ ne soit pas une puissance naturelle de $x_1 + y_1\sqrt{d}$. Il existe alors un entier k tel que

$$(x_1 + y_1\sqrt{d})^k < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{k+1},$$

ce qui implique que

$$1 < (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^k < x_1 + y_1\sqrt{d}.$$

Si on pose $(u + v\sqrt{d})(x_1 - y_1\sqrt{d})^k = t + w\sqrt{d}$, alors (t, w) est une solution telle que $1 < t + w\sqrt{d} < x_1 + y_1\sqrt{d}$, ce qui est absurde.

□

♦ **Remarques.**

1. L'équation $x^2 - y^2 d = 1$ admet en fait toujours des solutions dans $(\mathbb{N}^*)^2$. Il existe même un algorithme basé sur le développement de $\sqrt{d}$ en fraction continue qui permet de trouver la solution (x, y) pour laquelle $x + y\sqrt{d}$ est minimal.

2. Dans beaucoup de cas, il est possible de trouver par tâtonnement la solution (x, y) pour laquelle $x + y\sqrt{d}$ est minimal, solution qui permet de générer toutes les solutions possibles de l'équation de Pell-Fermat. Par exemple, $(2, 1)$ est la solution de base correspondant à l'équation

$$x^2 - 3y^2 = 1,$$

ce qui donne toutes les solutions $(x_n, y_n) \in (\mathbb{N}^*)^2$: $x_n + y_n\sqrt{3} = (2 + \sqrt{3})^n$, $n \geqslant 1$. On a alors les solutions : (2,1), (7,4), (26,15), ...

EXERCICES

1. Démontrer qu'il existe une infinité de naturels a tels que $n^4 + a$ ne soit premier pour aucune valeur de n.

(Olympiades internationales-1969/1)

---

2. Trouver toutes les solutions $(x, y, z, t) \in \mathbb{Z}^4$ du système :

$$\begin{cases} xz - 2yt &= 3, \\ xt + yz &= 1. \end{cases}$$

(Olympiades russes-1991)

---

3. Un triangle est dit pythagorique s'il est rectangle à côtés entiers ; il est dit pythagorique primitif si de plus ses côtés sont deux à deux premiers entre eux.

Prouver que le nombre de triangles pythagoriques primitifs avec un rayon du cercle inscrit fixé est une puissance de 2.

---

4. Pour tout entier $n \geqslant 3$, soit $f^{(1)}(n)$ le plus petit entier positif ne divisant pas n. Si $f^{(k)}(n) \geqslant 3$, $f(f^{(k)}(n))$ a un sens et on pose $f^{(k+1)}(n) = f^{(1)}(f^{(k)}(n))$. Pour tout entier $n \geqslant 3$, déterminer le rang k pour lequel $f^{(k)}(n) = 2$.

(Olympiades chinoises-1988)

---

5. Soit $(a_n)_{n \in \mathbb{N}}$ une suite strictement croissante d'entiers strictement positifs. Démontrer qu'il existe une infinité de termes a_m qui peuvent s'écrire sous la forme : $a_m = xa_p + ya_q$, avec x, y entiers positifs et $p \neq q$.

(Olympiades internationales-1975/2)

---

6. Soit d un entier strictement positif n'appartenant pas à l'ensemble $\{2, 5, 13\}$. Montrer que l'on peut trouver un couple (a, b) d'éléments de l'ensemble $\{2, 5, 13, d\}$ tel que $ab - 1$ ne soit pas le carré d'un entier.

(Olympiades internationales-1986/1)

---

7. Soient a, b, m et n des nombres naturels tels que $a > 1$ et $(a, b) = 1$. Prouver que si $a^m + b^m$ divise $a^n + b^n$, alors m divise n.

---

8. Déterminer tous les carrés parfaits qui s'écrivent dans le système de numération de base 9 à l'aide du chiffre 1 uniquement.

---

9. Trouver tous les entiers positifs x et y tels que

$$7^x - 3 \cdot 2^y = 1.$$

---

10. Résoudre dans $(\mathbb{N}^*)^3$ l'équation :

$$\frac{1}{x} + \frac{2}{y} - \frac{3}{z} = 1.$$

---

11. Les entiers strictement positifs a et b sont tels que les nombres $15a + 16b$ et $16a - 15b$ sont tous les deux des carrés d'entiers strictement positifs. Trouver la plus petite valeur pouvant être prise par le minimum de ces deux carrés.

(Olympiades internationales-1996/4)

---

12. On se donne des entiers naturels $k < l < m < n$ tels que $kn = lm$. Prouver qu'alors :

$$\left(\frac{n-k}{2}\right)^2 \geqslant k + 2.$$

(Olympiades russes-1992)

---

13. Soit A la somme des chiffres du nombre 4444^{4444} et B la somme des chiffres du nombre A. Trouver la somme des chiffres du nombre B (le système de numération utilisé est le système décimal).

(Olympiades internationales-1975/4)

---

14. Soient a, b, c, d des entiers positifs impairs vérifiant les conditions :

a) $a < b < c < d$;

b) $ad = bc$;

c) $a + d = 2^k$ et $b + c = 2^m$, k et m étant entiers.

Prouver que $a = 1$.

(Olympiades internationales-1984/6)

---

15. Montrer que les racines cubiques de trois nombres premiers distincts ne peuvent pas être trois termes (non nécessairement consécutifs) d'une progression arithmétique.

(Olympiades des États-Unis-1973)

---

16. Soient a et b deux entiers naturels premiers entre eux. Démontrer que pour tout entier naturel n tel que $n > ab$, il existe deux entiers naturels x et y tels que $n = ax + by$.

---

17. Soient a, b, c des entiers strictement positifs et premiers entre eux deux à deux. Montrer que $2abc - ab - bc - ca$ est le plus grand entier qui ne peut pas s'écrire sous la forme : $xbc + yca + zab$, avec x, y, z entiers positifs ou nuls.

(Olympiades internationales-1983/3)

---

18. On considère une suite $(a_n)_{n \in \mathbb{N}^*}$ strictement croissante, formée d'entiers naturels et telle que $a_{2n} = a_n + n$ pour tout entier n strictement positif. On suppose de plus que si a_n est premier, alors n l'est aussi. Trouver a_{1993}.

(Olympiades bulgares-1993)

---

19. Soient p et q des entiers strictement positifs vérifiant : $p/q = 1 - 1/2 + 1/3 - \cdots - 1/1318 + 1/1319$. Montrer que 1979 divise p.

(Olympiades internationales-1979/1)

---

20. Soit k un entier naturel non nul. Démontrer qu'il existe une infinité de carrés parfaits de la forme $n \cdot 2^k - 7$, où n est un entier naturel.

(Proposé à l'OIM-1995)

---

21. Montrer qu'il existe un ensemble infini d'entiers naturels, deux à deux premiers entre eux, de la forme $2^n - 3$, où $n \geqslant 2$.

(Olympiades internationales-1971/3)

---

22. Prouver qu'il existe une infinité d'ensembles de 1998 entiers positifs consécutifs tous divisibles par des nombres de la forme a^{1998} $(a > 1)$.

---

23. Démontrer que pour chaque entier strictement positif n, il existe n entiers strictement positifs consécutifs tels qu'aucun d'entre eux ne soit une puissance entière d'un nombre premier.

(Olympiades internationales-1989/5)

---

24. a) Existe-t-il 14 nombres naturels consécutifs tels que chacun d'entre eux est divisible par un ou plusieurs nombres premiers p tels que $2 \leqslant p \leqslant 11$?

b) Existe-t-il 21 nombres naturels consécutifs tels que chacun d'entre eux est divisible par un ou plusieurs nombres premiers p tels que $2 \leqslant p \leqslant 13$?

(Olympiades des États-Unis-1986)

---

25. Déterminer tous les entiers naturels x, y et z tels que : z divise $xy-1$; x divise $yz-1$ et y divise $zx-1$.

---

26. Déterminer tous les couples (m, n) d'entiers strictement positifs tels que

$$\frac{n^3+1}{mn-1}$$

soit entier.

(Olympiades internationales-1994/4)

---

27. Trouver tous les entiers a, b, c tels que $1 < a < b < c$ et

$$(a-1)(b-1)(c-1)$$

soit un diviseur de $abc-1$.

(Olympiades internationales-1992/1)

---

28. m et n sont deux entiers naturels tels que $n > m \geqslant 1$. On suppose que les 3 derniers chiffres de la représentation décimale de 1978^m sont respectivement égaux aux 3 derniers chiffres de la représentation décimale de 1978^n. Déterminer m et n de façon que $m+n$ soit minimal.

(Olympiades internationales-1978/1)

---

29. Trouver les entiers $n \geqslant 2$ pour lesquels tous les nombres naturels dont l'écriture décimale contient $n-1$ chiffres 1 et un chiffre 7 sont premiers.

(Proposé à l'OIM-1990)

---

30. Prouver qu'il n'existe aucun entier $n > 1$ pour lequel n divise $2^n - 1$.

---

31. Soit m un entier naturel impair > 2. Trouver le plus petit entier positif n tel que 2^{1989} divise $m^n - 1$.

(Proposé à l'OIM-1989)

---

32. Prouver que si x, y, z sont des entiers positifs tels que $x^2 + y^2 + z^2 = 1993$, alors $x + y + z$ n'est pas un carré parfait.

(Olympiades roumaines-1993)

---

33. Déterminer tous les entiers naturels $k > 1$ tels que, pour des entiers m et n distincts, les nombres $k^m + 1$ et $k^n + 1$ s'obtiennent l'un à partir de l'autre en inversant l'ordre des chiffres dans leur représentation décimale.

(Olympiades russes-1992)

---

34. Soit n un entier $\geqslant 2$. Prouver que si $k^2 + k + n$ est un nombre premier pour tout entier k, $0 \leqslant k \leqslant \sqrt{n/3}$, alors $k^2 + k + n$ est premier pour tout entier k, $0 \leqslant k \leqslant n - 2$.

(Olympiades internationales-1987/6)

---

35. Démontrer que, pour tout entier $n \geqslant 1$ fixé, la suite $2, 2^2, 2^{2^2}, \ldots$ est constante à partir d'un certain rang modulo n.

(Olympiades des États-Unis-1991)

---

36. Soit $n > 6$ un entier. On considère les nombres $a_1, a_2, \ldots, a_k$, inférieurs à n et premiers avec n, et on suppose que :

$$a_2 - a_1 = a_3 - a_2 = \cdots = a_k - a_{k-1} > 0.$$

Prouver qu'alors n est un nombre premier ou une puissance de 2.

(Olympiades internationales-1991/2)

---

37. Pour tout entier strictement positif n, on désigne par $S(n)$ le plus grand entier tel que, pour tout entier strictement positif $k \leqslant S(n)$, n^2 peut s'écrire comme la somme de k carrés parfaits.

a) Prouver que $S(n) \leqslant n^2 - 14$ pour tout $n \geqslant 4$.

b) Trouver un entier n tel que $S(n) = n^2 - 14$.

c) Prouver qu'il existe une infinité d'entiers n tels que $S(n) = n^2 - 14$.

(Olympiades internationales-1992/6)

---

38. Déterminer tous les entiers n strictement supérieurs à 1, tels que $\dfrac{2^n + 1}{n^2}$ soit entier.

(Olympiades internationales-1990/3)

---

39. Prouver qu'il existe un entier positif k tel que $k \cdot 2^n + 1$ est composé pour tout entier $n \geqslant 1$.

(Olympiades des États-Unis-1982)

---

40. Prouver que, pour tout entier $n \geqslant 3$, il existe des entiers positifs impairs x_n et y_n tels que :

$$7x_n^2 + y_n^2 = 2^n.$$

(Olympiades bulgares-1996)

---

41. Soient a et b deux entiers strictement positifs tels que $ab + 1$ divise $a^2 + b^2$. Montrer que

$$\frac{a^2 + b^2}{ab + 1}$$

est un carré parfait.

(Olympiades internationales-1988/6)

SOLUTIONS

1. On cherche un entier a tel que $n^4 + a$ soit un nombre non premier pour tout n. On commence par essayer de prendre a sous la forme $a = b^2$ ou $a = b^4$, et on se rend compte qu'avec le choix $a = 4b^4$, on obtient

$$\begin{aligned} n^4 + 4b^4 &= (n^2 + 2b^2)^2 - 4n^2b^2 \\ &= (n^2 + 2b^2 - 2nb)(n^2 + 2b^2 + 2nb) \\ &= \big[(n-b)^2 + b^2\big]\big[(n+b)^2 + b^2\big]. \end{aligned}$$

Il suffit alors de prendre $b > 1$.

Note. L'identité $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$ est connue sous le nom d'identité de Sophie Germain[11]. Elle est à la base de la solution de plusieurs exercices d'olympiades ; on pourra par exemple essayer l'exercice suivant, posé aux olympiades hongroises en 1978 : prouver que pour $n > 1$, le nombre $n^4 + 4^n$ n'est pas premier.

---

2. Le système proposé est équivalent à l'équation suivante :

$$\big(x + i\sqrt{2}y\big)\big(z + i\sqrt{2}t\big) = 3 + i\sqrt{2}.$$

Si x, y, z et t sont des entiers satisfaisant à la dernière égalité, alors :

$$(x^2 + 2y^2)(z^2 + 2t^2) = 11,$$

ce qui implique que $x^2 + 2y^2 = 1$ ou $z^2 + 2t^2 = 1$ car 11 est premier. Dans le premier cas, on trouve $x = \pm 1$, $y = 0$, ce qui conduit aux deux solutions $(1, 0, 3, 1)$ et $(-1, 0, -3, -1)$. Dans le deuxième cas, on trouve $z = \pm 1$, $t = 0$, ce qui donne deux nouvelles solutions : $(3, 1, 1, 0)$ et $(-3, -1, -1, 0)$.

---

3. Soient a, b et c les côtés d'un triangle pythagorique primitif dont le rayon du cercle inscrit est r. Si c est l'hypoténuse du triangle en question, alors $r = (a + b - c)/2$.

D'un autre côté, il existe des entiers m et n premiers entre eux et non tous les deux impairs tels que $a = 2mn$, $b = m^2 - n^2$ et $c = m^2 + n^2$. Ainsi, $r = n(m - n)$. Ceci étant, soient $p_1, p_2, \ldots, p_l$ des nombres premiers $\geqslant 3$ tels que $r = 2^k p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$. Comme $m - n$ est impair, 2^k divise n. Par ailleurs, pour $i = 1, 2, \ldots, l$, p_i divise n ou $m - n$, mais pas les deux à la fois.

11. Sophie Germain (1776-1831), mathématicienne française.

Il y a donc 2^l choix convenables pour m et n, et donc 2^l triangles pythagoriques primitifs dont r est le rayon du cercle inscrit.

---

4. On montre que $f^{(1)}(n) = p^m$ où p est un nombre premier, et m est un entier positif non nul : en effet, si $f^{(1)}(n) = \alpha\beta$, où α et β sont des entiers $\geqslant 2$ et premiers entre eux, alors $\alpha < f^{(1)}(n)$ et $\beta < f^{(1)}(n)$, ce qui implique que α et β divisent n, donc leur produit aussi divise n, ce qui est absurde.

Si maintenant $f^{(1)}(n) = 2^m$, alors $f^{(3)}(n) = 2$, et si $f^{(1)}(n) = p^m$ avec $p > 2$, alors $f^{(2)}(n) = 2$.

---

5. Soit p un rang fixé. Considérons les divisions euclidiennes des entiers a_{p+i} par a_p pour $i = 1, 2, \ldots, a_p + 1$. Parmi les $a_p + 1$ restes obtenus, il existe au moins deux restes identiques. Il s'ensuit que a_p divise $a_{p+i_2} - a_{p+i_1}$ pour deux indices $1 \leqslant i_1 < i_2 \leqslant a_p + 1$. Si on pose $a_{p+i_2} - a_{p+i_1} = xa_p$, on s'aperçoit que

$$a_{p+i_2} = xa_p + a_{p+i_1} \quad (x \in \mathbb{N}^*).$$

On peut donc construire une infinité de termes a_m pouvant s'écrire sous la forme $xa_p + ya_q$, où $x, y \in \mathbb{N}$ et $p \neq q$, en fixant à chaque fois un rang $p_m > a_{p_{m-1}} + 1$.

---

6. Pour $x \in \mathbb{N}$, x^2 est congru à 0, 1, 4 ou 9 modulo 16. Si $2d - 1$ est un carré alors $d \in \{1, 5, 9, 13\}$ modulo 16. Si $5d - 1$ est un carré alors $d \in \{1, 2, 10, 13\}$ modulo 16. Si $13d - 1$ est un carré alors $d \in \{2, 5, 9, 10\}$ modulo 16. L'intersection de ces trois ensembles est vide, ce qui permet de conclure.

---

7. Effectuons la division euclidienne de n par m : $n = mq + r$, où $0 \leqslant r < m$. On remarque que, si l et k sont deux nombres naturels tels que $l \geqslant k$,

$$a^l + b^l = a^{l-k}\left(a^k + b^k\right) - b^k\left(a^{l-k} - b^{l-k}\right),$$

et

$$a^l - b^l = a^{l-k}\left(a^k + b^k\right) - b^k\left(a^{l-k} + b^{l-k}\right).$$

Il s'ensuit que $a^r + (-1)^q b^r$ est divisible par $a^m + b^m$. Comme

$$0 \leqslant \left|a^r + (-1)^q b^r\right| < a^m + b^m,$$

on a $r = 0$ et q est nécessairement impair, d'où le résultat.

---

8. On démontre que 1 est l'unique solution au problème : en effet, soit x un entier naturel tel que $x^2 = 1 + 9 + 9^2 + \cdots + 9^n$. On a alors $8x^2 = 9^{n+1} - 1 = \left(3^{n+1} - 1\right)\left(3^{n+1} + 1\right)$. Or, $\left(3^{n+1} - 1, 3^{n+1} + 1\right) = 2$; il existe donc deux entiers naturels non nuls c et d tels que $3^{n+1} - 1 = 4c^2$ et $3^{n+1} + 1 = 2d^2$ ou bien $3^{n+1} - 1 = 2c^2$ et $3^{n+1} + 1 = 4d^2$.

Dans le premier cas, n doit être impair (car $3^{n+1} - 1$ est divisible par 4), d'où $1 = 3^{n+1} - 4c^2 = \left(3^{(n+1)/2} + 2c\right)\left(3^{(n+1)/2} - 2c\right)$ ce qui est impossible car $c \neq 0$.

Dans le second cas on aurait $3^{n+1} = 4d^2 - 1 = (2d-1)(2d+1)$, et comme $(2d-1, 2d+1) = 1$, on aurait $2d+1 = 3$ et $2d-1 = 1$, soit encore $n = 0$.

---

9. Les couples $(1,1)$ et $(2,4)$ sont des solutions de l'équation proposée. Par ailleurs, si $x > 2$ alors $y > 4$ et l'équation est équivalente à :

$$\begin{aligned} 7^x - 1 = 3 \times 2 \times 2^{y-1} \quad &\Longleftrightarrow \quad \frac{7^x - 1}{7-1} = 2^{y-1} \\ &\Longleftrightarrow \quad 7^{x-1} + 7^{x-2} + \cdots + 1 = 2^{y-1} \\ &\Longleftrightarrow \quad (7+1)(7^{x-2} + 7^{x-4} + \cdots + 1) = 2^{y-1} \\ &\Longleftrightarrow \quad 7^{x-2} + 7^{x-4} + \cdots + 1 = 2^{y-4}. \qquad (*) \end{aligned}$$

Les deux membres de cette dernière égalité sont pairs, donc $x/2$ est pair, i.e., $x \equiv 0 \pmod 4$. Il s'ensuit que

$$(*) \quad \Longleftrightarrow \quad (7^2+1)(7^{x-4} + 7^{x-8} + \cdots + 1) = 2^{y-4},$$

ce qui est impossible puisque 2^{y-4} n'est pas divisible par 50. Les seules solutions de l'équation initiale sont donc $(1,1)$ et $(2,4)$.

---

10. L'équation proposée est équivalente à $2xz + yz - 3xy = xyz$. On a donc $2xz + yz > xyz$, d'où $y + 2x > xy$, c'est-à-dire $y(x-1) < 2x$.

- Si $x = 1$, alors $3y = 2z$ et donc $y = 2k$, $z = 3k$, avec $k \in \mathbb{N}^*$.

- Si $x \neq 1$, alors

$$y < \frac{2x}{x-1} = 2 + \frac{2}{x-1}.$$

Pour $x = 2$, on a $y < 4$, ce qui donne les solutions $(2,1,2)$; $(2,2,6)$; $(2,3,18)$.

Pour $x = 3$, on aura $y < 3$. Or, $6z - 9y = 2yz$ ce qui implique que y est pair. On a ainsi la solution $(3,2,9)$.

Pour $x > 3$, on aura $y \leqslant 2$. Si $y = 1$ alors $z(x+1) = 3x$. Or, $(x, x+1) = 1$ et donc $x+1$ divise 3, ce qui est impossible. Si maintenant $y = 2$, on aura les solutions $(l, 2, 3l)$ avec $l \in \mathbb{N}^*$ et $l > 3$.

En conclusion, l'ensemble des solutions est formé des triplets : (2,1,2) ; (2,3,18) ; $(1, 2k, 3k)$; $(l, 2, 3l)$ avec $k \in \mathbb{N}^*$ et $l \in \mathbb{N}$, $l \geqslant 2$.

---

11. On sait qu'il existe deux entiers m et n tels que $15a + 16b = m^2$ et $16a - 15b = n^2$. On en déduit que :

$$a = \frac{15m^2 + 16n^2}{15^2 + 16^2} = \frac{15m^2 + 16n^2}{481} = \frac{15m^2 + 16n^2}{37 \times 13};$$

et on a donc $15m^2 + 16n^2 \equiv 0 \pmod{13}$ et $15m^2 + 16n^2 \equiv 0 \pmod{37}$.

Commençons d'abord par examiner la congruence modulo 13. Si n n'était pas divisible par 13, il y aurait un nombre $n^* \in \mathbb{Z}$ tel que $nn^* \equiv 1 \pmod{13}$. On aurait ainsi

$$3\underbrace{m^2n^{*2}}_{=m'^2} \equiv 2 \pmod{13}, \text{ i.e.,} \quad m'^2 \equiv 5 \pmod{13}.$$

Or, 5 n'est pas un carré dans $\mathbb{Z}/13\mathbb{Z}$: en effet, si $x^2 \equiv 5 \pmod{13}$, où $x \in \{0, \pm1, \pm2, \ldots, \pm6\}$, alors $x^2 \leqslant 36 < 3 \times 13 + 5$. Les valeurs pouvant être prises par x^2 sont donc 5, 18 et 31 mais aucune d'entre elles n'est un carré parfait. On en déduit que 13 divise n, donc m aussi.

De même, on démontre que $m \equiv n \equiv 0 \pmod{37}$. Ainsi, $481 \mid m$ et $481 \mid n$, ce qui implique que $\min(m, n) \geqslant 481$. Par ailleurs, on peut avoir $m = n = 481$ si on prend $a = 31 \times 481$ et $b = 481$. La réponse est donc 481^2.

---

12. On pose $l = k + a$, $m = k + b$, $n = k + c$, où a, b, c sont des entiers strictement positifs. L'égalité $kn = lm$ se réécrit donc :

$$k(k + c) = (k + a)(k + b),$$

d'où $kc = k(a + b) + ab > k(a + b)$. Ainsi, $c > a + b$, ce qui implique que

$$(n + k) - (m + l) \geqslant 1.$$

D'un autre côté,

$$(n-k)^2 = (n+k)^2 - 4ml > (n+k)^2 - (m+l)^2 = \big[(n+k) - (m+l)\big]\big[k+l+m+n\big],$$

ce qui donne :

$$(n - k)^2 > k + (k + 1) + (k + 2) + (k + 3) = 4k + 6.$$

Or, un carré ne peut pas être congru à 3 modulo 4. Il s'ensuit que

$$(n - k)^2 \geqslant 4k + 8,$$

d'où le résultat.

---

13. Soit C la somme des chiffres du nombre B. Comme $4444^{4444} < 10000^{4444}$, il s'ensuit que le nombre des chiffres de 4444^{4444} est inférieur à $4 \times 4444 + 1 < 20000$. On en déduit que $A < 9 \times 20000 = 180000$, d'où $B < 9 \times 5 = 45$ (pourquoi ?), et $C < 13$ (pourquoi ?).

Après avoir réussi à majorer C, on va examiner le reste de C modulo 9. On sait que $A \equiv B \equiv C \pmod 9$. Par ailleurs, $4444 \equiv -2 \pmod 9$ et $(-2)^{4444} \equiv 2^{3\times1481+1} \equiv 2 \times (-1)^{1481} \equiv -2 \equiv 7 \pmod 9$. On en déduit que $C = 7$.

---

14. Remarquons d'abord que :

$$\begin{aligned} a\big[(a + d) - (b + c)\big] &= a(a - c) + a(d - b) \\ &= a(a - c) + bc - ab = (a - b)(a - c) > 0, \end{aligned}$$

ce qui implique que $k > m$.

À partir de $a(2^k - a) = b(2^m - b)$ il s'ensuit que

$$a^2 - b^2 = 2^m(2^{k-m}a - b).$$

On en déduit que 2^m divise $a^2 - b^2 = (a-b)(a+b)$. Mais $b+a$ et $b-a$ ne sont pas tous les deux divisibles par 4 car leur somme $2b$ ne l'est pas. L'un des nombres $a+b$ et $b-a$ est donc divisible par 2^{m-1} ; notons le x. On a alors

$$0 < x \leqslant b + a < b + c = 2^m,$$

ce qui montre que $x = 2^{m-1}$, d'où $(a,b) = 1$: en effet, si d divisait a et b, alors d diviserait $x = 2^{m-1}$. Comme par ailleurs d est impair, il s'ensuit que $d = 1$.

D'un autre côté, $(b+c) - x = 2^m - 2^{m-1} = 2^{m-1}$ est égal à $c+a$ (si $x = b-a$) ou à $c-a$ (si $x = b+a$). Il s'ensuit de même que $(a,c) = 1$. Or, a divise bc et donc $a = 1$.

Note. En poussant plus loin notre investigation, on aurait pu trouver les nombres a, b, c, d satisfaisant aux conditions de l'énoncé. Comme

$$b - a < b < \frac{1}{2}(b+c) = 2^{m-1},$$

on a $b - a \neq 2^{m-1}$, et $x = b + a = 2^{m-1}$. Il s'ensuit que $b = 2^{m-1} - 1$ et $c = 2^m - b = 2^{m-1} + 1$, ce qui donne $d = bc = 2^{2m-2} - 1$. Ces nombres satisfont manifestement aux conditions de l'énoncé (avec $k = 2m - 2$).

---

15. S'il en était ainsi, on pourrait avoir

$$\sqrt[3]{p_1} = a, \quad \sqrt[3]{p_2} = a + md, \quad \sqrt[3]{p_3} = a + nd,$$

où p_1, p_2, p_3 sont des nombres premiers distincts et m, n sont des entiers. En éliminant a et d, on obtient

$$\frac{\sqrt[3]{p_2} - \sqrt[3]{p_1}}{\sqrt[3]{p_3} - \sqrt[3]{p_1}} = \frac{m}{n},$$

ce qui s'écrit encore :

$$m\sqrt[3]{p_3} - n\sqrt[3]{p_2} = (m-n)\sqrt[3]{p_1},$$

ce qui donne, après élévation au cube,

$$m^3p_3 - n^3p_2 - 3mn\sqrt[3]{p_2p_3}\underbrace{\left(m\sqrt[3]{p_3} - n\sqrt[3]{p_2}\right)}_{=(m-n)\sqrt[3]{p_1}} = (m-n)^3p_1.$$

On a donc finalement

$$\sqrt[3]{p_1p_2p_3} = \frac{m^3p_3 - n^3p_2 - (m-n)^3p_1}{3mn(m-n)},$$

ce qui est absurde puisque $\sqrt[3]{p_1p_2p_3}$ est irrationnel.

Note. On pourra essayer de montrer que les racines cubiques de trois nombres premiers distincts ne peuvent pas être trois termes (non nécessairement consécutifs) d'une progression géométrique, ni d'une progression harmonique.

---

16. Considérons les nombres : $n_1 = n - a$; $n_2 = n - 2a$;... ; $n_b = n - ba$ et leurs restes $r_1, r_2, \ldots, r_b$ dans la division euclidienne par b. Ces restes sont deux à deux distincts car si $r_i = r_j$ alors si on écrit $n - ia = bq_i + r_i$ et $n - ja = bq_j + r_j$, on obtient $(i-j)a = b(q_j - q_i)$ ce qui implique que $b \mid i - j$ (car $(a, b) = 1$). On a donc $i = j$ puisque $|i - j| < b$.

Puisque l'ensemble des restes possibles est $\{0, 1, \ldots, b-1\}$, il existe k tel que $r_k = 0$, c'est-à-dire $n - ka = bq_k$, ce qu'il fallait démontrer.

Note. On peut améliorer le résultat prouvé en l'étendant à tous les nombres $> ab - a - b$. En effet, si $n > ab - a - b$ alors écrivons-le sous la forme (identité de Bézout) :

$$n = au + bv, \quad u, v \in \mathbb{Z}.$$

On peut supposer $0 \leqslant v \leqslant a - 1$: en effet, si $v = v' + ka$, où $k \in \mathbb{Z}$ et $0 \leqslant v' \leqslant a-1$, alors $n = a(u + kb) + bv'$. On a alors

$$u = \frac{n - bv}{a} \geqslant \frac{ab - a - b - (a-1)b + 1}{a} = \frac{1-a}{a} > -1,$$

d'où $u \geqslant 0$.

On peut même démontrer que $ab - a - b$ est le plus grand entier qui ne peut pas s'écrire sous la forme $xa + yb$, où x et y sont des entiers positifs ou nuls (voir l'exercice suivant).

---

17. Montrons d'abord que $2abc - ab - bc - ca$ ne peut pas s'écrire sous la forme $xbc + yca + zab$ avec x, y et z entiers positifs ou nuls. Si $2abc - ab - bc - ca = xbc + yca + zab$, alors a doit diviser $x + 1$ puisque $(a, b) = (a, c) = 1$. De même, b doit diviser $y + 1$ et c doit diviser $z + 1$, ce qui donne $x + 1 \geqslant a$, $y + 1 \geqslant b$ et $z + 1 \geqslant c$. On aurait donc

$$2abc = (x+1)bc + (y+1)ca + (z+1)ab \geqslant abc + bca + cab = 3abc,$$

d'où la contradiction.

Soit maintenant un entier $n > 2abc - bc - ca - ab$. a, b, c étant premiers entre eux deux à deux, ab, bc et ca sont premiers entre eux dans leur ensemble ; il existe donc des entiers x, y et z tels que $n = xbc + yca + zab$ (identité de Bézout). Par ailleurs, on peut supposer $0 \leqslant x \leqslant a - 1$ et $0 \leqslant y \leqslant b - 1$ quitte à remplacer x par $x + pa$, y par $y + qb$ et z par $z - (p+q)c$. On a donc

$$n \leqslant abc - bc + abc - ca + zab < n + (z+1)ab,$$

ce qui implique que $z + 1 > 0$, soit encore $z \geqslant 0$.

Note. On pourra essayer de généraliser l'exercice à n entiers $a_1, a_2, \ldots, a_n$ deux à deux premiers entre eux en montrant que

$$a_1 a_2 \cdots a_n \left(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i} \right)$$

est le plus grand entier qui ne peut pas s'écrire sous la forme $\displaystyle\sum_{i=1}^{n} x_i \prod_{j \neq i} a_j$.

---

18. On remarque que $a_2 = a_1 + 1$ et $a_4 = a_2 + 2 = a_1 + 3$. Comme $(a_n)_{n \in \mathbb{N}^*}$ est strictement croissante, il s'ensuit que $a_3 = a_1 + 2$. Ceci suggère que $a_n = a_1 + n - 1$, ce que l'on démontre par récurrence : si $a_n = a_1 + n - 1$, alors $a_{2n} = a_1 + 2n - 1$ ce qui implique que $a_m = a_1 + m - 1$ pour $n < m < 2n$.

On démontre maintenant que $a_1 = 1$, ce qui donne $a_n = n$ pour tout $n \in \mathbb{N}$, et en particulier $a_{1993} = 1993$. Si $a_1 = 0$ alors $a_4 = 3$ ce qui est exclu. Supposons donc $a_1 \geqslant 2$ de telle sorte que $a_n = n + \alpha$ pour un certain $\alpha \in \mathbb{N}^*$. Il s'agit alors de trouver un entier premier m tel que $m - \alpha$ ne le soit pas.

Une première possibilité est de considérer la suite $(\alpha + 2)! + 2$, $(\alpha + 2)! + 3, \ldots$, $(\alpha + 2)! + (\alpha + 2)$ constituée de $\alpha + 1$ termes dont aucun n'est premier. En prenant le plus petit nombre premier p supérieur à $(\alpha + 2)! + (\alpha + 2)$, on est sûr que $p - \alpha$ n'est pas premier : en effet, $p - \alpha \geqslant (\alpha + 2)! + 2$ et $p - \alpha < p$.

Une deuxième possibilité serait d'utiliser le théorème de Dirichlet : la progression $(ak + b)$, $k \in \mathbb{N}$, où a et b sont deux entiers non nuls et premiers entre eux, contient une infinité de nombres premiers. En particulier, la progression $1, 1 + \alpha, 1 + 2\alpha, \ldots$ contient une infinité de nombres premiers. Si $1 + p\alpha$ est le plus petit nombre premier dans cette progression, alors $p \geqslant 1$, et on a aussi $a_{1+(p-1)\alpha} = 1 + p\alpha$, ce qui impose que $1 + (p - 1)\alpha$ est premier, ce qui contredit notre hypothèse de minimalité.

---

19. Les termes affectés de signes $-$ ont des dénominateurs pairs ; on décide d'écrire chaque terme $-1/2k$ sous la forme $1/2k - 1/k$.

On a alors

$$\begin{aligned} \frac{p}{q} &= \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{1319}\right) - 2\left(\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \cdots + \frac{1}{1318}\right) \\ &= \frac{1}{660} + \frac{1}{661} + \cdots + \frac{1}{1319}. \end{aligned}$$

Comme

$$\frac{1}{660 + j} + \frac{1}{1319 - j} = \frac{1979}{(660 + j)(1319 - j)},$$

il s'ensuit que

$$\begin{aligned}\frac{p}{q} &= \left(\frac{1}{660}+\frac{1}{1319}\right)+\left(\frac{1}{661}+\frac{1}{1318}\right)+\cdots+\left(\frac{1}{989}+\frac{1}{990}\right)\\ &= \frac{1979}{660\times 1319}+\frac{1979}{661\times 1318}+\cdots+\frac{1979}{989\times 990}\\ &= 1979\times\frac{p'}{q'},\end{aligned}$$

où q' est premier avec 1979 (qui est premier). On a ainsi $1979p'q = pq'$, et comme 1979 ne divise pas q', 1979 divise p.

---

20. On commence par démontrer que pour tout entier naturel k, il existe un entier naturel k tel que $a_k^2 \equiv -7 \pmod{2^k}$. On raisonne par récurrence sur k.

Si $k \leqslant 3$, $a_k = 1$ convient. Supposons donc qu'il existe a_k tel que $a_k^2 \equiv -7 \pmod{2^k}$ pour un certain $k \geqslant 3$. On a alors $a_k^2 \equiv -7 \pmod{2^{k+1}}$ ou $a_k^2 \equiv 2^k - 7 \pmod{2^{k+1}}$. Dans le premier cas, il suffit de prendre $a_{k+1} = a_k$ et dans le second cas, on prend $a_{k+1} = a_k + 2^{k-1}$ si bien que

$$a_{k+1}^2 = a_k^2 + 2^k a_k + 2^{2k-1} \equiv a_k^2 + 2^k a_k \equiv a_k^2 + 2^k \equiv -7 \pmod{2^{k+1}}$$

puisque $k \geqslant 3$ et a_k est impair, ce qui conclut la récurrence.

Finalement, on remarque que la suite $(a_k)_{k\in\mathbb{N}^*}$ n'est pas bornée puisque $a_k^2 \geqslant 2^k - 7$ pour tout $k \in \mathbb{N}^*$. Ceci suffit pour conclure puisque, pour tout $p \geqslant k$, $a_p^2 \equiv -7 \pmod{2^k}$.

---

21. 1ère solution. Supposons qu'il existe des nombres $n_1, n_2, \ldots, n_k$ tels que $2^{n_1}-3, 2^{n_2}-3, \ldots, 2^{n_k}-3$ soient deux à deux premiers entre eux. Montrons qu'on peut alors construire un entier n_{k+1} tel que $2^{n_{k+1}}-3$ soit premier avec tous les nombres $2^{n_i}-3$, $1 \leqslant i \leqslant k$.

On pose $n_{k+1} = (p_1-1)(p_2-1)\cdots(p_r-1)+1$, où $p_1, p_2, \ldots, p_r$ sont les nombres premiers intervenant dans la décomposition de $2^{n_1}-3, \ldots, 2^{n_k}-3$ en facteurs premiers. On a alors $2^{n_{k+1}}-3 = 2\times 2^{(p_1-1)(p_2-1)\cdots(p_r-1)} - 3 \equiv -1 \pmod{p_i}$ pour tout $i = 1, 2, \ldots, k$: en effet, on a $2^{p_i-1} \equiv 1 \pmod{p_i}$ d'après le petit théorème de Fermat. Il s'ensuit que p_i ne divise pas $2^{n_{k+1}}-3$ car $p_i > 2$, ce qui implique que $2^{n_{k+1}}-3$ est premier avec $2^{n_i}-3$, $1 \leqslant i \leqslant k$.

2ème solution. On peut proposer une autre construction : soit $l = (2^{n_1}-3)(2^{n_2}-3)\cdots(2^{n_k}-3)$. Considérons les nombres $2^0, 2^1, \ldots, 2^l$. En effectuant la division euclidienne de ces nombres par l, on obtient $l+1$ restes qui sont strictement inférieurs à l, il y a donc au moins deux restes qui sont égaux et par suite, il existe deux entiers positifs n_r et n_s ($n_r > n_s$) tels que $2^{n_r} - 2^{n_s} = \lambda l$, $\lambda \in \mathbb{N}$, d'où $l \,|\, 2^{n_r - n_s} - 1$. Si on pose $2^{n_r-n_s} - 1 = \alpha l$, le nombre $4\alpha l + 1 = 2^{n_r-n_s+2} - 3$ est premier avec $2^{n_i}-3$, $1 \leqslant i \leqslant k$.

---

22. On montrera de manière plus générale que, si m est un entier positif quelconque, il existe une infinité d'ensembles de n entiers consécutifs tous divisibles par des nombres de la forme a^m, où $a > 1$.

Pour ce faire, on va raisonner par récurrence sur n. La base $n = 1$ est triviale. Si $\{N_1, N_2, \ldots, N_n\}$ est un ensemble de n entiers consécutifs tel que chaque N_i est divisible par un nombre de la forme a_i^m, où $a_i > 1$, on va construire un ensemble de $n+1$ entiers consécutifs tous divisibles par des nombres de la forme a^m : soit $P = \left(\prod_{i=1}^{n} a_i\right)^m$, et soit $N = (N_n + 1)\left[(P+1)^m - 1\right]$. L'ensemble $\{M_1, M_2, \ldots, M_{n+1}\}$, où

$$\begin{cases} M_1 &= N + N_1, \\ M_2 &= N + N_2, \\ & \ldots \\ M_{n+1} &= N + N_n + 1, \end{cases}$$

constitué de $n+1$ entiers consécutifs convient puisque chaque M_i est divisible par a_i^m pour $i = 1, 2, \ldots, n$ et que M_{n+1} est divisible par $(P+1)^m$. Ceci conclut l'étape inductive.

---

23. 1ère solution. On considère $2n$ nombres premiers deux à deux distincts $p_1, p_2, \ldots, p_{2n}$, et on pose $q_1 = p_1p_2$, $q_2 = p_3p_4, \ldots, q_n = p_{2n-1}p_{2n}$.

D'après le théorème chinois, le système :

$$\begin{cases} x \equiv 0 \pmod{q_1}, \\ x \equiv -1 \pmod{q_2}, \\ \ldots \\ x \equiv -(n-1) \pmod{q_n} \end{cases}$$

admet une solution $x \in \mathbb{N}^*$. Aucun nombre des n entiers consécutifs $x, x+1, \ldots, x+n-1$ n'est alors une puissance d'un nombre premier.

2ème solution. Montrons que chacun des n entiers consécutifs $((n+1)!)^2 + k$, où $k = 2, 3, \ldots, n+1$, n'est pas une puissance d'un nombre premier : en effet, supposons que $((n+1)!)^2 + k = p^m$ pour un nombre premier p et un entier $m \geqslant 1$. Comme k divise $(n+1)!$, k divise p^m, et donc $k = p^\alpha$, où $1 \leqslant \alpha \leqslant m$. De plus, k^2 divise $((n+1)!)^2$, et donc $p^{\alpha+1}$ divise $((n+1)!)^2$ ainsi que p^m puisque $\alpha < m$. Ceci est impossible car on aurait alors $p^{\alpha+1}$ qui divise k.

---

24. a) La réponse est non. Supposons qu'une telle succession de nombres naturels existe. On peut d'ores et déjà se concentrer sur ceux parmi ces nombres naturels qui sont impairs puisque les nombres pairs sont divisibles par 2. Si on désigne par k, $k+2$, $k+4$, $k+6$, $k+8$, $k+10$, $k+12$, où k est impair, les sept nombres impairs intervenant dans la succession, alors trois au plus parmi eux sont divisibles par 3, deux au plus sont divisibles par 5, un au plus est divisible par 7 et un au plus est divisible par 11. Ainsi, chaque nombre parmi 3, 5, 7 et 11 divise exactement 3, 2, 1 et 1 termes parmi les sept nombres impairs considérés, et chacun de ces nombres est divisible par au plus un des nombres 3, 5, 7 et 11. Or, ceci est impossible : en effet, k, $k+6$ et $k+12$ doivent être divisibles par 3, et il ne peut y avoir qu'au plus un nombre parmi $k+2$, $k+4$, $k+8$, $k+10$ qui soit divisible par 5.

b) La réponse est oui. Soit n un nombre naturel divisible par $210 = 2\times3\times5\times7$. Si on considère la succession $n-10, n-9, \ldots, n, \ldots, n+9, n+10$, chacun des nombres considérés est divisible par l'un des nombres premiers 2, 3, 5, 7, à l'exception de $n+1$ et $n-1$. Or, on sait, d'après le théorème chinois, qu'il existe des nombres naturels n tels que :

$$\begin{cases} n \equiv 0 \pmod{210}, \\ n \equiv 1 \pmod{13}, \\ n \equiv -1 \pmod{11}, \end{cases}$$

ce qui conclut la preuve.

---

25. On a $xyz \mid (xy-1)(xz-1)(yz-1) = -\left[1-(xy+yz+zx)+x^2yz+y^2xz+z^2xy-(xyz)^2\right]$. Il s'ensuit que $xy+yz+zx-1 = kxyz$, $k \in \mathbb{N}$, ce qui s'écrit encore

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z} = \frac{1}{xyz}+k. \tag{1}$$

L'entier k est nécessairement $\leqslant 2$. Par ailleurs, on peut supposer $x \leqslant y \leqslant z$ et obtenir toutes les solutions en examinant toutes les permutations possibles de x, y et z.

- Si $k=0$ alors $1+\frac{x}{y}+\frac{x}{z} = \frac{1}{yz}$, ce qui est impossible car $1+\frac{x}{y}+\frac{x}{z} > 1$ et $\frac{1}{yz} \leqslant 1$.

- Si $k=1$ alors

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z} = \frac{1}{xyz}+1. \tag{2}$$

On a alors nécessairement $x \leqslant 2$: en effet, si $x \geqslant 3$ alors $\frac{1}{x}+\frac{1}{y}+\frac{1}{z} \leqslant 1$ et $\frac{1}{xyz}+1 > 1$. Si $x=1$ alors (2) s'écrit $\frac{1}{y}+\frac{1}{z} = \frac{1}{yz}$ ce qui est impossible. Si $x=2$ alors

$$(2) \iff \frac{1}{y}+\frac{1}{z} = \frac{1}{2yz}+\frac{1}{2} \iff (y-2)(z-2)=3 \iff y=3,\ z=5.$$

Ainsi, $(2,3,7)$ est solution et toute permutation est aussi solution.

- Si $k=2$ alors (1) s'écrit

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z} = \frac{1}{xyz}+2. \tag{3}$$

Si $x=y=1$ alors $(1,1,z)$ est solution et toute permutation l'est aussi. Si $x=1$ et $y>1$ alors

$$(3) \iff yz-(y+z)+1=0 \iff (y-1)(z-1)=0,$$

ce qui est impossible car $z \geqslant y > 1$. Si finalement $x \geqslant 2$ alors $\frac{1}{x}+\frac{1}{y}+\frac{1}{z} < \frac{3}{2}$ et $\frac{1}{xyz}+2 > 2$ et (3) ne peut être vérifiée.

En conclusion, l'ensemble des solutions est constitué des triplets $(2, 3, 5)$ et $(1, 1, z)$, $z \geqslant 1$, ainsi que de toutes les permutations possibles de x, y et z.

---

26. Si $mn-1$ divise n^3+1, alors $mn-1$ divise $m^3n^3+m^3 = (m^3+1)+(m^3n^3-1)$, ce qui implique que $mn-1$ divise m^3+1. Le problème étudié est donc symétrique et il suffit d'examiner les deux cas : $m = n$ et $m > n$.

Dans le premier cas, on trouve

$$\frac{n^3+1}{n^2-1} = n + \frac{1}{n-1}$$

qui doit donc être un entier. Ceci est vrai si et seulement si $n = 2$.

Dans le second cas, on commence d'abord par remarquer que $n^3 + 1 \equiv 1 \pmod n$ et $mn - 1 \equiv -1 \pmod n$, d'où

$$\frac{n^3+1}{mn-1} \equiv -1 \pmod n.$$

Il existe donc un entier $k \geqslant 0$ tel que $\dfrac{n^3+1}{mn-1} = kn - 1$. Si $n > 1$, on peut écrire $kn - 1 < n + \dfrac{1}{n-1}$, soit encore $(k-1)n < \dfrac{1}{n-1} + 1$, d'où $k = 1$. Il s'ensuit que

$$m = \frac{n^3+n}{n(n-1)} = n + 1 + \frac{2}{n-1},$$

ce qui implique que $n = 2$, $m = 5$ ou $n = 3$, $m = 5$.

Si maintenant $n = 1$, $2/(m-1)$ doit être entier, d'où $m = 2$ ou $m = 3$.

Finalement, on a les neuf solutions : (2,2) ; (2,1) ; (3,1) ; (1,2) ; (1,3) ; (2,5) ; (3,5) ; (5,2) et (5,3).

---

27. On pose

$$R(a, b, c) = \frac{abc-1}{(a-1)(b-1)(c-1)},$$

et on suppose $1 < a < b < c$, et que a, b, c et $R(a, b, c)$ sont tous des entiers.

On remarque d'abord que

$$\begin{aligned} R(a, b, c) &= 1 + \frac{1}{a-1} + \frac{1}{b-1} + \frac{1}{c-1} + \\ &\quad \frac{1}{(a-1)(b-1)} + \frac{1}{(b-1)(c-1)} + \frac{1}{(c-1)(a-1)}, \end{aligned}$$

d'où $R(a, b, c) > 1$. Il est également clair que si $a \geqslant a' > 1$, $b \geqslant b' > 1$, $c \geqslant c' > 1$, alors $R(a, b, c) \leqslant R(a', b', c')$. Remarquons maintenant que $abc - 1$ est impair sauf si a, b et c sont tous impairs, et que $(a-1)(b-1)(c-1)$ est pair sauf si a, b et c sont tous pairs. Comme $R(a, b, c)$ est un entier, il s'ensuit que a, b, c sont, soit tous pairs, soit tous impairs.

Si $a \geqslant 4$, alors $1 < R(a,b,c) \leqslant R(4,6,8) = (4 \times 6 \times 8 - 1)/(3 \times 5 \times 7) = 191/105 < 2$, et $R(a,b,c)$ ne peut pas être entier dans ce cas.

Si $a = 3$, alors $1 < R(a,b,c) \leqslant R(3,5,7) = (3\times5\times7-1)/(2\times4\times6) = 104/48 < 3$, et donc $R(a,b,c) = R(3,b,c) = (3bc-1)/(2(b-1)(c-1)) = 2$, ce qui donne $3bc - 1 = 4(bc - b - c + 1)$, ce que l'on réécrit sous la forme $bc - 4b - 4c + 5 = 0$, soit encore $(b-4)(c-4) = 11$. Ceci implique que $b = 5$ et $c = 15$ puisque 11 est premier et que $5 \leqslant b < c$.

Si $a = 2$, alors $1 < R(a,b,c) \leqslant R(2,4,6) = (2\times4\times6-1)/(1\times3\times5) = 47/15 < 4$, et $R(a,b,c) = R(2,b,c) = 2$ ou 3. Dans le premier cas, $2bc - 1 = 2(b-1)(c-1)$, ce qui est impossible. Dans le second cas, on obtient $2bc - 1 = 3(b-1)(c-1)$, ce qui se réécrit sous la forme $(b-3)(c-3) = 5$. Ceci donne $b = 4$ et $c = 8$ car 5 est premier et $4 \leqslant b < c$.

Finalement, il y a au maximum deux solutions au problème proposé, à savoir $(a,b,c) = (3,5,15)$ et $(a,b,c) = (2,4,8)$. Réciproquement, on vérifie facilement que ces deux triplets conviennent.

---

28. Dire que les 3 derniers chiffres de la représentation décimale de 1978^m sont respectivement égaux aux 3 derniers chiffres de la représentation décimale de 1978^n signifie que

$$1978^m \equiv 1978^n \pmod{1000},$$

ce qui implique que $2^3 \mid 1978^m$ et $5^3 \mid 1978^{n-m} - 1$. Comme $1978 = 2 \times 989$, il s'ensuit que $m \geqslant 3$.

D'un autre côté, $1978^{\varphi(125)} \equiv 1 \pmod{5^3}$, i.e., $1978^{100} \equiv 1 \pmod{5^3}$. Si d est le plus petit exposant strictement positif tel que $1978^d \equiv 1 \pmod{5^3}$, alors d divise 100 (théorème 2.7.3). Afin de réduire le nombre des valeurs candidates pour d, on va examiner la congruence modulo 5. On a manifestement $1978^d \equiv 3^d \equiv 1 \pmod 5$. Par ailleurs, le plus petit entier positif non nul k tel que $3^k \equiv 1 \pmod 5$ est $k = 4$. Par conséquent d est un multiple de 4. On se retrouve donc avec trois valeurs candidates pour d, à savoir 4, 20 ou 100. Mais,

$$\begin{aligned}
&1978 \equiv -22 \pmod{125};\\
&1978^2 \equiv 484 \equiv -16 \pmod{125};\\
&1978^4 \equiv (-16)^2 \equiv 256 \equiv 6 \pmod{125};\\
&1978^{20} \equiv 6^5 \equiv 7776 \equiv 26 \pmod{125}.
\end{aligned}$$

Finalement, $m \geqslant 3$ et $n - m \geqslant 100$, ce qui implique que les valeurs recherchées sont $m = 3$ et $n = 103$.

---

29. Tout nombre naturel dont l'écriture décimale contient $n-1$ chiffres 1 et un chiffre 7 est de la forme :

$$\frac{10^n - 1 + (54 \times 10^i)}{9}, \quad 0 \leqslant i \leqslant n-1.$$

On étudie la divisibilité d'un tel nombre par 7 pour n fixé : 10 étant une racine primitive (voir la définition ci-dessous) modulo 7, on peut effectivement choisir i

de telle sorte que le nombre étudié soit divisible par 7 si on suppose $n \geqslant 7$ non divisible par 6 (où intervient le fait que $n \geqslant 7$?).

Si maintenant n est divisible par 6, alors 6 divise la somme des chiffres du nombre en question qui est donc lui-même divisible par 3.

Il reste à discuter les cas $n = 2$, 3, 4 et 5. Or, 3 ne convient évidemment pas (tout nombre de la forme exigée est divisible par 3) ; 4 ne convient pas puisque $1711 = 29 \times 59$ et $7111 = 13 \times 547$ et 5 ne convient pas non plus puisque $11711 = 7^2 \times 239$, $17111 = 71 \times 241$ et $71111 = 17 \times 47 \times 89$.

$n = 2$ est donc l'unique valeur qui convient.

Note. Soit a un entier premier avec n. a est dit racine primitive modulo n si le plus petit entier strictement positif k tel que $a^k \equiv 1 \pmod{n}$ est égal à $\varphi(n)$. Les racines primitives modulo 7 par exemple sont 3 et 5.

L'intérêt de la notion de racine primitive modulo n est qu'une telle racine a permet de représenter convenablement tous les entiers $\leqslant n$ et premiers avec n puisque

$$a,\, a^2, \ldots, a^{\varphi(n)},$$

sont distincts modulo n et tous premiers avec n. Il s'ensuit que les autres racines primitives modulo n sont les puissances a^k telles que $\big(k, \varphi(n)\big) = 1$.

Le problème de savoir s'il existe une racine primitive modulo n n'est pas facile à résoudre. On énonce sans preuve le résultat : il existe des racines primitives modulo n si et seulement si n est de la forme 2, 4, p^α ou $2p^\alpha$, où p est un nombre premier impair. Ceci étant, la recherche d'une racine primitive lorsque n devient grand peut s'avérer laborieuse.

---

30. 1ère solution. Raisonnons par l'absurde et supposons que m est le plus petit entier > 1 tel que m divise $2^m - 1$. Il est alors clair que m est impair, ce qui permet d'appliquer le théorème d'Euler :

$$2^{\varphi(m)} \equiv 1 \pmod{m}.$$

D'un autre côté, si on pose $d = (m, \varphi(m))$, on sait déjà que $(2^m - 1, 2^{\varphi(m)} - 1) = 2^d - 1$, ce qui montre que $m \,|\, 2^d - 1$, d'où $d \,|\, 2^d - 1$.

Or, $d > 1$ puisque $m > 1$ et $m \,|\, 2^d - 1$. De plus, $d \leqslant \varphi(m) < m$, ce qui contredit l'hypothèse de minimalité imposée à m.

2ème solution. Soit $n > 1$ un entier, et supposons que n divise $2^n - 1$. Soit p le plus petit diviseur premier de n. Il existe un plus petit entier strictement positif k tel que

$$2^k \equiv 1 \pmod{p}.$$

D'après le théorème 2.7.3, k divise $\varphi(p) = p - 1$, ce qui implique que $k < p$. Or,

$$2^n \equiv 1 \pmod{p},$$

d'où $k \,|\, n$, ce qui contredit l'hypothèse de minimalité imposée à p puisque $k > 1$.

Note. Il existe une infinité d'entiers n tels que n divise $2^n + 1$: on pourra en effet essayer de montrer que 3^k divise $2^{3^k}+1$ pour tout $k \in \mathbb{N}$ (récurrence). Le problème 38 des olympiades internationales de 1990 étudie, lui, l'ensemble des entiers n tels que n^2 divise $2^n + 1$.

---

31. Si n se décompose sous la forme $2^s q$, où q est un nombre impair, alors :

$$m^n - 1 = m^{2^s q} - 1 = \left(m^{2^s}\right)^q - 1 = \left(m^{2^s} - 1\right)\left[\left(m^{2^s}\right)^{q-1} + \left(m^{2^s}\right)^{q-2} + \cdots + m^{2^s} + 1\right].$$

On en déduit que $2 \,|\, m^n - 1 \iff 2 \,|\, m^{2^s} - 1$, et comme on cherche le plus petit exposant n, on peut supposer $n = 2^s$. Distinguons deux cas :

- Si $m \equiv 1 \pmod 4$, alors la représentation de m en base 2 se présente sous la forme

$$m = 1\ldots1\underbrace{00\ldots01}_{k \text{ chiffres}},$$

k étant l'exposant maximal tel que $m \equiv 1 \pmod{2^k}$. On a alors $m^2 - 1 = (m-1)(m+1)$ qui est divisible par 2^{k+1} mais pas par 2^{k+2}, et on démontre par récurrence que 2^{k+s} est la plus grande puissance de 2 divisant $m^{2^s} - 1$.

- Si $m \equiv 3 \pmod 4$, alors la représentation de m en base 2 se présente sous la forme

$$m = 1\ldots0\,\underbrace{11\ldots1}_{k \text{ chiffres}},$$

k étant l'exposant maximal tel que $m \equiv -1 \pmod{2^k}$. En utilisant le même argument de récurrence que plus haut, on trouve que 2^{k+s} est la plus grande puissance de 2 divisant $m^{2^s} - 1$.

Finalement, si k est l'invariant défini précédemment, alors le plus petit entier positif n tel que 2^{1989} divise $m^n - 1$ est :

$$n = \begin{cases} 2^{1989-k} & \text{si } k \leqslant 1989, \\ 1 & \text{si } k > 1989. \end{cases}$$

---

32. Par raison de symétrie, on peut supposer que $0 \leqslant x \leqslant y \leqslant z$. On a donc

$$3z^2 \geqslant x^2 + y^2 + z^2 = 1993, \text{ i.e., } z^2 \geqslant 665,\ z \geqslant 26.$$

D'un autre côté, $z^2 \leqslant 1993$ ce qui implique $z \leqslant 44$, et par conséquent $26 \leqslant z \leqslant 44$.

Supposons maintenant que $x+y+z = \alpha^2$ ($\alpha \in \mathbb{N}$). On a alors, d'après l'inégalité de Cauchy-Schwarz,

$$\alpha^4 = (x+y+z)^2 \leqslant 3(x^2+y^2+z^2) = 5979,$$

soit encore $\alpha \leqslant 8$. On a ainsi $6 \leqslant \alpha \leqslant 8$, et comme $x + y + z$ doit être impair, $\alpha = 7$. On a donc $x + y + z = 49$.

Si maintenant on pose $z = 26 + \beta$, où $0 \leqslant \beta \leqslant 18$, alors

$$x^2 + y^2 = 1993 - z^2 = 1317 - 52\beta - \beta^2. \tag{1}$$

D'un autre côté,

$$x^2 + y^2 \leqslant 2y^2 \leqslant 2(23 - \beta)^2 = 1058 - 92\beta + 2\beta^2. \tag{2}$$

De (1) et (2), on obtient $3\beta^2 - 40\beta \geqslant 259$, ce qui est faux puisque $\beta(3\beta - 40) \leqslant 18 \times 14 = 252$.

Note. Le résultat est faux si les nombres x, y et z varient dans $\mathbb{Z}$. En effet,

$$1993 = (-11)^2 + 24^2 + 36^2,$$

mais $-11 + 24 + 36 = 49 = 7^2$.

---

33. On suppose que, pour des entiers m et n distincts tels que $m < n$, les nombres $k^m + 1$ et $k^n + 1$ s'obtiennent l'un à partir de l'autre en inversant l'ordre des chiffres dans leur représentation décimale. On a alors en particulier $k^n + 1 < 10(k^m + 1)$ puisque les deux nombres $k^m + 1$ et $k^n + 1$ ont le même nombre de chiffres.

Si $k > 10$, on a $k^n + 1 \geqslant k^{m+1} + 1 > 10k^m + 10$. On en déduit que, nécessairement, $k \leqslant 10$. De plus $k \neq 10$, d'où $k < 9$.

Par ailleurs, on doit avoir $m \geqslant \dfrac{n}{2}$: en effet, si $2m < n$, alors

$$k^n + 1 \geqslant k^m k^{m+1} > k^m(k^m + 1),$$

ce qui impose $k^m < 10$, d'où $k^m + 1 < 10$ puisque $k^m + 1 \neq 10$. Il s'ensuit que $k^m + 1 = k^n + 1$, ce qui contredit $m < n$.

Ainsi, $m \geqslant n - m$ et on a donc :

$$k^n + 1 > k^n - k^m + k^{n-m} - 1 = (k^{n-m} - 1)(k^m + 1),$$

ce qui impose $k^{n-m} - 1 < 10$, d'où $k^{n-m} - 1 < 9$ puisque $k \neq 10$.

D'un autre côté,

$$(k^n + 1) - (k^m + 1) = (k^{n-m} - 1)k^m$$

est un multiple de 9 (pourquoi ?), ce qui montre que 3 divise k.

Les cas $k = 6$ ou 9 sont impossibles : en effet, si c'était le cas, on aurait nécessairement $n - m = 1$ (car $k^{n-m} - 1 < 9$). Comme

$$k^m + 1 < (k - 1)(k^m + 1) < k^{m+1} + 1 = k^n + 1,$$

il s'ensuit que $k^m + 1$ et $(k - 1)(k^m + 1)$ ont le même nombre de chiffres ; $k^m + 1$ doit donc commencer par le chiffre 1. Mais alors, $k^n + 1$ se termine par 1, ce qui est impossible car k n'est pas un multiple de 10.

Il reste l'unique cas $k = 3$, et $(m, n) = (3, 4)$ est solution dans ce cas puisque $3^3 + 1 = 28$ et $3^4 + 1 = 82$.

---

34. On raisonne par l'absurde et on suppose qu'il existe k, $0 \leqslant k \leqslant n-2$, tel que $k^2 + k + n$ ne soit pas premier. Soit y le plus petit k tel que $k^2 + k + n$ n'est pas premier ; on a alors $y > \sqrt{n/3}$ et pour tout k, $0 \leqslant k \leqslant y - 1$, $k^2 + k + n$ est premier. Pour k, $0 \leqslant k \leqslant y - 1$, on a

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

si bien que $1 \leqslant y - k \leqslant y$ et $y + 1 \leqslant y + k + 1 \leqslant 2y$.

On considère maintenant le plus petit diviseur premier de $y^2 + y + n$ que l'on note q. On a alors $q \leqslant 2y$: en effet, si $q \geqslant 2y+1$ alors $y^2+y+n \geqslant q^2 \geqslant (2y+1)^2 = y^2+y+3y^2+3y+1 > y^2+y+n+3y+1$ puisque $y > \sqrt{n/3}$. Ceci donne $3y+1 \leqslant 0$ ce qui est impossible. Mais comme $q \leqslant 2y$, il existe k, $0 \leqslant k \leqslant y-1$ tel que $q = y - k$ ou $q = y + k + 1$. Il s'ensuit que q divise $k^2 + k + n$, d'où $k^2 + k + n = q$. Or, $y - k \leqslant n - 1 - k < k^2 + k + n = q$ et $y + k + 1 \leqslant n - 2 + k + 1 < k^2 + k + n = q$, d'où la contradiction.

Note. Les entiers n vérifiant cette propriété ne sont pas très nombreux : ce sont 2, 3, 5, 11, 17 et 41. C'est Euler qui fut le premier à considérer les valeurs prises par les polynômes $P_n(x) = x^2 + x + n$ pour x entier, $0 \leqslant x \leqslant n-2$ (pour $x = n-1$, $P_n(n-1) = n^2$ n'est pas un nombre premier). La caractérisation que l'on vient d'énoncer est par contre assez délicate à obtenir : on démontre que n convient si et seulement si l'anneau $\mathbb{Q}\left(\sqrt{1-4n}\right)$ est principal. Or, on sait depuis 1967 que les seules valeurs qui conviennent pour $1 - 4n$ sont -7, -11, -19, -43, -67 et -163, ce qui donne les valeurs précédemment citées de n.

---

35. Pour $n = 2$, le résultat est évident. Supposons la propriété vérifiée pour tout $k \leqslant n - 1$ et posons $n = 2^l m$, où m est impair.

En fait, c'est le facteur impair qui pose problème pour établir l'étape inductive : en effet, la suite $2, 2^2, 2^{2^2}, \ldots$ est constante à partir d'un certain rang modulo 2^l. Il suffit donc d'établir que cette suite est aussi constante à partir d'un certain rang modulo m. Pour ce faire, on va utiliser le théorème d'Euler : $2^{\varphi(m)} \equiv 1 \pmod m$.

Comme $\varphi(m) < n$, l'hypothèse de récurrence s'applique : si on note $a_n = 2^{2^{\cdot^{\cdot^{2}}}}$, où la dernière expression contient n fois le nombre 2, on peut trouver un entier p tel que

$$a_i \equiv a_j \pmod{\varphi(m)}$$

pour tous i, $j \geqslant p$. Si on écrit $a_j = a_i + \alpha\varphi(m)$, où $\alpha \in \mathbb{Z}$, on aura

$$2^{a_j} \equiv 2^{a_i}\left(2^{\varphi(m)}\right)^{\alpha} \equiv 2^{a_i} \pmod m.$$

Ceci montre que la suite $2, 2^2, 2^{2^2}, \ldots$ est constante à partir d'un certain rang modulo m.

D'après le théorème chinois, le système de congruences

$$\begin{cases} x \equiv a \pmod{2^l}, \\ x \equiv b \pmod{m}, \end{cases}$$

admet une unique solution modulo $2^l m = n$. Le résultat en découle immédiatement.

---

36. Soit p le plus petit nombre premier ne divisant pas n. On a alors $a_1 = 1$, $a_k = n-1$ et $a_2 = p$. On désigne par r la différence $a_{i+1} - a_i$, $i = 1, 2, \ldots, k-1$, qui est donc égale à $p-1$.

Si n est impair, alors $a_2 = 2$ et $r = 1$. La progression $(a_i)_i$ est donc $1, 2, \ldots, n-1$. Comme, pour $q < n$, $(q, n) = 1$, il s'ensuit que n est un nombre premier.

Si maintenant n est pair, $p \geqslant 3$. Si $p = 3$, alors $r = 2$, et la progression $(a_i)_i$ est $1, 3, 5, \ldots, n-1$. Comme, pour tout $q < n$ impair, $(q, n) = 1$, il s'ensuit que n est une puissance de 2.

Le cas $p > 3$ est impossible : en effet, si tel est le cas, n serait un multiple de 3. On a par ailleurs $a_k = a_1 + r(k-1)$, ce qui implique que $n - 1 = 1 + (p-1)(k-1)$. Ainsi, $p - 1 \mid n - 2$.

Il s'ensuit que tout nombre premier q divisant $p-1$, serait diviseur à la fois de $n-2$ et de n (car $q < p$). Il s'ensuit que $p - 1 = 2^l$, $l \in \mathbb{N}$, soit encore $p = 2^l + 1$. Or, p étant premier, l n'admet aucun diviseur impair, i.e., $p = 2^{2^t} + 1$, $t \in \mathbb{N}$.

On a donc $a_3 = a_1 + 2r = 1 + 2(p-1) = 2p - 1 = 2^{2^t+1} + 1$, et donc 3 divise a_3. Comme 3 divise n, on a une contradiction avec $(a_3, n) = 1$, ce qui conclut la preuve.

---

37. a) Il suffit de prouver que n^2 ne peut pas s'écrire comme la somme de $n^2 - 13$ carrés parfaits. Si en effet $n^2 = a_1^2 + a_2^2 + \cdots + a_{n^2-13}^2$ alors on doit avoir $1 \leqslant a_i \leqslant 3$, $i = 1, 2, \ldots, n^2 - 13$ si bien que

$$n^2 = \underbrace{1^2 + \cdots + 1^2}_{p \text{ termes}} + \underbrace{2^2 + \cdots + 2^2}_{q \text{ termes}} + \underbrace{3^2 + \cdots + 3^2}_{r \text{ termes}},$$

avec $p + q + r = n^2 - 13$. Il s'ensuit donc que $p + 4q + 9r = n^2$, ce qui implique que $3q + 8r = 13$, ce qui est impossible.

b) On montre que 13 est le plus petit n tel que $S(n) = n^2 - 14$. En effet, les seuls carrés parfaits < 169 qui sont la somme de deux carrés parfaits sont 25 et 100 et il est facile de vérifier qu'ils ne peuvent pas s'écrire sous la forme d'une somme de trois carrés parfaits, i.e., $S(5) = S(10) = 2$.

De plus, pour montrer que $S(13) = 13^2 - 14 = 155$, il faut prouver que 169 peut s'écrire comme la somme de k carrés parfaits pour $1 \leqslant k \leqslant 155$. Pour ce faire, on remarque que $(2r)^2 = r^2 + r^2 + r^2 + r^2$. Ainsi, si n^2 est somme de k carrés parfaits dont $(2r)^2$, alors n^2 peut s'écrire comme la somme de $k+3$ carrés parfaits.

Comme $169 = 8^2 + 8^2 + 4^2 + 4^2 + 3^2$, il s'ensuit que 169 est somme de $2 + 3t$ carrés parfaits pour tout t tel que $1 \leqslant t \leqslant 53$. Par ailleurs, si on remplace 3^2 par

$2^2+2^2+1^2$, le même argument montre que 169 peut s'écrire comme la somme de $1+3t$ carrés parfaits pour tout t tel que $2 \leqslant t \leqslant 56$. Enfin, de $169 = 12^2+4^2+3^2$, il s'ensuit que 169 peut s'écrire comme la somme de $3t$ carrés parfaits pour tout t tel que $1 \leqslant t \leqslant 51$. Il suffit maintenant pour conclure de montrer que 169 est la somme de quatre carrés parfaits, ce qui est vrai : $169 = 10^2+8^2+2^2+1^2$ par exemple.

c) On démontre que si $S(n) = n^2-14$, alors $S(2n) = 4n^2-14$. On part toujours de la remarque $(2r)^2 = r^2+r^2+r^2+r^2$, ce qui implique que $(2n)^2$ peut s'écrire comme la somme de $1, 2, \ldots, 4n^2-56$ carrés parfaits, soit encore $S(2n) \geqslant 4n^2-56$. Or, $4n^2$ peut s'écrire comme la somme de $3n^2+k$ carrés parfaits, avec $1 \leqslant k \leqslant n^2-14$:

$$\begin{aligned} 4n^2 &= \underbrace{1^2+1^2+\cdots+1^2}_{3n^2 \text{ termes}}+n^2 \\ &= \underbrace{1^2+1^2+\cdots+1^2}_{3n^2 \text{ termes}}+a_1^2+\cdots+a_k^2. \end{aligned}$$

Comme $n \geqslant 13$, on a $4n^2-56 > 3n^2$, ce qui montre que $S(2n) = 4n^2-14$ et termine la démonstration.

---

38. Il est facile de constater que $n=3$ est une solution. Montrons que c'est la seule. Toute solution n s'écrit sous la forme $n = 3^k l$, où k est un entier $\geqslant 0$ et l est un nombre premier avec 3. On a alors

$$2^n+1 = \left(2^l\right)^{3^k}+1 = \left(2^l+1\right)\prod_{i=0}^{k-1}\left(\left(2^{3^i l}\right)^2 - 2^{3^i l}+1\right).$$

Cette identité se découvre en examinant les petites valeurs de k : $x^3+1 = (x+1)(x^2-x+1)$, $x^9+1 = \left(x^3+1\right)\left(x^6-x^3+1\right) = (x+1)\left(x^2-x+1\right)\left(x^6-x^3+1\right)$, et ainsi de suite.

On montre maintenant que, pour tout entier impair q, $2^{2q}-2^q+1 \equiv 3 \pmod 9$: en effet, ceci équivaut à $2^{2q-1}-2^{q-1}-1 \equiv 0 \pmod 9$. Or, si $q = 2t+1$, où t est un entier, alors ceci se réécrit sous la forme $2^{4t+1}-2^{2t}-1 \equiv 0 \pmod 9$. Comme par ailleurs $2^{4t+1}-2^{2t}-1 = \left(2^{2t+1}+1\right)\left(2^{2t}-1\right)$, et $3 \mid 2^{2t}-1$, $2^{2t+1}+1$, on a acquis le résultat désiré.

Il s'ensuit que 3^k divise $\prod_{i=0}^{k-1}\left(\left(2^{3^i l}\right)^2-2^{3^i l}+1\right)$, mais pas 3^{k+1}. On en déduit que $3^k \mid 2^l+1$, mais puisque 9 ne divise pas 2^l+1 (car $(l,3)=1$), il s'ensuit que les seules valeurs possibles de k sont 0 ou 1.

Il reste maintenant à prouver que $l=1$. Si on avait $l>1$, on pourrait considérer l'un de ses facteurs premiers, disons p. On a donc forcément $p \geqslant 5$ puisque l est impair et premier avec 3. On a alors $2^n \equiv -1 \pmod p$, soit encore $2^{2n} \equiv 1 \pmod p$. D'un autre côté, on a d'après le petit théorème de Fermat $2^{p-1} \equiv 1 \pmod p$. On en déduit que $p \mid 2^\delta - 1$, où $\delta = (p-1, 2n)$. Comme $(p-1, l) = 1$, δ doit diviser 6. Ceci limite les valeurs possibles de p aux diviseurs premiers de 3, 7 ou 63. On a donc forcément $p = 7$.

Il suffit maintenant pour conclure de montrer que 7 ne divise pas un nombre de la forme $2^n + 1$. Or, ceci est immédiat puisque $2^3 \equiv 1 \pmod 7$, ce qui montre que les restes possibles de la division de $2^n + 1$ par 7 sont 2, 3 ou 5.

---

39. On commence par démontrer qu'il existe un entier positif k tel que $k \cdot 2^n + 1$ est composé pour tous les termes n d'une progression arithmétique.

En effet, si $(a + bm)_{m\in\mathbb{N}}$ est une telle progression, avec $0 \leqslant a < b$, on considère un diviseur premier p de $2^b - 1$ et on prend

$$k \equiv -2^{b-a} \pmod p.$$

On a donc, si $n = a + bm$,

$$k \cdot 2^n + 1 \equiv -2^{b-a}2^{a+bm} + 1 \equiv 0 \pmod p,$$

d'où le résultat souhaité.

Pour démontrer le résultat de l'énoncé, il suffit de construire une suite finie de triplets (p_i, a_i, b_i) telle que $0 \leqslant a_i < b_i$, $2^{b_i} \equiv 1 \pmod{p_i}$ où les p_i sont des nombres premiers distincts, et telle que tout entier n satisfait à l'une au moins des congruences $n \equiv a_i \pmod{b_i}$: en effet, il suffirait alors d'utiliser le théorème chinois pour affirmer que le système de congruences $k \equiv -2^{b_i - a_i} \pmod{p_i}$ admet au moins une solution k.

Pour que tout entier n satisfasse à l'une au moins des congruences $n \equiv a_i \pmod{b_i}$, il suffit de prouver que tout n, $0 \leqslant n \leqslant [b_1, b_2, \ldots] - 1$, l'une au moins des congruences $n \equiv a_i \pmod{b_i}$ est vérifiée. Si on prend comme plus petit commun multiple des b_i le nombre 24, on a les choix suivants pour b_i : 2, 3, 4, 6, 8, 12 et 24. Le choix d'un b_i peut interdire le choix d'un autre nombre puisque les p_i doivent être distincts. Après quelques tentatives, on arrive à une solution possible :

b_i	2	3	4	8	12	24
a_i	0	0	1	3	7	23
p_i	3	7	5	17	13	241

---

40. Pour $n = 3$, on peut prendre $x_3 = y_3 = 1$.

Supposons maintenant qu'il existe des entiers positifs impairs x_n et y_n tels que $7x_n^2 + y_n^2 = 2^n$. On va prouver que pour chacun des deux couples

$$\left(X = \frac{x_n + y_n}{2}, \quad Y = \frac{|7x_n - y_n|}{2}\right) \quad \text{et} \quad \left(X = \frac{|x_n - y_n|}{2}, \quad Y = \frac{7x_n + y_n}{2}\right)$$

on a $7X^2 + Y^2 = 2^{n+1}$: en effet,

$$7\Big(\frac{x_n \pm y_n}{2}\Big)^2 + \Big(\frac{7x_n \mp y_n}{2}\Big)^2 = 2(7x_n^2 + y_n^2) = 2 \times 2^n = 2^{n+1}.$$

Comme x_n et y_n sont impairs, i.e., $x_n = 2k + 1$ et $y_n = 2l + 1$ (k, l entiers), alors $\dfrac{x_n + y_n}{2} = k + l + 1$ et $\dfrac{|x_n - y_n|}{2} = |k - l|$, ce qui montre que l'un des deux nombres $\dfrac{x_n + y_n}{2}$ et $\dfrac{|x_n - y_n|}{2}$ est impair. Ainsi, il existe des entiers impairs x_{n+1} et y_{n+1} tels que $7x_{n+1}^2 + y_{n+1}^2 = 2^{n+1}$, ce qui conclut la récurrence.

---

41. 1ère solution. Cette solution a valu un prix spécial à Emanouil Atanassov.

On raisonne par l'absurde et on suppose qu'il existe des couples $(a, b) \in (\mathbb{N}^*)^2$ tels que $(a^2 + b^2)/(1 + ab)$ soit un entier mais pas un carré parfait. De l'ensemble de tous ces couples, choisissons un couple tel que $\max(a, b)$ est minimal. Posons enfin $k = (a^2 + b^2)/(1 + ab)$. On a alors $a \neq b$ puisque $a = b$ donnerait $k < 2$, d'où $k = 1$ qui est un carré parfait. Sans nuire à la généralité, on peut supposer que $a > b$. L'équation

$$a^2 + b^2 - k(1 + ab) = a^2 - kba + (b^2 - k) = 0$$

d'inconnue a possède deux racines. Si on désigne par a' l'autre racine de cette équation, alors $(a')^2 + b^2 = k(a'b + 1)$, et

$$a' = \frac{b^2 - k}{a} < \frac{b^2 - k}{b} < b$$

si bien que $\max(a', b) = b < a = \max(a, b)$, d'où la contradiction.

2ème solution. Soient a et b deux entiers strictement positifs tels que $(a^2 + b^2)/(1 + ab) = n$ soit un entier. Si $a = b$, alors $a = b = 1$ et l'assertion à prouver est évidente. Supposons donc que $1 < b < a$, et posons $a_1 = b$ et $a_2 = a$. On définit maintenant la suite $(a_k)_{k \in \mathbb{Z}}$ indexée par $\mathbb{Z}$ de la manière suivante :

$$\begin{cases} a_{k+2} = na_{k+1} - a_k & \text{si } k \geqslant 1, \\ a_k = na_{k+1} - a_{k+2} & \text{si } k \leqslant 0. \end{cases}$$

On a alors, pour tout $k \in \mathbb{Z}$,

$$\frac{a_{k+2}^2 + a_{k+1}^2}{a_{k+2}a_{k+1} + 1} = n.$$

Par ailleurs, comme $n > 1$, la suite $(a_k)_{k \in \mathbb{Z}}$ est strictement croissante, et donc $\lim\limits_{k \to -\infty} a_k = -\infty$. Comme n est strictement positif, il résulte de la dernière formule qu'il ne peut exister d'indice i tel que $a_i > 0$ et $a_{i-1} < 0$; la suite $(a_k)_{k \in \mathbb{Z}}$ doit donc forcément passer par 0. Si alors $a_{i-1} = 0$ pour un certain indice i, on obtient $n = a_i^2$, d'où le résultat.

Note. Il n'est pas très difficile d'adapter la première solution pour établir la généralisation suivante : si a, b, c sont trois entiers naturels non nuls tels que $0 < a^2 + b^2 - abc \leqslant c$, alors $a^2 + b^2 - abc$ est un carré parfait (dans le problème initial, on avait $a^2 + b^2 - abc = c$).

3

SUITES ET POLYNÔMES

Dans un souci de clarté, et afin d'éviter toute solution astucieuse mais artificielle, on a décidé de présenter ici au lecteur désireux d'approfondir ses connaissances sur les suites et les polynômes un petit nombre d'idées et de résultats pouvant s'avérer utiles dans les olympiades nationales et internationales.

On commence par examiner quelques propriétés générales concernant les suites numériques avant de se concentrer un peu sur la suite de Fibonacci, suite faisant sans cesse son apparition dans les compétitions mathématiques. On définit ensuite l'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans un corps commutatif $\mathbb{K}$ et on étudie ses propriétés « arithmétiques ». On s'intéresse enfin aux polynômes irréductibles lorsque $\mathbb{K} = \mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$, ainsi qu'aux problèmes d'interpolation.

3.1. Les suites numériques

Une suite numérique est une application de $\mathbb{N}$ (ou parfois $\mathbb{N}^*$) dans $\mathbb{R}$ ou $\mathbb{C}$ que l'on note souvent $(u_n)_{n\in\mathbb{N}}$ au lieu de

$$\begin{array}{rccl} u\colon & \mathbb{N} & \longrightarrow & \mathbb{R} \text{ (ou } \mathbb{C}) \\ & n & \longmapsto & u(n). \end{array}$$

3.1.1. Limite d'une suite. On dit qu'une suite numérique $(u_n)_{n\in\mathbb{N}}$ converge vers l si :

$$\forall \delta > 0,\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N}, \qquad (n \geqslant N \Longrightarrow |u_n - l| \leqslant \delta).$$

l est alors appelé limite de la suite $(u_n)_{n\in\mathbb{N}}$.

Théorème. *Si une suite numérique $(u_n)_{n\in\mathbb{N}}$ converge vers l_1 et vers l_2, alors $l_1 = l_2$.*

♦ **Preuve.** Si $l_1 \neq l_2$, posons $\delta = \dfrac{1}{2}|l_2 - l_1|$. Puisque $(u_n)_{n\in\mathbb{N}}$ converge vers l_1 et vers l_2, il existe $N_1, N_2 \in \mathbb{N}$ tels que :

$$\forall n \in \mathbb{N}, \qquad \begin{cases} n \geqslant N_1 & \Longrightarrow \quad |u_n - l_1| < \delta, \\ n \geqslant N_2 & \Longrightarrow \quad |u_n - l_2| < \delta. \end{cases}$$

Si $N = \max(N_1, N_2)$, alors

$$\begin{cases} |u_N - l_1| < \delta, \\ |u_N - l_2| < \delta, \end{cases}$$

et il s'ensuit que

$$|l_2 - l_1| \leqslant |l_2 - u_N| + |u_N - l_1| < 2\delta = |l_2 - l_1|,$$

d'où la contradiction.

□

On utilisera désormais le symbole $\lim\limits_{n\to+\infty} u_n$ pour désigner la limite de la suite $(u_n)_{n\in\mathbb{N}}$.

Théorème. *(théorème d'encadrement) Soient $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ trois suites réelles telles que :*

$$\begin{cases} \exists N \in \mathbb{N}, \quad \forall n \in \mathbb{N}, \qquad (n \geqslant N \quad \Longrightarrow \quad u_n \leqslant v_n \leqslant w_n), \\ (u_n)_{n\in\mathbb{N}} \text{ et } (w_n)_{n\in\mathbb{N}} \text{ convergent vers une même limite } l. \end{cases}$$

Alors $(v_n)_{n\in\mathbb{N}}$ converge également vers l.

♦ **Preuve.** Soit $\delta > 0$; il existe $N_1, N_2 \in \mathbb{N}$ tels que :

$$\begin{cases} \forall n \in \mathbb{N}, & (n \geqslant N_1 \quad \Longrightarrow \quad |u_n - l| \leqslant \delta), \\ \forall n \in \mathbb{N}, & (n \geqslant N_2 \quad \Longrightarrow \quad |w_n - l| \leqslant \delta). \end{cases}$$

On pose alors $N_0 = \max(N, N_1, N_2)$, et il s'ensuit que pour tout $n \in \mathbb{N}$:

$$n \geqslant N_0 \quad \Longrightarrow \quad -\delta \leqslant u_n - l \leqslant v_n - l \leqslant w_n - l \leqslant \delta \quad \Longrightarrow \quad |v_n - l| \leqslant \delta,$$

ce qui implique que $(v_n)_{n\in\mathbb{N}}$ converge et a l pour limite.

□

On établit sans peine le théorème suivant :

Théorème. *Soient $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ deux suites convergentes, et α un réel quelconque. Si $\lim\limits_{n\to+\infty} u_n = l$ et $\lim\limits_{n\to+\infty} v_n = l'$, alors*

$$\lim_{n\to+\infty} u_n + v_n = l + l', \qquad \lim_{n\to+\infty} \alpha u_n = \alpha l, \qquad \lim_{n\to+\infty} u_n v_n = ll'.$$

Si de plus $l' \neq 0$, alors $v_n \neq 0$ pour n assez grand et

$$\lim_{n\to+\infty} \frac{1}{v_n} = \frac{1}{l'}, \qquad \lim_{n\to+\infty} \frac{u_n}{v_n} = \frac{l}{l'}.$$

On dit qu'une suite réelle $(u_n)_{n\in\mathbb{N}}$ est croissante (resp. strictement croissante) si :

$$\forall n \in \mathbb{N}, \quad u_n \leqslant \text{ (resp. } <) \; u_{n+1},$$

et on dit qu'elle est décroissante (resp. strictement décroissante) si :

$$\forall n \in \mathbb{N}, \quad u_n \geqslant \text{ (resp. } >) \; u_{n+1}.$$

On dit qu'une suite $(u_n)_{n\in\mathbb{N}}$ est périodique de période $m \in \mathbb{N}$ si :

$$\forall n \in \mathbb{N}, \quad u_{n+m} = u_n.$$

Théorème. *Toute suite réelle croissante (resp. décroissante) et majorée (resp. minorée) est convergente.*

♦ **Preuve.** Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle supposée croissante et majorée, quitte à la remplacer par son opposée. L'ensemble $\{u_n \mid n \in \mathbb{N}\}$ est alors une partie de $\mathbb{R}$ non vide et majorée ; il admet donc une borne supérieure, notée l.

Soit $\delta > 0$. Par définition de la borne supérieure, il existe $N \in \mathbb{N}$ tel que :

$$l - \delta \leqslant u_N \leqslant l.$$

Il s'ensuit que

$$\forall n \in \mathbb{N}, \quad (n \geqslant N \quad \Longrightarrow \quad l - \delta \leqslant u_N \leqslant u_n \leqslant l \quad \Longrightarrow \quad |u_n - l| \leqslant \delta),$$

ce qui implique $\lim\limits_{n\to+\infty} u_n = l$.

□

♦ **Exemples.**

1. On définit la suite $(u_n)_{n\in\mathbb{N}^*}$ par :

$$u_n = 1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2}.$$

La suite $(u_n)_{n\in\mathbb{N}^*}$ est croissante, et

$$u_n = 1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2} \leqslant 1 + \sum_{k=2}^{n} \frac{1}{k(k-1)} = 1 + \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k}\right) < 2.$$

et il s'ensuit que $(u_n)_{n\in\mathbb{N}^*}$ converge vers une limite $\leqslant 2$.

2. Soit la suite $(x_n)_{n\in\mathbb{N}}$ définie par :

$$\begin{cases} x_0 = 0, \\ x_{n+1} = \sqrt{4 + 3x_n}, \quad n = 0, 1, 2, \ldots \end{cases}$$

Il est facile de voir par récurrence que $0 \leqslant x_n < 4$, $\forall n \in \mathbb{N}$. Il en résulte que $x_{n+1} > x_n$ pour $n \in \mathbb{N}$, et donc que $(x_n)_{n\in\mathbb{N}}$ converge vers une limite que l'on note l. On a alors

$$l = \sqrt{4 + 3l} \quad \Longrightarrow \quad l = -1 \text{ ou } l = 4,$$

et la valeur admissible est la valeur positive. La suite $(x_n)_{n\in\mathbb{N}}$ converge et admet pour limite $l = 4$.

3.1.2. Suites adjacentes. Deux suites réelles $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ sont dites adjacentes si $(u_n)_{n\in\mathbb{N}}$ est croissante, $(v_n)_{n\in\mathbb{N}}$ est décroissante et $\lim\limits_{n\to+\infty}(v_n - u_n) = 0$.

Théorème. *Si deux suites réelles $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ sont adjacentes, alors elles sont convergentes et ont la même limite. De plus, si l est la limite commune de ces deux suites, alors :*

$$\forall n \in \mathbb{N}, \quad u_n \leqslant u_{n+1} \leqslant l \leqslant v_{n+1} \leqslant v_n.$$

♦ **Preuve.** On pose, pour tout $n \in \mathbb{N}$: $w_n = v_n - u_n$. La suite $(w_n)_{n\in\mathbb{N}}$ est alors décroissante car :

$$w_{n+1} - w_n = (v_{n+1} - v_n) - (u_{n+1} - u_n) \leqslant 0.$$

Comme cette suite converge vers 0, on déduit que pour tout $n \in \mathbb{N}$, $u_n \leqslant v_n$. Il s'ensuit que

$$\forall n \in \mathbb{N}, \quad u_n \leqslant u_{n+1} \leqslant v_{n+1} \leqslant v_n.$$

D'un autre côté, $(u_n)_{n\in\mathbb{N}}$ est croissante majorée par v_0, donc converge vers une limite notée l. De même, $(v_n)_{n\in\mathbb{N}}$ est décroissante minorée par u_0, donc converge vers une limite notée l'. Mais comme $\lim\limits_{n\to+\infty} w_n = 0$, il s'ensuit que $l = l'$, de sorte que :

$$\forall n \in \mathbb{N}, \quad u_n \leqslant u_{n+1} \leqslant l \leqslant v_{n+1} \leqslant v_n.$$

□

♦ **Exemples.**

1. On considère les deux suites $(u_n)_{n\in\mathbb{N}^*}$ et $(v_n)_{n\in\mathbb{N}^*}$ définies par :

$$u_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}; \qquad v_n = u_n + \frac{1}{n \cdot n!}.$$

Il est clair que $(u_n)_{n\in\mathbb{N}^*}$ est strictement croissante et que $\lim\limits_{n\to+\infty}(v_n - u_n) = 0$. De plus,

$$\forall n \in \mathbb{N}^*, \quad v_{n+1} - v_n = \frac{-1}{n(n+1)(n+1)!} < 0,$$

et donc $(v_n)_{n\in\mathbb{N}^*}$ est strictement décroissante.

Ainsi, les deux suites $(u_n)_{n\in\mathbb{N}^*}$ et $(v_n)_{n\in\mathbb{N}^*}$ sont adjacentes. Leur limite commune est notée e, base des logarithmes népériens.

On se propose de démontrer que e est irrationnel : en effet, si $e = \dfrac{p}{q}$, $(p,q) \in \mathbb{N}^* \times \mathbb{N}^*$, alors

$$u_q < e < v_q \iff u_q < \frac{p}{q} < u_q + \frac{1}{q \cdot q!} \iff q!u_q < p(q-1)! < q!u_q + \frac{1}{q},$$

où $q!u_q$ est un entier, d'où la contradiction.

2. Soient a et b des nombres réels vérifiant $0 < a \leqslant b$, et $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ les suites positives définies par les relations de récurrence :

$$u_{n+1} = \sqrt{u_n v_n}, \qquad v_{n+1} = \frac{u_n + v_n}{2}, \quad n = 0, 1, 2, \ldots$$

avec $u_0 = a$ et $v_0 = b$.

Remarquons d'abord que $u_0 \leqslant v_0$ et que pour $n \in \mathbb{N}$,

$$u_{n+1} = \sqrt{u_n v_n} \leqslant \frac{u_n + v_n}{2} = v_{n+1}.$$

Il s'ensuit que la suite $(u_n)_{n\in\mathbb{N}}$ est croissante et que la suite $(v_n)_{n\in\mathbb{N}}$ est décroissante.

D'un autre côté, $(u_n)_{n\in\mathbb{N}}$ est croissante majorée par v_0 donc converge vers une limite que l'on note l_1. De même, $(v_n)_{n\in\mathbb{N}}$ est décroissante minorée par u_0 donc converge vers une limite notée l_2. Comme

$$v_{n+1} = \frac{u_n + v_n}{2},$$

il s'ensuit que $l_1 = l_2$. Ainsi, les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont adjacentes, et leur limite commune est appelée moyenne arithmético-géométrique de a et b.

3.1.3. Suites récurrentes. On s'intéresse dans ce paragraphe aux suites définies par des récurrences affines du premier ou du second ordre à coefficients constants.

• Soit $(u_n)_{n\in\mathbb{N}}$ une suite pour laquelle il existe $(a, b) \in \mathbb{C}^2$ tel que :

$$\forall n \in \mathbb{N}, \quad u_{n+1} = au_n + b. \tag{3.1}$$

- Si $a = 0$, alors $\forall n \in \mathbb{N}$, $u_n = b$.

- Si $a = 1$,alors $\forall n \in \mathbb{N}$, $u_n = u_0 + nb$.

- Si $a \neq 0$ et $a \neq 1$, on a $u_{n+1} = au_n + b \iff v_{n+1} = av_n$, où $v_n = u_n + \dfrac{b}{a-1}$.
Il s'ensuit que

$$\forall n \in \mathbb{N}, \quad u_n = a^n\Big(u_0 + \frac{b}{a-1}\Big) - \frac{b}{a-1}.$$

• On s'intéresse maintenant à des récurrences linéaires du second ordre à coefficients constants :

$$\forall n \in \mathbb{N}, \quad u_{n+2} = au_{n+1} + bu_n, \tag{3.2}$$

où $(a, b) \in \mathbb{C}^2$.

On commence par rechercher des solutions de la forme $u_n = r^n$, $n \in \mathbb{N}$. La suite $(r^n)_{n\in\mathbb{N}}$ est solution si et seulement si :

$$r^2 - ar - b = 0.$$

Cette équation du second degré, d'inconnue $r \in \mathbb{C}$, est appelée l'équation caractéristique associée à l'équation de récurrence.

- Si l'équation caractéristique admet deux solutions distinctes r_1 et r_2 dans $\mathbb{C}$, alors toute solution se met sous la forme :

$$\forall n \in \mathbb{N}, \quad u_n = \alpha r_1^n + \beta r_2^n. \tag{3.3}$$

En effet, l'ensemble des suites solutions est un espace vectoriel en bijection avec $\mathbb{C}^2$ par l'application linéaire $(u_n)_{n\in\mathbb{N}} \longmapsto (u_0, u_1)$, donc il est de dimension 2, et $\big((r_1^n)_{n\in\mathbb{N}}, (r_2^n)_{n\in\mathbb{N}}\big)$ en est une base.

- Si l'équation caractéristique admet une solution double $r \in \mathbb{C}$, alors toute suite solution se met sous la forme :

$$\forall n \in \mathbb{N}, \quad u_n = \alpha \cdot r^n + \beta n \cdot r^n = (\alpha + \beta n) r^n. \tag{3.4}$$

En effet, $\big((r^n)_{n\in\mathbb{N}}, (nr^n)_{n\in\mathbb{N}}\big)$ est une base de l'espace vectoriel des suites solutions.

• Étudions enfin les récurrences affines du second ordre. Soit $(u_n)_{n\in\mathbb{N}}$ une suite pour laquelle il existe $(a, b, c) \in \mathbb{C}^3$ tel que :

$$\forall n \in \mathbb{N}, \quad u_{n+2} = au_{n+1} + bu_n + c. \tag{3.5}$$

- Si $a + b \neq 1$, on a $u_{n+2} = au_{n+1} + bu_n + c \iff v_{n+2} = av_{n+1} + bv_n$, où $v_n = u_n + \dfrac{c}{a+b-1}$, ce qui résout le problème.

- Si $a + b = 1$, on se ramène à une récurrence affine du premier ordre en considérant la suite $(v_n)_{n\in\mathbb{N}}$, définie par $\forall n \in \mathbb{N}$, $v_n = u_{n+1} - u_n$.

♦ **Exemples.**

1. (*Problème des tours de Hanoi*) On dispose de trois tiges verticales, sur l'une d'entre elles sont enfilés n disques, aucun n'étant posé sur un plus petit. On veut transférer ces disques de la tige où ils se trouvent jusqu'à une autre tige, en respectant la condition de les prendre un par un et ne jamais en poser un sur un disque plus petit. Quel est le nombre minimum des manipulations nécessaires pour reformer la pile sur une autre tige ?

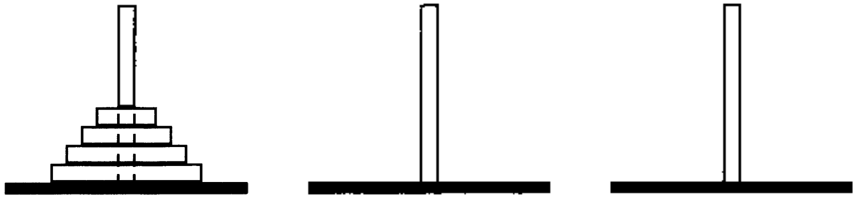


FIG. 3.1.

Ce problème a été popularisé par Édouard Lucas[1] qui l'a formulé et étudié en 1883. Si la pile initiale contient n disques ($n \geqslant 1$), on désigne par a_n le nombre recherché. Il est alors immédiat que $a_1 = 1$ et $a_2 = 3$.

1. Édouard Lucas (1842-1891), mathématicien français.

Si la tige initiale contient n disques, on doit commencer par transférer les $n-1$ premiers disques en a_{n-1} manipulations vers une autre tige. On transfère ensuite le dernier disque vers la seule tige vide, puis on déplace les $n-1$ disques précédemment transférés vers cette tige en a_{n-1} manipulations. Il s'ensuit que :

$$a_n = 2a_{n-1} + 1,$$

ce qui se résout sans peine :

$$a_n = 2^{n-1} + 2^{n-2} + \cdots + 2 + 1 = 2^n - 1, \quad n = 1, 2, \ldots$$

3.1.4. La suite de Fibonacci. La suite de Fibonacci[2] est définie par :

$$\begin{cases} F_0 = 0, \ F_1 = 1, \\ F_n = F_{n-1} + F_{n-2} \text{ si } n \geqslant 2, \end{cases}$$

Les premiers termes de cette suite sont : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, … Ces nombres sont appelés les nombres de Fibonacci.

L'équation caractéristique associée à cette relation de récurrence est : $r^2 - r - 1 = 0$, dont les racines sont

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}.$$

Il s'ensuit que

$$\forall n \in \mathbb{N}, \quad F_n = a\Big(\frac{1+\sqrt{5}}{2}\Big)^n + b\Big(\frac{1-\sqrt{5}}{2}\Big)^n,$$

où a et b sont tels que

$$a + b = 0, \quad a\Big(\frac{1+\sqrt{5}}{2}\Big) + b\Big(\frac{1-\sqrt{5}}{2}\Big) = 1.$$

On en déduit la formule de Binet[3] : pour tout $n \in \mathbb{N}$,

$$\boxed{F_n = \frac{1}{\sqrt{5}}\left[\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\right].} \tag{3.6}$$

♣ **Quelques conséquences de la formule de Binet.** Si on pose $\alpha = (1+\sqrt{5})/2$ et $\beta = (1-\sqrt{5})/2$, alors

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n = 0, 1, 2, \ldots$$

d'où,

$$\frac{F_{n+k}}{F_n} = \frac{\alpha^{n+k} - \beta^{n+k}}{\alpha^n - \beta^n} = \frac{\alpha^{n+k}\{1 - (\beta/\alpha)^{n+k}\}}{\alpha^n\{1 - (\beta/\alpha)^n\}}.$$

2. Leonardo Fibonacci (1175-1230), mathématicien italien.

3. Jacques Binet (1786-1856), mathématicien français.

Comme $|\beta/\alpha| < 1$, il s'ensuit que $\lim\limits_{n\to+\infty} (\beta/\alpha)^n = 0$, et donc

$$\boxed{\lim_{n\to+\infty} \frac{F_{n+k}}{F_n} = \alpha^k,} \tag{3.7}$$

pour tout entier positif fixé k.

D'un autre côté, si n est un entier positif alors

$$\sum_{k=0}^{n} \binom{n}{k} F_k = F_{2n}. \tag{3.8}$$

Cette formule est due à Cesaro[4] et on va la démontrer à l'aide de la formule de Binet :

$$\sum_{k=0}^{n} \binom{n}{k} F_k = \frac{1}{\alpha-\beta}\left[\sum_{k=0}^{n} \binom{n}{k}\alpha^k - \sum_{k=0}^{n} \binom{n}{k}\beta^k\right] = \frac{1}{\alpha-\beta}\big[(1+\alpha)^n - (1+\beta)^n\big].$$

Mais, comme $\alpha^2 - \alpha - 1 = \beta^2 - \beta - 1 = 0$, on en déduit que :

$$\sum_{k=0}^{n} \binom{n}{k} F_k = \frac{\alpha^{2n} - \beta^{2n}}{\alpha - \beta} = F_{2n}.$$

♣ **Les formules de sommation.** On établit facilement par récurrence les formules suivantes :

$$\boxed{\sum_{k=1}^{n} F_k = F_{n+2} - 1, \qquad \sum_{k=0}^{n} F_{2k} = F_{2n+1}, \qquad \sum_{k=0}^{n} F_{2k+1} = F_{2n+2}.} \tag{3.9}$$

♣ **Une approche matricielle.** On considère la matrice :

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_2 & F_1 \\ F_1 & F_0 \end{pmatrix}.$$

On prouve immédiatement par récurrence que

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}, \quad n \geqslant 1,$$

ce qui permet d'établir plusieurs identités faisant intervenir les nombres de Fibonacci. En particulier, si $\det A$ désigne le déterminant d'une matrice carrée A, alors

$$\det Q^n = (\det Q)^n = (-1)^n,$$

ce qui conduit à l'identité

$$\boxed{F_{n+1}F_{n-1} - F_n^2 = (-1)^n,} \tag{3.10}$$

4. Ernesto Cesaro (1859-1906), mathématicien italien.

qui peut aussi être établie directement par récurrence.

D'un autre côté, $Q^n \cdot Q^{m-1} = Q^{m+n-1}$, ce qui s'écrit encore :

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \begin{pmatrix} F_m & F_{m-1} \\ F_{m-1} & F_{m-2} \end{pmatrix} = \begin{pmatrix} F_{m+n} & F_{m+n-1} \\ F_{m+n-1} & F_{m+n-2} \end{pmatrix},$$

soit encore

$$\boxed{F_{m+n} = F_{m-1}F_n + F_mF_{n+1},} \tag{3.11}$$

valable en fait dès que $m \geqslant 1$ et $n \geqslant 0$.

En particulier, pour $m = n+1$, $n \geqslant 0$:

$$F_{2n+1} = F_n^2 + F_{n+1}^2. \tag{3.12}$$

♣ Propriétés arithmétiques des $\mathbf{F_n}$.

Théorème. *Si m divise n ($m \in \mathbb{N}^*$ et $n \in \mathbb{N}$), alors F_m divise F_n.*

♦ **Preuve.** En effet, fixons $m \geqslant 1$ et faisons une récurrence sur $k \geqslant 0$ afin de prouver que F_m divise F_{km}.

Supposons donc que F_m divise F_{km} pour un certain $k \geqslant 0$. Comme,

$$F_{(k+1)m} = F_{m-1}F_{km} + F_mF_{km+1},$$

il s'ensuit que F_m divise $F_{(k+1)m}$, d'où le résultat.

□

Théorème. *Soient m et n deux entiers strictement positifs. On a alors*

$$(F_m, F_n) = F_{(m,n)}. \tag{3.13}$$

♦ **Preuve.** Comme $(m,n) \,|\, m$ et $(m,n) \,|\, n$, alors $F_{(m,n)} \,|\, F_m$ et $F_{(m,n)} \,|\, F_n$, et il s'ensuit que

$$F_{(m,n)} \,|\, (F_m, F_n).$$

D'un autre côté, le théorème de Bézout assure l'existence de deux entiers u et v tels que :

$$um + vn = (m,n),$$

et, quitte à intervertir m et n, on peut supposer $u \leqslant 0$ et donc $v \geqslant 1$, ce qui permet d'écrire

$$F_{vn} = F_{(m,n)-1}F_{-um} + F_{(m,n)}F_{-um+1}.$$

Puisque $(F_m, F_n) \,|\, F_{vn}$ et $(F_m, F_n) \,|\, F_{-um}$, il s'ensuit que

$$(F_m, F_n) \,|\, F_{(m,n)}F_{-um+1}.$$

Par ailleurs, comme $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$, on a en particulier $(F_n, F_{n+1}) = 1$ pour tout $n \in \mathbb{N}$. Il en résulte que

$$(F_m, F_n) \,|\, F_{(m,n)}.$$

ce qui donne le résultat recherché.

□

EXERCICES

1. La suite $a_0, a_1, \ldots, a_n$ est telle que

$$\begin{cases} a_0 = a_n = 0, \\ a_{k-1} - 2a_k + a_{k+1} \geqslant 0, \quad k = 1, 2, \ldots, n-1. \end{cases}$$

Prouver que $a_k \leqslant 0$ pour tout $k \in \{0, 1, \ldots, n\}$.

---

2. Déterminer l'ensemble des valeurs de x_0, $x_1 \in \mathbb{R}$ pour lesquelles la suite $(x_n)_{n\in\mathbb{N}}$ définie par :

$$x_{n+1} = \frac{x_{n-1}x_n}{3x_{n-1} - 2x_n}, \quad n \geqslant 1,$$

contient une infinité d'entiers positifs.

(Olympiades autrichiennes-1986)

---

3. Soit $(a_n)_{n\in\mathbb{N}^*}$ la suite définie par :

$$\begin{cases} a_1 = 1, \\ a_{n+1} = 1 + a_1 a_2 \cdots a_n, \quad n = 1, 2, \ldots \end{cases}$$

On pose $S_n = \sum_{k=1}^{n} 1/a_k$. Calculer $\lim_{n\to+\infty} S_n$.

---

4. La suite $(a_n)_{n\in\mathbb{N}}$ est définie par :

$$\begin{cases} a_0 = 0, \ a_1 = 1, \\ a_n = 2a_{n-1} + a_{n-2}, \quad n \geqslant 2. \end{cases}$$

Prouver que 2^k divise a_n si et seulement si 2^k divise n.

(Proposé à l'OIM-1988)

---

5. Soit $(a_n)_{n\in\mathbb{N}^*}$ la suite définie par :

$$a_n = \left\lfloor \sqrt{(n+1)^2 + n^2} \right\rfloor, \quad n = 1, 2, \ldots$$

a) Montrer que l'équation $(x+1)^2 + x^2 = y^2$ admet une infinité de solutions dans $\mathbb{N} \times \mathbb{N}$.

b) Montrer qu'il existe une infinité d'indices m tels que $a_{m+1} - a_m > 1$.

(Proposé à l'OIM-1988)

---

6. Trouver une suite $a_0, a_1, \ldots$ dont tous les termes soient strictement positifs et telle que $a_0 = 1$ et $a_n - a_{n+1} = a_{n+2}$ pour $n = 0, 1, 2, \ldots$ Montrer qu'une telle suite est unique.

---

7. Soit $(a_n)_{n\in\mathbb{N}^*}$ une suite dont tous les termes sont des réels strictement positifs et tels que $a_k - 2a_{k+1} + a_{k+2} \geqslant 0$ et $\sum_{i=1}^{k} a_i \leqslant 1$ pour tout $k \in \mathbb{N}^*$. Prouver que

$$\forall k \in \mathbb{N}^*, \quad 0 \leqslant a_k - a_{k+1} < \frac{2}{k^2}.$$

(Proposé à l'OIM-1988)

---

8. Soient a et b deux réels strictement positifs. Déterminer toutes les fonctions f de $\mathbb{R}_+$ dans $\mathbb{R}_+$ vérifiant l'équation fonctionnelle :

$$\forall x \in \mathbb{R}^+, \quad f(f(x)) + af(x) = b(a+b)x.$$

(Proposé à l'OIM-1992)

---

9. Une suite $(x_n)_{n\in\mathbb{N}}$ est définie comme suit :

$$\begin{cases} x_0 = 1989, \\ x_n = \dfrac{-1989}{n} \displaystyle\sum_{k=0}^{n-1} x_k, \quad n = 1, 2, \ldots \end{cases}$$

Évaluer la somme $\displaystyle\sum_{n=0}^{1989} 2^n x_n$.

(Proposé à l'OIM-1989)

---

10. Une suite $(a_n)_{n\in\mathbb{N}^*}$ est telle que :

$$\forall m, n \in \mathbb{N}^*, \quad |a_m + a_n - a_{m+n}| \leqslant \frac{1}{m+n}.$$

Prouver que $(a_n)_{n\in\mathbb{N}^*}$ est une progression arithmétique.

(Olympiades russes-1989)

---

11. Soit $(a_n)_{n\in\mathbb{N}^*}$ une suite de réels strictement positifs telle que

$$\forall n \in \mathbb{N}^*, \quad a_{n+1}^2 = a_n + 1.$$

Prouver que la suite $(a_n)_{n\in\mathbb{N}^*}$ contient des termes irrationnels.

---

12. Prouver que les suites $(a_n)_{n\in\mathbb{N}^*}$ et $(b_n)_{n\in\mathbb{N}^*}$ définies par :

$$a_n = \left\lfloor n + \sqrt{n/3} + 1/2 \right\rfloor, \quad b_n = 3n^2 - 2n, \quad n = 1, 2, \ldots,$$

sont complémentaires dans $\mathbb{N}^*$, autrement dit que leurs ensembles de valeurs respectifs forment une partition de $\mathbb{N}^*$.

(Proposé à l'OIM-1988)

---

13. La suite $(a_n)_{n\in\mathbb{N}^*}$ est définie par

$$a_1 = 1, \quad a_{n+1} = \frac{a_n}{n} + \frac{n}{a_n}, \; n \geqslant 1.$$

Prouver que $\lfloor a_n^2 \rfloor = n$ pour tout $n \geqslant 4$.

(Olympiades bulgares-1996)

---

14. Soient A et E deux sommets diamétralement opposés d'un octagone régulier convexe. Un pion qui peut occuper tous les huit sommets de cet octagone se déplace, à chaque coup, d'un sommet à l'un des deux sommets voisins ; le pion part de A et le jeu se termine quand il atteint pour la première fois le point E. On désigne par a_n le nombre de « parties » distinctes de n coups se terminant en E. Prouver que pour tout entier k, $k = 1, 2, 3, \ldots$

$$\begin{cases} a_{2k-1} = 0, \\ a_{2k} = \dfrac{1}{\sqrt{2}}(x^{k-1} - y^{k-1}), \end{cases}$$

où $x = 2 + \sqrt{2}$ et $y = 2 - \sqrt{2}$.

Note. Une partie de n coups est une suite de sommets $(P_0, P_1, \ldots, P_n)$ vérifiant les conditions suivantes :

a) $P_0 = A$, $P_n = E$;

b) pour tout i, $0 \leqslant i \leqslant n-1$, P_i est distinct de E ;

c) pour tout i, $0 \leqslant i \leqslant n-1$, P_i et P_{i+1} sont des sommets voisins.

(Olympiades internationales-1979/6)

---

15. On considère une suite $(x_n)_{n\in\mathbb{N}}$ telle que

$$x_n = 3x_{n-1} + 2, \quad n \geqslant 1.$$

Prouver qu'il existe une valeur entière de x_0 pour laquelle 1988 divise x_{100}.

(Olympiades chinoises-1988)

---

16. Trouver la plus grande valeur de x_0 pour laquelle il existe une suite x_0, x_1, $\ldots$, x_{1995} de nombres réels strictement positifs vérifiant les deux conditions :

a) $x_0 = x_{1995}$;

b) pour tout i, $1 \leqslant i \leqslant 1995$;

$$x_{i-1} + \frac{2}{x_{i-1}} = 2x_i + \frac{1}{x_i}.$$

(Olympiades internationales-1995/4)

---

17. On considère une suite $(a_n)_{n\in\mathbb{N}^*}$ d'entiers strictement positifs et tous inférieurs ou égaux à 1988 telle que a_{m+n} divise $a_m + a_n$ pour tous $m, n \in \mathbb{N}^*$. Prouver qu'une telle suite est périodique à partir d'un certain rang.

(Olympiades russes-1988)

---

18. Soient m et n deux entiers ($1 \leqslant m, n \leqslant 1981$) vérifiant

$$(n^2 - mn - m^2)^2 = 1.$$

Déterminer le maximum de $m^2 + n^2$.

(Olympiades internationales-1981/3)

---

19. Pour tout réel x_1, la suite $(x_n)_{n\geqslant 1}$ est définie par la relation de récurrence :

$$x_{n+1} = x_n\left(x_n + \frac{1}{n}\right), \quad n \geqslant 1.$$

Montrer qu'il existe un et un seul réel x_1 tel que la suite $(x_n)_{n\geqslant 1}$ vérifie

$$0 < x_n < x_{n+1} < 1$$

pour tout n supérieur ou égal à 1.

(Olympiades internationales-1985/6)

3.2. Les polynômes

3.2.1. L'anneau $\mathbf{K}[X]$. Soit $\mathbb{K}$ un corps commutatif. On appelle *polynôme* à coefficients dans $\mathbb{K}$ toute suite dans $\mathbb{K}$ dont tous les termes sont nuls à partir d'un certain rang.

Pour tous polynômes $P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_i)_{i\in\mathbb{N}}$ à coefficients dans $\mathbb{K}$, on définit les polynômes $P+Q = (a_i+b_i)_{i\in\mathbb{N}}$ et $PQ = (c_i)_{i\in\mathbb{N}}$, où $c_i = a_ib_0+a_{i-1}b_1+\cdots+a_0b_i$. Muni de l'addition et de la multiplication ainsi définies, l'ensemble des polynômes à coefficients dans $\mathbb{K}$, noté $\mathbb{K}[X]$, est un anneau commutatif.

Si $P = (a_i)_{i\in\mathbb{N}}$ est non nul, le plus grand indice i tel que $a_i \neq 0$ est appelé degré de P, et noté $\deg(P)$. Soit $n = \deg(P)$, a_n est alors appelé coefficient dominant de P. Un polynôme est dit unitaire si son coefficient dominant est égal à 1. On posera finalement par convention $\deg(P) = -\infty$ si $P = 0$.

Soit A une $\mathbb{K}$-algèbre (par exemple, le corps $\mathbb{K}$ lui-même). À tout polynôme $P = (a_i)_{i\in\mathbb{N}} \in \mathbb{K}[X]$, on associe la *fonction polynomiale* : $A \longrightarrow A \quad x \longmapsto \sum_{i\geqslant 0} a_ix^i$. Lorsqu'il n'y aura pas d'ambiguïté, on parlera indifféremment de polynôme et de fonction polynomiale (cependant, lorsque le corps $\mathbb{K}$ est fini, une fonction polynomiale peut être nulle alors que son polynôme associé est non nul[5]). Dans toute la suite, on conservera toutefois la notation $\sum_{i=0}^n a_ix^i$ pour désigner le polynôme $P = (a_i)_{i\in\mathbb{N}}$ de degré n.

Les propriétés arithmétiques de l'anneau $\mathbb{K}[X]$ ressemblent beaucoup aux propriétés de l'anneau $\mathbb{Z}$, ce qui tient au fait que dans les deux ensembles on dispose d'une division euclidienne.

3.2.1.1. Théorème. (*Division euclidienne dans* $\mathbb{K}[X]$) *Soient A et B deux polynômes dans $\mathbb{K}[X]$ avec $B \neq 0$. Il existe Q et R dans $\mathbb{K}[X]$ uniques tels que $A = BQ + R$ avec $\deg(R) < \deg(B)$.*

♦ **Remarque.**

Lorsque le corps $\mathbb{K}$ est remplacé par un anneau commutatif unitaire $\mathbb{A}$, on note toujours $\mathbb{A}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{A}$. Cet ensemble est encore un anneau commutatif, mais ne vérifie pas toutes les propriétés de $\mathbb{K}[X]$.

En particulier, la division euclidienne dans $\mathbb{Z}[X]$ est licite si le coefficient dominant de B est inversible. Dans le cas contraire, il apparaît en reprenant la preuve de la division euclidienne dans $\mathbb{K}[X]$ que celle-ci ne peut pas être généralisée dans $\mathbb{A}[X]$.

3.2.1.2. Théorème. (*Identité de Bézout*) *Si P et Q sont des polynômes de $\mathbb{K}[X]$ premiers entre eux (c'est-à-dire n'ayant comme diviseurs communs que les constantes non nulles) il existe $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1$.*

De l'identité de Bézout on déduit, comme dans $\mathbb{Z}$, le théorème de Gauss :

3.2.1.3. Théorème. (*Théorème de Gauss*) *Si P, Q et R sont des polynômes de $\mathbb{K}[X]$ tels que P divise QR et tels que P et Q sont premiers entre eux, alors P divise R.*

L'analogue des nombres premiers dans $\mathbb{Z}$ est ici appelé polynôme irréductible : un polynôme P est dit *irréductible* dans $\mathbb{K}[X]$ si P n'est pas constant et si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes et les polynômes proportionnels à P non nuls.

5. Le polynôme $x^p - x$ de $\mathbb{Z}/p\mathbb{Z}[X]$, où p est premier, en est un exemple.

3.2.1.4. Théorème. (*Théorème de décomposition*) *Tout polynôme non nul P de $\mathbb{K}[X]$ se décompose de manière unique, à l'ordre des facteurs près, sous la forme*

$$P = kP_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k},$$

où $k \in \mathbb{K}^*$, $\alpha_i \in \mathbb{N}^*$ et les P_i sont des polynômes distincts unitaires et irréductibles dans $\mathbb{K}[X]$.

3.2.2. Racines d'un polynôme. On dit que $\alpha \in \mathbb{K}$ est une *racine* de $P \in \mathbb{K}[X]$ si $P(\alpha) = 0$.

3.2.2.1. Théorème. *$\alpha \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si et seulement si $x - \alpha$ divise P.*

♦ **Preuve.** La division euclidienne de P par $x-\alpha$ donne $P(x) = (x-\alpha)Q(x)+R(x)$ avec $\deg(R) < \deg(x-\alpha) = 1$. On en déduit que R est une constante valant $P(\alpha)$.

□

♦ **Remarque.**

$\alpha \in \mathbb{Z}$ est racine de $P \in \mathbb{Z}[X]$ si et seulement si $x - \alpha$ divise P dans $\mathbb{Z}[X]$: en effet, $x-\alpha$ étant unitaire, il existe Q, $R \in \mathbb{Z}[X]$ tels que $P(x) = (x-\alpha)Q(x)+R(x)$ avec R constante valant $P(\alpha)$.

Une manière voisine pour retrouver ce résultat est d'appliquer le théorème précédent avec $\mathbb{K} = \mathbb{Q}$. Ainsi, si $\alpha \in \mathbb{Z}$ est racine de $P \in \mathbb{Z}[X]$, alors $x - \alpha$ divise P dans $\mathbb{Q}[X]$, i.e., il existe $Q \in \mathbb{Q}[X]$ tel que $P(x) = (x - \alpha)Q(x)$. Posons donc $P(x) = a_0 + a_1x + \cdots + a_nx^n$, avec $a_k \in \mathbb{Z}$ pour $0 \leqslant k \leqslant n$, et $Q(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. On a alors

$$\begin{aligned} b_{n-1} &= a_n, \\ b_{n-2} &= a_{n-1} + \alpha\, b_{n-1}, \\ &\cdots \\ b_0 &= a_1 + \alpha\, b_1. \end{aligned}$$

Comme $\alpha \in \mathbb{Z}$, il apparaît que $Q \in \mathbb{Z}[X]$, ce qu'on cherchait à démontrer.

□

On dit que $\alpha \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ de multiplicité m ($m \geqslant 1$) si $(x - \alpha)^m$ divise P et $(x - \alpha)^{m+1}$ ne divise pas P. On vérifie aisément :

3.2.2.2. Théorème. *Si $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{K}$ sont des racines du polynôme $P \in \mathbb{K}[X]$, de multiplicités respectives $m_1, m_2, \ldots, m_r$, alors il existe $Q \in \mathbb{K}[X]$ tel que*

$$P(x) = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \cdots (x - \alpha_r)^{m_r} Q(x). \tag{3.14}$$

♦ **Exemples.**

1. Si $P \in \mathbb{K}[X]$ est de degré $n \geqslant 1$, alors P a au plus n racines ; cela est une conséquence du théorème précédent et du fait que $\deg(PQ) = \deg(P) + \deg(Q)$.

2. Soit p un nombre premier. Considérons le polynôme $P(x) = x^{p-1} - 1$ de

$\mathbb{Z}/p\mathbb{Z}[X]$. D'après le petit théorème de Fermat, P possède les $p-1$ racines $1, 2, \dots, p-1$. Il s'ensuit que (on rappelle que $\mathbb{Z}/p\mathbb{Z}$ est un corps) :

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-p+1),$$

et on retrouve, en comparant les termes constants, le théorème de Wilson : $(p-1)! \equiv -1 \pmod p$.

3.2.2.3. Relations de Viète[6]**.** *Soit* $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{K}[X]$ *avec* $a_n \neq 0$. *Si* $\alpha_1, \alpha_2, \dots, \alpha_n$ *sont les racines de* P *(il est entendu que chaque racine est répétée selon sa multiplicité), alors* $P(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$*, et donc*

$$\sigma_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \alpha_{i_1}\cdots\alpha_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}, \qquad 1 \leqslant k \leqslant n,$$

ce qui s'écrit encore :

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}, \quad \sum_{1 \leqslant i < j \leqslant n} \alpha_i \alpha_j = \frac{a_{n-2}}{a_n}, \dots, \quad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}. \qquad (3.15)$$

♦ **Exemples.**

1. En reprenant l'égalité du dernier exemple, valable dans $\mathbb{Z}/p\mathbb{Z}$:

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-p+1),$$

il s'ensuit que, pour $p \geqslant 3$ et $1 \leqslant i \leqslant p-2$, la somme A_i de tous les produits de i éléments du sous-ensemble $\{1, 2, \dots, p-1\}$ de $\mathbb{Z}$ est divisible par p.

2. On peut utiliser ce résultat pour démontrer un résultat arithmétique dû à Wolstenholme[7] : le numérateur de la fraction (sous forme irréductible)

$$\frac{a}{b} = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

est divisible par $p \geqslant 3$; cela tient au fait que l'on a

$$\frac{a}{b} = \frac{A_{p-2}}{(p-1)!} \quad \Longleftrightarrow \quad A_{p-2}b = (p-1)!a,$$

avec $p \mid A_{p-2}$ et $\big(p, (p-1)!\big) = 1$.

On peut même montrer que pour p premier > 3, ce numérateur est divisible par p^2 : en effet, on a dans $\mathbb{Z}[X]$:

$$(x-1)(x-2)\cdots(x-p+1) = x^{p-1} - A_1 x^{p-2} + \cdots + A_{p-1}.$$

6. François Viète (1540-1603), mathématicien français.

7. Joseph Wolstenholme (1829-1891), mathématicien anglais.

En écrivant la dernière identité pour $x = p$, il s'ensuit que

$$(p-1)! = p^{p-1} - A_1 p^{p-2} + \cdots - A_{p-2}\, p + A_{p-1}.$$

Comme $A_{p-1} = (p-1)!$, on obtient $A_{p-2} = p^{p-2} - A_1 p^{p-3} + \cdots + A_{p-3}\, p$, ce qui montre (car $p \geqslant 5$) que p^2 divise A_{p-2}, d'où le résultat puisque $\big(p^2, (p-1)!\big) = 1$.

3.2.3. Polynômes irréductibles de $\mathbb{K}[X]$. Le problème de l'étude des polynômes irréductibles dans $\mathbb{C}[X]$ est complètement résolu grâce au théorème fondamental de l'algèbre[8] énoncé par d'Alembert[9] et entièrement démontré par Gauss[10]. Ce théorème, que nous ne démontrerons pas ici, peut être énoncé de diverses façons, dont : tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.

Il s'ensuit que les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes du premier degré. Ainsi, tout polynôme non constant $P \in \mathbb{C}[X]$ se décompose (théorème de décomposition) sous la forme :

$$\boxed{P(x) = k(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),} \tag{3.16}$$

où $\alpha_1, \alpha_2, \ldots, \alpha_n$ désignent les racines (répétées selon leurs multiplicités respectives) du polynôme P dans $\mathbb{C}$, et où $k \in \mathbb{C}^*$.

Si P est dans $\mathbb{R}[X]$, et si $\alpha \in \mathbb{C}$ est racine de P alors $\overline{\alpha}$ est aussi racine de P. Ainsi, $P \in \mathbb{R}[X]$ non constant se décompose sous la forme :

$$\boxed{P(x) = k\prod_{i=1}^{r}(x-\alpha_i)\prod_{i=1}^{s}(x^2 + a_i x + b_i),} \tag{3.17}$$

où $k \in \mathbb{R}^*$, $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{R}$, $a_1, b_1, \ldots, a_s, b_s \in \mathbb{R}$ et $\Delta_i = a_i^2 - 4b_i < 0$ pour $i = 1, 2, \ldots, s$. Comme par ailleurs tout polynôme du second degré à discriminant négatif est irréductible dans $\mathbb{R}[X]$, il s'ensuit que les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes du premier degré et ceux du second degré à discriminant négatif.

Dans $\mathbb{Q}[X]$, il n'existe pas de caractérisation satisfaisante des polynômes irréductibles. Toutefois, il existe plusieurs techniques permettant d'étudier certains cas particuliers. On peut ainsi commencer par rechercher les racines rationnelles du polynôme étudié, puis utiliser le théorème 3.2.2.1. Si par exemple $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ (pour étudier l'irréductibilité dans $\mathbb{Q}[X]$, il suffit d'étudier l'irréductibilité de polynômes de $\mathbb{Z}[X]$ dans $\mathbb{Q}[X]$), avec $a_n \neq 0$ et $a_0 \neq 0$, toute racine $\dfrac{p}{q}$ dans $\mathbb{Q}$ de P vérifie

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p\, q^{n-1} + a_0\, q^n = 0,$$

ce qui montre que p divise a_0 et q divise a_n. Comme les diviseurs de a_0 et a_n sont en nombre fini, le problème est théoriquement résolu.

8. La démonstration de ce théorème se trouve dans de nombreux ouvrages.

9. Jean le Rond d'Alembert (1717-1783), mathématicien français.

10. Carl Friedrich Gauss (1777-1855), mathématicien allemand.

Dans le cas de polynômes de degré 2 ou 3, ceci est particulièrement efficace : en effet, il est alors équivalent de dire que le polynôme en question est irréductible dans $\mathbb{Q}[X]$ ou qu'il ne possède pas de racines dans $\mathbb{Q}[X]$.

Dans le cas général, on dispose du critère suivant :

3.2.3.1. Le critère d'Eisenstein[11]. *Soit $P(x) = a_n x^n + \cdots + a_1 x + a_0$ un polynôme de $\mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que :*

a) p divise $a_0, a_1, \ldots, a_{n-1}$;

b) p ne divise pas a_n ;

c) p^2 ne divise pas a_0.

Alors P est irréductible dans $\mathbb{Q}[X]$.

♦ **Preuve.** On commence d'abord par démontrer que P est irréductible dans $\mathbb{Z}[X]$: en effet, si Q et R sont deux polynômes non constants de $\mathbb{Z}[X]$ tels que $P(x) = Q(x)R(x)$, avec $Q(x) = q_a x^a + \cdots + q_0$ et $R(x) = r_b x^b + \cdots + r_0$, alors $a_0 = q_0 r_0$. Il s'ensuit que p divise q_0 ou r_0, mais pas les deux à la fois (d'après c)). On peut donc supposer, sans nuire à la généralité, que p divise q_0 et ne divise pas r_0.

D'un autre côté, p ne divise pas q_a, sinon il diviserait $a_n = q_a r_b$. Soit alors k le plus petit indice i, $1 \leqslant i \leqslant a$, tel que p ne divise pas q_i. On a alors $a_k = q_k r_0 + q_{k-1} r_1 + \cdots + q_0 r_k$. Comme $k \leqslant a < n$, p divise a_k, et donc p divise $q_k r_0$, ce qui impose $p \mid r_0$, ce qui est contradictoire.

La suite de la preuve repose sur le résultat suivant :

3.2.3.2. Théorème. *Si un polynôme P de $\mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, il est irréductible dans $\mathbb{Q}[X]$.*

♦ **Preuve.** Si $P = QR$, avec Q et R polynômes non constants de $\mathbb{Q}[X]$, alors il existe $k \in \mathbb{N}^*$ tel que $kP = Q_1 R_1$, avec Q_1 et R_1 polynômes non constants de $\mathbb{Z}[X]$.

Soit p un diviseur premier de k ; démontrons que p peut être mis en facteur soit dans Q_1, soit dans R_1 : en effet, dans le cas contraire, posons $Q_1(x) = q_a x^a + \cdots + q_0$ et $R_1(x) = r_b x^b + \cdots + r_0$, et soient j le plus petit indice i, $0 \leqslant i \leqslant a$, tel que p ne divise pas q_i, et h le plus petit indice i, $0 \leqslant i \leqslant b$, tel que p ne divise pas r_i. Comme p est un diviseur premier de k, il divise tous les coefficients de $Q_1 R_1$, donc en particulier celui de x^{j+h}. Il s'ensuit que p divise $q_j r_h$, ce qui est absurde.

□

♦ **Exemples.**

1. Le polynôme $x^3 + x^2 - 2x - 1$ est irréductible dans $\mathbb{Q}[X]$: en effet, il est sans racine dans $\mathbb{Q}$ (car 1 et -1 sont les seuls candidats).

2. Soit p un nombre premier et $P(x) = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[X]$. Montrer que P est irréductible dans $\mathbb{Q}[X]$.

11. Max Eisenstein (1823-1852), mathématicien allemand.

L'idée est d'appliquer le critère d'Eisenstein au polynôme $Q(x) = P(x+1)$:

$$Q(x) = \frac{(x+1)^p - 1}{x} = x^{p-1} + p\,x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p.$$

Il est alors facile de vérifier que Q satisfait les hypothèses du critère d'Eisenstein (on rappelle que p étant premier, p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$). Ainsi Q, et donc P, est irréductible dans $\mathbb{Q}[X]$.

3.2.4. Les problèmes d'interpolation. Soient $a_0, a_1, \ldots, a_n$ des scalaires deux à deux distincts. On cherche un polynôme P de degré $\leqslant n$ tel que

$$P(a_j) = b_j, \quad j = 0, 1, \ldots, n, \tag{3.18}$$

où $b_0, b_1, \ldots, b_n$ sont des scalaires donnés.

Remarquons tout de suite qu'un tel polynôme, s'il existe, est unique (la différence de deux tels polynômes est un polynôme de degré $\leqslant n$ possédant $n+1$ racines distinctes donc est nécessairement nul).

On présente ici deux formules permettant d'expliciter ce polynôme. La première est due à Lagrange[12] et la deuxième est due à Newton[13].

3.2.4.1. Formule d'interpolation de Lagrange. *Le polynôme solution du problème d'interpolation s'écrit $P = \sum_{k=0}^{n} b_k L_k$, où*

$$L_k(x) = \prod_{i \neq k} \left(\frac{x - a_i}{a_k - a_i}\right), \quad k = 0, 1, \ldots, n. \tag{3.19}$$

Ce polynôme est appelé polynôme interpolateur de Lagrange.

♦ **Preuve.** Les polynômes L_k, $k = 0, 1, \ldots, n$, sont tels que :

$$L_k(a_j) = \begin{cases} 1 & \text{si } k = j, \\ 0 & \text{si } k \neq j. \end{cases}$$

Ceci étant, on a bien $\left(\sum_{k=0}^{n} b_k L_k\right)(a_j) = b_j$ pour $j = 0, 1, \ldots, n$.

□

L'idée de Newton est de considérer un polynôme P tel que

$$P(x) = c_0 + c_1(x-a_0) + c_2(x-a_0)(x-a_1) + \cdots + c_n(x-a_0)(x-a_1)\cdots(x-a_{n-1}),$$

où $c_0, c_1, \ldots, c_n$ sont des constantes à déterminer. Le polynôme P ainsi considéré est de degré $\leqslant n$, et les contraintes $P(a_j) = b_j$, $j = 0, 1, \ldots, n$, permettent de déterminer successivement les constantes $c_0, c_1, \ldots, c_n$. On a en effet $c_0 = P(a_0) = b_0$; $c_1 = (b_1 - b_0)/(a_1 - a_0)$; $c_2 = \left(\frac{b_2 - b_0}{a_2 - a_0} - \frac{b_1 - b_0}{a_1 - a_0}\right)/(a_2 - a_1)$; ...

12. Louis de Lagrange (1736-1813), mathématicien français.

13. Isaac Newton (1646-1727), mathématicien et physicien anglais.

3.2.4.2. Formule d'interpolation de Newton. *Le polynôme solution du problème d'interpolation s'écrit*

$$\begin{aligned} P(x) &= c_0 + c_1(x-a_0) + c_2(x-a_0)(x-a_1) + \\ &\quad \cdots + c_n(x-a_0)(x-a_1)\cdots(x-a_{n-1}), \end{aligned} \tag{3.20}$$

où $c_0, c_1, \ldots, c_n$ sont des constantes qui s'expriment au moyen des a_j et des b_j.

♦ **Exemples.**

1. Soit P un polynôme de degré $\leqslant n$ tel que $P(j) = 1 \Big/ \binom{n+1}{j}$, pour $j = 0, 1, 2, \ldots, n$. Déterminer $P(n+1)$.

Le polynôme P est donné par la formule d'interpolation de Lagrange :

$$P(x) = \sum_{k=0}^{n} \prod_{i \neq k} \left(\frac{x-i}{k-i}\right) P(k).$$

Or,

$$\begin{aligned} \prod_{\substack{i \neq k \\ i=0}}^{n} \left(\frac{n+1-i}{k-i}\right) &= \frac{n+1}{k} \times \frac{n}{k-1} \times \cdots \times \frac{n-k+2}{1} \times \frac{n-k}{-1} \times \cdots \times \frac{1}{k-n} \\ &= (-1)^{n-k} \binom{n+1}{k} \end{aligned}$$

et il s'ensuit que

$$P(n+1) = \sum_{k=0}^{n} (-1)^{n-k} = \begin{cases} 0 & \text{si } n \text{ est impair,} \\ 1 & \text{si } n \text{ est pair.} \end{cases}$$

2. Soit P un polynôme de degré $\leqslant 998$ tel que

$$P(k) = F_k, \quad k = 1000, 1001, \ldots, 1998,$$

où $(F_n)_{n \geqslant 0}$ est la suite de Fibonacci. Prouver que $P(1999) = F_{1999} - 1$.

Ici encore, les valeurs prises par P correspondent à des points régulièrement espacés, avec un pas égal à l'unité. Dans ce cas particulier important, les constantes intervenant dans la formule d'interpolation de Newton sont assez facilement déterminées :

$$c_j = \frac{1}{j!} \Delta^j b_0, \quad j = 0, 1, \ldots, n,$$

où $\Delta^j b_0$ sont les différences successives en b_0 de la suite $b_0, b_1, \ldots, b_n$. Ces différences sont définies récursivement par : $\Delta^1 b_i = b_{i+1} - b_i$, $\Delta^2 b_i = \Delta^1 b_{i+1} - \Delta^1 b_i = b_{i+2} - 2b_{i+1} + b_i$, etc ...

Dans le tableau :

$$\begin{array}{ccccccccccc}
\mathbf{b_0} & & b_1 & & b_2 & & b_3 & & \dots & & b_n \\
& \mathbf{\Delta^1 b_0} & & \Delta^1 b_1 & & \Delta^1 b_2 & & \dots & & \Delta^1 b_{n-1} & \\
& & \mathbf{\Delta^2 b_0} & & \Delta^2 b_1 & & \dots & & \Delta^2 b_{n-2} & & \\
& & & \ddots & & & & \iddots & & & \\
& & & & & \mathbf{\Delta^n b_0} & & & & &
\end{array}$$

les coefficients c_j s'obtiennent à partir des éléments de la diagonale gauche du tableau. Le polynôme interpolateur de Newton s'écrit :

$$\boxed{P(x) = \sum_{j=0}^{n} \binom{x-a_0}{j} \Delta^j b_0,} \tag{3.21}$$

où $\Delta^1 b_0 = b_0$, $\binom{x-a_0}{0} = 1$ et pour $1 \leqslant j \leqslant n$,

$$\binom{x-a_0}{j} = \frac{(x-a_0)(x-a_0-1)\cdots(x-a_0-j+1)}{j!}.$$

Dans le cas particulier de l'exemple étudié, une simplification majeure a lieu. Vu la définition de la suite de Fibonacci, le tableau des différences successives s'écrit :

$$\begin{array}{ccccccccccc}
\mathbf{F_{1000}} & & F_{1001} & & F_{1002} & & F_{1003} & & \dots & & F_{1998} \\
& \mathbf{F_{999}} & & F_{1000} & & F_{1001} & & \dots & & F_{1996} & \\
& & \mathbf{F_{998}} & & F_{999} & & \dots & & F_{1994} & & \\
& & & \ddots & & & & \iddots & & & \\
& & & & & \mathbf{F_2} & & & & &
\end{array}$$

et on a :

$$P(x) = \sum_{j=0}^{998} \binom{x-1000}{j} F_{1000-j}.$$

On est maintenant en mesure de prouver le résultat demandé. Considérons le polynôme Q de degré $\leqslant 999$ tel que $Q(k) = F_k$ pour $1000 \leqslant k \leqslant 1999$. En appliquant le même raisonnement que précédemment, on obtient

$$Q(x) = \sum_{j=0}^{999} \binom{x-1000}{j} F_{1000-j},$$

ce qui prouve que $Q(1999) = 1 + P(1999)$, d'où $P(1999) = F_{1999} - 1$.

EXERCICES

20. Les nombres a, b, c et d sont tels que :

$$a = \sqrt{4-\sqrt{5-a}}, \quad b = \sqrt{4+\sqrt{5-b}}, \quad c = \sqrt{4-\sqrt{5+c}}, \quad d = \sqrt{4+\sqrt{5+d}}.$$

Calculer le produit $abcd$.

---

21. Soit P un polynôme à coefficients réels tel que $P(x) \geqslant 0$ pour tout $x \in \mathbb{R}$. Prouver qu'il existe des polynômes P_1, $P_2 \in \mathbb{R}[X]$ tels que

$$P = P_1^2 + P_2^2.$$

---

22. On considère les polynômes : $P_1(x) = x^2 - 2$ et $P_j(x) = P_1(P_{j-1}(x))$ pour $j = 2, 3, \ldots$ Démontrer que pour tout entier positif n, les racines de l'équation $P_n(x) = x$ sont des nombres réels distincts.

(Olympiades internationales-1976/2)

---

23. Soient $a_0, a_1, \ldots, a_{n-1}$ des réels tels que $0 < a_0 \leqslant a_1 \leqslant \cdots \leqslant a_{n-1} \leqslant 1$. Soit λ une racine du polynôme $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ vérifiant $|\lambda| \geqslant 1$.

Prouver que $\lambda^{n+1} = 1$.

(Olympiades chinoises-1992)

---

24. Trouver tous les polynômes P, autres que les polynômes constants, à coefficients dans $\mathbb{R}$ et tels que

$$P(x^2) = P(x)P(x-1), \quad \forall x \in \mathbb{C}.$$

(Olympiades roumaines-1995)

---

25. On se donne $2n$ réels distincts $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$, que l'on utilise pour former un tableau $n \times n$ dont l'élément situé à l'intersection de la ligne i et de la colonne j est $a_i + b_j$.

Prouver que si les produits des éléments d'une même colonne sont identiques, alors les produits des éléments d'une même ligne sont aussi identiques.

(Olympiades russes-1991)

---

26. Soient P et Q deux polynômes non nuls dans $\mathbb{C}[X]$. Prouver que P et Q ont les mêmes racines (avec les mêmes ordres de multiplicité) si et seulement si la fonction $f : \mathbb{C} \to \mathbb{R}$ définie par $f(z) = |P(z)| - |Q(z)|$ garde un signe constant ou est identiquement nulle.

(Olympiades roumaines-1978)

---

27. Soit $P(z) = z^n + c_1 z^{n-1} + c_2 z^{n-2} + \cdots + c_n$ un polynôme de la variable complexe z, à coefficients réels c_k. On suppose que $|P(i)| < 1$.

Prouver qu'il existe des réels a et b tels que $P(a + ib) = 0$ et $(a^2 + b^2 + 1)^2 < 4b^2 + 1$.

(Olympiades des États-Unis-1989)

---

28. Si P, Q, R et S sont des polynômes tels que

$$P(x^5) + xQ(x^5) + x^2 R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x),$$

Prouver que 1 est une racine de P.

(Olympiades des États-Unis-1976)

---

29. Trouver tous les polynômes f à deux variables tels que :

a) pour tous réels t, x, y : $f(tx, ty) = t^n f(x, y)$, où n est un entier (f est homogène de degré n) ;

b) pour tous réels a, b, c : $f(a + b, c) + f(b + c, a) + f(c + a, b) = 0$;

c) $f(1, 0) = 1$.

(Olympiades internationales-1975/6)

---

30. Soit $f(x)$ un polynôme à coefficients rationnels et α un réel tel que $\alpha^3 - 3\alpha + 1 = \big(f(\alpha)\big)^3 - 3f(\alpha) + 1 = 0$.

Prouver que, pour tout $n \geqslant 1$,

$$\big(f^n(\alpha)\big)^3 - 3f^n(\alpha) + 1 = 0,$$

où $f^n(x) = f(f(\ldots f(x)))$.

---

31. Soit $n > 1$ un entier. On pose $f(x) = x^n + 5x^{n-1} + 3$. Montrer que $f(x)$ est irréductible sur $\mathbb{Z}[X]$.

(Olympiades internationales-1993/1)

---

32. Montrer que l'ensemble des réels x qui vérifient l'inéquation

$$\sum_{k=1}^{70} \frac{k}{x - k} \geqslant \frac{5}{4}$$

est la réunion d'intervalles disjoints dont la somme des longueurs a pour valeur 1988.

(Olympiades internationales-1988/4)

---

33. On se donne m entiers relatifs $a_1, a_2, \ldots, a_m$. Le polynôme P à coefficients entiers est tel que, pour tout entier n, il existe au moins un indice $i \in \{1, 2, \ldots, m\}$ tel que a_i divise $P(n)$. Prouver qu'il existe un indice k tel que a_k divise $P(n)$ pour tout entier n.

(Olympiades russes-1990)

---

34. On suppose que la suite d'entiers $(q_n)_{n\in\mathbb{N}}$ est telle que :

a) $m - n$ divise $q_m - q_n$ pour $m > n \geqslant 0$;

b) il existe un polynôme P tel que $|q_n| < P(n)$ pour tout $n \in \mathbb{N}$.

Prouver qu'il existe un polynôme Q tel que $q_n = Q(n)$ pour tout $n \in \mathbb{N}$.

(Olympiades des États-Unis-1995)

---

35. P est un polynôme de degré $3n$ tel que :

$$\begin{aligned} P(0) = P(3) = \cdots = P(3n) &= 2; \\ P(1) = P(4) = \cdots = P(3n-2) &= 1; \\ P(2) = P(5) = \cdots = P(3n-1) &= 0. \end{aligned}$$

Déterminer n sachant que $P(3n+1) = 730$.

(Olympiades des États-Unis-1984)

---

36. Soit P un polynôme non constant à coefficients entiers. Si $n(P)$ est le nombre d'entiers k tels que $\big(P(k)\big)^2 = 1$, prouver que $n(P) - \deg(P) \leqslant 2$, où $\deg(P)$ désigne le degré du polynôme P.

(Olympiades internationales-1974/6)

---

37. Si P est un polynôme à coefficients entiers, on désigne par $w(P)$ le nombre de ses coefficients qui sont impairs.

Pour tout entier positif i, on pose $Q_i = (1+x)^i$. Montrer que, pour toute famille finie d'entiers $i_1, i_2, \ldots, i_n$ tels que $0 \leqslant i_1 < i_2 < \cdots < i_n$, on a :

$$w(Q_{i_1} + Q_{i_2} + \cdots + Q_{i_n}) \geqslant w(Q_{i_1}).$$

(Olympiades internationales-1985/3)

---

38. Soit n un entier > 1. On place n lampes autour d'un cercle et on les numérote dans le sens trigonométrique : $L_0, L_1, \ldots, L_{n-1}$. Chacune de ces lampes peut être allumée ou éteinte. On considère la situation où toutes les lampes sont allumées, et on applique une suite d'opérations : opération 0, opération 1,..., l'opération j consistant à changer l'état de la lampe L_j si la lampe L_{j-1} est allumée, et à ne rien modifier si L_{j-1} est éteinte. Prouver que :

a) il existe un entier strictement positif $M(n)$ tel qu'après $M(n)$ opérations, toutes les lampes redeviennent allumées ;

b) si n est de la forme 2^k, toutes les lampes redeviennent allumées après $n^2 - 1$ opérations ;

c) si n est de la forme $2^k + 1$, toutes les lampes redeviennent allumées après $n^2 - n + 1$ opérations.

(Olympiades internationales-1993/6)

SOLUTIONS

1. Supposons qu'il existe un indice k tel que $a_k > 0$, et supposons qu'il soit choisi de telle sorte que $a_j \leqslant 0$ pour tout j tel que $j < k$. On a alors

$$a_n - a_{n-1} \geqslant a_{n-1} - a_{n-2} \geqslant \cdots \geqslant a_k - a_{k-1} > 0,$$

d'où $a_n \geqslant a_{n-1} \geqslant \cdots \geqslant a_k > 0$, ce qui contredit l'hypothèse $a_n = 0$.

---

2. Si $x_n = 0$, alors $x_{n+1} = 0$ et la suite n'est pas définie pour les indices $\geqslant n+2$. Supposons donc $x_n \neq 0$ pour tout $n \in \mathbb{N}$, et posons $u_n = 1/x_n$. Il s'ensuit de la relation de récurrence que

$$u_{n+2} - 3u_{n+1} + 2u_n = 0.$$

La solution générale de cette équation de récurrence se met sous la forme :

$$u_n = \alpha + 2^n \beta,$$

où α et β sont des constantes. Si $\beta \neq 0$, alors $\lim\limits_{n \to +\infty} |u_n| = +\infty$ et donc $\lim\limits_{n \to +\infty} x_n = 0$, ce que signifie que la suite $(x_n)_{n \in \mathbb{N}}$ ne prend pas une infinité de valeurs entières. Il s'ensuit que $(x_n)_{n \in \mathbb{N}}$ contient une infinité d'entiers positifs si et seulement si $x_0 = x_1 \in \mathbb{N}^*$.

---

3. On remarque que

$$\frac{a_{n+1}}{a_n} - \frac{1}{a_n} = a_n - 1, \quad n \geqslant 2$$

c'est-à-dire $a_{n+1} - 1 = a_n(a_n - 1)$ pour $n \geqslant 2$, soit encore

$$\frac{1}{a_n} = \frac{1}{a_n - 1} - \frac{1}{a_{n+1} - 1}, \quad n \geqslant 2.$$

Or, $a_1 = 1$, donc

$$\sum_{k=1}^{n} \frac{1}{a_k} = 1 + \sum_{k=2}^{n} \left[\frac{1}{a_k - 1} - \frac{1}{a_{k+1} - 1}\right] = 2 - \frac{1}{a_{n+1} - 1},$$

mais comme $\lim\limits_{n \to +\infty} a_n = +\infty$, on obtient

$$\lim_{n \to +\infty} S_n = 2.$$

---

4. 1ère solution. On définit une nouvelle suite $(b_n)_{n\in\mathbb{N}}$ par :

$$\begin{cases} b_0 = b_1 = 2, \\ b_n = 2b_{n-1} + b_{n-2}, \ n \geqslant 2. \end{cases}$$

Les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ s'expriment à l'aide des solutions de l'équation caractéristique $t^2 - 2t - 1 = 0$:

$$a_n = \frac{\alpha^n - \beta^n}{2\sqrt{2}}, \ b_n = \alpha^n + \beta^n, \quad n = 0, 1, 2, \ldots,$$

où $\alpha = 1 + \sqrt{2}$ et $\beta = 1 - \sqrt{2}$.

Il s'ensuit en utilisant la formule du binôme que :

$$\begin{aligned} a_n &= \binom{n}{1} + 2\binom{n}{3} + 4\binom{n}{5} + 8\binom{n}{7} + \cdots, \\ b_n &= 2\binom{n}{0} + 4\binom{n}{2} + 8\binom{n}{4} + \cdots \end{aligned}$$

On en déduit que a_n est impair si n est impair, et que b_n est divisible par 2 mais pas par 4 pour tout $n \in \mathbb{N}$. Comme $a_{2n} = a_n b_n$, $\forall n \in \mathbb{N}$, il s'ensuit que

$$a_{2^k m} = a_m b_m b_{2m} \cdots b_{2^{k-1}m}, \quad \forall k, m \in \mathbb{N}.$$

Ainsi, la plus grande puissance de 2 divisant a_n, où $n = 2^k m$ (m impair), est égale à 2^k.

2ème solution. En examinant les premières valeurs que prend la suite $(a_n)_{n\in\mathbb{N}}$, on remarque que

$$\begin{cases} a_{2n+1} = a_n^2 + a_{n+1}^2, \\ a_{2n} = 2a_n(a_n + a_{n-1}), \end{cases}$$

ce que l'on vérifie facilement par récurrence. Le résultat demandé en résulte immédiatement (par récurrence).

---

5. a) On remarque que $(x, y) = (3, 5)$ est une solution de l'équation proposée. D'un autre côté, si (x_0, y_0) est solution alors $(3x_0 + 2y_0 + 1, 4x_0 + 3y_0 + 2)$ est aussi solution.

b) Soit k un entier naturel non nul tel que $2k^2 + 2k + 1 = y^2$ et soit

$$a_k = \sqrt{2k^2 + 2k + 1} = y.$$

Montrons que $a_k - a_{k-1} > 1$. Pour ce faire, il suffit de prouver que

$$a_{k-1} = \left\lfloor \sqrt{k^2 + (k-1)^2} \right\rfloor < y - 1 \quad \text{ou} \quad \sqrt{k^2 + (k-1)^2} < y - 1.$$

Supposons que $\sqrt{k^2+(k-1)^2} \geqslant y-1$. On a alors $2y \geqslant 4k+1$ (car $y^2 = 2k^2+2k+1$), soit encore $8k^2 \leqslant 3$, ce qui est exclu. Ainsi, $a_k - a_{k-1} > 1$ pour tous les entiers strictement positifs k tels que $2k^2+2k+1$ soit un carré parfait.

---

6. 1ère solution. L'équation $1-z=z^2$ a une racine positive et une seule :

$$z = \frac{\sqrt{5}-1}{2}.$$

Ce nombre satisfait aux relations :

$$1-z=z^2, \quad z-z^2=z^3, \ldots, \quad z^n - z^{n+1} = z^{n+2}, \ldots,$$

ce qui prouve que la suite $(z^n)_{n\in\mathbb{N}}$ satisfait les conditions de l'énoncé.

Soit $b_0, b_1, \ldots$ une autre suite satisfaisant aux conditions de l'énoncé. On doit avoir

$$b_0 = 1, \quad b_n - b_{n+1} = b_{n+2}, \ \forall n \in \mathbb{N}.$$

Posons donc $b_1 = t$; on a alors $b_2 = 1-t$, $b_3 = 2t-1$, $b_4 = 2-3t$, $b_5 = 5t-3$, et on vérifie sans peine que, pour $n = 1, 2, \ldots$

$$\begin{cases} b_{2n} = F_{2n-1} - F_{2n}t > 0, \\ b_{2n-1} = F_{2n-1}t - F_{2n-2} > 0, \end{cases}$$

où $(F_n)_{n\in\mathbb{N}}$ est la suite de Fibonacci. Il s'ensuit que

$$\frac{F_{2n}}{F_{2n+1}} < t < \frac{F_{2n+1}}{F_{2n+2}}, \quad n = 0, 1, 2, \ldots$$

Comme,

$$\lim_{n\to+\infty} \frac{F_n}{F_{n+1}} = \frac{\sqrt{5}-1}{2} = z,$$

il s'ensuit que $b_1 = z$, et que les deux suites $(b_n)_{n\in\mathbb{N}}$ et $(z^n)_{n\in\mathbb{N}}$ coïncident.

2ème solution. La solution de la récurrence de l'énoncé s'écrit sous la forme :

$$a_n = \alpha x^n + \beta y^n, \quad \forall n \in \mathbb{N},$$

où $(\alpha, \beta) \in \mathbb{R}^2$, $x = \dfrac{-1-\sqrt{5}}{2}$ et $y = \dfrac{-1+\sqrt{5}}{2}$. Les constantes α et β se calculent en fonction de $a_0 = 1$ et a_1, d'où

$$\forall n \in \mathbb{N}, \quad a_n = \frac{1}{y-x}\left[(y-a_1)x^n + (a_1 - x)y^n\right].$$

- Si $a_1 \neq y$, alors $(-1)^n a_n \to \pm\infty$ suivant que $y - a_1 >$ ou < 0. Il s'ensuit que $(a_n)_{n\in\mathbb{N}}$ n'est pas à termes positifs.

- Si maintenant $a_1 = y$, alors

$$\forall n \in \mathbb{N}, \quad a_n = y^n \geqslant 0,$$

et cette suite vérifie bien les conditions de l'énoncé.

---

7. Montrons que la suite $(a_n)_{n\in\mathbb{N}^*}$ est décroissante : s'il existe un indice k tel que $a_k - a_{k+1} = -\alpha$ avec $\alpha > 0$, alors $a_m - a_{m+1} \leqslant -\alpha$ pour tout $m \geqslant k$ (car $a_n - a_{n+1} \geqslant a_{n+1} - a_{n+2}$, $\forall n \in \mathbb{N}^*$). Il s'ensuit que

$$a_k - a_m = (a_k - a_{k+1}) + (a_{k+1} - a_{k+2}) + \cdots + (a_{m-1} - a_m) \leqslant -(m-k)\alpha,$$

soit encore

$$a_m \geqslant a_k + (m-k)\alpha, \quad \forall m \geqslant k.$$

Ainsi, pour m assez grand, $a_m > 1$ ce qui est impossible. Ainsi, $a_k - a_{k+1} \geqslant 0$ pour tout $k \in \mathbb{N}^*$.

Supposons maintenant qu'il existe un indice k tel que $a_k - a_{k+1} \geqslant 2/k^2$. On a alors $a_m - a_{m+1} \geqslant a_k - a_{k+1} \geqslant 2/k^2$ pour tout $m \leqslant k$, d'où

$$a_m \geqslant a_{m+1} + \frac{2}{k^2} \geqslant a_{m+2} + 2\frac{2}{k^2} \geqslant \cdots \geqslant a_{k+1} + (k-m+1)\frac{2}{k^2},$$

et en particulier,

$$a_1 + a_2 + \cdots + a_k \geqslant (1 + 2 + \cdots + k)\frac{2}{k^2} + ka_{k+1} > 1 + ka_{k+1} \geqslant 1,$$

ce qui contredit l'hypothèse de l'énoncé.

---

8. Notons $f^n(x) = f(f^{n-1}(x))$, $n = 1, 2, \ldots$ où $f^0(x) = x$ et $f^1(x) = f(x)$. On a donc

$$f^{n+2}(x) + af^{n+1}(x) - b(a+b)f^n(x) = 0, \quad n = 0, 1, 2, \ldots$$

Le polynôme caractéristique de cette équation est :

$$y^2 + ay - b(a+b) = (y + a + b)(y - b),$$

donc

$$f^n(x) = \lambda_1 b^n + \lambda_2(-a-b)^n, \quad n = 0, 1, \ldots,$$

où λ_1 et λ_2 sont des constantes. Mais comme $x = f^0(x) = \lambda_1 + \lambda_2$ et $f(x) = f^1(x) = \lambda_1 b - \lambda_2(a+b)$, il s'ensuit que

$$\lambda_1 = \frac{(a+b)x + f(x)}{a+2b}, \quad \lambda_2 = \frac{bx - f(x)}{a+2b},$$

et

$$\frac{1}{(a+b)^n} f^n(x) = \lambda_1 \left(\frac{b}{a+b}\right)^n + (-1)^n \lambda_2.$$

Comme $f: \mathbb{R}^+ \to \mathbb{R}^+$, $f^n: \mathbb{R}^+ \to \mathbb{R}^+$, et donc

$$-\lambda_1 \left(\frac{b}{a+b}\right)^{2n} \leqslant \lambda_2 \leqslant \lambda_1 \left(\frac{b}{a+b}\right)^{2n+1}, \quad n = 0, 1, 2, \ldots$$

En faisant tendre n vers $+\infty$, on obtient $\lambda_2 = 0$ $(a+b > b \geqslant 0)$, soit encore $f(x) = bx$, et on vérifie facilement que $f(x) = bx$ est bien solution de l'équation proposée.

---

9. Notons c le nombre 1989. Pour $n \geqslant 2$, on a

$$nx_n = -c \cdot \sum_{k=0}^{n-1} x_k,$$

ce qui permet d'écrire

$$nx_n - (n-1)x_{n-1} = -c\,x_{n-1}, \quad n \geqslant 2,$$

et donc

$$x_n = -\left(\frac{c-n+1}{n}\right)x_{n-1}, \quad n \geqslant 2,$$

soit encore pour $0 \leqslant n \leqslant c$,

$$x_n = (-1)^n \frac{(c-n+1)(c-n+2)\cdots(c-1)c}{n!} \cdot x_0 = (-1)^n \binom{c}{n} c.$$

On a donc finalement

$$\sum_{n=0}^{c} 2^n x_n = c \cdot \sum_{n=0}^{c} 2^n (-1)^n \binom{c}{n} = c(1-2)^c = -c.$$

---

10. Soit $k \in \mathbb{N}^*$ fixé, et soit m un entier strictement positif quelconque. On a alors

$$|a_{m+1} + a_k - a_{m+k+1}| \leqslant \frac{1}{m+k+1},$$

et

$$|a_m + a_{k+1} - a_{m+k+1}| \leqslant \frac{1}{m+k+1},$$

ce qui donne

$$|(a_{m+1} - a_m) - (a_{k+1} - a_k)| \leqslant \frac{2}{m+k+1} < \frac{2}{m}.$$

Il s'ensuit que la suite $(a_{m+1} - a_m)_{m \in \mathbb{N}^*}$ converge et a pour limite $(a_{k+1} - a_k)$. Ceci étant vrai pour tout $k \in \mathbb{N}$, il en résulte que

$$a_{m+1} - a_m = a_{n+1} - a_n, \quad \forall m, n \in \mathbb{N}^*,$$

autrement dit $(a_n)_{n \in \mathbb{N}^*}$ est une progression arithmétique.

---

11. Supposons que tous les termes de la suite $(a_n)_{n \in \mathbb{N}^*}$ soient rationnels. On peut donc écrire pour tout $n \in \mathbb{N}^*$: $a_n = \dfrac{p_n}{q_n}$ avec $(p_n, q_n) = 1$. Comme

$$a_{n+1}^2 = a_n + 1 = \frac{p_n + q_n}{q_n},$$

il s'ensuit que $q_{n+1}^2 = q_n$, $n = 1, 2, \dots$ ce qui implique que $q_n = 1$ à partir d'un certain rang n_0, i.e. a_n est un entier pour $n \geqslant n_0$.

Soit $n \geqslant n_0$ un entier. Si $a_n = 1$ alors $a_{n+1} = \sqrt{2}$, ce qui est exclu. On a donc $a_n \geqslant 2$, et il en résulte que $a_{n+1} < a_n$. La suite $(a_n)_{n \geqslant n_0}$ est une suite strictement décroissante d'entiers positifs et on sait qu'une telle suite ne peut exister, d'où la contradiction.

---

12. Soit $m \in \mathbb{N}^*$ une valeur qui n'est pas prise par la suite $(a_n)_{n \in \mathbb{N}^*}$. Il existe donc $n \in \mathbb{N}^*$ tel que

$$n + \sqrt{\frac{n}{3}} + \frac{1}{2} < m \quad \text{et} \quad m + 1 \leqslant n + 1 + \sqrt{\frac{n+1}{3}} + \frac{1}{2},$$

mais alors

$$\begin{aligned} \sqrt{\frac{n}{3}} < m - n - \frac{1}{2} \leqslant \sqrt{\frac{n+1}{3}} \quad &\Longrightarrow \quad \frac{n}{3} < (m-n)^2 - (m-n) + \frac{1}{4} \leqslant \frac{n+1}{3} \\ &\Longrightarrow \quad n < 3(m-n)^2 - 3(m-n) + \frac{3}{4} \leqslant n + 1 \\ &\Longrightarrow \quad m < 3(m-n)^2 - 2(m-n) + \frac{3}{4} \leqslant m + 1, \end{aligned}$$

par conséquent,

$$m = 3(m-n)^2 - 2(m-n)$$

est de la forme $3k^2 - 2k$ où $k \in \mathbb{N}^*$.

Le reste de la preuve est un simple argument de dénombrement : il y a d'une part exactement n nombres de la forme $3k^2 - 2k$ ne dépassant pas $3n^2 - 2n + n = 3n^2 - n$. D'un autre côté

$$\left\lfloor 3n^2 - 2n + \sqrt{n^2 - \frac{2}{3}n} + \frac{1}{2} \right\rfloor = 3n^2 - n$$

puisque

$$\sqrt{n^2 - \frac{2}{3}n} + \frac{1}{2} < n + \frac{1}{2} \quad \text{et} \quad \sqrt{n^2 - \frac{2}{3}n} + \frac{1}{2} > \sqrt{n^2 - n + \frac{1}{4}} + \frac{1}{2} = n.$$

Il s'ensuit qu'il existe exactement $3n^2 - 2n$ nombres de la forme $\lfloor k + \sqrt{k/3} + 1/2 \rfloor$ ne dépassant pas $3n^2 - n$. Il en résulte que tous les nombres de la forme $3n^2 - 2n, n \in \mathbb{N}^*$, ne sont pas pris par la suite $(a_n)_{n \in \mathbb{N}^*}$, et qu'il n'y a que ces nombres que cette suite ne prend pas.

---

13. On pose $f(x) = \dfrac{x}{n} + \dfrac{n}{x}$. Comme,

$$f(a) - f(b) = \frac{(a-b)(ab - n^2)}{abn},$$

il s'ensuit que f est décroissante sur l'intervalle $]0, n]$.

On va d'abord prouver que

$$\sqrt{n} \leqslant a_n \leqslant \frac{n}{\sqrt{n-1}}, \quad n \geqslant 3,$$

en effet, $\sqrt{3} \leqslant a_3 = 2 \leqslant \dfrac{3}{\sqrt{2}}$. Si maintenant $\sqrt{n} \leqslant a_n \leqslant \dfrac{n}{\sqrt{n-1}}$ pour un entier $n \geqslant 3$, alors

$$a_{n+1} = f(a_n) \leqslant f(\sqrt{n}) = \frac{n+1}{\sqrt{n}},$$

et

$$a_{n+1} = f(a_n) \geqslant f\left(\frac{n}{\sqrt{n-1}}\right) = \frac{n}{\sqrt{n-1}} > \sqrt{n+1},$$

ce qui achève la récurrence.

Il suffit maintenant de prouver que $a_n < \sqrt{n+1}$ pour $n \geqslant 4$. On a

$$a_{n+1} = f(a_n) \geqslant f\left(\frac{n}{\sqrt{n-1}}\right) = \frac{n}{\sqrt{n-1}}, \quad n \geqslant 3,$$

ce qui donne

$$a_n \geqslant \frac{n-1}{\sqrt{n-2}}, \quad n \geqslant 4,$$

et par conséquent

$$a_{n+1} = f(a_n) < f\left(\frac{n-1}{\sqrt{n-2}}\right) = \frac{(n-1)^2 + n^2(n-2)}{(n-1)n\sqrt{n-2}} < \sqrt{n+2}, \quad n \geqslant 4.$$

Il s'ensuit que $\lfloor a_n^2 \rfloor = n$ pour $n \geqslant 5$, et on vérifie facilement que $\lfloor a_4^2 \rfloor = 4$.

---

14. Comme aucune partie d'un nombre impair de coups ne se termine en E, on a $a_{2k-1} = 0$, $k = 1, 2, \ldots$

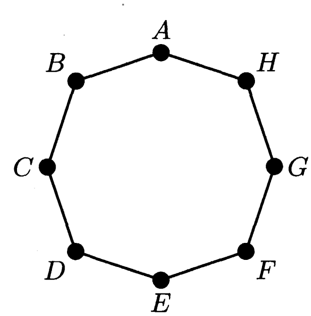


FIG. 3.2.

D'un autre côté, $a_2 = 0$ et $a_4 = 2$. Afin de pouvoir trouver une relation de récurrence pour a_{2k}, on introduit une suite supplémentaire $(b_n)_{n \in \mathbb{N}^*}$ que l'on définit comme suit : b_n est le nombre de parties de n coups commençant en C et se terminant en E.

Partant de A, le pion peut suivre 4 chemins différents lors de ses deux premiers mouvements :

$$A \longrightarrow B \longrightarrow A, \qquad A \longrightarrow H \longrightarrow A,$$
$$A \longrightarrow B \longrightarrow C, \qquad A \longrightarrow H \longrightarrow G.$$

Il s'ensuit que

$$a_{2k} = 2a_{2k-2} + 2b_{2k-2}, \quad k = 1, 2, \ldots$$

D'un autre côté, un pion qui part de C a 3 façons pour effectuer ses deux premiers mouvements sans atteindre E

$$C \longrightarrow B \longrightarrow C, \qquad C \longrightarrow D \longrightarrow C, \qquad C \longrightarrow B \longrightarrow A.$$

Il s'ensuit que

$$b_{2k} = 2b_{2k-2} + a_{2k-2}, \quad k = 1, 2, \ldots$$

On doit donc résoudre le système d'équations de récurrence

$$\begin{cases} a_{2k} = 2a_{2k-2} + 2b_{2k-2}, \\ b_{2k} = 2b_{2k-2} + a_{2k-2}. \end{cases} \qquad (k = 1, 2, \ldots)$$

Comme $a_{2k+2} = 2a_{2k} + 2b_{2k}$ et $a_{2k} = 2a_{2k-2} + 2b_{2k-2}$, il s'ensuit que

$$a_{2k+2} - 4a_{2k} + 2a_{2k-2} = 0, \quad k = 1, 2, \ldots,$$

ce qui conduit à l'expression

$$a_{2k} = \alpha(2+\sqrt{2})^k + \beta(2-\sqrt{2})^k, \quad k \geqslant 1,$$

où α et β sont des constantes :

$$\alpha = \frac{1}{\sqrt{2}}\Big(\frac{1}{2+\sqrt{2}}\Big), \quad \beta = \frac{-1}{\sqrt{2}}\Big(\frac{1}{2-\sqrt{2}}\Big),$$

d'où le résultat.

---

15. 1ère solution. (théorème de Bézout) On pose $x_n = 3^n y_n$, $n = 0, 1, 2, \ldots$ La suite $(y_n)_{n\in\mathbb{N}}$ satisfait à l'équation de récurrence $y_n = y_{n-1} + 2/3^n$. On a alors

$$x_n = 3^n y_n = (x_0 + 1)3^n - 1, \quad n = 0, 1, 2, \ldots,$$

et en particulier

$$x_{100} = (x_0 + 1)3^{100} - 1.$$

D'un autre côté, on sait qu'il existe deux entiers k et r tels que

$$3^{100} = 1988k + r, \quad 0 < r < 1988.$$

Il suffit maintenant de prouver qu'il existe un couple $(x_0, m) \in \mathbb{Z}^2$ tel que

$$r(x_0 + 1) - 1 = 1988m,$$

mais comme $(1988, r) = 1$, le théorème de Bézout assure l'existence d'une infinité de tels couples.

2$^{\text{ème}}$ solution. (théorème chinois) On a les équivalences suivantes :

$$x_{100} \equiv 0 \pmod{1988} \iff \begin{cases} x_{100} \equiv 0 \pmod 4, \\ x_{100} \equiv 0 \pmod 7, \\ x_{100} \equiv 0 \pmod{71}. \end{cases}$$

$$\iff \begin{cases} x_0 \equiv 0 \pmod 4, \\ x_0 \equiv 1 \pmod 7, \\ x_0 \equiv 29 \pmod{71}. \end{cases}$$

En effet, $x_{100} = (x_0+1)3^{100} - 1$ et

$$\begin{cases} 3^{100} \equiv (3^6)^{16} \cdot 3^4 \equiv 4 \pmod 7, \\ 3^{100} \equiv 3^{70} \cdot 3^{30} \equiv 3^2 \cdot (3^4)^7 \equiv 90 \cdot 6^2 \equiv 45 \pmod{71}, \end{cases}$$

d'après le petit théorème de Fermat et les règles de congruences.

D'après le théorème chinois, le système précédent admet une unique solution $x_0 = 1520$ modulo 1988.

---

16. La condition de l'énoncé équivaut à

$$2x_i^2 - \left(x_{i-1} + \frac{2}{x_{i-1}}\right)x_i + 1 = 0,$$

qui a pour solutions

$$x_i = \frac{1}{2}x_{i-1} \quad \text{et} \quad x_i = \frac{1}{x_{i-1}}.$$

On montre par récurrence que, pour $i \geqslant 0$, $x_i = 2^{k_i}x_0^{\varepsilon_i}$, où k_i est un entier vérifiant $|k_i| \leqslant i$ et où $\varepsilon_i = (-1)^{k_i+i}$:

- si $i = 0$ alors $k_0 = 0$ et $\varepsilon_0 = 1$;

- si $x_{i-1} = 2^{k_{i-1}}x_0^{\varepsilon_{i-1}}$ avec $\varepsilon_{i-1} = (-1)^{k_{i-1}+(i-1)}$ et $|k_{i-1}| \leqslant i-1$, alors $x_i = 1/x_{i-1}$ ou $x_i = x_{i-1}/2$. Dans le premier cas, $k_i = -k_{i-1}$ et $\varepsilon_i = -\varepsilon_{i-1}$ et dans le deuxième cas $k_i = k_{i-1} - 1$ et $\varepsilon_i = \varepsilon_{i-1}$. Dans chaque cas, il est immédiat que $|k_i| \leqslant i$ et que $\varepsilon_i = (-1)^{k_i+i}$.

On en déduit que $x_{1995} = 2^k x_0^\varepsilon$, où $k = k_{1995}$ et $\varepsilon = (-1)^{1995+k}$. Il s'ensuit que $x_0 = x_{1995} = 2^k x_0^\varepsilon$. Si k est impair, alors $\varepsilon = 1$ et $2^k = 1$ ce qui est impossible. On en déduit que k est pair et donc que

$$x_0^2 = 2^k, \quad |k| \leqslant 1995.$$

Il s'ensuit que la plus grande valeur possible de x_0 est 2^{997} ($k = 1994$). Cette valeur est atteinte pour la suite

$$\begin{cases} x_0 = 2^{997}, \\ x_i = \dfrac{1}{2}x_{i-1}, \quad i = 1, 2, \ldots, 1994, \qquad x_{1995} = \dfrac{1}{x_{1994}}. \end{cases}$$

---

17. Soit M la plus grande valeur prise par la suite $(a_n)_{n\in\mathbb{N}^*}$ une infinité de fois, et choisissons l'indice n_0 de telle sorte que, pour tout $k \geqslant n_0$, on ait $a_k \leqslant M$.

On va montrer que tout entier $m \geqslant n_0$ tel que $a_m = M$ est une période de la suite $(a_n)_{n\geqslant n_0}$: en effet, soient $i \geqslant n_0$ et m un entier $\geqslant n_0$ tel que $a_m = M$.

- Si $a_{i+m} = M$, alors M divise $a_i + a_m = a_i + M$, ce qui prouve que $a_i = M = a_{i+m}$.

- Si $a_{i+m} < M$, alors prenons un indice $j \geqslant n_0$ tel que $a_{i+j+m} = M$. On a alors $a_{i+j} = M$ (c'est le cas qui vient d'être discuté). D'un autre côté, M divise $a_{i+m} + a_j$, et $a_j \leqslant M$, par conséquent

$$a_{i+m} + a_j = M.$$

On a donc $a_j < M$, et puisque $a_{i+j} = M$, alors

$$a_i + a_j = M,$$

et il s'ensuit que $a_i = a_{i+m}$, ce qui achève la démonstration.

---

18. Un couple (n, m) d'entiers sera dit admissible si $m, n \in \{1, 2, \ldots, 1981\}$ et

$$(n^2 - nm - m^2)^2 = 1,$$

c'est-à-dire

$$n^2 - nm - m^2 = \pm 1.$$

Partant d'un couple admissible (n_1, n_2) avec $n_2 > 1$, on pose $n_3 = n_1 - n_2$. Comme

$$n_1(n_1 - n_2) = n_2^2 \pm 1 > 0,$$

il s'ensuit que $n_1 > n_2$, et donc $n_3 \in \{1, 2, \ldots, 1981\}$.

D'un autre côté,

$$n_1^2 - n_2n_1 - n_2^2 = (n_2 - n_1)^2 - n_2(n_2 - n_1) - n_2^2 = -\left[n_2^2 - (n_1 - n_2)n_2 - (n_1 - n_2)^2\right].$$

Il en résulte que

$$n_2^2 - n_2n_3 - n_3^2 = \pm 1,$$

et donc (n_2, n_3) est également un couple admissible, et on a de plus $n_2 > n_3$ si $n_3 \neq 1$.

On peut réitérer ce procédé pour construire une suite $n_1, n_2, \ldots, n_k$ telle que :

a) (n_i, n_{i+1}) est un couple admissible pour $i = 1, 2, \ldots, k-1$;

b) $n_k = 1$ et $n_i \neq 1$ pour $i = 1, 2, \ldots, k-1$.

Comme, par construction,

$$\begin{cases} n_{k-(i+2)} = n_{k-(i+1)} + n_{k-i}, & i = 0, 1, \ldots, \\ n_k = 1, \ n_{k-1} = 2, \end{cases}$$

il s'ensuit que les nombres n_k, $n_{k-1}, \ldots, n_2$, n_1, sont des termes consécutifs de la suite de Fibonacci. En particulier, n_1 et n_2 sont deux termes consécutifs de cette suite.

Réciproquement, le procédé qui vient d'être décrit est réversible, ce qui implique que tout couple d'éléments consécutifs de la suite de Fibonacci est admissible (en prenant les deux éléments dans l'ordre qui convient). Les éléments de cette suite qui interviennent dans l'exercice sont ceux, inférieurs à 1981, c'est-à-dire :

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233,\ 377,\ 610,\ 987,\ 1597,$$

d'où le maximum de $m^2 + n^2 = 987^2 + 1597^2$.

---

19. On définit par récurrence la suite de fonctions $(f_n)_{n\in\mathbb{N}^*}$:

$$\begin{cases} f_1(x) = x, \\ f_{n+1}(x) = f_n(x)\Big(f_n(x) + \dfrac{1}{n}\Big), \quad n = 1, 2, \ldots \end{cases}$$

de façon à ce que x_n soit égal à $f_n(x_1)$.

On voit facilement par récurrence que f_n est strictement croissante, et convexe sur $\mathbb{R}_+$ (car elle est polynomiale à coefficients positifs). On a également

$$f_n(0) = 0, \quad f_n(1) \geqslant 1, \quad n = 1, 2, \ldots$$

Comme la condition $x_{n+1} > x_n$ équivaut à

$$x_n > 1 - \frac{1}{n},$$

on peut reformuler le problème comme suit : montrer qu'il existe un unique réel $t > 0$ tel que, pour tout $n \geqslant 1$,

$$1 - \frac{1}{n} < f_n(t) < 1,$$

c'est-à-dire

$$f_n^{-1}\Big(1 - \frac{1}{n}\Big) < t < f_n^{-1}(1),$$

où f_n^{-1} désigne la bijection réciproque de la restriction de f_n à $\mathbb{R}_+$.

Posons $x'_n = f_n^{-1}\Big(1 - \dfrac{1}{n}\Big)$ et $y'_n = f_n^{-1}(1)$, et montrons que les deux suites $(x'_n)_{n\in\mathbb{N}^*}$ et $(y'_n)_{n\in\mathbb{N}^*}$ sont adjacentes :

- Puisque f_n est convexe, la fonction

$$x \longmapsto \frac{f_n(x) - f_n(0)}{x - 0} = \frac{f_n(x)}{x}$$

est croissante sur $\mathbb{R}_+^*$. Il s'ensuit que

$$\frac{f_n(y'_n)}{y'_n} \geqslant \frac{f_n(x'_n)}{x'_n},$$

soit encore
$$0 \leqslant y'_n - x'_n \leqslant \frac{y'_n}{n} \leqslant \frac{1}{n},$$
par conséquent $\lim_{n\to+\infty} (y'_n - x'_n) = 0$.

- La suite $(x'_n)_{n\in\mathbb{N}^*}$ est croissante : en effet,
$$f_{n+1}(x'_n) = f_n(x'_n)\Big(f_n(x'_n) + \frac{1}{n}\Big) = 1 - \frac{1}{n},$$
et
$$f_{n+1}(x'_{n+1}) = 1 - \frac{1}{n+1},$$
ce qui implique que $x'_{n+1} \geqslant x'_n, \quad \forall n \in \mathbb{N}^*$.

- La suite $(y'_n)_{n\in\mathbb{N}^*}$ est décroissante : en effet,
$$f_{n+1}(y'_n) = f_n(y'_n)\Big(f_n(y'_n) + \frac{1}{n}\Big) = 1 + \frac{1}{n} > f_{n+1}(y'_{n+1}) = 1,$$
ce qui implique que $y'_n \geqslant y'_{n+1}$, $\forall n \in \mathbb{N}^*$.

Si l désigne la limite commune des deux suites $(x'_n)_{n\in\mathbb{N}^*}$ et $(y'_n)_{n\in\mathbb{N}^*}$, alors
$$1 - \frac{1}{n} < f_n(t) < 1,\ \forall n \in \mathbb{N}^* \iff x'_n < t < y'_n,\ \forall n \in \mathbb{N}^* \iff t = l.$$

Il existe donc un et un seul réel $x_1 = l$ tel que la suite $(x_n)_{n\geqslant 1}$ vérifie
$$0 < x_n < x_{n+1} < 1, \quad n \geqslant 1.$$

---

20. a et b sont solutions de l'équation $x^4 - 8x^2 + x + 11 = 0$; c et d sont solutions de l'équation $y^4 - 8y^2 - y + 11 = 0$. Il s'ensuit que a, b, $-c$ et $-d$ sont les racines du polynôme $x^4 - 8x^2 + x + 11 = 0$; leur produit vaut donc 11.

---

21. Tout polynôme P de $\mathbb{R}[X]$ peut s'écrire sous la forme :
$$P(x) = \prod_{i=1}^{r} (x - \alpha_i) \prod_{i=1}^{s} (x^2 + a_i x + b_i), \quad \alpha_i,\, a_i,\, b_i \in \mathbb{R},$$
avec $\Delta_i = a_i^2 - 4b_i < 0,\ \forall i \in \{1, 2, \ldots, s\}$.

Si P vérifie de plus l'inégalité $P(x) \geqslant 0$ pour tout $x \in \mathbb{R}$, alors toute racine réelle a un ordre de multiplicité pair. Il suffit donc pour résoudre le problème proposé de montrer que si R_1 et R_2 s'écrivent sous la forme $Q_1^2 + Q_2^2$ et $Q_3^2 + Q_4^2$ respectivement, alors R_1R_2 se met aussi sous la même forme. Or, ceci se vérifie sans difficulté :
$$R_1R_2 = (Q_1Q_3 + Q_2Q_4)^2 + (Q_1Q_4 - Q_2Q_3)^2.$$

Note. On peut démontrer de façon analogue que si $P \in \mathbb{R}[X]$ est tel que $P(x) \geqslant 0$ pour tout $x \in \mathbb{R}_+$, alors il existe des polynômes P_1 et $P_2 \in \mathbb{R}[X]$ tels que $P = P_1^2 + xP_2^2$: en effet, les facteurs intervenant dans la décomposition de $P(x)$ sont de l'une des trois formes :

$$x + \lambda \ (\lambda \in \mathbb{R}_+), \quad (x-\lambda)^\mu \ (\lambda \in \mathbb{R}, \mu \text{ pair}) \text{ ou } x^2 + 2px + q \ (p^2 < q).$$

Mais

$$\begin{aligned} x + \lambda &= \left(\sqrt{\lambda}\right)^2 + x \cdot (1)^2, \\ (x-\lambda)^\mu &= \left\{(x-\lambda)^{\mu/2}\right\}^2 + x \cdot (0)^2, \\ x^2 + 2px + q &= \left(x - q^{1/2}\right)^2 + x \cdot \left\{\sqrt{2(q^{1/2}+p)}\right\}^2, \end{aligned}$$

ce qui permet de conclure, compte tenu de l'égalité :

$$(Q_1^2 + xQ_2^2)(Q_3^2 + xQ_4^2) = (Q_1Q_3 + xQ_2Q_4)^2 + x(Q_2Q_3 - Q_1Q_4)^2.$$

---

22. Soit $x = 2\cos\theta$ un réel compris entre -2 et 2. On a alors

$$P_1(x) = 4\cos^2\theta - 2 = 2\cos 2\theta, \ldots, P_k(x) = 2\cos 2^k\theta, \ldots$$

L'équation $P_n(x) = x$ est vérifiée si et seulement si $\cos 2^n\theta = \cos\theta$, i.e., si et seulement si $2^n\theta = \pm\theta + 2k\pi$.

Cette dernière relation donne lieu à 2^n valeurs réelles distinctes de x qui satisfont l'équation $P_n(x) = x$. P_n étant de degré 2^n, ce sont toutes les racines possibles de l'équation proposée qui a donc 2^n racines réelles distinctes.

---

23. On a $\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0 = 0$, ce qui donne, en multipliant par $1-\lambda$,

$$\lambda^{n+1} = (1-a_{n-1})\lambda^n + (a_{n-1} - a_{n-2})\lambda^{n-1} + \cdots + (a_1 - a_0)\lambda + a_0.$$

Comme tous les coefficients dans le terme de droite sont $\geqslant 0$, il s'ensuit que :

$$\begin{aligned} |\lambda|^{n+1} &\leqslant (1-a_{n-1})|\lambda|^n + (a_{n-1} - a_{n-2})|\lambda|^{n-1} + \cdots + (a_1 - a_0)|\lambda| + a_0 \\ &\leqslant \big[(1-a_{n-1}) + (a_{n-1} - a_{n-2}) + \cdots + (a_1 - a_0) + a_0\big]|\lambda|^n = |\lambda|^n. \end{aligned}$$

On en déduit que $|\lambda| \leqslant 1$, soit encore $|\lambda| = 1$. On a ainsi

$$|\lambda^{n+1}| = |(1-a_{n-1})\lambda^n| + |(a_{n-1} - a_{n-2})\lambda^{n-1}| + \cdots + |(a_1 - a_0)\lambda| + |a_0|,$$

et comme a_0 est un réel positif, tous les nombres λ^{n+1}, $(1-a_{n-1})\lambda^n, \ldots, (a_1 - a_0)\lambda$ sont des réels positifs : en effet, l'égalité $|z_1 + z_2 + \cdots + z_n| = |z_1| + |z_2| + \cdots + |z_n|$ a lieu si et seulement si $z_1, z_2, \ldots, z_n$ sont situés sur une même demi-droite partant de l'origine du plan complexe.

On a donc enfin $\lambda^{n+1} = |\lambda^{n+1}| = 1$.

---

24. Si a est une racine non nulle de P, alors $P(a^2) = P(a)P(a-1) = 0$, et en réitérant, on trouve

$$0 = P(a) = P(a^2) = P(a^4) = \cdots,$$

et comme P est non constant, donc en particulier non nul, on doit avoir $|a| = 1$ car P n'a qu'un nombre fini de racines.

D'un autre côté, $(a+1)^2$ est aussi racine de P, et on a donc

$$0 = P\big((a+1)^2\big) = P\big((a+1)^4\big) = \cdots,$$

ce qui montre que $|a+1| = 1$. Il s'ensuit que $a = -\dfrac{1}{2} \pm i\dfrac{\sqrt{3}}{2}$. Or, P étant à coefficients réels, si a est racine de P, $\overline{a}$ l'est aussi. De plus, comme $P(1) \neq 0$, il s'ensuit que $P(0) = 1$, ce qui montre que P doit être de la forme $(x^2+x+1)^n$, où n est un entier positif non nul.

Réciproquement, tout polynôme P de la forme précédente vérifie $P(x^2) = P(x)P(x-1)$ pour tout $x \in \mathbb{C}$.

---

25. On considère le polynôme

$$P(x) = \prod_{i=1}^{n}(x+a_i) - \prod_{j=1}^{n}(x-b_j),$$

dont le degré est $< n$. On a ainsi

$$P(b_j) = \prod_{i=1}^{n}(b_j+a_i) = \text{cste}, \quad \forall j \in \{1, 2, \ldots, n\}.$$

Le polynôme $P - \text{cste}$ est ainsi un polynôme de degré $< n$ ayant n racines distinctes ; il est donc nul, d'où :

$$\prod_{j=1}^{n}(a_i+b_j) = (-1)^{n+1}P(-a_i) = (-1)^{n+1}\cdot\text{cste}, \quad \forall i \in \{1, 2, \ldots, n\},$$

d'où le résultat désiré.

---

26. Il suffit de prouver que si $f(z) = |P(z)| - |Q(z)| \geqslant 0$, $\forall z \in \mathbb{C}$, alors P et Q ont les mêmes racines avec les mêmes ordres de multiplicité.

Il est clair que toute racine de P est aussi racine de Q, et que son ordre de multiplicité comme racine de P est au plus égal à son ordre de multiplicité comme racine de Q. D'un autre côté, l'inégalité $f(z) \geqslant 0$ devant être vérifiée pour tout $z \in \mathbb{C}$, le degré de P est au moins égal à celui de Q, sans quoi $f(z)$ deviendrait négatif pour des z de module suffisamment élevé. Ceci achève la démonstration.

---

27. Soient $r_1, r_2, \ldots, r_n$ les racines du polynôme P dans $\mathbb{C}$. On peut donc écrire :

$$P(i) = (i - r_1)(i - r_2)\cdots(i - r_n),$$

d'où,

$$|i - r_1| \cdot |i - r_2| \cdots |i - r_n| < 1.$$

Comme P est à coefficients réels, ses racines non réelles peuvent être regroupées deux à deux, chaque paire étant constituée de nombres conjugués. Or, si $r \in \mathbb{R}$, $|i - r| = \sqrt{1 + r^2} \geqslant 1$. Il existe donc deux réels a et b tels que $P(a + ib) = 0$ et

$$1 > |i - (a + ib)| \cdot |i - (a - ib)| = \sqrt{(a^2 + b^2 + 1)^2 - 4b^2},$$

d'où :

$$4b^2 + 1 > (a^2 + b^2 + 1)^2.$$

---

28. On remarque que le terme de droite dans l'égalité de l'énoncé s'annule pour toutes les racines 5-ièmes de l'unité, à savoir $1, \omega, \omega^2, \omega^3, \omega^4$, où $\omega = e^{2i\pi/5}$. On a ainsi

$$\begin{aligned} P(1) + \omega Q(1) + \omega^2 R(1) &= 0, & (1)\\ P(1) + \omega^2 Q(1) + \omega^4 R(1) &= 0, & (2)\\ P(1) + \omega^3 Q(1) + \omega R(1) &= 0, & (3)\\ P(1) + \omega^4 Q(1) + \omega^3 R(1) &= 0. & (4) \end{aligned}$$

Comme $1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$, la somme de ces égalités donne $4P(1) - Q(1) - R(1) = 0$. D'un autre côté, en considérant la combinaison $\omega \times (1) + \omega^2 \times (2) + \omega^3 \times (3) + \omega^4 \times (4)$, on trouve $-P(1) - Q(1) - R(1) = 0$. Il s'ensuit que $P(1) = 0$, ce qu'il fallait démontrer.

Note. Plus généralement, on peut démontrer que si $P_0, P_1, \ldots, P_{n-2}$ ($n \geqslant 2$) et S sont des polynômes tels que

$$P_0(x^n) + xP_1(x^n) + \cdots + x^{n-2}P_{n-2}(x^n) = (x^{n-1} + x^{n-2} + \cdots + 1)S(x),$$

alors 1 est racine de P_i pour tout $i \in \{0, 1, \ldots, n-2\}$.

Soient ω_i, $i = 1, 2, \ldots, n-1$ les racines n-ièmes de l'unité, autres que 1. On a alors

$$1 + \omega_i + \omega_i^2 + \cdots + \omega_i^{n-1} = 0$$

pour tout i. On en déduit que

$$P_0(1) + \omega_i P_1(1) + \cdots + \omega_i^{n-2} P_{n-2}(1) = 0, \quad i = 1, 2, \ldots, n-1.$$

Ainsi, le polynôme $\sum_{k=0}^{n-2} P_k(1)x^k$ a $n-1$ racines distinctes ; il s'ensuit qu'il est nul, soit encore $P_0(1) = P_1(1) = \cdots = P_{n-2}(1) = 0$.

---

29. L'hypothèse $f(a+b,c)+f(b+c,a)+f(c+a,b)=0$ donne en posant $a=b=c$: $P(2a,a)=0$ pour tout $a \in \mathbb{R}$. Il s'ensuit que

$$f(x,y)=(x-2y)g(x,y),$$

où g est un polynôme homogène de degré $n-1$, i.e., $g(tx,ty)=t^{n-1}g(x,y)$ pour tous x, $y \in \mathbb{R}$. On a aussi $g(1,0)=f(1,0)=1$.

On va montrer que si $x+y=1$, alors $f(x,y)=x-2y$: en effet, $f(x,y)=f(x,1-x)$ peut être considéré comme un polynôme de la variable $z=x-2y=3x-2$. Ainsi, si on pose $f(x,1-x)=P(z)$, et si on applique la condition b) pour $a=b=\dfrac{x}{2}$ et $c=1-x$, on obtient

$$f(x,1-x)+f(1-x/2,x/2)+f(1-x/2,x/2)=0,$$

i.e.,

$$P(z)=-2P(-z/2) \quad \Longrightarrow \quad P(2^{2k})=2^{2k},\ k=0,\,1,\,2,\ldots$$

L'unique polynôme satisfaisant à la dernière égalité est le polynôme $P(z)=z$, ce qu'on voulait démontrer.

Si x et y sont tels que $x+y\neq 0$, alors

$$\frac{x}{x+y}+\frac{y}{x+y}=1,$$

ce qui donne :

$$f(x,y)=(x+y)^n f\left(\frac{x}{x+y},\frac{y}{x+y}\right)=(x+y)^{n-1}(x-2y),$$

et par continuité de f,

$$f(x,y)=(x+y)^{n-1}(x-2y), \quad \forall x,\ y\in\mathbb{R}.$$

---

30. Le polynôme x^3-3x+1 est irréductible sur $\mathbb{Q}[X]$: en effet, si a est une racine rationnelle de x^3-3x+1, alors a est nécessairement un entier. Mais a^3-3a est pair, ce qui est impossible. Il s'ensuit que α et $f(\alpha)$ sont irrationnels.

Par ailleurs, α ne peut pas être une racine d'un polynôme de degré 2 à coefficients rationnels : en effet, si on avait $g(\alpha)=0$, où g est de degré 2, alors on pourrait écrire

$$x^3-3x+1=g(x)h(x)+r(x),$$

où g, h, $r\in\mathbb{Q}[X]$ et r est de degré $\leqslant 1$. Mais alors $r(\alpha)=0$, ce qui est impossible.

Maintenant, on prouve le résultat demandé par récurrence sur n : si on suppose que $\left(f^{n-1}(\alpha)\right)^3-3f^{n-1}(\alpha)+1=0$, alors x^3-3x+1 divise le polynôme $\left(f^{n-1}(x)\right)^3-3f^{n-1}(x)+1$ dans $\mathbb{Q}[X]$: en effet, si on écrit :

$$\left(f^{n-1}(x)\right)^3-3f^{n-1}(x)+1=(x^3-3x+1)h(x)+r(x), \tag{1}$$

où h, $r \in \mathbb{Q}[X]$ et r est de degré $\leqslant 2$, on obtient $r(\alpha) = 0$ ce qui est impossible si r est non nul. En posant $x = f(\alpha)$ dans l'équation (1), on obtient $\left(f^n(\alpha)\right)^3 - 3f^n(\alpha) + 1 = 0$, ce qui conclut la démonstration.

Note. Le raisonnement précédent reste valable pour tout polynôme de degré 3 qui est irréductible sur $\mathbb{Q}[X]$. Cependant, pour que l'exercice ne soit pas trivial, il faut que le polynôme possède 3 racines réelles distinctes. Dans le cas contraire, le polynôme n'aurait qu'une seule racine réelle, et on aurait trivialement $\alpha = f(\alpha)$.

---

31. 1ère solution. Raisonnons par l'absurde et supposons qu'il existe deux polynômes g et h, à coefficients entiers, tels que $f = gh$. Comme $f(0) = 3$, on peut supposer, sans perte de généralité, que $|g(0)| = 1$ et que

$$g(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0 \quad (a_0 = \pm 1).$$

Comme $f(\pm 1) \neq 0$, on a nécessairement $k > 1$. Si $\alpha_1, \alpha_2, \ldots, \alpha_k$ sont les racines de g dans $\mathbb{C}$, alors

$$g(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_k).$$

On a ainsi $|g(0)| = |\alpha_1 \times \alpha_2 \times \cdots \times \alpha_k| = 1$. Comme $\alpha_i^{n-1}(\alpha_i + 5) = 3$, $\forall i \in \{1, 2, \ldots, k\}$, alors $|(\alpha_1 + 5) \times (\alpha_2 + 5) \times \cdots \times (\alpha_k + 5)| = 3^k$. Mais $3 = f(-5) = g(-5)h(-5)$, d'où :

$$|(\alpha_1 + 5) \times (\alpha_2 + 5) \times \cdots \times (\alpha_k + 5)| = 1 \text{ ou } 3,$$

ce qui est impossible car $k > 1$.

2ème solution. Supposons de même qu'il existe deux polynômes g et h, à coefficients entiers, tels que $f = gh$. Comme $f(0) = 3$, on peut supposer, sans perte de généralité, que $|g(0)| = 3$ et on écrit

$$g(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0 \quad (a_0 = \pm 3).$$

On s'inspire maintenant de la démonstration du critère d'Eisenstein : soit j le plus petit indice tel que a_j ne soit pas divisible par 3. Si on pose $h(x) = x^p + b_{p-1}x^{p-1} + \cdots + b_0$ et $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$, il apparaît que le coefficient

$$c_j = a_j b_0 + a_{j-1}b_1 + \cdots$$

n'est pas divisible par 3 car $b_0 a_0 = 3$ et $a_0 = \pm 3$. On en déduit que $j \geqslant n - 1$, d'où $k \geqslant n - 1$, i.e., $p \leqslant 1$. Le polynôme h s'écrit donc $\pm x \pm 1$, ce qui est absurde puisque $f(\pm 1) \neq 0$.

---

32. Posons de manière plus générale pour un entier $n \geqslant 1$

$$f(x) = \sum_{k=1}^{n} \frac{k}{x - k}.$$

Cette fonction est strictement décroissante sur chacun des intervalles où elle est définie. Pour tout $a > 0$, l'équation $f(x) = a$ admet n solutions réelles $x_1, x_2, \ldots, x_n$, où $i < x_i < i+1$ pour $i = 1, 2, \ldots, n-1$, et $x_n > n$. L'ensemble des réels x tels que $f(x) \geqslant a$ est donc la réunion des intervalles $]i, x_i]$, où $i = 1, 2, \ldots, n$, dont la somme des longueurs est

$$\Big(\sum_{i=1}^{n} x_i\Big) - \frac{n(n+1)}{2}.$$

Afin de pouvoir calculer $\sum_{i=1}^{n} x_i$, on va expliciter un polynôme de degré n dont les racines sont $x_1, x_2, \ldots, x_n$. Pour ce faire, écrivons

$$\sum_{k=1}^{n} \frac{k}{x_i - k} = a.$$

En posant $P(x) = (x-1)(x-2)\cdots(x-n)$, il apparaît que le polynôme

$$aP(x) - \sum_{k=1}^{n} k\Big(\prod_{j\neq k}(x-j)\Big)$$

admet $x_1, x_2, \ldots, x_n$ comme racines. Comme il est de degré n, ce sont manifestement les seules racines de ce polynôme. Le coefficient de x^{n-1} dans le dernier polynôme est

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

On en déduit que

$$\sum_{i=1}^{n} x_i = \frac{a+1}{2a}n(n+1).$$

Ainsi, pour $a = \dfrac{5}{4}$ et $n = 70$, on obtient une longueur totale égale à $\dfrac{n(n+1)}{2a} =$ 1988.

---

33. Supposons qu'il existe m entiers $x_1, x_2, \ldots, x_m$, tels que, pour tout $k \in \{1, 2, \ldots, m\}$, a_k ne divise pas $P(x_k)$. Il s'ensuit qu'il existe des nombres $y_k = p_k^{\alpha_k}$, où p_k est premier, tels que y_k divise a_k mais pas $P(x_k)$.

Si les deux nombres y_i et y_j $(i, j \in \{1, 2, \ldots, m\})$ sont tels que $p_i = p_j$, alors on écarte de l'ensemble $\{y_1, y_2, \ldots, y_m\}$ celui de ces deux nombres qui possède la plus grande puissance de $p_i = p_j$. On se retrouve alors avec un sous-ensemble S non vide de $\{1, 2, \ldots, m\}$ tel que $(y_r, y_s) = 1$ pour $r, s \in S$. D'après le théorème chinois, il existe un entier N tel que $N \equiv x_r \pmod{y_r}$ pour tout $r \in S$. Il s'ensuit que y_r divise $P(N) - P(x_r)$, par conséquent y_r ne divise pas $P(N)$ si $r \in S$. Ainsi, $P(N)$ n'est divisible par aucun des nombres y_k, $k \in \{1, 2, \ldots, m\}$, et donc par aucun a_k, $k \in \{1, 2, \ldots, m\}$, d'où la contradiction.

---

34. Le polynôme Q dont on cherche l'existence est nécessairement de degré $\leqslant$ deg(P). D'un autre côté, soit d le degré du polynôme P ; on peut trouver, grâce à la formule d'interpolation de Lagrange, un polynôme Q de degré $\leqslant d$ tel que

$$Q(i) = q_i, \quad i = 0,\, 1, \ldots,\, d.$$

On se propose de démontrer que $Q(n) = q_n$ pour tout $n \in \mathbb{N}$. Pour ce faire, posons $r_n = k(Q(n) - q_n)$, $n = 0, 1, \ldots$, où k est le dénominateur commun des coefficients de Q (ces coefficients sont rationnels par construction même du polynôme interpolateur de Lagrange). On a ainsi $r_i = 0$ pour $i = 0, 1, \ldots, d$. Par ailleurs, si P est un polynôme quelconque à coefficients entiers, on sait que $m - n$ divise $P(m) - P(n)$ pour tous entiers m, n. Il s'ensuit que $m - n$ divise $r_m - r_n$ pour $m > n \geqslant 0$.

Remarquons maintenant qu'il existe un polynôme R de degré $\leqslant d$ tel que $|r_n| \leqslant R(n)$ pour $n \geqslant 0$: en effet, $|r_n| \leqslant k\big(|Q(n)| + P(n)\big)$. Comme $n - i$ divise $r_n - r_i = r_n$ pour tout $n > d$ et tout i, $0 \leqslant i \leqslant d$, il s'ensuit que $[n, n-1, \ldots, n-d]$ divise r_n pour $n > d$.

On démontre maintenant que $[n, n-1, \ldots, n-d] > R(n)$ pour n assez grand : en effet (voir la note ci-dessous),

$$[n, n-1, \ldots, n-d] \geqslant \frac{\prod\limits_{0 \leqslant i \leqslant d} (n-i)}{\prod\limits_{0 \leqslant i < j \leqslant d} (n-i, n-j)}. \tag{1}$$

Ayant cette inégalité, on obtient

$$[n, n-1, \ldots, n-d] \geqslant \frac{\prod\limits_{0 \leqslant i \leqslant d} (n-i)}{\prod\limits_{0 \leqslant i < j \leqslant d} (j-i)}.$$

Or, R est de degré d et $\prod\limits_{0 \leqslant i \leqslant d} (x-i)$ est de degré $d+1$; il existe donc un entier N tel que $[n, n-1, \ldots, n-d] > R(n)$ pour $n \geqslant N$, ce qui implique que $r_n = 0$ pour $n \geqslant N$.

Finalement, $r_n = 0$ pour $n < N$ puisque, pour $m \geqslant N$, $m - n$ divise $r_m - r_n = -r_n$. Ceci étant vrai pour tout $m \geqslant N$, il s'ensuit que $r_n = 0$ pour tout $n \geqslant 0$, ce qu'il fallait démontrer.

Note. On se propose de démontrer l'inégalité (1) : soit p un nombre premier quelconque et soient $e_1, e_2, \ldots, e_m$ les exposants respectifs de p dans les décompositions en produit de nombres premiers de $a_1, a_2, \ldots, a_m$. L'exposant de p dans la décomposition en produit de nombres premiers de $(a_1, a_2, \ldots, a_m)$ est donc $\max(e_1, e_2, \ldots, e_m)$. Par ailleurs, l'exposant de p dans la décomposition en produit de nombres premiers de

$$\frac{\prod\limits_{0 \leqslant i \leqslant m} a_i}{\prod\limits_{0 \leqslant i < j \leqslant m} (a_i, a_j)}$$

est égal à $\sum_{i=1}^{m} e_i - \sum_{1\leqslant i<j\leqslant m} \min(e_i, e_j)$, ce qui est clairement inférieur à $\max(e_1, e_2, \ldots, e_m)$, d'où le résultat désiré.

---

35. On pose $Q(x) = P(x) - 1$ pour tout x. La formule d'interpolation de Lagrange donne alors

$$Q(3n+1) = \sum_{i=0}^{3n} (-1)^{3n-i} \binom{3n+1}{i} Q(i).$$

Si on pose $\alpha_i = (-1)^i Q(i)$, $i = 0, 1, \ldots, 3n$, alors $\alpha_i = 1, 0, -1, -1, 0$ ou 1 suivant que $i \equiv 0, 1, 2, 3, 4$ ou 5 modulo 6. Pour simplifier l'expression de $Q(3n+1)$, on va utiliser les racines de l'unité, et plus précisément la formule de multisection : on part de la fonction f définie par

$$f(x) = \sum_{i=0}^{3n+1} \binom{3n+1}{i} x^i = (1+x)^{3n+1}.$$

On a alors

$$6Q(3n+1) = (-1)^{3n} \sum_{i=0}^{5} f(\omega_i)(1 - \omega_i^{-2} - \omega_i^{-3} + \omega_i^{-5}),$$

où $\omega_0, \omega_1, \ldots, \omega_5$ sont les racines sixièmes de l'unité. Or,

$$1 - \omega_i^{-2} - \omega_i^{-3} + \omega_i^{-5} = 1 - \omega_i^4 - \omega_i^3 + \omega_i = (1 - \omega_i^3)(1 + \omega_i),$$

d'où :

$$\begin{aligned} 6Q(3n+1) &= (-1)^{3n} \sum_{i=1}^{5} (1+\omega_i)^{3n+2}(1-\omega_i^3) \\ &= 2(-1)^{3n}\big[(1+\omega_1)^{3n+2} + (1+\omega_5)^{3n+2}\big], \end{aligned}$$

où $\omega_1 = e^{i\pi/3}$ et $\omega_5 = e^{-i\pi/3}$.

On en déduit que

$$\begin{aligned} 3Q(3n+1) &= (-1)^{3n}\big(e^{i\pi(3n+2)/6} + e^{-i\pi(3n+2)/6}\big)\big(\sqrt{3}\big)^{3n+2} \\ &= 2 \times (-1)^{3n} \times 3^{(3n+2)/2} \times \cos(\pi n/2 + \pi/3). \end{aligned}$$

Comme $Q(3n+1) = 730 - 1 = 3^6$, il s'ensuit que $n = 4$.

---

36. Si le degré de P est inférieur ou égal à 2, alors $\deg(P^2) = 2 \cdot \deg(P)$ et il s'ensuit que :

$$n(P) - \deg(P) \leqslant \deg(P^2) - \deg(P) = \deg(P) \leqslant 2.$$

On suppose maintenant $\deg(P) \geqslant 3$ et on note $\mathcal{S}^+ = \{k \in \mathbb{Z} \mid P(k) = 1\}$ et $\mathcal{S}^- = \{k \in \mathbb{Z} \mid P(k) = -1\}$. Il s'agit de prouver que $|\mathcal{S}^+ \cup \mathcal{S}^-| \leqslant \deg(P) + 2$. Ceci est immédiat si $\mathcal{S}^+$ ou $\mathcal{S}^-$ est vide : en effet, on aurait dans ce cas $|\mathcal{S}^+ \cup \mathcal{S}^-| \leqslant \deg(P)$ car un polynôme P non réduit à une constante possède au plus $\deg(P)$ racines distinctes.

On se place donc dans le cas où $\mathcal{S}^+$, $\mathcal{S}^- \neq \varnothing$ et on va montrer que $|\mathcal{S}^+ \cup \mathcal{S}^-| \leqslant 4$ ce qui permettra de conclure. Pour ce faire, on considère un entier $\alpha \in \mathcal{S}^+$ et on démontre que, soit $\mathcal{S}^- \subseteq \{\alpha-2,\, \alpha-1,\, \alpha+1\}$, soit $\mathcal{S}^- \subseteq \{\alpha-1,\, \alpha+1,\, \alpha+2\}$: en effet, on sait que si Q est un polynôme à coefficients entiers admettant une racine entière k, il existe un polynôme R tel que $Q = (x-k)R$ et le polynôme R est aussi à coefficients entiers. Si alors $\mathcal{S}^- = \{\beta_1, \beta_2, \ldots, \beta_m\}$, alors $P(x) + 1 = (x-\beta_1)\cdots(x-\beta_m)Q(x)$, où Q est un polynôme à coefficients entiers. En remplaçant x par α, on obtient $(\alpha-\beta_1)\cdots(\alpha-\beta_m)Q(\alpha) = 2$, ce qui prouve que chacun des facteurs $(\alpha-\beta_1), \ldots, (\alpha-\beta_m)$ est, soit ± 1, soit ± 2, 2 et -2 ne pouvant intervenir à la fois. De manière identique, on montre que si $\alpha \in \mathcal{S}^-$ alors, soit $\mathcal{S}^+ \subseteq \{\alpha-2,\, \alpha-1,\, \alpha+1\}$, soit $\mathcal{S}^+ \subseteq \{\alpha-1,\, \alpha+1,\, \alpha+2\}$. Raisonnons maintenant par l'absurde en supposant $\mathcal{S}^+ \cup \mathcal{S}^- = \{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ et $m \geqslant 5$. On peut supposer, sans nuire à la généralité $\gamma_1 < \gamma_2 < \cdots < \gamma_m$ et $\gamma_1 \in \mathcal{S}^+$. On a donc $\mathcal{S}^- \subseteq \{\gamma_1+1,\, \gamma_1+2\}$, ce qui implique que $\{\gamma_4, \ldots, \gamma_m\} \subseteq \mathcal{S}^+$. Mais ni $\gamma_2 \in \mathcal{S}^-$, ni $\gamma_3 \in \mathcal{S}^-$ n'est possible puisque $m \geqslant 5$, ce qui conclut la démonstration.

Note. Il ne peut y avoir égalité que lorsque $\deg(P) = 2$. Dans ce cas, l'égalité est possible si on prend par exemple $P(x) = x^2 - 3x + 1$, ce qui donne $\mathcal{S}^+ \cup \mathcal{S}^- = \{0,\, 1,\, 2,\, 3\}$.

---

37. On commence d'abord par remarquer que lorsque $i = 2^r$, tous les coefficients dans le développement de $(1+x)^i$ sont pairs à l'exception du coefficient dominant et du terme constant, de sorte que l'on puisse écrire dans $\mathbb{Z}/2\mathbb{Z}[X]$:

$$(1+x)^i = 1 + x^i.$$

Ceci se démontre par récurrence sur r en utilisant le fait que dans $\mathbb{Z}/2\mathbb{Z}[X]$, $\left(1+x^i\right)^2 = 1 + x^{2i}$.

Remarquons ensuite que si P et Q sont des polynômes à coefficients entiers, alors $w(P + x^k Q) = w(P) + w(Q)$ pour tout $k > \deg(P)$. Enfin, on a l'inégalité triangulaire $w(P+Q) \leqslant w(P) + w(Q)$ qui résulte du fait que la somme de deux coefficients de même puissance dans P et Q est impaire si et seulement si un et un seul d'entre eux l'est.

Nous allons maintenant établir le résultat par récurrence sur i_n. Les cas $i_n = 0$ ou 1 sont triviaux. Supposons donc le résultat établi pour tout $i_n < N$, et choisissons une famille $i_1, i_2, \ldots, i_n$ telle que $i_n = N$.

Soit m tel que $k = 2^m \leqslant i_n < 2^{m+1}$, et notons $Q = Q_{i_1} + Q_{i_2} + \cdots + Q_{i_n}$. On distingue alors deux cas :

1er cas. On suppose $i_1 < k$ et on écrit

$$Q = \underbrace{Q_{i_1} + Q_{i_2} + \cdots + Q_{i_r}}_{R} + \underbrace{Q_{i_{r+1}} + \cdots + Q_{i_n}}_{(1+x)^k S} = R + (1+x)^k S,$$

où r est tel que $i_r < k \leqslant i_{r+1}$. On a donc $w(Q) = w(R + (1+x)^k S)$, et comme $\deg(R) < k$ et $\deg(S) < k$, il s'ensuit que $w(Q) = w(R + S + x^k S) = w(R+S) +$

$w(S)$. Par ailleurs $w(S) = w(-S)$, et l'inégalité triangulaire donne $w(Q) \geqslant w(R)$. Enfin, par hypothèse de récurrence, $w(R) \geqslant w(Q_{i_1})$.

2ème cas. On suppose $i_1 \geqslant k$ et on écrit

$$Q = (1+x)^k S,$$

avec $\deg(S) < k$. On a ainsi $w(Q) = w(S + x^k S) = 2w(S)$. Si maintenant on écrit $Q_{i_1} = (1+x)^k R$, où $\deg(R) < k$, on a par hypothèse de récurrence $w(S) \geqslant w(R)$. On en déduit que $w(Q) = 2w(S) \geqslant 2w(R) = w(R + x^k R) = w(Q_{i_1})$, et la démonstration est achevée.

---

38. 1ère solution. On reformule le problème en introduisant l'opération de rotation $\mathcal{R}$. Son effet est de mettre à la place de la lampe L_j la lampe L_{j+1}, $j = 0, 1, \ldots, n-1$. Ainsi, la suite d'opérations décrite dans l'énoncé conduit, à une rotation près, à la même configuration que l'application successive de l'opération 0 suivie de la rotation $\mathcal{R}$. Comme, dans notre problème, on s'intéresse uniquement à la situation où toutes les lampes sont allumées, on peut étudier la nouvelle suite d'opérations : $\mathcal{R} \circ$ opération 0, $\mathcal{R} \circ$ opération 0, ...

L'état du système à l'instant j peut être décrit par un polynôme P_j à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ tel que

$$P_j(x) = v_{n-2} + v_{n-3}x + \cdots + v_0 x^{n-2} + v_{n-1}x^{n-1},$$

où $v_k = 0$ ou 1 suivant que la lampe L_k est éteinte ou allumée.

Quand le vecteur $\vec{v} = (v_0, v_1, \ldots, v_{n-1})$ est transformé par l'application de l'opération $\mathcal{R} \circ$ opération 0, le polynôme P_j est transformé au polynôme P_{j+1} de degré $< n$ et tel que

$$P_{j+1} \equiv xP_j(x) \pmod{x^n + x^{n-1} + 1}$$

(les coefficients de P_{j+1} sont réduits modulo 2) : en effet, si $v_{n-1} = 0$, $\mathcal{R} \circ$ opération 0 $= \mathcal{R}$ et $P_{j+1}(x) = xP_j(x)$ et si $v_{n-1} = 1$, alors

$$P_{j+1}(x) = 1 + v_{n-2}x + \cdots + v_1 x^{n-2} + (1 - v_0)x^{n-1} \equiv xP_j(x) \pmod{x^n + x^{n-1} + 1}.$$

Dorénavant, toutes les congruences seront prises modulo $x^n + x^{n-1} + 1$.

Pour prouver a), il suffit de prouver qu'il existe $M(n)$ tel que $x^{M(n)} \equiv 1$. Or, les classes de résidus étant en nombre fini, il existe h et q tels que $x^h = x^{h+q}$, i.e., $x^h(x^q - 1) \equiv 0$ et donc $x^q \equiv 1$.

Pour prouver b), on prend $n = 2^k$ et on cherche à prouver que $x^{n^2-1} \equiv 1$. On a

$$x^{n^2} \equiv \left(x^{n-1} + 1\right)^n \equiv x^{n^2-n} + 1$$

car $\binom{n}{i}$ est pair pour $i = 1, 2, \ldots, n-1$. Il s'ensuit que

$$(1 + x^n)x^{n^2-n} \equiv 1,$$

et le résultat de b) s'ensuit puisque $1 + x^n \equiv x^{n-1}$.

Pour prouver c), on prend $n = 2^k + 1$ et on cherche à prouver que $x^{n^2-n+1} \equiv 1$. On a

$$x^{n^2-1} \equiv \left(x^{n+1}\right)^{n-1} \equiv \left(x + x^n\right)^{n-1} \equiv x^{n-1} + x^{n(n-1)}$$

toujours puisque $\binom{n-1}{i}$ est pair pour $i = 1, 2, \ldots, n-2$. Il s'ensuit que

$$\left(1 + x^{n-1}\right)x^{n^2-n} \equiv x^{n-1},$$

et le résultat de c) en découle puisque $1 + x^{n-1} \equiv x^n$.

2ème solution. Cette solution est due à Marcin Kuczma, leader de l'équipe polonaise.

On associe à chaque lampe L_j un entier $x_j = 0$ ou 1 suivant que L_j est éteinte ou allumée. L'effet de l'opération j consiste donc à changer l'état x_{j-n} de la lampe L_j en x_j tel que

$$x_j \equiv x_{j-n} + x_{j-1} \pmod 2. \tag{1}$$

Ceci est valable pour tout $j \geqslant n$, et aussi pour $j = 0, \ldots, n-1$ en posant

$$x_{-n} = x_{-n+1} = x_{-n+2} = \cdots = x_{-2} = x_{-1} = 1.$$

L'état du système à l'instant j peut être représenté par le vecteur $\vec{v}_j = (x_{j-n}, \ldots, x_{j-1})$. Comme il n'y a que 2^n vecteurs possibles, il s'ensuit qu'il existe j et m tels que $\vec{v}_{j+m} = \vec{v}_j$. Or, ceci impose $\vec{v}_m = \vec{v}_0$ puisque chaque opération est bijective. On a ainsi prouvé a).

Pour prouver b) et c), on observe que

$$\begin{aligned} x_j &\equiv x_{j-n} + x_{j-1} \equiv \left(x_{j-2n} + x_{j-n+1}\right) + \left(x_{j-1-n} + x_{j-2}\right) \\ &\equiv x_{j-2n} + 2x_{j-n-1} + x_{j-2} \\ &\equiv x_{j-3n} + 3x_{j-2n-1} + 3x_{j-n-2} + x_{j-3} \pmod 2, \end{aligned}$$

et ainsi de suite. On arrive ainsi à l'égalité

$$x_j \equiv \sum_{i=0}^{r} \binom{r}{i} x_{j-(r-i)n-i} \pmod 2$$

valable pour tous j et r tels que $j - (r-i)n - i \geqslant -n$. En particulier, si r est de la forme $r = 2^k$, alors $\binom{r}{i}$ est pair pour $i = 1, 2, \ldots, 2^k - 1$. On obtient ainsi

$$x_j \equiv x_{j-rn} + x_{j-r}, \text{ où } r = 2^k, \tag{2}$$

pour tout $j \geqslant (r-1)n$.

Si $n = 2^k$, choisissons $j \geqslant n^2 - n$ et prenons $r = n$. L'égalité (2) se réécrit donc sous la forme :

$$x_j \equiv x_{j-n^2} + x_{j-n} \equiv x_{j-n^2} + (x_j - x_{j-1}) \pmod 2,$$

ce qui implique que $x_{j-n^2} = x_{j-1}$ et donc que la suite (x_j) est périodique de période $n^2 - 1$, d'où b).

Si $n = 2^k + 1$, choisissons $j \geqslant n^2 - 2n$ et prenons $r = n - 1$. On obtient donc, par application de (2),

$$x_j \equiv x_{j-n^2+n} + x_{j-n+1} \equiv x_{j-n^2+n} + (x_{j+1} - x_j) \equiv x_{j-n^2+n} - x_{j+1} + x_j \pmod 2$$

car $x \equiv -x \pmod 2$. Il s'ensuit que $x_{j-n^2+n} = x_{j+1}$, ce qui prouve que (x_j) est périodique de période $n^2 - n + 1$ et termine la démonstration de c).

3ème solution. On représente l'état du système par un vecteur $(a_0, a_1, \ldots, a_{n-1})$, où pour $0 \leqslant i \leqslant n-1$, $a_i = 0$ ou 1 suivant que la lampe L_i est éteinte ou allumée.

On introduit les deux transformations linéaires R et T définies sur $X = \{0,1\}^n$ par (on réduit bien sûr modulo 2) :

$$\begin{aligned} R\colon (a_0, a_1, \ldots, a_{n-1}) &\longmapsto (a_1, a_2, \ldots, a_{n-1}, a_0) \\ T\colon (a_0, a_1, \ldots, a_{n-1}) &\longmapsto (a_1, a_2, \ldots, a_{n-1}, a_{n-1} + a_0) \end{aligned}$$

Il est facile de voir que l'opération j s'identifie à la transformation $S_j = R^{-(j+1)}TR^j$. Si on désigne par $\vec{v}_j$ l'état du système à l'instant j, alors $\vec{v}_j = S_jS_{j-1}\ldots S_0(\vec{v}_0) = R^{-j}T^j(\vec{v}_0)$, où $\vec{v}_0 = (1, 1, \ldots, 1)$.

Comme R laisse inchangé le vecteur $\vec{v}_0$, il s'ensuit que $\vec{v}_j = \vec{v}_0$ si et seulement si $T^j(\vec{v}_0) = \vec{v}_0$.

On a alors a) puisque $X = \{0,1\}^n$ est fini et la transformation T est bijective.

On remarque maintenant que la transformation T vérifie $T^n = T^{n-1} + \mathrm{Id}$. Si on pose $S = T^{-1}$ alors S vérifie $S^n = S + \mathrm{Id}$. Pour prouver b), il suffit de prouver que $S^{n^2-1} = \mathrm{Id}$ si n est une puissance de 2. Or,

$$S^{n^2} = \left(S^n\right)^n = (S + \mathrm{Id})^n = S^n + \mathrm{Id} = S,$$

car n étant une puissance de 2, on a $(S + \mathrm{Id})^n = S^n + \mathrm{Id}$.

Pour prouver c), il suffit de montrer que $S^{n^2-n+1} = \mathrm{Id}$ si n est de la forme $2^k + 1$. Or,

$$S^{n^2-n} = \left(S^n\right)^{n-1} = \left(S + \mathrm{Id}\right)^{n-1} = S^{n-1} + \mathrm{Id},$$

ce qui donne $S^{n^2-n+1} = S^n + S = \mathrm{Id}$.

4

LES INÉGALITÉS

Dans ce chapitre, on étudiera quelques inégalités d'une grande importance dans la résolution des exercices des olympiades. Notre inégalité de base sera l'inégalité du réordonnement. En effet, elle nous permettra d'établir deux autres inégalités d'une grande utilité : l'inégalité de la moyenne et l'inégalité de Chebychev.

Notre objectif sera ensuite de démontrer l'inégalité de Cauchy-Schwarz qui s'avère d'une grande efficacité dans tous les domaines des mathématiques. Sa démonstration a un intérêt en soi, en ce sens qu'elle illustre l'utilisation des trinômes du second degré pour établir des inégalités.

Les techniques d'analyse peuvent s'avérer efficaces dans certaines situations. Il est vrai que l'utilisation de ces techniques est mal vue dans les olympiades, mais le candidat sérieux ne peut pas se permettre d'ignorer l'inégalité de convexité dont l'application est tout à fait possible dans les différentes épreuves d'olympiades. En effet, on appliquera l'inégalité de convexité pour arriver à deux généralisations importantes de l'inégalité de la moyenne : l'inégalité de la moyenne pondérée et l'inégalité de la moyenne généralisée.

On étudiera ensuite les sommes symétriques et l'inégalité de Muirhead. Il s'agit en effet d'un outil assez puissant dans la résolution des problèmes d'inégalités dans les épreuves d'olympiades. Très souvent, il est possible de démontrer ces inégalités sans avoir recours à l'inégalité de Muirhead. Cependant, cette inégalité a l'avantage d'offrir une approche plus systématique quand on a affaire à des sommes symétriques.

On terminera enfin ce chapitre par une présentation de plusieurs exemples d'inégalités dont la solution repose sur des manipulations algébriques où le prérequis principal est simplement une combinaison d'observation, d'adresse et de patience.

4.1. L'inégalité du réordonnement

On considère les nombres $1, 2, \ldots, n$. Chaque réordonnement de ces nombres peut être représenté par une bijection σ de l'ensemble $\{1, 2, \ldots, n\}$ sur lui-même appelée permutation. Ainsi, si on prend les nombres $1, 2, \ldots, n$, et on les range dans l'ordre $n, n-1, \ldots, 2, 1$, on définit la permutation σ telle que $\sigma(i) = n+1-i$.

4.1.1. Théorème. *(Inégalité du réordonnement) La somme $S_\sigma = \sum_{i=1}^{n} a_i b_{\sigma(i)}$, où σ est une permutation de $\{1, 2, \ldots, n\}$, est maximale lorsque les deux suites de nombres réels $a_1, a_2, \ldots, a_n$ et $b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(n)}$ sont rangées dans le même ordre d'inégalités (au sens large), et est minimale lorsqu'elles sont rangées dans l'ordre inverse.*

♦ **Preuve.** S'il existe deux indices i et j tels que $a_i > a_j$ et $b_{\sigma(i)} < b_{\sigma(j)}$, alors on considère les deux sommes

$$\begin{aligned} S &= a_1 b_{\sigma(1)} + \cdots + a_i b_{\sigma(i)} + \cdots + a_j b_{\sigma(j)} + \cdots + a_n b_{\sigma(n)}, \\ S' &= a_1 b_{\sigma(1)} + \cdots + a_i b_{\sigma(j)} + \cdots + a_j b_{\sigma(i)} + \cdots + a_n b_{\sigma(n)}. \end{aligned}$$

On a alors

$$S' - S = (a_i - a_j)(b_{\sigma(j)} - b_{\sigma(i)}) > 0.$$

L'argument précédent montre que si σ ne met pas les b_i dans le même ordre d'inégalités larges que les a_i, la somme $\sum_{i=1}^{n} a_i b_{\sigma(i)}$ n'est pas le plus grand élément de E. Comme l'ensemble décrit par les sommes $\sum_{i=1}^{n} a_i b_{\sigma(i)}$, où σ est une permutation de $\{1, 2, \ldots, n\}$, est fini, il possède un plus grand élément. Ainsi, le plus grand élément de E est atteint lorsque les deux suites sont rangées dans le même ordre. Un raisonnement analogue permet de prouver que le plus petit élément est atteint lorsque les deux suites sont rangées dans l'ordre inverse.

□

♦ **Exemples.**

1. Soient x et y des réels quelconques. On retrouve, grâce à l'inégalité du réordonnement, le fait que

$$x^2 + y^2 \geqslant 2xy.$$

2. Montrer que si $x, y, z \in \mathbb{R}_+$, alors

$$x^3 + y^3 + z^3 \geqslant 3xyz.$$

Par raison de symétrie, on peut supposer que $x \geqslant y \geqslant z$. On a alors $x^2 \geqslant y^2 \geqslant z^2$, et donc

$$x \cdot x^2 + y \cdot y^2 + z \cdot z^2 \geqslant x \cdot y^2 + y \cdot z^2 + z \cdot x^2 = xy \cdot y + yz \cdot z + zx \cdot x.$$

Or, $xy \geqslant xz \geqslant yz$, donc

$$xy \cdot y + yz \cdot z + zx \cdot x \geqslant xy \cdot z + yz \cdot x + zx \cdot y = 3xyz.$$

4.2. L'inégalité de Chebychev

4.2.1. Théorème. *(Inégalité de Chebychev[1]) Si les deux suites $a_1, a_2, \ldots, a_n$ et $b_1, b_2, \ldots, b_n$ sont rangées dans le même ordre d'inégalités au sens large, alors*

$$\sum_{i=1}^{n} a_i b_i \geqslant \frac{1}{n}\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right), \tag{4.1}$$

l'inégalité changeant de sens si les deux suites sont rangées dans l'ordre inverse.

♦ **Preuve.** Supposons que les deux suites $a_1, a_2, \ldots, a_n$ et $b_1, b_2, \ldots, b_n$ soient rangées dans le même ordre, l'inégalité du réordonnement permet alors d'écrire

$$\begin{array}{rcl} a_1b_1 + \cdots + a_nb_n & = & a_1b_1 + \cdots + a_nb_n, \\ a_1b_1 + \cdots + a_nb_n & \geqslant & a_1b_2 + \cdots + a_nb_1, \\ & \cdots & \\ a_1b_1 + \cdots + a_nb_n & \geqslant & a_1b_n + \cdots + a_nb_{n-1}. \end{array}$$

En sommant toutes ces inégalités, on obtient :

$$\begin{array}{rcl} n(a_1b_1 + \cdots + a_nb_n) & \geqslant & a_1(b_1 + b_2 + \cdots + b_n) + \cdots + a_n(b_1 + b_2 + \cdots + b_n) \\ & = & (a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n), \end{array}$$

ce qui prouve l'inégalité énoncée.

□

♦ **Remarque.**

On peut obtenir l'inégalité de Chebychev sans passer par l'intermédiaire de l'inégalité du réordonnement : en effet, quitte à réindexer les deux suites, on peut supposer que $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_n$ et $b_1 \geqslant b_2 \geqslant \cdots \geqslant b_n$, si bien que :

$$\sum_{\substack{i=1 \\ j=1}}^{n} (a_i - a_j)(b_i - b_j) \geqslant 0,$$

ce qui permet de retrouver l'inégalité de Chebychev.

♦ **Exemples.**

1. Soient $a, b, c \in \mathbb{R}_+^*$. Montrer *l'inégalité* dite de *Nesbitt* :

$$\boxed{\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geqslant \frac{3}{2}.} \tag{4.2}$$

Par raison de symétrie, on peut supposer que $a \geqslant b \geqslant c$, d'où $\dfrac{1}{b+c} \geqslant \dfrac{1}{c+a} \geqslant \dfrac{1}{a+b}$, et l'inégalité de Chebychev s'applique

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geqslant \frac{1}{3}(a+b+c)\left[\frac{1}{b+c} + \frac{1}{c+a} + \frac{1}{a+b}\right].$$

1. Pafnouti Lvovitch Chebychev (1821-1894), mathématicien russe.

D'un autre côté, pour tous réels strictement positifs $x_1, x_2, \dots, x_n$, l'inégalité de Chebychev permet d'écrire

$$n = \sum_{i=1}^{n} x_i \times \frac{1}{x_i} \leqslant \frac{1}{n}\Big(\sum_{i=1}^{n} x_i\Big)\Big(\sum_{i=1}^{n} \frac{1}{x_i}\Big),$$

ce qui donne, en prenant $x_1 = b + c$, $x_2 = c + a$ et $x_3 = a + b$:

$$\frac{1}{b+c} + \frac{1}{c+a} + \frac{1}{a+b} \geqslant \frac{9}{2(a+b+c)},$$

d'où,

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geqslant 9 \times \frac{1}{6} = \frac{3}{2}.$$

2. a et b sont deux nombres strictement positifs. Minimiser l'expression

$$E = \frac{x^2}{(ay+bz)(az+by)} + \frac{y^2}{(ax+bz)(az+bx)} + \frac{z^2}{(ax+by)(ay+bx)},$$

où x, y et z sont des réels strictement positifs.

La forme des dénominateurs n'étant pas appropriée pour appliquer les inégalités dont on dispose, on va commencer par effectuer certaines manipulations :

$$\begin{aligned}(ay+bz)(az+by) &= (a^2+b^2)yz + ab(y^2+z^2) \\ &\leqslant \left[\left(\frac{a^2+b^2}{2}\right) + ab\right](y^2+z^2) = \frac{1}{2}(a+b)^2(y^2+z^2).\end{aligned}$$

On remarque au passage que lorsque $y = z$, l'inégalité précédente se réduit à une égalité. On a donc, en appliquant la même transformation à chacun des trois dénominateurs,

$$E \geqslant \frac{2}{(a+b)^2}\left[\frac{x^2}{y^2+z^2} + \frac{y^2}{z^2+x^2} + \frac{z^2}{x^2+y^2}\right].$$

D'après l'inégalité de Nesbitt,

$$E \geqslant \frac{3}{2} \times \frac{2}{(a+b)^2} = \frac{3}{(a+b)^2}.$$

Or, quand $x = y = z$, $E = 3/(a+b)^2$; c'est bien donc la valeur minimale de E.

4.3. L'inégalité de la moyenne

4.3.1. Théorème. *(Inégalité de la moyenne) Soient $x_1, x_2, \dots, x_n$ des nombres strictement positifs. On a alors l'inégalité :*

$$\sqrt[n]{\prod_{i=1}^{n} x_i} \leqslant \frac{1}{n}\left(\sum_{i=1}^{n} x_i\right), \tag{4.3}$$

avec égalité si et seulement si tous les x_i, $i \in \{1, 2, \dots, n\}$, sont égaux.

♦ **Remarques.**

1. La quantité $\prod_{i=1}^{n} {x_i}^{1/n}$ est appelée moyenne géométrique des nombres x_1, x_2, $\ldots$, x_n, et $\sum_{i=1}^{n} x_i/n$ est leur moyenne arithmétique.

2. Dans le cas de $n = 2$, on retrouve l'inégalité bien connue $x^2 + y^2 \geqslant 2xy$ (au moins dans le cas particulier x, $y > 0$), qui s'écrit encore $(x - y)^2 \geqslant 0$, et qui devient donc égalité si et seulement si $x = y$.

3. Dans le cas de $n = 3$, on retrouve l'inégalité qu'on a déjà démontrée à l'aide de l'inégalité du réordonnement

$$x^3 + y^3 + z^3 \geqslant 3xyz.$$

♦ **Preuve. (du théorème)**

1ère méthode. On va appliquer l'inégalité du réordonnement, en choisissant les suites de manière judicieuse. Si on pose

$$a_1 = \frac{x_1}{\left(\prod_{i=1}^{n} x_i\right)^{1/n}}, \quad a_2 = \frac{x_1 x_2}{\left(\prod_{i=1}^{n} x_i\right)^{2/n}}, \ldots, \quad a_n = \frac{x_1 x_2 \cdots x_n}{\left(\prod_{i=1}^{n} x_i\right)^{n/n}} = 1,$$

$$b_1 = \frac{1}{a_1}, \quad b_2 = \frac{1}{a_2}, \ldots, \quad b_n = \frac{1}{a_n} = 1,$$

on a d'après l'inégalité du réordonnement

$$a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \leqslant a_1 b_n + a_2 b_1 + \cdots + a_n b_{n-1},$$

soit encore

$$1 + 1 + \cdots + 1 \leqslant \frac{x_1}{\left(\prod_{i=1}^{n} x_i\right)^{1/n}} + \frac{x_2}{\left(\prod_{i=1}^{n} x_i\right)^{1/n}} + \cdots + \frac{x_n}{\left(\prod_{i=1}^{n} x_i\right)^{1/n}},$$

soit enfin

$$\sqrt[n]{\prod_{i=1}^{n} x_i} \leqslant \frac{1}{n}\left(\sum_{i=1}^{n} x_i\right).$$

□

Cette méthode ne nous permet pas d'étudier le cas d'égalité, ce qui sera fait grâce à la méthode suivante, appelée « méthode de Cauchy ».

2ème méthode. On raisonne par récurrence descendante sur le nombre des réels considérés. En effet, on va d'abord prouver le résultat pour les puissances de 2, puis montrer que si le résultat est vrai pour un entier positif $n \geqslant 2$, alors il l'est également pour $n - 1$.

Le résultat est en effet acquis pour $n = 2$. S'il est vrai pour $k \in \mathbb{N}^*$, alors il est vrai pour $2k$. En effet, soit $x_1, x_2, \ldots, x_{2k}$, des nombres strictement positifs. On a alors

$$\frac{x_1 + x_2 + \cdots + x_{2k}}{2k} = \frac{1}{2}\left\{\frac{(x_1 + x_2 + \cdots + x_k)}{k} + \frac{(x_{k+1} + x_{k+2} + \cdots + x_{2k})}{k}\right\}$$

$$\geqslant \frac{1}{2}\left(\sqrt[k]{\prod_{i=1}^{k} x_i} + \sqrt[k]{\prod_{i=k+1}^{2k} x_i}\right) \geqslant \sqrt[2k]{\prod_{i=1}^{2k} x_i}.$$

car $a+b \geqslant 2\sqrt{ab}$, pour tous réels positifs a et b. Par ailleurs, pour avoir l'égalité générale, il faut que toutes les inégalités intermédiaires se réduisent à des égalités, ce qui implique par hypothèse de récurrence que les nombres $x_1, x_2, \ldots, x_k$ d'une part, et $x_{k+1}, x_{k+2}, \ldots, x_{2k}$ d'autre part sont égaux. Mais puisqu'on a encore l'égalité entre $\left(\prod_{i=1}^{k} x_i\right)^{1/k}$ et $\left(\prod_{i=k+1}^{2k} x_i\right)^{1/k}$, on en déduit que l'on a égalité générale si et seulement si les $2k$ nombres $x_1, x_2, \ldots, x_{2k}$, sont égaux.

Montrons maintenant que si l'inégalité est vrai pour $n \geqslant 2$, elle l'est également pour $n-1$. En effet, soient $x_1, x_2, \ldots, x_{n-1}$ des nombres strictement positifs, et posons $x_n = (x_1 + x_2 + \cdots + x_{n-1})/(n-1)$. Puisque l'inégalité est supposée être vraie pour tout ensemble de n nombres strictement positifs, on peut écrire :

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geqslant (x_1 x_2 \cdots x_{n-1})^{1/n} \cdot x_n^{1/n},$$

par conséquent

$$\frac{n-1}{n} \cdot x_n + \frac{x_n}{n} \geqslant (x_1 x_2 \cdots x_{n-1})^{1/n} \cdot x_n^{1/n},$$

soit

$$x_n \geqslant \sqrt[n-1]{\prod_{i=1}^{n-1} x_i}.$$

Le cas d'égalité pour $n-1$ nombres se déduit sans peine de celui correspondant à n nombres. La démonstration est donc achevée.

□

♦ **Remarques.**

1. Ayant l'inégalité entre la moyenne géométrique et la moyenne arithmétique, on peut établir l'inégalité suivante

$$\frac{n}{\left(\displaystyle\sum_{i=1}^{n} \frac{1}{x_i}\right)} \leqslant \sqrt[n]{\prod_{i=1}^{n} x_i},$$

reliant la moyenne dite harmonique à la moyenne géométrique de n nombres strictement positifs (il suffit d'appliquer le théorème (4.3.1) en prenant les n nombres $1/x_1$, $1/x_2, \ldots, 1/x_n$).

2. L'inégalité de Chebychev appliquée en prenant la même suite $x_1, x_2, \ldots, x_n$ donne immédiatement

$$\frac{1}{n}\left(\sum_{i=1}^{n} x_i\right) \leqslant \left(\frac{1}{n}\sum_{i=1}^{n} x_i^2\right)^{1/2}.$$

Le terme de droite dans la dernière inégalité s'appelle moyenne quadratique des nombres $x_1, x_2, \ldots, x_n$.

3. On peut résumer les inégalités précédentes en écrivant pour tous réels strictement positifs $x_1, x_2, \ldots, x_n$,

$$\min(x_1, x_2, \ldots, x_n) \leqslant \frac{n}{\dfrac{1}{x_1} + \dfrac{1}{x_2} + \cdots + \dfrac{1}{x_n}} \leqslant \sqrt[n]{x_1 x_2 \cdots x_n} \leqslant \frac{x_1 + x_2 + \cdots + x_n}{n}$$

$$\leqslant \sqrt{\frac{{x_1}^2 + x_2^2 + \cdots + x_n^2}{n}} \leqslant \max(x_1, x_2, \ldots, x_n). \tag{4.4}$$

♦ **Exemples.**

1. Soient $x_1, x_2, \ldots, x_n$ des nombres réels strictement positifs. On a alors

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + \cdots + \frac{x_n}{x_1} \geqslant n,$$

en effet,

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + \cdots + \frac{x_n}{x_1} \geqslant n \sqrt[n]{\frac{x_1}{x_2} \frac{x_2}{x_3} \cdots \frac{x_n}{x_1}} = n.$$

On aurait pu également démontrer la dernière inégalité sans appliquer l'inégalité de la moyenne : en effet, l'inégalité est vraie pour $n = 2$ (car $(x_1 - x_2)^2 \geqslant 0$). On se propose alors de prouver le résultat pour tout entier $n \geqslant 2$ en raisonnant par récurrence.

Supposons le résultat vrai pour tout ensemble constitué de $n-1$ nombres strictement positifs, et prenons n nombres $x_1, x_2, \ldots, x_n$, dans $\mathbb{R}_+^*$. Appliquons l'hypothèse de récurrence aux $n-1$ premiers nombres. Il nous suffirait alors de montrer que

$$\frac{x_{n-1}}{x_n} + \frac{x_n}{x_1} - \frac{x_{n-1}}{x_1} \geqslant 1.$$

Or, si l'on prend, ce que l'on peut toujours faire quitte à réindexer les n nombres considérés, $x_n = \min(x_1, x_2, \ldots, x_n)$, on s'aperçoit que l'inégalité précédente est bien vérifiée puisque $x_{n-1} - x_n \geqslant 0$ et $x_1 \geqslant x_n$.

2. Pour tout entier $n > 1$, on a

$$n! < \left(\frac{n+1}{2}\right)^n,$$

ce qui découle du fait que

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

3. Soient $a_1, a_2, \ldots, a_n$ des nombres réels strictement positifs tels que $a_1 \times a_2 \times \cdots \times a_n = 1/2^{n^2+n}$. Montrer que

$$(1 + 2^2 a_1)(1 + 2^4 a_2) \cdots (1 + 2^{2n} a_n) \geqslant 2^n,$$

et déterminer les cas d'égalité.

(Olympiades maghrébines-1985)

On utilisera l'inégalité $a+b \geqslant 2\sqrt{ab}$, valable pour tous réels positifs a et b. On a alors :

$$\begin{gathered}
1+2^2a_1 \geqslant 2\times 2\sqrt{a_1},\\
1+2^4a_2 \geqslant 2\times 2^2\sqrt{a_2},\\
\dots\\
1+2^{2n}a_n \geqslant 2\times 2^n\sqrt{a_n},
\end{gathered}$$

par conséquent,

$$(1+2^2a_1)(1+2^4a_2)\cdots(1+2^{2n}a_n) \geqslant 2^n,$$

avec égalité si et seulement si

$$a_1 = \frac{1}{2^2},\quad a_2 = \frac{1}{2^4},\dots,\quad a_n = \frac{1}{2^{2n}}.$$

4.4. L'inégalité de Cauchy-Schwarz

4.4.1. Théorème. *(Inégalité de Cauchy[2]-Schwarz[3]) Soient $(x_1,x_2,\dots,x_n)$ et $(y_1,y_2,\dots,y_n)$ deux vecteurs de $\mathbb{R}^n$. On a alors l'inégalité*

$$\left|\sum_{i=1}^n x_iy_i\right| \leqslant \sqrt{\sum_{i=1}^n x_i^2}\sqrt{\sum_{i=1}^n y_i^2}, \tag{4.5}$$

avec égalité si et seulement si les deux vecteurs $(x_1,x_2,\dots,x_n)$ et $(y_1,y_2,\dots,y_n)$ sont proportionnels.

♦ **Preuve.** Le théorème est évident dans le cas particulier $x_1=x_2=\cdots=x_n=0$. On suppose ce cas exclu dans la suite et on considère le trinôme du second degré

$$P(x) = \left(\sum_{i=1}^n x_i^2\right)x^2 - 2\left(\sum_{i=1}^n x_iy_i\right)x + \left(\sum_{i=1}^n y_i^2\right);$$

on a alors

$$P(x) = \sum_{i=1}^n (x_i^2x^2 - 2x_iy_ix + y_i^2) = \sum_{i=1}^n (x_ix-y_i)^2,$$

et donc $P(x)\geqslant 0$, pour tout $x\in\mathbb{R}$. Il s'ensuit que le discriminant réduit de $P(x)$ est négatif ou nul, c'est à dire $(\sum_{i=1}^n x_iy_i)^2 - (\sum_{i=1}^n x_i^2)(\sum_{i=1}^n y_i^2) \leqslant 0$, qui est l'inégalité de Cauchy-Schwarz.

2. Augustin Cauchy (1789-1857), mathématicien français.
3. Hermann Schwarz (1843-1921), mathématicien allemand.

L'égalité a lieu si et seulement s'il existe x_0 tel que $P(x_0) = 0$, c'est-à-dire $x_i x_0 - y_i = 0$, pour tout $i \in \{1, 2, \ldots, n\}$, ce qui revient à dire que les deux vecteurs $(x_1, x_2, \ldots, x_n)$ et $(y_1, y_2, \ldots, y_n)$ de $\mathbb{R}^n$ sont proportionnels.

□

♦ **Remarques.**

1. L'inégalité de Cauchy-Schwarz peut également s'établir à l'aide d'un raisonnement par récurrence sur le nombre des réels considérés (laissé au soin du lecteur), mais la technique utilisée plus haut a un intérêt en soi. En effet, on va la mettre en œuvre pour démontrer l'inégalité suivante :

$$\frac{\left(\sum\limits_{i=1}^{n} a_i^2\right)\left(\sum\limits_{i=1}^{n} b_i^2\right)}{\left(\sum\limits_{i=1}^{n} a_i b_i\right)^2} \leqslant \frac{(m+M)^2}{4mM}, \tag{4.6}$$

valable pour tous réels $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$, vérifiant $0 < m \leqslant a_i/b_i \leqslant M$ pour tout $i \in \{1, 2, \ldots, n\}$. Considérons le trinôme du second degré

$$P(x) = \left(m \sum_{i=1}^{n} a_i^2\right) x^2 - \left((m+M) \sum_{i=1}^{n} a_i b_i\right) x + M \sum_{i=1}^{n} b_i^2.$$

Il suffit d'établir que le discriminant de ce trinôme est positif ou nul, ce qui revient à prouver que P s'annule ou change de signe sur $\mathbb{R}$. Écrivons alors $P(x) = \sum_{i=1}^{n} \varphi_i(x)$, où

$$\varphi_i(x) = m a_i^2 x^2 - (m+M) a_i b_i x + M b_i^2 = (m a_i x - M b_i)(a_i x - b_i).$$

Il apparaît que $\varphi_i(1/m) \leqslant 0$ et $\varphi_i(1/M) \geqslant 0$, ce qui montre que $P(1/m) \leqslant 0$ et $P(1/M) \geqslant 0$, d'où le résultat.

2. En regroupant l'inégalité de Cauchy-Schwarz et l'inégalité de Chebychev, on arrive à un encadrement de la somme $\sum_{i=1}^{n} a_i b_i$:

$$\frac{1}{n}\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) \leqslant \sum_{i=1}^{n} a_i b_i \leqslant \sqrt{\sum_{i=1}^{n} a_i^2}\sqrt{\sum_{i=1}^{n} b_i^2},$$

valable pour toutes suites de nombres réels $a_1, a_2, \ldots, a_n$, et $b_1, b_2, \ldots, b_n$, rangées dans le même ordre d'inégalités au sens large.

3. On peut dériver de l'inégalité de Cauchy-Schwarz l'inégalité suivante :

$$\boxed{\left(\sum_{i=1}^{n} \alpha_i x_i\right)\left(\sum_{i=1}^{n} \frac{x_i}{\alpha_i}\right) \geqslant \left(\sum_{i=1}^{n} x_i\right)^2,} \tag{4.7}$$

où $\forall\, i \in \{1, 2, \ldots, n\}$, α_i et x_i sont des réels strictement positifs. Plusieurs exercices proposés en fin de ce chapitre permettront d'illustrer la raison pour laquelle cette forme un peu particulière est souvent plus facile à reconnaître que l'inégalité de Cauchy-Schwarz telle qu'elle est énoncée dans le théorème 4.4.1.

♦ **Exemples.**

1. Soient $a_1, a_2, \dots, a_n$ des réels strictement positifs et soit $s = \sum_{i=1}^{n} a_i$. Prouver que

$$\frac{s}{s-a_1} + \frac{s}{s-a_2} + \cdots + \frac{s}{s-a_n} \geqslant \frac{n^2}{n-1}.$$

On applique l'inégalité de Cauchy-Schwarz sous la forme 4.7

$$\left(\frac{s}{s-a_1} + \frac{s}{s-a_2} + \cdots + \frac{s}{s-a_n}\right) \underbrace{\left(\frac{s-a_1}{s} + \frac{s-a_2}{s} + \cdots + \frac{s-a_n}{s}\right)}_{=n-1} \geqslant n^2,$$

d'où le résultat.

On aurait aussi pu utiliser l'inégalité entre moyennes harmonique et arithmétique

$$\frac{n}{1/x_1 + 1/x_2 + \cdots + 1/x_n} \leqslant \frac{x_1 + x_2 + \cdots + x_n}{n},$$

signalée en remarque au paragraphe 4.3.

On remarque par ailleurs que l'inégalité de Nesbitt, démontrée en exemple au paragraphe 4.2, est un cas particulier de l'inégalité précédente où $n = 3$.

2. Prouver que, pour tous réels strictement positifs a, b, c, d,

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

On applique l'inégalité de Cauchy-Schwarz sous la forme 4.7 :

$$\left[\frac{a}{b+c} + \frac{b}{c+d} + \frac{c}{d+a} + \frac{d}{a+b}\right] \times P \geqslant (a+b+c+d)^2,$$

où $P = \big[a\,(b+c) + b\,(c+d) + c\,(d+a) + d\,(a+b)\big]$.

Ceci étant, pour pouvoir démontrer le résultat recherché, il suffit de s'assurer que

$$ab + 2ac + cb + cd + da + 2db \leqslant \frac{1}{2}(a+b+c+d)^2;$$

or, en faisant la différence entre les deux membres de la dernière inégalité, on s'aperçoit qu'elle est égale à $\frac{1}{2}(a-c)^2 + \frac{1}{2}(b-d)^2$. Ainsi, on a établi l'inégalité énoncée, avec égalité si et seulement si $a = c$ et $b = d$.

3. Utiliser l'inégalité de Cauchy-Schwarz pour trouver la valeur maximale de

$$f(x, y, z) = 3x + y + 2z,$$

sachant que $x^2 + y^2 + z^2 = 1$.

On considère les deux vecteurs (x, y, z) et $(3, 1, 2)$. On a donc

$$(3x + y + 2z)^2 \leqslant (x^2 + y^2 + z^2)(3^2 + 1^2 + 2^2) = 14.$$

Ainsi, $3x + y + 2z \leqslant \sqrt{14}$, avec égalité lorsqu'il existe $\lambda \in \mathbb{R}_+$ tel que

$$\lambda = \frac{x}{3} = y = \frac{z}{2},$$

mais alors $\lambda = 1/\sqrt{14}$, et donc

$$x = \frac{3}{\sqrt{14}}, \quad y = \frac{1}{\sqrt{14}}, \quad z = \frac{2}{\sqrt{14}}.$$

Ainsi, la valeur maximale de f est $\sqrt{14}$, et elle est atteinte pour les valeurs précédemment mentionnées de x, y et z.

4. $a_1, a_2, \ldots, a_n$ sont des réels donnés non tous nuls. Déterminer les réels r_1, r_2, $\ldots$, r_n tels que

$$\sum_{i=1}^{n} r_i(x_i - a_i) \leqslant \sqrt{\sum_{i=1}^{n} x_i^2} - \sqrt{\sum_{i=1}^{n} a_i^2},$$

pour tous réels $x_1, x_2, \ldots, x_n$.

(Olympiades chinoises-1988)

Si $x_1 = x_2 = \cdots = x_n = 0$, alors

$$\sqrt{\sum_{i=1}^{n} a_i^2} \leqslant \sum_{i=1}^{n} r_i a_i. \tag{1}$$

Si $x_i = 2a_i$ pour tout i, $1 \leqslant i \leqslant n$, alors

$$\sqrt{\sum_{i=1}^{n} a_i^2} \geqslant \sum_{i=1}^{n} r_i a_i, \tag{2}$$

et il s'ensuit de (1) et (2) que :

$$\sqrt{\sum_{i=1}^{n} a_i^2} = \sum_{i=1}^{n} r_i a_i. \tag{3}$$

Or, par l'inégalité de Cauchy-Schwarz,

$$\sum_{i=1}^{n} r_i a_i \leqslant \sqrt{\sum_{i=1}^{n} a_i^2}\sqrt{\sum_{i=1}^{n} r_i^2}. \tag{4}$$

Comme $\sum_{i=1}^{n} a_i^2 \neq 0$, on obtient $\sqrt{\sum_{i=1}^{n} r_i^2} \geqslant 1$. Si maintenant on prend $x_i = r_i$ pour $1 \leqslant i \leqslant n$, alors

$$\sum_{i=1}^{n} r_i^2 - \sum_{i=1}^{n} r_i a_i \leqslant \sqrt{\sum_{i=1}^{n} r_i^2} - \sqrt{\sum_{i=1}^{n} a_i^2}.$$

Il s'ensuit de (3) que $\sqrt{\sum_{i=1}^{n} r_i^2} \leqslant 1$, ce qui implique que l'inégalité (4) se réduit à une égalité. Il existe donc une constante $\lambda \in \mathbb{R}_+$ telle que $r_i = \lambda a_i$ pour tout i, $1 \leqslant i \leqslant n$. De (3), on tire alors :

$$\lambda = \frac{1}{\left(\sum_{i=1}^{n} a_i^2\right)^{1/2}}, \qquad r_i = \frac{a_i}{\left(\sum_{i=1}^{n} a_i^2\right)^{1/2}}.$$

4.5. L'inégalité triangulaire

4.5.1. Théorème. *(Inégalité de Minkowski[4]) Soient* $(x_1, x_2, \ldots, x_n)$ *et* $(y_1, y_2, \ldots, y_n)$ *des vecteurs de* $\mathbb{R}^n$*. On a alors*

$$\sqrt{\sum_{i=1}^{n} (x_i + y_i)^2} \leqslant \sqrt{\sum_{i=1}^{n} x_i^2} + \sqrt{\sum_{i=1}^{n} y_i^2}. \tag{4.8}$$

♦ **Remarques.**

1. Le cas $n = 2$ est bien connu : c'est l'inégalité triangulaire dans le plan euclidien, qui exprime le fait que la somme des longueurs de deux des côtés d'un triangle est supérieure à la longueur du troisième.

2. Le cas $n = 1$ est le plus élémentaire certes, mais également le plus fréquent,

$$(\forall\, x, y \in \mathbb{R}) \quad |x + y| \leqslant |x| + |y|.$$

♦ **Preuve.** On a les équivalences :

$$\begin{aligned}
& \sqrt{\sum_{i=1}^{n} (x_i + y_i)^2} \leqslant \sqrt{\sum_{i=1}^{n} x_i^2} + \sqrt{\sum_{i=1}^{n} y_i^2} \\
\iff\quad & \sum_{i=1}^{n} (x_i + y_i)^2 \leqslant \sum_{i=1}^{n} x_i^2 + \sum_{i=1}^{n} y_i^2 + 2\sqrt{\sum_{i=1}^{n} x_i^2}\sqrt{\sum_{i=1}^{n} y_i^2} \\
\iff\quad & \sum_{i=1}^{n} x_i y_i \leqslant \sqrt{\sum_{i=1}^{n} x_i^2}\sqrt{\sum_{i=1}^{n} y_i^2}.
\end{aligned}$$

La dernière inégalité étant vraie pour tous vecteurs $(x_1, x_2, \ldots, x_n)$ et $(y_1, y_2, \ldots, y_n)$ de $\mathbb{R}^n$ (inégalité de Cauchy-Schwarz), le théorème 4.5.1 est donc démontré. □

4. Hermann Minkowski (1864-1909), mathématicien allemand.

4.5.2. Transformation de Ravi. Lorsque l'inégalité à prouver porte sur les longueurs a, b, c des côtés d'un triangle, il est souvent utile de faire la transformation suivante :

$$a = x + y, \quad b = y + z, \quad c = z + x,$$

où

$$x = \frac{a+c-b}{2}, \quad y = \frac{a+b-c}{2}, \quad z = \frac{b+c-a}{2},$$

sont des réels strictement positifs.

Géométriquement, x, y, z représentent respectivement les longueurs BQ, CR, AP où P, Q, R sont les points où le cercle inscrit dans le triangle ABC vient toucher les côtés du triangle.

L'intérêt de cette transformation est de pouvoir se débarrasser de la contrainte imposée par les inégalités triangulaires reliant les nombres a, b et c, et de ne plus avoir à manipuler qu'une inégalité portant sur des nombres positifs.

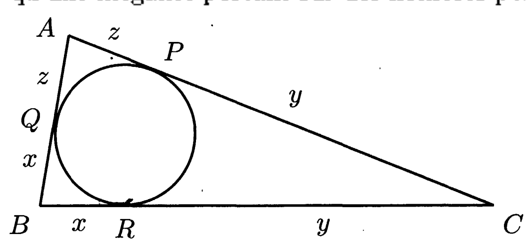


FIG. 4.1.

♦ **Exemples.**

1. Soient a, b, c les longueurs des côtés d'un triangle. Prouver que

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

(Olympiades indiennes-1989)

On pose $a = x + y$, $b = y + z$, $c = z + x$, où $x, y, z > 0$. On a alors

$$\begin{aligned} \frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} &= \frac{x+y}{x+2z+y} + \frac{y+z}{y+2x+z} + \frac{z+x}{z+2y+x} \\ &< \frac{x+y}{x+z+y} + \frac{y+z}{y+x+z} + \frac{z+x}{z+y+x} = 2. \end{aligned}$$

4.6. Les fonctions convexes

4.6.1. Définition. *Soient I un intervalle et $f : I \to \mathbb{R}$ une fonction numérique. La fonction f est dite convexe (resp. concave) sur I si pour tous x_1 et x_2 dans I, on a :*

$$f(\lambda x_1 + (1-\lambda)x_2) \leqslant (\text{resp.} \geqslant)\ \lambda f(x_1) + (1-\lambda) f(x_2),$$

pour tout $\lambda \in [0, 1]$.

♦ **Remarques.**

1. (*Interprétation géométrique*) Soit f une fonction définie sur un intervalle I, et $A(a, f(a))$, $B(b, f(b))$ deux points du graphe de f. Si f est convexe, alors le segment $[AB]$ est en dessus du graphe de f, et si elle est concave, le segment $[AB]$ est en dessous du graphe :

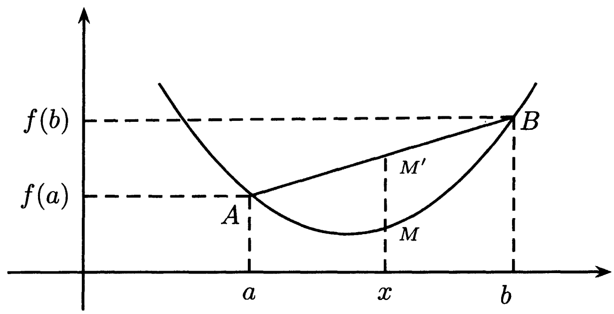


FIG. 4.2.

En effet, si $x \in [a, b]$, alors on peut l'écrire sous la forme $x = \lambda a + (1 - \lambda)b$ où $\lambda \in [0, 1]$. Ainsi,

$$\overline{MM'} = [\lambda f(a) + (1 - \lambda) f(b)] - f(\lambda a + (1 - \lambda)b).$$

4.6.2. Théorème. *(Inégalité de convexité) Soit f une fonction convexe (resp. concave) sur un intervalle I. Pour tous nombres $x_1, x_2, \ldots, x_n$ appartenant à I, on a l'inégalité :*

$$f(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n) \leqslant \text{(resp. } \geqslant) \ \alpha_1 f(x_1) + \alpha_2 f(x_2) + \cdots + \alpha_n f(x_n), \quad (4.9)$$

pour tous réels positifs $\alpha_1, \alpha_2, \ldots, \alpha_n$ vérifiant $\alpha_1 + \alpha_2 + \cdots + \alpha_n = 1$.

♦ **Preuve.** Si f est convexe, $-f$ est concave et réciproquement ; on peut donc supposer f convexe.

- Pour $n = 2$, c'est précisément la définition de la convexité.

- Supposons le résultat vrai pour n. Soient alors $x_1, x_2, \ldots, x_{n+1}$, des éléments de l'intervalle I, et $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ des réels strictement positifs vérifiant $\alpha_1 + \alpha_2 + \cdots + \alpha_{n+1} = 1$ (si l'un des α_i est nul, le résultat est déjà acquis par l'hypothèse de récurrence). On a donc

$$\begin{aligned} f\left(\sum_{i=1}^{n+1} \alpha_i x_i\right) &= f\left(\sum_{i=1}^{n} \alpha_i \cdot \frac{\sum_{i=1}^{n} \alpha_i x_i}{\sum_{i=1}^{n} \alpha_i} + \alpha_{n+1} x_{n+1}\right) \\ &\leqslant \sum_{i=1}^{n} \alpha_i \cdot f\left(\frac{\sum_{i=1}^{n} \alpha_i x_i}{\sum_{i=1}^{n} \alpha_i}\right) + \alpha_{n-1} f(x_{n+1}), \end{aligned}$$

et par hypothèse de récurrence, on peut écrire

$$f\left(\frac{\sum_{i=1}^{n}\alpha_i x_i}{\sum_{i=1}^{n}\alpha_i}\right) \leqslant \frac{\sum_{i=1}^{n}\alpha_i f(x_i)}{\sum_{i=1}^{n}\alpha_i},$$

ce qui prouve que $f\left(\sum_{i=1}^{n+1}\alpha_i x_i\right) \leqslant \sum_{i=1}^{n+1}\alpha_i f(x_i)$.

□

4.6.3. Propriétés.

1. *Dans le cas où f est convexe (resp. concave), et qu'elle n'est affine sur aucun intervalle de longueur strictement positive, et si $\alpha_i > 0$ pour tout $i \in \{1, 2, \dots, n\}$, on a $f(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n) = \alpha_1 f(x_1) + \alpha_2 f(x_2) + \cdots + \alpha_n f(x_n)$ si et seulement si $x_1 = x_2 = \cdots = x_n$.*
2. *Soit I un intervalle, α un élément de I et $f\colon I \to \mathbb{R}$ une fonction numérique; désignons par f_α la fonction définie sur $I \setminus \{\alpha\}$ par :*

$$(\forall\, x \in I \setminus \{\alpha\})\ f_\alpha(x) = \frac{f(x) - f(\alpha)}{x - \alpha}.$$

f est convexe sur I si et seulement si, pour tout x_0 de I, la fonction f_{x_0} est croissante sur $I \setminus \{x_0\}$, et elle est concave si et seulement si, pour tout x_0 de I, la fonction f_{x_0} est décroissante.
3. *Une fonction convexe définie sur un segment est continue sur l'intérieur de ce segment et atteint son maximum en l'une de ses deux extrémités. Ce résultat se généralise à une fonction de plusieurs variables, définie sur un produit de segments de $\mathbb{R}$, et convexe en chacune de ses variables (c'est dire qu'en fixant toutes les variables sauf une, la fonction dépendant de cette dernière variable est convexe).*
4. *Soit f une fonction deux fois dérivable sur un intervalle I. Si la dérivée seconde de f est positive ou nulle en tout point alors f est convexe sur I.*

♦ **Remarques.**

1. La deuxième propriété est illustrée par le schéma suivant :

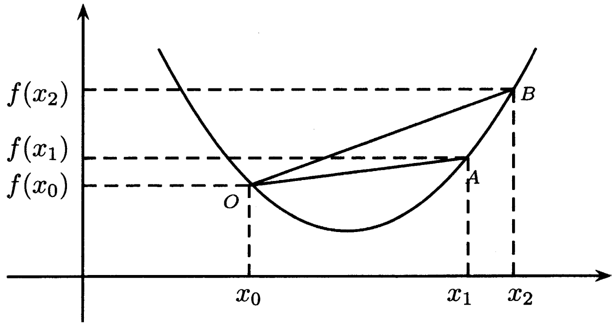


FIG. 4.3.

Le fait que f_{x_0} est croissante sur $I\setminus\{x_0\}$ signifie que la pente de la droite (OB) est supérieure ou égale à celle de la droite (OA).

2. Une fonction peut être convexe sans admettre des dérivées secondes en tout point. Cependant, la quatrième propriété constitue souvent un critère rapide pour vérifier qu'une fonction est convexe.

♦ **Preuve. (du dernier point)** Soient a, $b \in I$ tels que $a < b$ par exemple. Soit $x = \lambda a + (1-\lambda)b$; appliquons le théorème des accroissements finis à f sur $[a, x]$ et $[x, b]$; il existe $c \in]a, x[$ et $d \in]x, b[$ tels que

$$\begin{cases} f(x) - f(a) = (x-a)f'(c) = (1-\lambda)(b-a)f'(c), \\ f(b) - f(x) = (b-x)f'(d) = \lambda(b-a)f'(d). \end{cases}$$

f' étant croissante, on obtient :

$$\lambda\big(f(x) - f(a)\big) \leqslant (1-\lambda)\big(f(b) - f(x)\big),$$

ce qui montre que f est convexe.

□

♦ **Exemples.**

1. On a l'inégalité suivante, qui généralise l'inégalité entre les moyennes géométrique et arithmétique de n nombres positifs :

4.6.4 Théorème. *(Inégalité de la moyenne pondérée) Si $x_1, x_2, \ldots, x_n$ sont des réels strictement positifs, et $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont des réels strictement positifs tels que $\alpha_1 + \alpha_2 + \cdots + \alpha_n = 1$, alors :*

$$\sum_{i=1}^{n} \alpha_i x_i \geqslant \prod_{i=1}^{n} {x_i}^{\alpha_i}, \tag{4.10}$$

avec égalité si et seulement si tous les $x_i, i \in \{1, 2, \ldots, n\}$, sont égaux.

La fonction logarithme népérien est concave sur $\mathbb{R}_+^*$ ($\ln''(x) = -1/x^2 < 0$). Il s'ensuit que

$$\ln\left(\sum_{i=1}^{n} \alpha_i \cdot x_i\right) \geqslant \sum_{i=1}^{n} \alpha_i \cdot \ln(x_i),$$

ce qui donne

$$\sum_{i=1}^{n} \alpha_i \cdot x_i \geqslant \prod_{i=1}^{n} {x_i}^{\alpha_i};$$

l'égalité n'a lieu que si $x_i = x_j$ pour tous $i, j \in \{1, 2, \ldots, n\}$ (car la fonction logarithme népérien n'est affine sur aucun intervalle de longueur strictement positive inclus dans $\mathbb{R}_+^*$).

2. Retrouver l'inégalité entre la moyenne arithmétique et la moyenne quadratique : si $x_1, x_2, \ldots, x_n$ sont des réels quelconques, alors

$$\frac{1}{n}\left[\sum_{i=1}^{n} x_i\right] \leqslant \sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}.$$

En effet, la fonction $x \mapsto x^2$ est convexe, d'où :

$$\left(\sum_{i=1}^{n} \frac{1}{n} x_i\right)^2 \leqslant \sum_{i=1}^{n} \frac{1}{n} x_i^2.$$

3. Soient $x_1, x_2, \ldots, x_n$ des réels dans l'intervalle $]0,1[$ tels que $\sum_{i=1}^{n} x_i = 1$. Prouver que

$$\sum_{i=1}^{n} \frac{x_i}{\sqrt{1-x_i}} \geqslant \frac{\sum_{i=1}^{n} \sqrt{x_i}}{\sqrt{n-1}}.$$

(Olympiades chinoises-1989)

La fonction $t \mapsto \dfrac{t}{\sqrt{1-t}}$ est convexe sur $[0,1[$ (s'assurer que $f'' > 0$). On a donc

$$\frac{1}{n} \sum_{i=1}^{n} \frac{x_i}{\sqrt{1-x_i}} \geqslant \frac{1/n}{\sqrt{1-1/n}} = \frac{1}{\sqrt{n}\sqrt{n-1}},$$

ce qui s'écrit encore

$$\sum_{i=1}^{n} \frac{x_i}{\sqrt{1-x_i}} \geqslant \frac{\sqrt{n}}{\sqrt{n-1}}.$$

Pour conclure, il suffit de prouver que $\displaystyle\sum_{i=1}^{n} \sqrt{x_i} \leqslant \sqrt{n}$. Or, l'inégalité de Cauchy-Schwarz nous donne

$$\sum_{i=1}^{n} \sqrt{x_i} \leqslant \sqrt{\sum_{i=1}^{n} x_i} \sqrt{\sum_{i=1}^{n} 1} = \sqrt{n}.$$

4. Soient a, b, c des réels tels que $0 \leqslant a, b, c \leqslant 1$. Prouver l'inégalité

$$\frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c) \leqslant 1.$$

(Olympiades des États-Unis-1980)

On remarque que la fonction

$$f(a,b,c) = \frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c)$$

est convexe en chacune de ses variables sur un cube de $\mathbb{R}^3$. Elle atteint donc son maximum en un point extrémal du cube, soit l'un des 8 sommets du cube. Ceci permet de conclure.

4.6.5. Compléments.

1. Théorème. *(Inégalité de Hölder[5]) Soient les nombres strictement positifs* $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$, α *et* β *avec,* $\alpha + \beta = 1$. *On a l'inégalité*

$$\sum_{i=1}^{n} x_i^{\alpha} \cdot y_i^{\beta} \leqslant \left(\sum_{i=1}^{n} x_i\right)^{\alpha} \left(\sum_{i=1}^{n} y_i\right)^{\beta}, \tag{4.11}$$

avec égalité si et seulement si les deux vecteurs $(x_1, x_2, \ldots, x_n)$ *et* $(y_1, y_2, \ldots, y_n)$ *sont proportionnels dans* $\mathbb{R}^n$.

♦ **Preuve.** Posons $\sum_{i=1}^{n} x_i = X$ et $\sum_{i=1}^{n} y_i = Y$. On a alors

$$\begin{aligned} \frac{1}{X^{\alpha} Y^{\beta}} \cdot \sum_{i=1}^{n} x_i^{\alpha} y_i^{\beta} &= \sum_{i=1}^{n} \left(\frac{x_i}{X}\right)^{\alpha} \cdot \left(\frac{y_i}{Y}\right)^{\beta} \\ &\leqslant \sum_{i=1}^{n} \left(\alpha \frac{x_i}{X} + \beta \frac{y_i}{Y}\right) = 1; \end{aligned}$$

la dernière inégalité résultant de la concavité de la fonction $x \mapsto \ln(x)$ sur $\mathbb{R}_+^*$ et de la croissance de la fonction exponentielle sur $\mathbb{R}$.

□

Notons que lorsque $\alpha = \beta = \frac{1}{2}$, on retrouve l'inégalité de Cauchy-Schwarz.

2. Théorème. *(Inégalité de la moyenne généralisée) Soient* $x_1, x_2, \ldots, x_n$ *des nombres strictement positifs. Pour* $r \in \mathbb{R}$, *on définit la quantité* $P_r(x_1, x_2, \ldots, x_n)$ *par :*

$$P_r(x_1, x_2, \ldots, x_n) = \begin{cases} \left(\prod_{i=1}^{n} x_i\right)^{1/n} & \text{si } r = 0, \\ \left(\frac{1}{n} \sum_{i=1}^{n} x_i^r\right)^{1/r} & \text{si } r \neq 0. \end{cases}$$

Si $r, s \in \mathbb{R}$ *sont tels que* $r < s$, *alors*

$$P_r(x_1, x_2, \ldots, x_n) \leqslant P_s(x_1, x_2, \ldots, x_n), \tag{4.12}$$

avec égalité si et seulement si tous les x_i, $i \in \{1, 2, \ldots, n\}$, *sont égaux.*

♦ **Preuve.** Étudions d'abord le cas où $0 < r < s$. On peut alors écrire $r = s\alpha$, avec $0 < \alpha < 1$. On a ainsi

$$\sum_{i=1}^{n} x_i^r = \sum_{i=1}^{n} (x_i^s)^{\alpha} \cdot 1^{1-\alpha} \leqslant \left(\sum_{i=1}^{n} x_i^s\right)^{\alpha} \cdot \left(\sum_{i=1}^{n} 1\right)^{1-\alpha},$$

5. Ludwig Otto Hölder (1859-1937), mathématicien allemand.

ce qui donne

$$\left(\frac{1}{n}\sum_{i=1}^{n} x_i^r\right)^{1/r} \leqslant \left(\frac{1}{n}\sum_{i=1}^{n} x_i^s\right)^{1/s},$$

avec égalité si et seulement si les x_i sont tous égaux.

Si maintenant $r = 0 < s$, alors

$$P_0(x_1, x_2, \ldots, x_n)^s = \left(\prod_{i=1}^{n} x_i\right)^{s/n} = \left(\prod_{i=1}^{n} x_i^s\right)^{1/n} \leqslant \frac{1}{n}\sum_{i=1}^{n} x_i^s,$$

et donc $P_0(x_1, x_2, \ldots, x_n) \leqslant P_s(x_1, x_2, \ldots, x_n)$, avec de nouveau égalité si et seulement si les x_i sont tous égaux.

Les deux cas $r < s < 0$ et $r < s = 0$ se traitent grâce à la remarque suivante :

$$P_{-r}(x_1, x_2, \ldots, x_n) = \frac{1}{P_r\left(\frac{1}{x_1}, \frac{1}{x_2}, \ldots, \frac{1}{x_n}\right)}.$$

□

♦ **Exemples.**

1. Soient x, y et z des réels strictement positifs. Prouver que

$$8(x^3 + y^3 + z^3)^2 \geqslant 9(x^2 + yz)(y^2 + zx)(z^2 + xy).$$

L'inégalité entre les moyennes géométrique et arithmétique permet d'écrire

$$(x^2 + yz)(y^2 + zx)(z^2 + xy) \leqslant \left(\frac{x^2 + y^2 + z^2 + yz + zx + xy}{3}\right)^3,$$

et comme $xy + yz + zx \leqslant x^2 + y^2 + z^2$,

$$(x^2 + yz)(y^2 + zx)(z^2 + xy) \leqslant \frac{8}{27}(x^2 + y^2 + z^2)^3.$$

D'un autre côté,

$$\left(\frac{x^3 + y^3 + z^3}{3}\right)^{1/3} \geqslant \left(\frac{x^2 + y^2 + z^2}{3}\right)^{1/2},$$

ce qui permet d'obtenir l'inégalité désirée.

4.7. L'inégalité de Muirhead

Soient $x_1, x_2, \ldots, x_n$ des nombres réels strictement positifs. Pour tout vecteur $\vec{a} = (a_1, a_2, \ldots, a_n)$, on définit la moyenne pondérée par $\vec{a}$ des nombres $x_1, x_2, \ldots, x_n$ comme ceci :

$$\boxed{\left[(a_1, a_2, \ldots, a_n)\right] = \frac{1}{n!}\sum_{\sigma \in S_n} x_{\sigma(1)}^{a_1} x_{\sigma(2)}^{a_2} \cdots x_{\sigma(n)}^{a_n},} \tag{4.13}$$

où S_n est l'ensemble de toutes les permutations de l'ensemble $\{1, 2, \dots, n\}$.

Par exemple, $[(1, 0, \dots, 0)]$ est la moyenne arithmétique de $x_1, x_2, \dots, x_n$, et $[(1/n, 1/n, \dots, 1/n)] = x_1^{1/n} x_2^{1/n} \cdots x_n^{1/n}$ est leur moyenne géométrique.

On dit que le vecteur $\vec{a} = (a_1, a_2, \dots, a_n)$ majore le vecteur $\vec{b} = (b_1, b_2, \dots, b_n)$ si :

1) $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_n$ et $b_1 \geqslant b_2 \geqslant \cdots \geqslant b_n$,

2) $a_1 \geqslant b_1$, $a_1 + a_2 \geqslant b_1 + b_2$, ..., $a_1 + a_2 + \cdots + a_{n-1} \geqslant b_1 + b_2 + \cdots + b_{n-1}$, et

3) $a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_n$.

4.7.1. Théorème. *(Inégalité de Muirhead[6]) Soient $x_1, x_2, \dots, x_n$ des nombres réels strictement positifs, et $\vec{a} = (a_1, a_2, \dots, a_n)$ et $\vec{b} = (b_1, b_2, \dots, b_n)$ deux vecteurs appartenant à $\mathbb{R}^n$.*

Si $\vec{a}$ majore $\vec{b}$, alors

$$\Big[(a_1, a_2, \dots, a_n)\Big] \geqslant \Big[(b_1, b_2, \dots, b_n)\Big], \tag{4.14}$$

avec égalité si et seulement si tous les x_i, $i \in \{1, 2, \dots, n\}$, sont égaux.

♦ **Preuve.** Soient $\vec{a} = (a_1, a_2, \dots, a_n)$ et $\vec{b} = (b_1, b_2, \dots, b_n)$ deux vecteurs dans $\mathbb{R}^n$ tels que $\vec{a}$ majore $\vec{b}$ et $\vec{a} \neq \vec{b}$. Il y a alors deux indices j, k, $1 \leqslant j < k \leqslant n$, tels que $a_j > b_j$, $a_k < b_k$ et $a_i = b_i$ pour tout i, $j < i < k$.

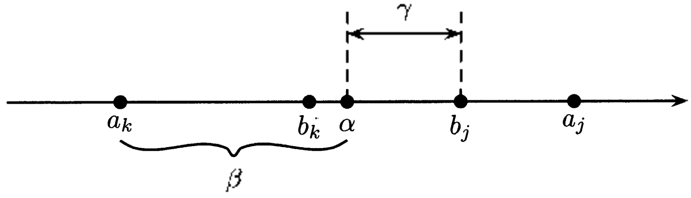


FIG. 4.4.

On pose alors $\alpha = (a_j + a_k)/2$ et $\beta = (a_j - a_k)/2$. On définit ensuite γ comme suit :

$$\gamma = \max\big(|b_j - \alpha|, |b_k - \alpha|\big).$$

On considère maintenant le vecteur $\vec{c} = (c_1, c_2, \dots, c_n)$ tel que $c_j = \alpha + \gamma$, $c_k = \alpha - \gamma$ et $c_i = a_i$ pour tout $i \in \{1, 2, \dots, n\}$, $i \neq j, k$. On remarque que $\vec{a}$ majore $\vec{c}$ et $\vec{c}$ majore $\vec{b}$. De plus, on a soit $c_j = b_j$, soit $c_k = b_k$.

On va montrer que $[\vec{a}] \geqslant [\vec{c}]$. En effet,

6. Robert Franklin Muirhead (1861-1941), mathématicien écossais.

$$\begin{aligned} n! \cdot ([\vec{a}] - [\vec{c}]) &= \sum_{\sigma \in S_n} \left(\prod_{i=1}^{n} x_{\sigma(i)}^{a_i} - \prod_{i=1}^{n} x_{\sigma(i)}^{c_i} \right) \\ &= \sum_{\sigma \in S_n} \left(\prod_{\substack{i=1 \\ i \neq j,k}}^{n} x_{\sigma(i)}^{a_i} \right) \left(x_{\sigma(j)}^{a_j} x_{\sigma(k)}^{a_k} - x_{\sigma(j)}^{c_j} x_{\sigma(k)}^{c_k} \right). \end{aligned}$$

Pour toute permutation $\sigma \in S_n$, il existe une permutation $\rho \in S_n$ telle que $\rho(i) = \sigma(i)$ pour tout $i \in \{1, 2, \ldots, n\}$, $i \neq j, k$, et $\rho(j) = \sigma(k)$ et $\rho(k) = \sigma(j)$. En regroupant les termes correspondant à σ et ρ dans l'inégalité précédente, on peut écrire :

$$\begin{aligned} &\left(x_{\sigma(j)}^{a_j} x_{\sigma(k)}^{a_k} - x_{\sigma(j)}^{c_j} x_{\sigma(k)}^{c_k} \right) - \left(x_{\sigma(j)}^{a_k} x_{\sigma(k)}^{a_j} - x_{\sigma(j)}^{c_k} x_{\sigma(k)}^{c_j} \right) \\ &= \left(x_{\sigma(j)}^{\alpha+\beta} x_{\sigma(k)}^{\alpha-\beta} - x_{\sigma(j)}^{\alpha+\gamma} x_{\sigma(k)}^{\alpha-\gamma} \right) - \left(x_{\sigma(j)}^{\alpha-\beta} x_{\sigma(k)}^{\alpha+\beta} - x_{\sigma(j)}^{\alpha-\gamma} x_{\sigma(k)}^{\alpha+\gamma} \right) \\ &= \left(x_{\sigma(j)} x_{\sigma(k)} \right)^{\alpha-\beta} \left(x_{\sigma(j)}^{\beta+\gamma} - x_{\sigma(k)}^{\beta+\gamma} \right) \left(x_{\sigma(j)}^{\beta-\gamma} - x_{\sigma(k)}^{\beta-\gamma} \right) \geqslant 0. \end{aligned}$$

Il en résulte que $[\vec{a}] \geqslant [\vec{c}]$. L'égalité a lieu si et seulement si $x_{\sigma(j)} = x_{\sigma(k)}$ pour toute permutation $\sigma \in S_n$, ce qui est encore équivalent à $x_1 = x_2 = \cdots = x_n$.

On a donc réussi à trouver un vecteur $\vec{c}$ qui majore $\vec{b}$, et qui est plus proche de $\vec{b}$ que $\vec{a}$, puisque $\vec{c}$ a une coordonnée de plus en commun avec $\vec{b}$. Il suffit donc de répéter cet algorithme un nombre fini de fois pour arriver au résultat souhaité.

□

♦ Remarques.

1. Dans l'inégalité de Muirhead, la somme dans la moyenne pondérée par $\vec{a}$ contient toutes les permutations $\sigma \in S_n$, et pas uniquement les permutations circulaires. On dit que $[\vec{a}]$ est une somme symétrique des nombres $x_i > 0$, $i \in \{1, 2, \ldots, n\}$.

2. Dans l'inégalité de Muirhead, les nombres $a_1, a_2, \ldots, a_n$ et $b_1, b_2, \ldots, b_n$ sont des réels positifs ou négatifs. Les nombres $x_1, x_2, \ldots, x_n$, par contre, sont des réels strictement positifs.

3. Puisque $(2, 0)$ majore $(1, 1)$, on retrouve encore l'inégalité bien connue $x^2 + y^2 \geqslant 2xy$ (au moins dans le cas particulier $x, y > 0$). En effet,

$$\frac{1}{2!}(x^2 y^0 + y^2 x^0) \geqslant \frac{1}{2!}(x^1 y^1 + x^1 y^1).$$

De même, puisque $(3, 0, 0)$ majore $(1, 1, 1)$, on retrouve l'inégalité de la moyenne dans le cas $n = 3$:

$$x^3 + y^3 + z^3 \geqslant 3xyz.$$

Plus généralement, puisque $(1, 0, \ldots, 0)$ majore $(1/n, 1/n, \ldots, 1/n)$, on retrouve l'inégalité de la moyenne comme un cas particulier de l'inégalité de Muirhead.

4. Si le produit des nombres x_i, $i \in \{1, 2, \ldots, n\}$, est égal à 1, alors pour tout nombre réel α :

$$\boxed{\Big[(a_1, a_2, \ldots, a_n)\Big] = \Big[(a_1 + \alpha, a_2 + \alpha, \ldots, a_n + \alpha)\Big].} \tag{4.15}$$

De même, si le produit des nombres x_i, $i \in \{1, 2, \ldots, n\}$, est $\geqslant 1$, alors pour tout nombre réel $\alpha \geqslant 0$:

$$\boxed{\Big[(a_1, a_2, \ldots, a_n)\Big] \geqslant \Big[(a_1 - \alpha, a_2 - \alpha, \ldots, a_n - \alpha)\Big].} \tag{4.16}$$

Cette remarque peut être assez utile quand on a une condition portant sur le produit des x_i, $i \in \{1, 2, \ldots, n\}$, puisqu'elle permet d'« ajuster » deux vecteurs $\vec{a} = (a_1, a_2, \ldots, a_n)$ et $\vec{b} = (b_1, b_2, \ldots, b_n)$ afin d'établir une relation de majoration dans le cas où les sommes $\sum_{i=1}^n a_i$ et $\sum_{i=1}^n b_i$ ne sont pas égales.

5. Pour tous vecteurs $\vec{a}, \vec{b} \in \mathbb{R}^n$, on a l'inégalité :

$$\boxed{\frac{[\vec{a}] + [\vec{b}]}{2} \geqslant \Big[\frac{\vec{a} + \vec{b}}{2}\Big].} \tag{4.17}$$

En effet, si $\vec{a} = (a_1, a_2, \ldots, a_n)$ et $\vec{b} = (b_1, b_2, \ldots, b_n)$, on a d'après l'inégalité de la moyenne :

$$\frac{x_{\sigma(1)}^{a_1} x_{\sigma(2)}^{a_2} \cdots x_{\sigma(n)}^{a_n} + x_{\sigma(1)}^{b_1} x_{\sigma(2)}^{b_2} \cdots x_{\sigma(n)}^{b_n}}{2} \geqslant x_{\sigma(1)}^{(a_1+b_1)/2} x_{\sigma(2)}^{(a_2+b_2)/2} \cdots x_{\sigma(n)}^{(a_n+b_n)/2}.$$

♦ **Exemples.**

1. Soient x, y et z des nombres réels strictement positifs. Prouver que :

$$(x^2y + y^2z + z^2x)(xy^2 + yz^2 + zx^2) \geqslant 9x^2y^2z^2.$$

En développant le terme de gauche, on obtient l'inégalité équivalente :

$$x^3y^3 + x^2y^2z^2 + x^4yz + y^3z^3 + x^2y^2z^2 + y^4zx + z^3x^3 + x^2y^2z^2 + z^4xy \geqslant 9x^2y^2z^2,$$

ce qui se réécrit encore sous la forme :

$$3\Big[(3, 3, 0)\Big] + 3\Big[(2, 2, 2)\Big] + 3\Big[(4, 1, 1)\Big] \geqslant 9\Big[(2, 2, 2)\Big],$$

qui se déduit immédiatement de l'inégalité de Muirhead, puisque $(3, 3, 0)$ et $(4, 1, 1)$ majorent $(2, 2, 2)$.

On peut aussi démontrer l'inégalité recherchée sans utiliser l'inégalité de Muirhead. Par exemple, en utilisant l'inégalité de Cauchy-Schwarz, on peut écrire :

$$(x^2y + y^2z + z^2x)(yz^2 + zx^2 + xy^2) \geqslant \left(3\sqrt{x^2y^2z^2}\right)^2 = 9x^2y^2z^2,$$

ou encore en appliquant l'inégalité de la moyenne :

$$(x^2y + y^2z + z^2x)(xy^2 + yz^2 + zx^2) \geqslant \left(3\sqrt[3]{x^3y^3z^3}\right)\left(3\sqrt[3]{x^3y^3z^3}\right) = 9x^2y^2z^2.$$

2. Soient x, y et z des nombres réels strictement positifs. Prouver que :

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

(Olympiades des États-Unis-1997)

En éliminant les dénominateurs, on obtient l'inégalité équivalente :

$$\begin{aligned} &3\Big[(7,1,1)\Big] + 9\Big[(4,4,1)\Big] + 12\Big[(5,2,2)\Big] + 3\Big[(3,3,3)\Big] \\ &\leqslant 3\Big[(3,3,3)\Big] + 6\Big[(6,3,0)\Big] + 9\Big[(4,4,1)\Big] + 6\Big[(5,2,2)\Big] + 3\Big[(7,1,1)\Big]. \end{aligned}$$

Puisque $(6,3,0)$ majore $(5,2,2)$, l'inégalité précédente est une conséquence immédiate de l'inégalité de Muirhead.

3. Soient x, y et z des nombres réels strictement positifs tels que $xyz = 1$. Prouver que :

$$\frac{x^3}{(1+y)(1+z)} + \frac{y^3}{(1+z)(1+x)} + \frac{z^3}{(1+x)(1+y)} \geqslant \frac{3}{4}.$$

(Proposé à l'OIM-1998)

En éliminant les dénominateurs, on obtient l'inégalité équivalente :

$$4(x^4 + y^4 + z^4 + x^3 + y^3 + z^3) \geqslant 3(1 + x + y + z + xy + yz + zx + xyz),$$

qu'on peut encore réécrire :

$$4\Big[(4,0,0)\Big] + 4\Big[(3,0,0)\Big] \geqslant \Big[(0,0,0)\Big] + 3\Big[(1,0,0)\Big] + 3\Big[(1,1,0)\Big] + \Big[(1,1,1)\Big].$$

Puisque $xyz = 1$, on a pour tout vecteur $(a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$ et tout réel α :

$$\Big[(a_1, a_2, \ldots, a_n)\Big] = \Big[(a_1 + \alpha, a_2 + \alpha, \ldots, a_n + \alpha)\Big].$$

En appliquant l'inégalité de Muirhead, on obtient alors :

$$\Big[(4,0,0)\Big] \geqslant \Big[(\tfrac{4}{3}, \tfrac{4}{3}, \tfrac{4}{3})\Big] = \Big[(0,0,0)\Big],$$

et
$$3\Big[(4,0,0)\Big] \geqslant 3\Big[(2,1,1)\Big] = 3\Big[(1,0,0)\Big],$$
et
$$3\Big[(3,0,0)\Big] \geqslant 3\Big[(\frac{4}{3},\frac{4}{3},\frac{1}{3})\Big] = 3\Big[(1,1,0)\Big],$$
et enfin
$$\Big[(3,0,0)\Big] \geqslant \Big[(1,1,1)\Big],$$
ce qui permet d'aboutir à l'inégalité désirée.

4.8. Exemples particuliers

La résolution des problèmes d'olympiades ne dépend pas simplement de la connaissance d'une collection d'inégalités célèbres. En effet, il faut souvent parvenir à mener des calculs avec patience, ou bien faire des remarques judicieuses pour simplifier les problèmes étudiés. Les exercices qui suivent illustrent cet aspect :

1. x, y, z sont des réels vérifiant $x^2 + y^2 + z^2 = 2$. Montrer que
$$x + y + z \leqslant xyz + 2.$$

Solution. On a d'une part
$$\begin{aligned}(x+y+z-xyz)^2 &= x^2+y^2+z^2+x^2y^2z^2 \\ &\quad -2(x^2yz+xy^2z+xyz^2)+2xy+2yz+2zx.\end{aligned}$$

D'autre part,
$$\begin{aligned}(1-xy)(1-yz)(1-zx) &= 1-(xy+yz+zx) \\ &\quad +(x^2yz+xy^2z+xyz^2)-x^2y^2z^2,\end{aligned}$$
et
$$\begin{aligned}(1-xy)(1-yz)(1-zx) = {} & \frac{\big[(x-y)^2+z^2\big]}{2} \times \frac{\big[(y-z)^2+x^2\big]}{2} \\ & \times \frac{\big[(z-x)^2+y^2\big]}{2} \geqslant 0.\end{aligned}$$

Il s'ensuit que
$$(x+y+z-xyz)^2 \leqslant 2+2 = 4.$$

2. Soient α et β deux nombres positifs ou nuls. On pose
$$a = \alpha\beta, \quad b = (1-\alpha)\beta + (1-\beta)\alpha, \quad c = (1-\alpha)(1-\beta).$$
Montrer qu'au moins un des nombres a, b ou c est supérieur ou égal à $4/9$.

Solution. Supposons que $a < 4/9$, $b < 4/9$ et $c < 4/9$. On a alors
$$\begin{aligned} b = \alpha+\beta-2\alpha\beta < \frac{4}{9} &\implies 2\sqrt{\alpha\beta}-2\alpha\beta < \frac{4}{9} \\ &\implies \sqrt{\alpha\beta}-\alpha\beta < \frac{2}{9},\end{aligned}$$

ce qui donne $\alpha\beta - \sqrt{\alpha\beta} + 2/9 > 0$, soit encore $(\sqrt{\alpha\beta} - 1/3)(\sqrt{\alpha\beta} - 2/3) > 0$. Ainsi, $\sqrt{\alpha\beta} < 1/3$ ou $\sqrt{\alpha\beta} > 2/3$, mais comme $a < 4/9$, on a nécessairement $\alpha\beta < 1/9$. Par ailleurs $c < 4/9$, ce qui donne $\alpha + \beta - \alpha\beta > 5/9$. Finalement $b > 5/9 - \alpha\beta > 5/9 - 1/9 = 4/9$, d'où la contradiction.

3. Soient m et n deux entiers strictement positifs. Prouver que

$$\frac{1}{\sqrt[m]{n+1}} + \frac{1}{\sqrt[n]{m+1}} \geqslant 1$$

Solution. On commence par le lemme suivant :

Lemme. *(Inégalité de Bernoulli[7]) Si $x > -1$ et n un entier positif, alors*

$$(1+x)^n \geqslant 1 + nx; \tag{4.18}$$

en effet, le résultat s'établit aisément par récurrence sur l'entier $n \geqslant 0$.

Revenons maintenant à notre problème. D'après le lemme précédent, on peut écrire :

$$\left(1 + \frac{m}{n}\right)^n \geqslant 1 + m, \quad \left(1 + \frac{n}{m}\right)^m \geqslant 1 + n,$$

ce qui donne

$$\frac{1}{\sqrt[m]{n+1}} + \frac{1}{\sqrt[n]{m+1}} \geqslant \frac{1}{1 + \dfrac{n}{m}} + \frac{1}{1 + \dfrac{m}{n}} = 1.$$

4. On pose :

$$a = \frac{m^{m+1} + n^{n-1}}{m^m + n^n},$$

où m et n sont des entiers strictement positifs. Prouver que

$$a^m + a^n \geqslant m^m + n^n.$$

(Olympiades des États-Unis-1991)

Solution. On applique l'inégalité de Bernoulli à chacune des deux expressions suivantes : $\left(1 + \dfrac{a-m}{m}\right)^m$ et $\left(1 + \dfrac{a-n}{n}\right)^n$ pour obtenir

$$\begin{aligned} a^m + a^n &= m^m\left(1 + \frac{a-m}{m}\right)^m + n^n\left(1 + \frac{a-n}{n}\right)^n \\ &\geqslant m^m\big[1 + (a-m)\big] + n^n\big[1 + (a-n)\big] = m^m + n^n. \end{aligned}$$

On peut aussi utiliser l'inégalité : $\forall\, a,\, k > 0$, $a^k - k^k = (a-k)(a^{k-1} + a^{k-2}k + \cdots + k^{k-1}) \geqslant k^k(a-k)$, ce qui donne :

$$\begin{aligned} (a^m + a^n) - (m^m + n^n) &= (a^m - m^m) + (a^n - n^n) \\ &\geqslant (a-m)m^m + (a-n)n^n \\ &= a(m^m + n^n) - (m^{m+1} + n^{n+1}) = 0. \end{aligned}$$

7. Jacques Bernoulli (1654-1705), mathématicien suisse d'origine anversoise.

5. Soient $x, y, z \geqslant 0$. Prouver l'inégalité

$$x(x-z)^2 + y(y-z)^2 \geqslant (x-z)(y-z)(x+y-z)$$

Solution. On réécrit l'inégalité à prouver sous la forme

$$x(x-z)^2 + y(y-z)^2 - (x-z)(y-z)(x+y-z) \geqslant 0,$$

ce qui s'écrit, en regroupant les termes convenablement, sous la forme

$$\begin{aligned} &x(x-z)[(x-z)-(y-z)] + y(y-z)[(y-z)-(x-z)] + z(x-z)(y-z) \\ &= x(x-y)(x-z) + y(y-x)(y-z) + z(z-x)(z-y) \geqslant 0. \end{aligned}$$

Cette dernière inégalité est un cas particulier du lemme suivant :

Lemme. *(Inégalité de Schur[8]) Soient x, y et z des nombres réels positifs, et n un entier positif. On a alors l'inégalité*

$$x^n(x-y)(x-z) + y^n(y-z)(y-x) + z^n(z-x)(z-y) \geqslant 0. \tag{4.19}$$

♦ **Preuve.** Par raison de symétrie, on peut supposer que $x \geqslant y \geqslant z \geqslant 0$. L'inégalité est alors vérifiée car $x^n(x-y)(x-z) \geqslant y^n(x-y)(y-z)$ et $z^n(z-x)(z-y) \geqslant 0$. □

♦ **Remarques.**

1. Le même raisonnement s'applique à tous nombres réels $\alpha \in \mathbb{R}$ et $\beta \in \mathbb{R}_+$:

$$x^\alpha(x^\beta - y^\beta)(x^\beta - z^\beta) + y^\alpha(y^\beta - z^\beta)(y^\beta - x^\beta) + z^\alpha(z^\beta - x^\beta)(z^\beta - y^\beta) \geqslant 0.$$

2. L'inégalité précédente se réécrit encore sous la forme :

$$\boxed{\Big[(\alpha+2\beta,0,0)\Big] + \Big[(\alpha,\beta,\beta)\Big] \geqslant 2\Big[(\alpha+\beta,\beta,0)\Big],\ \alpha \in \mathbb{R}, \beta \in \mathbb{R}_+.} \tag{4.20}$$

où on a utilisé les notations de l'inégalité de Muirhead. Cette remarque peut être assez utile puisqu'elle permet de combiner l'inégalité de Schur et l'inégalité de Muirhead pour établir des inégalités portant sur des sommes symétriques.

8. Issai Schur (1875-1941), mathématicien allemand.

EXERCICES

1. Soient a, b et c des nombres réels strictement positifs. Prouver que :

a) $abc \geqslant (a+b-c)(a+c-b)(b+c-a)$.

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

c) $\dfrac{a^2}{b^2}+\dfrac{b^2}{c^2}+\dfrac{c^2}{a^2} \geqslant \dfrac{b}{a}+\dfrac{c}{b}+\dfrac{a}{c}$.

d) $\dfrac{a^2}{b^2}+\dfrac{b^2}{c^2}+\dfrac{c^2}{a^2} \geqslant \dfrac{a}{b}+\dfrac{b}{c}+\dfrac{c}{a}$.

---

2. a, b, c sont les longueurs des côtés d'un triangle. Prouver que :

$$a^2(b+c-a)+b^2(c+a-b)+c^2(a+b-c) \leqslant 3abc.$$

(Olympiades internationales-1964/2)

---

3. Soient m et n deux entiers positifs vérifiant $n \leqslant m$. Prouver que :

$$2^n \cdot n! \leqslant \frac{(m+n)!}{(m-n)!} \leqslant (m^2+m)^n.$$

(Olympiades du pacifique asiatique-1996)

---

4. Soient x_i, y_i $(i=1,2,\ldots,n)$ des nombres réels tels que :

$$x_1 \geqslant x_2 \geqslant \cdots \geqslant x_n,$$
$$y_1 \geqslant y_2 \geqslant \cdots \geqslant y_n.$$

On considère une permutation arbitraire $(z_1, z_2, \ldots, z_n)$ des nombres $y_1, y_2, \ldots, y_n$. Démontrer que :

$$\sum_{i=1}^{n}(x_i-y_i)^2 \leqslant \sum_{i=1}^{n}(x_i-z_i)^2.$$

(Olympiades internationales-1975/1)

---

5. Soient a, b et c les longueurs des côtés d'un triangle. Démontrer que :

$$\sqrt{a+b-c}+\sqrt{b+c-a}+\sqrt{c+a-b} \leqslant \sqrt{a}+\sqrt{b}+\sqrt{c},$$

et déterminer les cas d'égalité.

(Olympiades du pacifique asiatique-1996)

---

6. Prouver que, pour tous réels $x_1 \geqslant x_2 \geqslant \cdots \geqslant x_n > 0$,

$$\frac{x_1}{x_2}+\frac{x_2}{x_3}+\cdots+\frac{x_n}{x_1} \leqslant \frac{x_2}{x_1}+\frac{x_3}{x_2}+\cdots+\frac{x_1}{x_n}.$$

---

7. Soient n un entier supérieur ou égal à 2 et $x_1, x_2, \ldots, x_n$ des réels strictement positifs. Prouver l'inégalité :

$$\frac{x_1^2}{x_1^2+x_2x_3}+\frac{x_2^2}{x_2^2+x_3x_4}+\cdots+\frac{x_n^2}{x_n^2+x_1x_2} \leqslant n-1.$$

---

8. Soient $n \in \mathbb{N}$ et $A \in \mathbb{R}_+^*$. Maximiser la somme $x_1x_2+x_2x_3+\cdots+x_{n-1}x_n$, où $\{x_1, x_2, \ldots, x_n\}$ est un ensemble de réels positifs vérifiant $x_1+x_2+\cdots+x_n = A$.

(Olympiades australiennes-1986)

---

9. Démontrer que pour tous réels x, y et z tels que $x \geqslant y \geqslant z > 0$, on a l'inégalité :

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

---

10. Soit $(a_k)_{k\in\mathbb{N}^*}$ une suite de nombres naturels non nuls et distincts. Montrer que pour tout n :

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

(Olympiades internationales-1978/5)

---

11. Soient x et y deux réels strictement positifs vérifiant :

$$x+y+\sqrt{2x^2+2xy+3y^2} = 4.$$

Montrer que $x^2y \leqslant 4$.

---

12. Soit n un entier supérieur ou égal à 3, et soient $a_1, a_2, \ldots, a_n$ des réels vérifiant $2 \leqslant a_i \leqslant 3$ pour tout $i \in \{1, 2, \ldots, n\}$. On pose $s = a_1 + a_2 + \cdots + a_n$. Démontrer l'inégalité :

$$\frac{a_1^2 + a_2^2 - a_3^2}{a_1 + a_2 - a_3} + \frac{a_2^2 + a_3^2 - a_4^2}{a_2 + a_3 - a_4} + \cdots + \frac{a_n^2 + a_1^2 - a_2^2}{a_n + a_1 - a_2} \leqslant 2s - 2n.$$

(Proposé à l'OIM-1995)

---

13. Démontrer l'inégalité :

$$\frac{8}{(x_1 + x_2)(y_1 + y_2) - (z_1 + z_2)^2} \leqslant \frac{1}{x_1 y_1 - z_1^2} + \frac{1}{x_2 y_2 - z_2^2},$$

sous les conditions :

$$x_1 > 0,\ x_2 > 0,\ x_1 y_1 > z_1^2,\ x_2 y_2 > z_2^2.$$

Dans quelles conditions a-t-on égalité ?

(Olympiades internationales-1969/6)

---

14. Soient x, y et z des réels strictement positifs vérifiant la relation $xy + yz + zx = 1$. Prouver l'inégalité :

$$\frac{2x(1 - x^2)}{(1 + x^2)^2} + \frac{2y(1 - y^2)}{(1 + y^2)^2} + \frac{2z(1 - z^2)}{(1 + z^2)^2} \leqslant \frac{x}{1 + x^2} + \frac{y}{1 + y^2} + \frac{z}{1 + z^2}.$$

---

15. Soient $a, b, c, d > 0$. Trouver toutes les valeurs possibles de la quantité :

$$S = \frac{a}{a + b + d} + \frac{b}{a + b + c} + \frac{c}{b + c + d} + \frac{d}{a + c + d}.$$

(Olympiades internationales-1974/5)

---

16. Pour tout entier n strictement positif, on définit S_n comme étant le minimum de la somme

$$\sum_{k=1}^{n} \sqrt{(2k - 1)^2 + a_k^2},$$

où $a_1, a_2, \ldots, a_n$ sont des réels strictement positifs dont la somme vaut 17. Il y a un entier unique n pour lequel S_n est aussi un entier. Déterminer n.

---

17. Soient a, b, c et d des réels strictement positifs. Montrer que :

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

(Proposé à l'OIM-1993)

---

18. Les nombres a_1, $a_2, \ldots$, a_n constituent une permutation des nombres 1, 1/2, $\ldots$, $1/n$, ainsi que les nombres b_1, $b_2, \ldots$, b_n. De plus $a_1+b_1 \geqslant a_2+b_2 \geqslant \cdots \geqslant a_n+b_n$. Prouver que $a_m+b_m \leqslant 4/m$ pour tout m compris entre 1 et n.

(Olympiades russes-1968)

---

19. Soient a, b et c les longueurs des trois côtés d'un triangle. Démontrer que :

$$a^2b(a-b)+b^2c(b-c)+c^2a(c-a)\geqslant 0,$$

et déterminer les cas d'égalité.

(Olympiades internationales-1983/6)

---

20. Déterminer toutes les valeurs du réel a pour lesquelles il existe cinq réels positifs ou nuls $x_1, x_2, \ldots, x_5$ vérifiant les relations suivantes :

$$\sum_{k=1}^{5} kx_k = a,\quad \sum_{k=1}^{5} k^3x_k = a^2,\quad \sum_{k=1}^{5} k^5x_k = a^3.$$

(Olympiades internationales-1979/5)

---

21. Trouver toutes les solutions $(x_1, x_2, \ldots, x_5) \in (\mathbb{R}_+^*)^5$ du système d'inéquations :

$$\begin{aligned}
(x_1^2-x_3x_5)(x_2^2-x_3x_5)&\leqslant 0,\\
(x_2^2-x_4x_1)(x_3^2-x_4x_1)&\leqslant 0,\\
(x_3^2-x_5x_2)(x_4^2-x_5x_2)&\leqslant 0,\\
(x_4^2-x_1x_3)(x_5^2-x_1x_3)&\leqslant 0,\\
(x_5^2-x_2x_4)(x_1^2-x_2x_4)&\leqslant 0.
\end{aligned}$$

(Olympiades internationales-1972/4)

---

22. On se donne trois nombres strictement positifs a, b et c vérifiant la relation $abc = 1$. Démontrer que :

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

(Olympiades internationales-1995/2)

---

23. Soient x, y, z des réels positifs vérifiant la relation $x + y + z = 1$. Démontrer la double inégalité :

$$0 \leqslant xy + yz + zx - 2xyz \leqslant \frac{7}{27}.$$

(Olympiades internationales-1984/1)

---

24. Soient a, b, c des nombres strictement positifs. Prouver que :

$$\sqrt{a^2 - ab + b^2} + \sqrt{b^2 - bc + c^2} \geqslant \sqrt{a^2 + ac + c^2}.$$

---

25. $x_1, x_2, \ldots, x_n$ sont des réels strictement positifs. On pose $x_{n+1} = x_1$ et $a = \min(x_1, x_2, \ldots, x_n)$. Montrer que :

$$\sum_{i=1}^{n} \frac{1 + x_i}{1 + x_{i+1}} \leqslant n + \frac{1}{(1+a)^2} \sum_{i=1}^{n} (x_i - a)^2.$$

(Olympiades chinoises-1992)

---

26. Soient $x_1, x_2, \ldots, x_n$ des réels tels que $|x_i| \leqslant \dfrac{(n+1)}{2}$ pour $i = 1, 2, \ldots, n$, et vérifiant la relation $|x_1 + x_2 + \cdots + x_n| = 1$. Prouver qu'il existe une permutation $(y_1, y_2, \ldots, y_n)$ de $x_1, x_2, \ldots, x_n$ telle que

$$|y_1 + 2y_2 + \cdots + ny_n| \leqslant \frac{(n+1)}{2}.$$

(Olympiades internationales-1997/3)

---

27. Si x est un réel positif, et n un entier $\geqslant 1$, alors

$$\lfloor nx \rfloor \geqslant \sum_{k=1}^{n} \frac{\lfloor kx \rfloor}{k}.$$

(Olympiades des États-Unis-1981)

---

28. Soient $a_1, a_2, \ldots, a_n$ des entiers non nuls $\leqslant N$. Le plus petit commun multiple de deux quelconques d'entre eux est $> N$. Montrer que :

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} < 2.$$

---

29. Soit N un entier naturel $\geqslant 2$ et soit $\{a_1, a_2, \ldots, a_n\}$ un ensemble fini d'entiers naturels distincts, différents de 0 et dont aucun n'est divisible par un nombre premier $\geqslant N$. Prouver que :

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} \leqslant N.$$

(Olympiades russes-1989)

---

30. Soient $x_1, x_2, \ldots, x_n$ des réels strictement positifs tels que $\sum_{i=1}^{n} x_i = 1$, et soit s le plus grand parmi les nombres

$$\frac{x_1}{1+x_1}, \quad \frac{x_2}{1+x_1+x_2}, \ldots, \quad \frac{x_n}{1+x_1+x_2+\cdots+x_n}.$$

Trouver la plus petite valeur de s, lorsque les nombres $x_1, x_2, \ldots, x_n$ varient, leur somme étant égale à 1. Pour quelles valeurs est-elle atteinte ?

(Olympiades russes-1972)

---

31. On considère n nombres réels $x_1, x_2, \ldots, x_n$ vérifiant :

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 1,$$

et soit k un entier supérieur à 2. Prouver qu'il existe n entiers non tous nuls $a_1, a_2, \ldots, a_n$ vérifiant :

a) pour tout i, $1 \leqslant i \leqslant n$, $|a_i| \leqslant k-1$;

b) $|a_1x_1 + a_2x_2 + \cdots + a_nx_n| \leqslant (k-1)\sqrt{n}/(k^n - 1)$.

(Olympiades internationales-1987/3)

---

32. Prouver que pour tous réels strictement positifs x, y, z tels que $xyz \geqslant 1$:

$$\frac{x^5 - x^2}{x^5 + y^2 + z^2} + \frac{y^5 - y^2}{y^5 + z^2 + x^2} + \frac{z^5 - z^2}{z^5 + x^2 + y^2} \geqslant 0.$$

(Olympiades internationales-2005/3)

---

33. Prouver que pour tous réels strictement positifs x, y, z :

$$(xy + yz + zx)\left(\frac{1}{(x+y)^2} + \frac{1}{(y+z)^2} + \frac{1}{(z+x)^2}\right) \geqslant \frac{9}{4}.$$

(Olympiades iraniennes-1996)

---

34. Soient x, y, z des réels strictement positifs. Démontrer que :

$$\frac{x}{\sqrt{x+y}} + \frac{y}{\sqrt{y+z}} + \frac{z}{\sqrt{z+x}} \leqslant \frac{5}{4}\sqrt{x+y+z}.$$

---

35. Soient a, b, c, d des réels positifs satisfaisant la condition $a + b + c + d = 1$. Prouver l'inégalité :

$$abc + bcd + cda + dab \leqslant \frac{1}{27} + \frac{176}{27}abcd.$$

(Proposé à l'OIM-1993)

---

36. Trouver le plus grand entier qui soit le produit d'entiers positifs dont la somme est égale à 1976. Justifier votre réponse.

(Olympiades internationales-1976/4)

---

37. Soit V un ensemble fini formé de points de coordonnées entières dans l'espace euclidien et soient V_x, V_y et V_z les ensembles formés des projections de V sur les plans yz, xz, xy respectivement. Démontrer que :

$$|V|^2 \leqslant |V_x| \cdot |V_y| \cdot |V_z|,$$

où $|A|$ désigne le nombre d'éléments de l'ensemble fini A.

(Olympiades internationales-1992/5)

SOLUTIONS

1. a) Si a, b, c ne sont pas les longueurs des côtés d'un triangle, le terme de droite dans l'inégalité est négatif, et le terme de gauche est positif. Dans le cas contraire, on pose

$$a+b-c=x, \quad a+c-b=y, \quad b+c-a=z,$$

avec $x, y, z \geqslant 0$.

L'inégalité à démontrer devient donc $(x+y)(y+z)(z+x) \geqslant 8xyz$, ce qui résulte des inégalités

$$x+y \geqslant 2\sqrt{xy}, \quad y+z \geqslant 2\sqrt{yz}, \quad z+x \geqslant 2\sqrt{zx}.$$

b) Les suites a, b, c et a^2, b^2, c^2 sont rangées dans le même ordre, et l'inégalité du réordonnement s'applique

$$a \cdot a^2 + b \cdot b^2 + c \cdot c^2 \geqslant b \cdot a^2 + c \cdot b^2 + a \cdot c^2.$$

c) On peut réécrire l'inégalité à prouver sous la forme :

$$\frac{a}{b} \cdot \frac{a}{b} + \frac{b}{c} \cdot \frac{b}{c} + \frac{c}{a} \cdot \frac{c}{a} \geqslant \frac{b}{c} \cdot \frac{c}{a} + \frac{c}{a} \cdot \frac{a}{b} + \frac{a}{b} \cdot \frac{b}{c},$$

ce qui découle de l'inégalité du réordonnement.

d) En éliminant les dénominateurs, on s'aperçoit que l'inégalité à prouver se met sous la forme

$$a^4c^2 + b^4a^2 + c^4b^2 \geqslant a^3bc^2 + b^3ca^2 + c^3ab^2,$$

cette inégalité étant invariante par permutation circulaire de a, b, c, on peut toujours supposer que b est situé entre a et c. L'inégalité précédente se met alors sous la forme :

$$a^3c^2(a-b) + b^3a^2(b-c) + c^3b^2(c-a) \geqslant 0.$$

On a alors

$$\begin{aligned}
& a^3c^2(a-b) + b^3a^2(b-c) + c^3b^2(c-a) \\
= \; & (a^3c^2 - c^3b^2)(a-b) + (b^3a^2 - c^3b^2)(b-c) \\
= \; & c^2(a^3 - cb^2)(a-b) + b^2(ba^2 - c^3)(b-c) \\
\geqslant \; & 0.
\end{aligned}$$

---

2. On applique la transformation de Ravi

$$a = x+y, \quad b = y+z, \quad c = z+x,$$

où $x, y, z > 0$.

L'inégalité à prouver se transforme alors en

$$2z(x+y)^2 + 2x(y+z)^2 + 2y(z+x)^2 \leqslant 3(x+y)(y+z)(z+x),$$

soit encore

$$(x+y)(x-z)(y-z) + (y+z)(y-x)(z-x) + (z+x)(z-y)(z-x) \leqslant 0.$$

La dernière inégalité étant invariante par permutation quelconque de x, y, z, on peut supposer, sans perte de généralité, que $x \geqslant y \geqslant z$, et dans ce cas, l'inégalité est évidemment vérifiée.

On a égalité si et seulement si $x = y = z$, c'est à dire si et seulement si le triangle considéré est équilatéral.

---

3. On a :

$$\begin{aligned} \frac{(m+n)!}{(m-n)!} &= (m+n)(m+n-1)\cdots(m-n+1) \\ &\geqslant 2n \cdot (2n-1)\cdots 1 \geqslant 2n \cdot (2n-2)\cdots 2 = 2^n n!. \end{aligned}$$

m étant supposé fixé, on va montrer l'autre inégalité par récurrence sur n :

- $n = 1$, $\dfrac{(m+1)!}{(m-1)} = m(m+1) = m^2 + m$.

- Supposons maintenant que, pour un entier k $(1 \leqslant k \leqslant m-1)$, on ait

$$\frac{(m+k)!}{(m-k)!} \leqslant (m^2+m)^k,$$

on a alors

$$\frac{(m+k+1)!}{(m-k-1)!} = (m-k)(m+k+1) \cdot \frac{(m+k)!}{(m-k)!} \leqslant (m^2+m)(m^2+m)^k = (m^2+m)^{k+1}$$

---

4. L'inégalité considérée est équivalente à $\sum_{i=1}^n x_i z_i \leqslant \sum_{i=1}^n x_i y_i$, ce qui est une conséquence immédiate de l'inégalité du réordonnement.

---

5. On applique la transformation de Ravi

$$a = x+y, \quad b = y+z, \quad c = z+x,$$

avec $x, y, z > 0$.

L'inégalité à démontrer s'écrit alors sous la forme

$$\sqrt{2}(\sqrt{x} + \sqrt{y} + \sqrt{z}) \leqslant \sqrt{x+y} + \sqrt{y+z} + \sqrt{z+x}.$$

Or, la fonction $x \mapsto \sqrt{x}$ est concave, et donc

$$\frac{1}{2}(\sqrt{x}+\sqrt{y}) \leqslant \sqrt{\frac{1}{2}(x+y)},$$

soit encore $\sqrt{x+y} \geqslant \frac{\sqrt{2}}{2}(\sqrt{x}+\sqrt{y})$ et de même $\sqrt{y+z} \geqslant \frac{\sqrt{2}}{2}(\sqrt{y}+\sqrt{z})$ et $\sqrt{z+x} \geqslant \frac{\sqrt{2}}{2}(\sqrt{z}+\sqrt{x})$. En sommant les trois dernières inégalités, on obtient

$$\sqrt{2}(\sqrt{x}+\sqrt{y}+\sqrt{z}) \leqslant \sqrt{x+y}+\sqrt{y+z}+\sqrt{z+x}.$$

ce qui termine la démonstration.

---

6. On raisonne par récurrence sur l'entier $n \geqslant 2$.

- Pour $n = 2$, l'inégalité demandée est évidente.

- Supposons le résultat vrai pour tout ensemble de n nombres, $n \geqslant 2$, satisfaisant aux conditions de l'énoncé. Soient donc $x_1, x_2, \ldots, x_{n+1}$, $(n+1)$ nombres tels que $x_1 \geqslant x_2 \geqslant \cdots \geqslant x_{n+1}$.

On considère alors les termes faisant intervenir x_{n+1} dans les deux côtés de l'inégalité proposée, et on pose

$$f(x) = \frac{x_1}{x} + \frac{x}{x_n} - \frac{x_n}{x} - \frac{x}{x_1}.$$

On a alors

$$f'(x) = (x_1 - x_n)\left(\frac{1}{x_1 x_n} - \frac{1}{x^2}\right) \leqslant 0, \quad \forall\, x \geqslant x_n,$$

et ainsi

$$f(x_{n+1}) \geqslant f(x_n) = \frac{x_1}{x_n} - \frac{x_n}{x_1}.$$

Il suffirait donc de montrer que

$$\left(\frac{x_1}{x_2} + \frac{x_2}{x_3} + \cdots + \frac{x_{n-1}}{x_n}\right) - \left(\frac{x_2}{x_1} + \frac{x_3}{x_2} + \cdots + \frac{x_n}{x_{n-1}}\right) \leqslant \frac{x_1}{x_n} - \frac{x_n}{x_1},$$

ce qui est manifestement vrai par hypothèse de récurrence.

---

7. 1ère solution. Posons $y_i = \frac{x_i^2}{x_{i+1}x_{i+2}}$, $i = 1, 2, \ldots, n$, et $x_{n+i} = x_i$. On a alors $y_1 y_2 \cdots y_n = 1$. On écrit donc

$$\frac{x_i^2}{x_i^2 + x_{i+1}x_{i+2}} = \frac{1}{1 + 1/y_i} = 1 - \frac{1}{1+y_i}.$$

L'inégalité désirée est alors équivalente à

$$\sum_{i=1}^{n} \frac{1}{1+y_i} \geqslant 1, \quad y_i > 0, \quad y_1 y_2 \cdots y_n = 1,\ n \geqslant 2.$$

Comme $y_1y_2\cdots y_n = 1$, il existe deux indices i et j tels que $y_iy_j \leqslant 1$. Maintenant

$$\frac{1}{1+y_i}+\frac{1}{1+y_j}\geqslant 1,$$

et le résultat en découle.

2ème solution. On pose

$$\Sigma_n = \sum_{i=1}^{n}\frac{x_i^2}{x_i^2+x_{i+1}x_{i+2}},\quad x_{n+i}=x_i.$$

Démontrons l'inégalité $\Sigma_n \leqslant n-1$ par récurrence sur $n\geqslant 2$.

- Pour $n=2$, on a :

$$\Sigma_2 = \frac{x_1^2}{x_1^2+x_1x_2}+\frac{x_2^2}{x_2^2+x_1x_2}=1.$$

- Supposons $\Sigma_n \leqslant n-1$ pour un entier $n\geqslant 3$, et considérons la somme Σ_{n+1} relative à $n+1$ nombres positifs $x_1, x_2, \ldots, x_{n+1}$. On peut donc supposer, sans perte de généralité, que $x_{n+1} = \max(x_1, x_2, \ldots, x_{n+1})$. On a alors

$$\begin{aligned}\Sigma_{n+1} &= \Sigma_n + \frac{x_{n-1}^2}{x_{n-1}^2+x_nx_{n+1}}+\frac{x_n^2}{x_n^2+x_{n+1}x_1}+\frac{x_{n+1}^2}{x_{n+1}^2+x_1x_2}\\ &\quad -\frac{x_{n-1}^2}{x_{n-1}^2+x_nx_1}-\frac{x_n^2}{x_n^2+x_1x_2},\end{aligned}$$

mais puisque

$$\frac{x_{n-1}^2}{x_{n-1}^2+x_nx_{n+1}}\leqslant\frac{x_{n-1}^2}{x_{n-1}^2+x_nx_1},\ \frac{x_n^2}{x_n^2+x_{n+1}x_1}\leqslant\frac{x_n^2}{x_n^2+x_1x_2},\ \frac{x_{n+1}^2}{x_{n+1}^2+x_1x_2}\leqslant 1,$$

alors $\Sigma_{n+1}\leqslant \Sigma_n+1\leqslant n+1$.

---

8. Si $x_n \geqslant x_{n-1}$, on arrive à rendre l'expression $x_1x_2+x_2x_3+\cdots+x_{n-1}x_n$ plus grande en échangeant x_n et x_{n-1}. Pour la même raison, on peut supposer que $x_{n-2}\geqslant x_n$. Maintenant, en remplaçant x_{n-2} et x_n par $x_{n-2}+x_n$ et 0 respectivement, l'expression à maximiser augmente d'une quantité égale à $x_{n-3}x_n$.

Ceci montre que pour des ensembles contenant au moins trois nombres, on peut supposer, dans la recherche du maximum de l'expression, que le dernier membre est égal à 0. Ainsi, on est amené à maximiser l'expression $x_1x_2+x_2x_3$ avec $x_1+x_2+x_3=A$. Mais

$$x_1x_2+x_2x_3 = x_2(A-x_2),$$

qui est maximale lorsque $x_2 = A/2$. Ainsi, le maximum recherché est $A^2/4$.

---

9. L'inégalité est vraie si deux des trois nombres x, y, z sont égaux.

Supposons que $x > y > z > 0$. Puisque $\forall a > 0$, $a + 1/a \geqslant 2$, on a

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

Ainsi, pour démontrer l'inégalité demandée, il suffirait de démontrer que

$$x^2\frac{y}{z} + y^2\frac{z}{x} + z^2\frac{x}{y} \geqslant x^2\frac{z}{y} + y^2\frac{x}{z} + z^2\frac{y}{x}. \tag{1}$$

Or,

$$\begin{aligned}
(1) \quad &\iff \quad x^3y^2 + y^3z^2 + z^3x^2 \geqslant x^3z^2 + y^3x^2 + z^3y^2 \\
&\iff \quad y^2(x^3 - z^3) + x^2z^2(z - x) \geqslant y^3(x^2 - z^2) \\
&\iff \quad y^2(x^2 + xz + z^2) - x^2z^2 \geqslant y^3(x + z) \\
&\iff \quad y^2x(x - y) + y^2z(x - y) + z^2(y^2 - x^2) \geqslant 0 \\
&\iff \quad y^2x + y^2z - z^2y - z^2x \geqslant 0 \\
&\iff \quad x(y^2 - z^2) + yz(y - z) \geqslant 0,
\end{aligned}$$

ce qui est vrai puisque $x > y > z > 0$.

---

10. L'inégalité du réordonnement montre que la quantité $\sum_{k=1}^{n} a_k/k^2$ est minimale lorsque $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n$.

Supposons donc que c'est bien le cas. On a alors $a_i \geqslant i$ pour tout i, $1 \leqslant i \leqslant n$ (le voir à l'aide d'une récurrence sur i par exemple).

Il s'ensuit donc que la valeur minimale que peut prendre $\sum_{k=1}^{n} a_k/k^2$ est elle même supérieure ou égale à $\sum_{k=1}^{n} 1/k$.

---

11. D'après l'inégalité de la moyenne, on a

$$x + y = \frac{x}{2} + \frac{x}{2} + y \geqslant \frac{3}{4^{1/3}}(x^2y)^{1/3}.$$

On a ainsi réussi à faire apparaître le terme x^2y. Nous aimerions alors faire la même chose avec la racine carrée. Supposons avoir décomposé $2x^2$ en i termes égaux à $\dfrac{2x^2}{i}$, $2xy$ en j termes égaux à $\dfrac{2xy}{j}$ et $3y^2$ en k termes égaux à $\dfrac{3y^2}{k}$. On aimerait bien avoir

$$2i + j = 2(j + 2k), \quad \frac{2i + j}{2(i + j + k)} = \frac{2}{3}.$$

Une solution possible est $i = 8$, $j = 4$, $k = 3$. On a alors

$$2x^2 + 2xy + 3y^2 \geqslant 15\left(\frac{2}{8}\right)^{8/15}\left(\frac{2}{4}\right)^{4/15}\left(\frac{3}{3}\right)^{3/15}(x^2y)^{2/3} = 15\left(\frac{1}{4}\right)^{2/3}(x^2y)^{2/3},$$

et il s'ensuit que

$$4 = x + y + \sqrt{2x^2 + 2xy + 3y^2} \geqslant \left(\frac{3}{4^{1/3}} + \frac{\sqrt{15}}{4^{1/3}}\right)(x^2y)^{1/3},$$

soit encore

$$x^2y \leqslant 4\left(\frac{4}{3+\sqrt{15}}\right)^3 \leqslant 4$$

---

12. On pose

$$A_i = \frac{a_i^2 + a_{i+1}^2 - a_{i+2}^2}{a_i + a_{i+1} - a_{i+2}}, \quad (a_{n+i} = a_i).$$

On a alors

$$A_i = a_i + a_{i+1} + a_{i+2} - \frac{2a_ia_{i+1}}{a_i + a_{i+1} - a_{i+2}},$$

et puisque $(a_i - 2)(a_{i+1} - 2) \geqslant 0$, alors $-2a_ia_{i+1} \leqslant -4(a_i + a_{i+1} - 2)$ et par suite

$$A_i \leqslant a_i + a_{i+1} + a_{i+2} - 4\left(1 + \frac{a_{i+2} - 2}{a_i + a_{i+1} - a_{i+2}}\right).$$

Comme $1 \leqslant a_i + a_{i+1} - a_{i+2} \leqslant 4$, on a

$$A_i \leqslant a_i + a_{i+1} + a_{i+2} - 4\left(1 + \frac{a_{i+2} - 2}{4}\right) = a_i + a_{i+1} - 2,$$

soit enfin $\sum_{i=1}^n A_i \leqslant 2s - 2n$.

---

13. On commence par appliquer l'inégalité de Cauchy-Schwarz

$$(x_1 + x_2)(y_1 + y_2) \geqslant (\sqrt{x_1y_1} + \sqrt{x_2y_2})^2.$$

Pour prouver l'inégalité demandée, il suffirait donc de montrer que

$$\frac{8}{(\sqrt{x_1y_1} + \sqrt{x_2y_2})^2 - (z_1 + z_2)^2} \leqslant \frac{1}{(x_1y_1 - z_1^2)} + \frac{1}{(x_2y_2 - z_2^2)}.$$

On pose alors

$u_1 = \sqrt{x_1y_1} - z_1 > 0$, $u_2 = \sqrt{x_2y_2} - z_2 > 0$, $v_1 = \sqrt{x_1y_1} + z_1$, $v_2 = \sqrt{x_2y_2} + z_2 > 0$;

la dernière inégalité devient alors

$$8 \leqslant (u_1 + v_1)(v_1 + v_2)\left(\frac{1}{u_1v_1} + \frac{1}{u_2v_2}\right),$$

mais

$$u_1 + u_2 \geqslant 2\sqrt{u_1u_2}, \quad v_1 + v_2 \geqslant 2\sqrt{v_1v_2}, \quad \frac{1}{u_1v_1} + \frac{1}{u_2v_2} \geqslant 2\frac{1}{\sqrt{u_1u_2v_1v_2}};$$

ce qui donne l'inégalité recherchée.

Il y a égalité si et seulement si $u_1 = u_2$, $v_1 = v_2$ et $\exists \lambda \in \mathbb{R}_+$, $(x_1, y_1) = \lambda(x_2, y_2)$, i.e., $x_1 = x_2, y_1 = y_2$ et $z_1 = z_2$.

Note. On peut prouver de manière analogue la généralisation suivante :

Soient $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n, z_1, z_2, \ldots, z_n$ des réels tels que, pour tout $i \in \{1, 2, \ldots, n\}$, $x_i > 0$ et $x_i y_i - z_i^2 > 0$. Prouver alors l'inégalité

$$\frac{n^3}{(\sum_{i=1}^n x_i)(\sum_{i=1}^n y_i) - (\sum_{i=1}^n z_i)^2} \leqslant \sum_{i=1}^n \frac{1}{(x_i y_i - z_i^2)}$$

---

14. On va utiliser un raisonnement géométrique. En effet, on applique la transformation trigonométrique suivante :

$$x = \tan\frac{\alpha}{2}, \quad y = \tan\frac{\beta}{2}, \quad z = \tan\frac{\gamma}{2},$$

avec α, β, $\gamma \in]0, \pi[$.

Comme $xy + yz + zx = 1$, il s'ensuit que $\tan(\gamma/2) = 1\Big/\tan\left(\dfrac{\alpha+\beta}{2}\right)$, d'où $\alpha + \beta + \gamma = \pi$.

D'un autre côté, l'inégalité à prouver se réécrit sous la forme :

$$\sin\alpha\cos\alpha + \sin\beta\cos\beta + \sin\gamma\cos\gamma \leqslant \frac{1}{2}(\sin\alpha + \sin\beta + \sin\gamma),$$

i.e.,

$$\sin 2\alpha + \sin 2\beta + \sin 2\gamma \leqslant \sin\alpha + \sin\beta + \sin\gamma.$$

On considère alors un triangle dont les mesures des angles valent α, β et γ. On désigne par S et p la surface et le demi périmètre du triangle ainsi considéré, et par r et R les rayons des cercles inscrit et circonscrit respectivement.

On a d'une part (loi des sinus) :

$$\sin\alpha + \sin\beta + \sin\gamma = \frac{a+b+c}{2R} = \frac{2p}{2R} = \frac{S}{rR}, \quad (\text{car } pr = S),$$

et d'autre part :

$$\begin{aligned} \sin 2\alpha + \sin 2\beta + \sin 2\gamma &= \frac{a\cos\alpha + b\cos\beta + c\cos\gamma}{R} \\ &= \frac{1}{R}\left(a \cdot \frac{x}{R} + b \cdot \frac{y}{R} + c \cdot \frac{y}{R}\right) = \frac{2S}{R^2}. \end{aligned}$$

Il s'ensuit que :

$$\frac{\sin\alpha + \sin\beta + \sin\gamma}{\sin 2\alpha + \sin 2\beta + \sin 2\gamma} = \frac{R}{2r},$$

et on conclut alors grâce à l'inégalité d'Euler.

---

15. On remarque que

$$S > \frac{a}{a+b+c+d} + \frac{b}{a+b+c+d} + \frac{c}{a+b+c+d} + \frac{d}{a+b+c+d} = 1,$$

et que

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

Par ailleurs, en prenant $a = b = 1$ et $c = d = x$, on obtient

$$S'(x) = \frac{2}{2+x} + \frac{2x}{1+2x}, \quad \lim_{x\to 0} S'(x) = 1,$$

et en prenant $a = c = 1$ et $b = d = x$, on obtient

$$S''(x) = \frac{2}{1+2x} + \frac{2x}{2+x}, \quad \lim_{x\to 0} S''(x) = 2.$$

Comme S est continue, le théorème des valeurs intermédiaires prouve que S décrit l'intervalle $]1,2[$ lorsque les réels a, b, c et d varient dans $\mathbb{R}_+^*$.

---

16. 1ère solution. Dans le plan rapporté à un repère orthonormé $(O, \vec{\imath}, \vec{\jmath})$, plaçons les points

$$A_0 = 0,\ A_1 = (1, a_1),\ A_2(1+3, a_1+a_2), \ldots,\ A_n(\sum_{i=1}^{n}(2i-1), \sum_{i=1}^{n} a_i);$$

on a alors

$$\begin{aligned}\sum_{i=1}^{n}\sqrt{(2i-1)^2 + a_i^2} = \sum_{i=0}^{n-1} A_iA_{i+1} \quad &\geqslant \quad A_0A_n \\ &= \quad \sqrt{\left(\sum_{i=1}^{n}(2i-1)\right)^2 + \left(\sum_{i=1}^{n} a_i\right)^2} \\ &= \quad \sqrt{n^4 + 17^2}.\end{aligned}$$

Le minimum de S_n est bien égal à $\sqrt{n^4+17^2}$ (faire une figure pour se rendre compte du cas d'égalité).

D'un autre côté,

$$\begin{aligned} S_n \in \mathbb{N} \quad &\iff \quad \sqrt{n^4+17^2} = p \quad (p \in \mathbb{N}) \\ &\iff \quad (p-n^2)(p+n^2) = 17^2 \quad (p \in \mathbb{N}) \\ &\iff \quad p - n^2 = 1,\ p + n^2 = 17^2 \quad (p \in \mathbb{N}) \\ &\iff \quad 2p = 290, \quad n^2 = p - 1 \quad (p \in \mathbb{N}) \\ &\iff \quad n = 12. \end{aligned}$$

2ème solution. Puisque $x \mapsto \sqrt{x^2+1}$ est convexe, on a :

$$\begin{aligned}
\sum_{i=1}^{n} \sqrt{(2i-1)^2 + a_i^2} &= 17 \sum_{i=1}^{n} \frac{a_i}{17} \sqrt{\left(\frac{2i-1}{a_i}\right)^2 + 1} \\
&\geqslant 17 \sqrt{\left(\sum_{i=1}^{n} \frac{a_i}{17} \cdot \frac{2i-1}{a_i}\right)^2 + 1} \\
&= \sqrt{\left(\sum_{i=1}^{n} (2i-1)\right)^2 + 17^2} = \sqrt{n^4 + 17^2},
\end{aligned}$$

l'égalité ayant lieu si et seulement si

$$\frac{1}{a_1} = \frac{3}{a_2} = \frac{5}{a_3} = \cdots = \frac{2n-1}{a_n} = \frac{n^2}{17} \quad \Longrightarrow \quad a_i = \frac{17}{n^2} \cdot (2i-1), \quad i \in \{1, 2, \ldots, n\}.$$

Il s'ensuit que $\sqrt{n^4 + 17^2}$ est le minimum de S_n. On continue alors comme dans la première solution.

Note. L'avantage de la deuxième solution par rapport à la solution géométrique est qu'elle permet de généraliser l'exercice. Par exemple, on pourra étudier la variante suivante : on prend au lieu des carrés les cubes et de la racine carrée la racine cubique.

---

17. 1ère solution. On pose $(x_1, x_2, x_3, x_4) = (a, b, c, d)$ et $(y_1, y_2, y_3, y_4) = (b + 2c + 3d, c + 2d + 3a, d + 2a + 3b, a + 2b + 3c)$. On sait que

$$\left(\sum_{i=1}^{n} \frac{x_i}{y_i}\right)\left(\sum_{i=1}^{n} x_i y_i\right) \geqslant \left(\sum_{i=1}^{n} x_i\right)^2,$$

ce qui donne

$$\begin{aligned}
&\frac{a}{b+2c+3d} + \frac{b}{c+2d+3a} + \frac{c}{d+2a+3b} + \frac{d}{a+2b+3c} \\
\geqslant\ &\frac{(a+b+c+d)^2}{4(ab+ac+ad+bc+bd+cd)}.
\end{aligned}$$

On reconnaît alors l'inégalité de Maclaurin[9] :

$$(ab+ac+ad+bc+bd+cd) \leqslant \frac{3}{8}(a+b+c+d)^2,$$

qui résulte du fait que

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

Le résultat recherché en découle aussitôt, et l'égalité a lieu si et seulement si $a = b = c = d$.

9. Colin Maclaurin (1698-1746), mathématicien écossais.

2$^{\text{ème}}$ solution. Sans perte de généralité, on peut supposer, quitte à multiplier les nombres a, b, c, d, par un même facteur, que $a + b + c + d = 1$. La fonction $f\colon x \mapsto 1/x$ est convexe sur $\mathbb{R}_+^*$. On peut alors appliquer l'inégalité de convexité

$$\begin{aligned}
A &= \frac{a}{b+2c+3d} + \frac{b}{c+2d+3a} + \frac{c}{d+2a+3b} + \frac{d}{a+2b+3c} \\
&= af(b+2c+3d) + bf(c+2d+3a) + cf(d+2a+3b) + df(a+2b+3c) \\
&\geqslant f\big(4(ab+ac+ad+bc+bd+cd)\big) \\
&= \frac{1}{4(ab+ac+ad+bc+bd+cd)}.
\end{aligned}$$

On conclut alors grâce à l'inégalité de Maclaurin.

3$^{\text{ème}}$ solution. Cette méthode est plus systématique que les deux dernières méthodes. L'idée principale est de considérer la transformation suivante :

$$A = b + 2c + 3d, \quad B = c + 2d + 3a, \quad C = d + 2a + 3b, \quad D = a + 2b + 3c$$

Des calculs sans difficultés particulières permettent d'exprimer a, b, c, d, en fonction de A, B, C, D,

$$\begin{aligned}
a &= \frac{1}{24}(-5A + 7B + C + D), \\
b &= \frac{1}{24}(-5B + 7C + D + A), \\
c &= \frac{1}{24}(-5C + 7D + A + B), \\
d &= \frac{1}{24}(-5D + 7A + B + C),
\end{aligned}$$

et le côté gauche de l'inégalité de l'énoncé se met sous la forme

$$\frac{a}{A} + \frac{b}{B} + \frac{c}{C} + \frac{d}{D} = \frac{-20}{24} + \frac{1}{24}\left(\frac{7B}{A} + \frac{C}{A} + \frac{D}{A} + \cdots + \frac{7A}{D} + \frac{B}{D} + \frac{C}{D}\right).$$

En considérant les termes $7B/A$ comme $B/A + B/A + \cdots + B/A$, on a 36 termes entre les parenthèses dont le produit vaut 1. L'inégalité de la moyenne donne alors

$$\frac{a}{A} + \frac{b}{B} + \frac{c}{C} + \frac{d}{D} \geqslant \frac{-20 + 36}{24} = \frac{2}{3}.$$

---

18. Raisonnons par l'absurde, et supposons que $a_m + b_m > 4/m$ pour un certain m compris entre 1 et n. On a ainsi $a_1 + b_1 \geqslant a_2 + b_2 \geqslant \cdots \geqslant a_m + b_m > 4/m$. Par conséquent, pour chaque i, $1 \leqslant i \leqslant m$, l'ensemble $\{a_i, b_i\}$ contient au moins un élément $> 2/m$. Mais alors, une des deux permutations $a_i, b_i, i = 1, 2, \ldots, n$ de $\{1, 1/2, \ldots, 1/n\}$ contient au moins $\lfloor m/2 \rfloor$ éléments supérieurs à $2/m$. Or, une permutation de $\{1, 1/2, \ldots, 1/n\}$ ne peut contenir que $\lfloor (m-1)/2 \rfloor$ éléments supérieurs à $2/m$, d'où la contradiction.

---

19. 1$^{\text{ère}}$ solution. On applique la transformation de Ravi

$$a = x + y, \quad b = y + z, \quad c = z + x,$$

avec $x, y, z > 0$. On a alors

$$a^2b(a-b) + b^2c(b-c) + c^2a(c-a) = 2(x^3z + y^3x + z^3y) - 2(xy^2z + x^2yz + xyz^2).$$

Il suffit alors de prouver que

$$x^3z + y^3x + z^3y \geqslant x^2yz + y^2zx + z^2xy \iff \frac{x^2}{y} + \frac{y^2}{z} + \frac{z^2}{x} \geqslant x + y + z.$$

Cette dernière inégalité résulte immédiatement de l'inégalité du réordonnement, mais l'application de l'inégalité de Cauchy-Schwarz nous donnerait aussi les cas d'égalité :

$$\left(x \cdot \frac{x}{y} + y \cdot \frac{y}{z} + z \cdot \frac{z}{x}\right)\left(x \cdot \frac{y}{x} + y \cdot \frac{z}{y} + z \cdot \frac{x}{z}\right) \geqslant (x+y+z)^2.$$

Il y a égalité si et seulement si $x = y = z$, i.e., le triangle est équilatéral.

2$^{\text{ème}}$ solution. Cette solution a valu un prix spécial à Bernhard Leeb.

Sans perte de généralité, on peut supposer que $a \geqslant b, c$ (l'inégalité à prouver étant invariante par permutation circulaire de a, b, c). Après quelques manipulations, l'inégalité proposée se met sous la forme :

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

Sous cette forme, l'inégalité devient évidente. On a égalité si et seulement si $a = b = c$.

---

20. 1$^{\text{ère}}$ solution. On a $a^2\sum_{k=1}^5 kx_k + \sum_{k=1}^5 k^5x_k = 2a\sum_{k=1}^5 k^3x_k$, soit encore

$$\sum_{k=1}^{5} k(a-k^2)^2x_k = 0,$$

i.e., $k(a-k^2)^2x_k = 0$, $k = 1, 2, \ldots, 5$.

S'il existe $j \in \{1, 2, \ldots, 5\}$ tel que $x_j \neq 0$, alors nécessairement $a = j^2$, et donc, pour $k \neq j$, $x_k = 0$, et en revenant aux formules de l'énoncé, on obtient $x_j = j$.

Si $x_j = 0$ pour tout $j \in \{1, 2, \ldots, 5\}$, alors $a = 0$.

On en tire les 6 valeurs possibles pour a :

$$0, \quad 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16, \quad 5^2 = 25.$$

2$^{\text{ème}}$ solution. L'inégalité de Cauchy-Schwarz permet d'écrire

$$\left(\sum_{k=1}^{5} \sqrt{kx_k}\sqrt{k^5x_k}\right)^2 \leqslant \left(\sum_{k=1}^{5} kx_k\right)\left(\sum_{k=1}^{5} k^5x_k\right).$$

Par ailleurs, les formules de l'énoncé montrent en fait que l'inégalité précédente se réduit à une égalité, et donc $\exists\lambda \in \mathbb{R}$ tel que $k^5 x_k = \lambda^2 k x_k$, i.e. $x_k(k^4 - \lambda^2) = 0$, $k = 1, 2, \ldots, 5$.

On continue alors comme dans la première solution.

---

21. 1ère solution. Tous les indices seront pris modulo 5. Il pourrait être utile d'imaginer que les nombres $x_1, x_2, \ldots, x_5$ sont placés, dans cet ordre, autour d'un cercle.

Chaque équation est de la forme

$$(x_i^2 - x_{i+2}x_{i+4})(x_{i+1}^2 - x_{i+2}x_{i+4}) \leqslant 0.$$

On a donc $x_i^2 \leqslant x_{i+2}x_{i+4} \leqslant x_{i+1}^2$ ou $x_{i+1}^2 \leqslant x_{i+2}x_{i+4} \leqslant x_i^2$, ce qui s'écrit

$$\min(x_i, x_{i+1}) \leqslant \sqrt{x_{i-1}x_{i+2}} \leqslant \max(x_i, x_{i+1}).$$

Supposons alors que x_1 soit le plus grand des nombres $x_1, x_2, \ldots, x_5$. Deux cas peuvent se présenter :

- Le nombre qui vient juste après x_1 est l'un de ses deux voisins, soit par exemple x_5. On a alors $x_5 \leqslant \sqrt{x_2x_4} \leqslant x_1$. Mais comme $\min(x_2, x_4) \leqslant \sqrt{x_2x_4} \leqslant \max(x_2, x_4)$, alors $x_5 = x_2 = x_4$. Maintenant, $\min(x_2, x_3) \leqslant \sqrt{x_1x_4} \leqslant \max(x_2, x_3)$, mais comme $x_2 = x_4 = x_5$, alors $\max(x_2, x_3) = x_2$ et $\min(x_2, x_3) = x_3$, et donc $x_1 = x_2 = x_3 = x_4 = x_5$.

- Le nombre qui vient juste après x_1 n'est pas parmi ses deux voisins. Soit par exemple x_4 ce nombre. Comme $\min(x_2, x_3) \leqslant \sqrt{x_1x_4} \leqslant \max(x_2, x_3)$, alors $\max(x_2, x_3) = x_1 = x_4$. Par raison de symétrie, on peut supposer que $x_1 = x_2 = x_4$. De nouveau, $\min(x_1, x_2) \leqslant \sqrt{x_3x_5} \leqslant \max(x_1, x_2)$, et donc tous les nombres sont égaux.

2ème solution. On remarque que

$$\begin{aligned}&\sum_{i=1}^{5}(x_i^2 - x_{i+2}x_{i+4})(x_{i+1}^2 - x_{i+2}x_{i+4})\\ = \;&\frac{1}{2}\sum_{i=1}^{5}\Big[(x_ix_{i+1} - x_ix_{i+3})^2 + (x_{i-1}x_{i+1} - x_{i-1}x_{i+3})^2\Big].\end{aligned}$$

---

22. 1ère solution. On pose $x = 1/a,\ y = 1/b,\ z = 1/c$. On a donc $xyz = 1$ et

$$\frac{1}{a^3(b+c)} + \frac{1}{b^3(c+a)} + \frac{1}{c^3(a+b)} = \frac{x^2}{y+z} + \frac{y^2}{z+x} + \frac{z^2}{x+y}.$$

On applique alors l'inégalité de Cauchy-Schwarz

$$\left[x\cdot\frac{x}{y+z} + y\cdot\frac{y}{z+x} + z\cdot\frac{z}{x+y}\right]\left[(y+z)+(z+x)+(x+y)\right] \geqslant (x+y+z)^2,$$

soit encore
$$\frac{x^2}{y+z}+\frac{y^2}{z+x}+\frac{z^2}{x+y}\geqslant\frac{1}{2}(x+y+z).$$

Or, l'inégalité de la moyenne donne
$$x+y+z\geqslant 3\sqrt[3]{xyz}=3,$$

d'où l'inégalité désirée.

Il y a égalité si et seulement si $x=y=z=1$, i.e., $a=b=c=1$.

On aurait pu également utiliser l'inégalité de Chebychev (faire la comparaison avec l'inégalité de Nesbitt) :
$$\begin{aligned}\frac{x^2}{y+z}+\frac{y^2}{z+x}+\frac{z^2}{x+y} &\geqslant \frac{1}{3}(x+y+z)\left(\frac{x}{y+z}+\frac{y}{z+x}+\frac{z}{x+y}\right)\\ &\geqslant \frac{1}{3}(x+y+z)\times\frac{3}{2}=\frac{1}{2}(x+y+z),\end{aligned}$$
puis conclure comme précédemment.

2$^{\text{ème}}$ solution. En éliminant les dénominateurs, on obtient l'inégalité :
$$\begin{aligned}&2\times\left(a^4b^4+b^4c^4+c^4a^4\right)+\\ &2\times\left(a^4b^3c+a^3b^4c+b^4c^3a+b^3c^4a+c^4a^3b+c^3a^4b\right)+\\ &2\times\left(a^3b^3c^2+b^3c^3a^2+c^3a^3b^2\right)\\ &\geqslant 3\times a^3b^3c^3\times(b+c)\times(c+a)\times(a+b)\\ &=3\times\left(a^5b^4c^3+a^4b^5c^3+b^5c^4a^3+b^4c^5a^3+c^5a^4b^3+c^4a^5b^3\right)+6\times a^4b^4c^4.\end{aligned}$$

Cette inégalité est équivalente à ;
$$\Big[(4,4,0)\Big]+2\Big[(4,3,1)\Big]+\Big[(3,3,2)\Big]\geqslant 3\Big[(5,4,3)\Big]+\Big[(4,4,4)\Big],$$
où on a utilisé les notations de l'inégalité de Muirhead.

On remarque que $4+4+0=4+3+1=3+3+2=8$, mais que $5+4+3=4+4+4=12$. Puisque $abc=1$, on peut appliquer l'identité :
$$\Big[(a_1,a_2,\ldots,a_n)\Big]=\Big[(a_1+\alpha,a_2+\alpha,\ldots,a_n+\alpha)\Big],$$
où on choisit $\alpha=-\frac{4}{3}$. On a alors :
$$\Big[(5,4,3)\Big]=\Big[(5-\frac{4}{3},4-\frac{4}{3},3-\frac{4}{3})\Big]=\Big[(\frac{11}{3},\frac{8}{3},\frac{5}{3})\Big],$$
et
$$\Big[(4,4,4)\Big]=\Big[(4-\frac{4}{3},4-\frac{4}{3},4-\frac{4}{3})\Big]=\Big[(\frac{8}{3},\frac{8}{3},\frac{8}{3})\Big].$$

On peut alors réécrire l'inégalité précédente sous la forme :
$$\Big[(4,4,0)\Big]+2\Big[(4,3,1)\Big]+\Big[(3,3,2)\Big]\geqslant 3\Big[(\frac{11}{3},\frac{8}{3},\frac{5}{3})\Big]+\Big[(\frac{8}{3},\frac{8}{3},\frac{8}{3})\Big].$$

Puisque $(4,4,0)$ majore $(11/3, 8/3, 5/3)$, $(4,3,1)$ majore $(11/3, 8/3, 5/3)$ et $(3,3,2)$ majore $(8/3, 8/3, 8/3)$, on applique l'inégalité de Muirhead, ce qui nous permet d'obtenir l'inégalité désirée.

---

23. 1ère solution. À partir des hypothèses, il est clair que l'un des nombres x, y, z est inférieur ou égal à $1/2$. Soit z ce nombre. On a donc

$$G = yz + zx + xy - 2xyz = z(x+y) + xy(1-2z) \geqslant 0.$$

Par ailleurs $x + y \geqslant 2\sqrt{xy}$ et $(1-z)^2 = (x+y)^2 \geqslant 4xy$, d'où

$$\begin{aligned}
G - \frac{7}{27} &= z(x+y) + xy(1-2z) - \frac{7}{27} \\
&\leqslant z(1-z) + \frac{1}{4}(1-2z)(1-z)^2 - \frac{7}{27} \\
&= \left(\frac{1}{4\times 27}\right)\left[4\times 27\times(1-z)z + 27(1-2z)(1-z)^2 - 7\times 4\right] \\
&= \left(\frac{1}{4\times 27}\right)\left[-1 + 27z^2 - 54z^3\right] = \left(\frac{-1}{4\times 27}\right)(3z-1)^2(6z+1) \\
&\leqslant 0.
\end{aligned}$$

2ème solution. (pour retrouver la majoration) Si l'un des nombres x, y ou z est $> 1/2$, disons $z > 1/2$, l'inégalité est évidente :

$$xy + yz + zx - 2xyz = xy(1-2z) + z(x+y) \leqslant \frac{1}{4} < \frac{7}{27}.$$

Dans le cas où x, y, $z < 1/2$, on peut appliquer l'inégalité de la moyenne, de sorte que :

$$\left(\left(\frac{1}{2} - x\right)\left(\frac{1}{2} - y\right)\left(\frac{1}{2} - z\right)\right)^{1/3} \leqslant \frac{1}{6}.$$

Il s'ensuit que

$$\frac{1}{8} - \frac{1}{4}(x+y+z) + \frac{1}{2}(xy+yz+zx) - xyz \leqslant \frac{1}{216},$$

ce qui donne l'inégalité recherchée.

3ème solution. On a d'une part,

$$xy + yz + zx - 2xyz = (x+y+z)(xy+yz+zx) - 2xyz = 6\Big[(2,1,0)\Big] + \Big[(1,1,1)\Big].$$

Il en découle que :

$$xy + yz + zx - 2xyz \geqslant 0.$$

D'autre part,

$$\frac{7}{27} = \frac{7}{27}(x+y+z)^3 = \frac{7}{27}\Big(3\Big[(3,0,0)\Big] + 18\Big[(2,1,0)\Big] + 6\Big[(1,1,1)\Big]\Big).$$

La majoration est alors équivalente à :

$$12\Big[(2,1,0)\Big] \leqslant 7\Big[(3,0,0)\Big] + 5\Big[(1,1,1)\Big].$$

D'après l'inégalité de Muirhead :

$$2\Big[(2,1,0)\Big] \leqslant 2\Big[(3,0,0)\Big],$$

et d'après l'inégalité de Schur (dans le cas $n = 1$) :

$$10\Big[(2,1,0)\Big] \leqslant 5\Big[(3,0,0)\Big] + 5\Big[(1,1,1)\Big],$$

d'où le résultat recherché.

---

24. La forme des termes considérés nous suggère une interprétation géométrique.

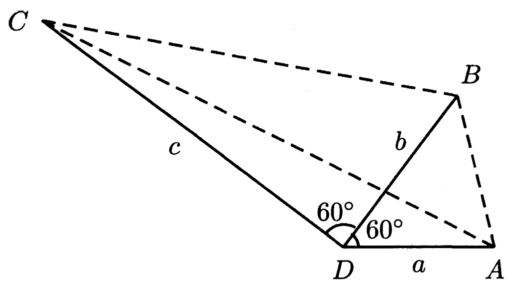


FIG. 4.5.

Dans la figure précédente, on a

$$AB = \sqrt{a^2 - ab + b^2}, \quad BC = \sqrt{b^2 - bc + c^2}, \quad CA = \sqrt{a^2 + ac + c^2}.$$

L'inégalité demandée n'est autre que l'inégalité triangulaire dans le triangle ABC.

---

25. Soit $y_1, y_2, \ldots, y_n$ une permutation de $x_1, x_2, \ldots, x_n$ telle que $0 \leqslant y_1 \leqslant y_2 \leqslant \cdots \leqslant y_n$. Ainsi $1 \leqslant 1 + y_1 \leqslant \cdots \leqslant 1 + y_n$. L'inégalité du réordonnement permet alors d'écrire :

$$\sum_{i=1}^{n} \frac{1 + x_i}{1 + x_{i+1}} \leqslant \sum_{i=1}^{n} \frac{1 + y_i}{1 + y_{n+1-i}},$$

les indices étant pris modulo n. Il suffit alors de prouver que

$$\sum_{i=1}^{n} \frac{1 + y_i}{1 + y_{n+1-i}} \leqslant n + \frac{1}{(1+a)^2} \sum_{i=1}^{n} (y_i - a)^2.$$

Comme

$$\begin{aligned}\frac{1+y_i}{1+y_{n+1-i}}+\frac{1+y_{n+1-i}}{1+y_i}-2 &= \frac{(y_i-y_{n+1-i})^2}{(1+y_i)(1+y_{n+1-i})}\\ &\leqslant \frac{(y_i-y_{n+1-i})^2}{(1+a)^2},\end{aligned}$$

il s'ensuit que

$$\sum_{i=1}^{n}\frac{1+y_i}{1+y_{n+1-i}}\leqslant n+\frac{1}{(1+a)^2}\sum_{i=\lfloor n/2\rfloor}^{n}(y_i-a)^2.$$

On a égalité si et seulement si $y_i=y_{n+1-i}$ ou $y_i\neq y_{n+1-i}$ mais $(1+a)^2=(1+y_i)(1+y_{n+1-i})$. De $a\leqslant y_i,y_{n+1-i}$, il s'ensuit que $y_i=y_{n+1-i}=a$, $i=1,2,\ldots,n$, soit encore $y_1=y_2=\cdots=y_n=a$, i.e., $x_1=x_2=\cdots=x_n=a$.

---

26. On remarque que l'étude du cas $x_1+x_2+\cdots+x_n=1$ suffit pour conclure; plaçons-nous alors dans ce cas. Il existe une permutation $(z_1,z_2,\ldots,z_n)$ de x_1, $x_2,\ldots,x_n$ telle que $z_1+2z_2+\cdots+nz_n>0$. Supposons que $z_1+2z_2+\cdots+nz_n>(n+1)/2$ (car dans le cas contraire, le problème serait résolu). Comme $(z_1+2z_2+\cdots+nz_n)+(z_n+2z_{n-1}+\cdots+nz_1)=n+1$, alors $z_n+2z_{n-1}+\cdots+nz_1<-(n+1)/2$.

Il faut maintenant remarquer que pour passer d'une permutation à une autre, il suffit d'appliquer un nombre fini de fois des échanges entre des éléments voisins. Mais, si on pose

$$\begin{aligned}S_\sigma&=x_{\sigma(1)}+\cdots+ix_{\sigma(i)}+(i+1)x_{\sigma(i+1)}+\cdots+nx_{\sigma(n)},\\ S_{\sigma'}&=x_{\sigma(1)}+\cdots+ix_{\sigma(i+1)}+(i+1)x_{\sigma(i)}+\cdots+nx_{\sigma(n)},\end{aligned}$$

alors

$$|S_\sigma-S_{\sigma'}|=|x_{\sigma(i)}-x_{\sigma(i+1)}|\leqslant\frac{n+1}{2}\times 2=n+1.$$

Ainsi, en considérant la suite permettant de passer de la permutation $(z_n$, $z_{n-1},\ldots,z_1)$ à la permutation $(z_1,z_2,\ldots,z_n)$, on s'aperçoit qu'à un certain moment, on arrivera à une permutation $(y_1,y_2,\ldots,y_n)$ de $(x_1,x_2,\ldots,x_n)$ pour laquelle la somme $y_1+2y_2+\cdots+ny_n$ se situe entre $-(n+1)/2$ et $(n+1)/2$.

---

27. Il est facile de généraliser la démonstration du théorème 2.6.2 concernant les systèmes complets de résidus pour obtenir le lemme suivant : si $(p,q)=d$ et si on pose $\dfrac{p}{q}=l$, alors $(q,\,2q,\ldots,\,lq)$ est une permutation des nombres $0,\,d,\,2d,\ldots,\,(l-1)d$ modulo p.

1$^{\text{ère}}$ solution. Il suffit de montrer que l'inégalité de l'énoncé est vraie pour les nombres rationnels de la forme p/q où $p\in\mathbb{N}$, $q\in\mathbb{N}^*$ et $(p,q)=1$, qui sont compris entre 0 et 1.

Dans ce cas, on introduit les nombres a_k et b_k, où $1\leqslant k\leqslant n$, définis par :

$$kp=a_kq+b_k,\ 0\leqslant b_k\leqslant q-1.$$

L'inégalité à démontrer est alors équivalente à $\lfloor n \cdot p/q \rfloor \geqslant \sum_{k=1}^{n} a_k/k$. Or

$$\sum_{k=1}^{n} \frac{a_k}{k} + \frac{1}{q} \cdot \sum_{k=1}^{n} \frac{b_k}{k} = n \cdot \frac{p}{q},$$

et comme $b_1, b_2, \ldots, b_{q-1}$ est une permutation de l'ensemble $\{1, 2, \ldots, q-1\}$ (résultat préliminaire),

$$\sum_{k=1}^{q-1} \frac{b_k}{k} \geqslant q - 1$$

d'après l'inégalité du réordonnement.

Ainsi,

$$\frac{q-1}{q} + \sum_{k=1}^{n} \frac{a_k}{k} \leqslant n \cdot \frac{p}{q} = a_n + \frac{b_n}{q} \leqslant a_n + \frac{q-1}{q},$$

soit enfin

$$a_n \geqslant \sum_{k=1}^{n} \frac{a_k}{k},$$

qui est l'inégalité à laquelle on voulait aboutir.

2ème solution. On note $\{x\} = x - \lfloor x \rfloor$ la partie fractionnaire de x. L'inégalité à démontrer est équivalente à :

$$\{nx\} \leqslant \sum_{k=1}^{n} \frac{\{kx\}}{k}.$$

Le graphe représentatif de la fonction $x \mapsto \{x\}$ a l'allure suivante :

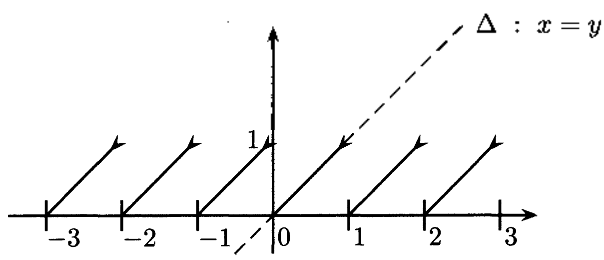


FIG. 4.6.

On remarque que toutes les discontinuités de $x \mapsto \{nx\}$ se produisent aux points k/n ($k \in \mathbb{Z}$). On pose alors $x = (k/n) - \varepsilon$ avec $0 < \varepsilon \leqslant 1/n$. Si $(n, k) = d$ et $n/d = c$, les nombres $k, 2k, \ldots, ck$ forment une permutation des nombres $d, 2d, \ldots, cd$ modulo n (résultat préliminaire). Ainsi,

$$\{ix\} = \{\frac{ik}{n} - i\varepsilon\} = \{\frac{\sigma(i)d}{n} - i\varepsilon\} \quad , \quad i \in \{1, 2, \ldots, c\},$$

où $\sigma(1), \sigma(2), \ldots, \sigma(c)$ est une permutation de l'ensemble $\{1, 2, \ldots, c\}$. Mais puisque

$$\frac{\sigma(i)d}{n} - i\varepsilon < \frac{cd}{n} = 1, \quad \forall i \in \{1, 2, \ldots, c\},$$

alors $\{ix\} \geqslant \sigma(i)d/n - i\varepsilon$, $\forall i \in \{1, 2, \ldots, c\}$, et il s'ensuit que

$$\begin{aligned}\{x\} + \frac{\{2x\}}{2} + \cdots + \frac{\{cx\}}{c} &\geqslant \frac{d}{n}\left(\sum_{i=1}^{c}\frac{\sigma(i)}{i}\right) - c\varepsilon \\ &\geqslant \frac{cd}{n} - n\varepsilon \\ &= 1 - n\varepsilon = \{k - n\varepsilon\} = \{nx\}\end{aligned}$$

toujours en appliquant l'inégalité du réordonnement. On a ainsi l'inégalité désirée.

---

28. Pour $1 \leqslant i \leqslant n$, on note

$$A_i = \{p \in \{1, 2, \ldots, N\} \mid a_i \text{ divise } p\}$$

D'après les hypothèses de l'énoncé $A_i \cap A_j = \varnothing$ pour tous $i, j \in \{1, 2, \ldots, n\}$ distincts. Ainsi

$$\operatorname{card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \operatorname{card}(A_i),$$

mais comme $\bigcup_{i=1}^{n} A_i \subseteq \{1, 2, \ldots, N\}$, on a :

$$\sum_{i=1}^{n} \operatorname{card}(A_i) \leqslant N.$$

Or, $\operatorname{card}(A_i) = \lfloor N/a_i \rfloor$, $i \in \{1, 2, \ldots, n\}$, et donc

$$N > N\left[\sum_{i=1}^{n}\frac{1}{a_i}\right] - n,$$

soit encore

$$\sum_{i=1}^{n}\frac{1}{a_i} < 1 + \frac{n}{N} \leqslant 2.$$

---

29. Le cas $N = 2$ est trivial : en effet,

$$\sum_{k=0}^{+\infty}\frac{1}{2^k} = 2.$$

Supposons le résultat vrai pour tout entier $k < N$, et prouvons que le résultat est encore vrai pour N. On divise alors l'ensemble considéré en deux sous-ensembles, le premier étant constitué par les nombres dont tous les diviseurs premiers sont inférieurs ou égaux à $N - 1$, et le second par le reste.

On note $b_1, b_2, \ldots, b_m$ ($\{b_1, b_2, \ldots, b_m\} \subseteq \{a_1, a_2, \ldots, a_n\}$) les éléments du deuxième sous-ensemble. Il suffirait évidemment de prouver que $\sum_{i=1}^{m} 1/b_i \leqslant 1$. Or,

$$\sum_{i=1}^{m}\frac{1}{b_i} \leqslant S \cdot \sum_{i=1}^{k}\frac{1}{N^i},$$

où S est la somme de tous les entiers positifs qui n'ont aucun diviseur premier $\geqslant N-1$, et k est la plus grande puissance de N intervenant dans la décomposition en nombres premiers des b_i, $i \in \{1, 2, \ldots, m\}$.

Par hypothèse de récurrence $S \leqslant N-1$. Ainsi,

$$\sum_{i=1}^{m} \frac{1}{b_i} \leqslant (N-1)\frac{1-1/N^k}{1-1/N} \leqslant 1,$$

ce qui achève la démonstration.

---

30. On pose $y_0 = 1$, $y_i = 1 + x_1 + x_2 + \cdots + x_i$ $(1 \leqslant i \leqslant n)$. On a ainsi

$$\forall i,\ 1 \leqslant i \leqslant n, \quad \frac{x_i}{y_i} = 1 - \frac{y_{i-1}}{y_i} \leqslant s,$$

ce qui donne

$$1 - s \leqslant \frac{y_{i-1}}{y_i},$$

soit encore (car $y_n = 2$)

$$s \geqslant 1 - \frac{1}{2^{1/n}}.$$

On a égalité si et seulement si

$$y_0 = 1, \quad y_1 = 2^{1/n}, \quad y_2 = 2^{2/n}, \ldots, \quad y_n = 2,$$

soit encore

$$x_i = 2^{i/n} - 2^{(i-1)/n}, \quad i = 1, 2, \ldots, n.$$

---

31. Il suffit de traiter l'exercice dans le cas où les nombres $x_1, x_2, \ldots, x_n$ sont positifs. Étant donné que $x_1^2 + x_2^2 + \cdots + x_n^2 = 1$, alors, en employant l'inégalité de Cauchy-Schwarz,

$$x_1 + x_2 + \cdots + x_n \leqslant \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}\sqrt{n} = \sqrt{n}.$$

Toutes les sommes de la forme $e_1x_1 + e_2x_2 + \cdots + e_nx_n$ avec $e_i \in \{0, 1, 2, \ldots, k-1\}$ doivent donc être dans l'intervalle fermé $\left[0, (k-1)\sqrt{n}\right]$. Cet intervalle peut être recouvert avec $k^n - 1$ sous-intervalles fermés de longueur $(k-1)\sqrt{n}/(k^n-1)$. Par le principe des tiroirs, nous pouvons affirmer qu'il existe au moins deux sommes qui se trouvent dans le même sous-intervalle. La valeur absolue de leur différence ne dépasse pas la longueur du sous-intervalle. Ainsi, il existe des nombres $e_i \in \{0, \pm 1, \ldots, \pm(k-1)\}$, $i \in \{1, 2, \ldots, n\}$, pour lesquels

$$|e_1x_1 + e_2x_2 + \cdots + e_nx_n| \leqslant \frac{(k-1)\sqrt{n}}{k^n - 1}.$$

---

32. 1ère solution. L'inégalité demandée est équivalente à l'inégalité :

$$\frac{1}{x^5+y^2+z^2}+\frac{1}{y^5+z^2+x^2}+\frac{1}{z^5+x^2+y^2}\leqslant\frac{3}{x^2+y^2+z^2}.$$

Or, d'après l'inégalité de Cauchy-Schwarz, et le fait que $xyz \geqslant 1$:

$$\begin{aligned}\left(x^5+y^2+z^2\right)\left(yz+y^2+z^2\right) &\geqslant \left(\sqrt{x^5yz}+y^2+z^2\right)^2\\ &\geqslant \left(x^2+y^2+z^2\right)^2.\end{aligned}$$

On a alors :

$$\frac{1}{x^5+y^2+z^2}\leqslant\frac{yz+y^2+z^2}{\left(x^2+y^2+z^2\right)^2}\leqslant\frac{\dfrac{y^2+z^2}{2}+y^2+z^2}{\left(x^2+y^2+z^2\right)^2}.$$

En appliquant la même approche, on a aussi :

$$\frac{1}{y^5+z^2+x^2}\leqslant\frac{\dfrac{z^2+x^2}{2}+z^2+x^2}{\left(x^2+y^2+z^2\right)^2},$$

et

$$\frac{1}{z^5+x^2+y^2}\leqslant\frac{\dfrac{x^2+y^2}{2}+x^2+y^2}{\left(x^2+y^2+z^2\right)^2}.$$

En additionnant membre à membre ces inégalités, on obtient l'inégalité recherchée.

2ème solution. En éliminant les dénominateurs, on obtient l'inégalité équivalente :

$$\begin{aligned}&\Big[(9,0,0)\Big]+4\Big[(7,5,0)\Big]+\Big[(5,2,2)\Big]+\Big[(5,5,5)\Big]\\ \geqslant&\Big[(6,0,0)\Big]+\Big[(5,5,2)\Big]+2\Big[(5,4,0)\Big]+2\Big[(4,2,0)\Big]+\Big[(2,2,2)\Big],\end{aligned}$$

où on a utilisé les notations de l'inégalité de Muirhead.

Puisque $xyz \geqslant 1$, on peut appliquer la remarque :

$$\Big[(a_1,a_2,\ldots,a_n)\Big]\geqslant\Big[(a_1-\alpha,a_2-\alpha,\ldots,a_n-\alpha)\Big],$$

pour tout vecteur $(a_1,a_2,\ldots,a_n)\in\mathbb{R}^n$ et pour tout réel $\alpha\geqslant 0$.

On a ainsi, puisque $(9,0,0)$ majore $(7,1,1)$:

$$\Big[(9,0,0)\Big]\geqslant\Big[(7,1,1)\Big]\geqslant\Big[(6,0,0)\Big].$$

De même, puisque $(7,5,0)$ majore $(5,5,2)$:

$$\Big[(7,5,0)\Big] \geqslant \Big[(5,5,2)\Big].$$

De manière similaire, $(7,5,0)$ majore $(6,5,1)$, donc :

$$2\Big[(7,5,0)\Big] \geqslant 2\Big[(6,5,1)\Big] \geqslant 2\Big[(5,4,0)\Big].$$

En appliquant l'inégalité de la moyenne, on a aussi :

$$\Big[(7,5,0)\Big] + \Big[(5,2,2)\Big] \geqslant 2\Big[(6,\frac{7}{2},1)\Big],$$

et puisque $(6,7/2,1)$ majore $(11/2,7/2,3/2)$, on obtient :

$$\Big[(7,5,0)\Big] + \Big[(5,2,2)\Big] \geqslant 2\Big[(\frac{11}{2},\frac{7}{2},\frac{3}{2})\Big] \geqslant 2\Big[(4,2,0)\Big].$$

On a enfin :

$$\Big[(5,5,5)\Big] \geqslant \Big[(2,2,2)\Big].$$

En additionnant membre à membre les inégalités précédentes, on obtient l'inégalité recherchée.

---

33. 1ère solution. Sans perte de généralité, on peut supposer que $x \geqslant y \geqslant z > 0$. Posons alors

$$u = \frac{x+y}{2z}, \quad v = \frac{xy}{z^2};$$

on a alors

$$xy + yz + zx = z^2\left(\frac{x+y}{z} + \frac{xy}{z^2}\right) = z^2(2u+v),$$

et

$$\begin{aligned} z^2\left(\frac{1}{(y+z)^2} + \frac{1}{(z+x)^2}\right) &= \frac{z^2 \cdot [(x+y)^2 - 2xy + 2z^2 + 2z(x+y)]}{(z^2+xy+yz+zx)^2} \\ &= \frac{4u^2 - 2v + 2 + 4u}{(1+2u+v)^2}. \end{aligned}$$

Ainsi, l'inégalité à démontrer s'écrit

$$(2u+v)\left(\frac{1}{4u^2} + \frac{4u^2 - 2v + 2 + 4u}{(1+2u+v)^2}\right) \geqslant \frac{9}{4},$$

avec $1 \leqslant v \leqslant u^2$.

L'inégalité précédente se réécrit encore sous la forme :

$$(2u+v)\big[(1+2u+v)^2 + 4u^2(4u^2 - 2v + 2 + 4u)\big] \geqslant 9u^2(1+2u+v)^2.$$

Pour u fixé, on considère la fonction de v définie sur $[1, u^2]$ par :

$$\begin{aligned} f(v) &= v^3 - (17u^2 - 6u - 2)v^2 + (16u^4 - 36u^3 + 2u^2 + 8u + 1)v + \\ &\quad (35u^5 - 4u^4 - 12u^3 - u^2 + 2u). \end{aligned}$$

on a alors $f''(v) < 0$ si $u \geqslant 1$, i.e. f est concave. Comme $f(1) \geqslant 0$ et $f(u^2) \geqslant 0$, alors $f(v) \geqslant 0$ pour tout v, $1 \leqslant v \leqslant u^2$, ce qui conclut la démonstration.

2$^{\text{ème}}$ solution. En réduisant au même dénominateur, l'inégalité se réécrit sous la forme :

$$\begin{aligned} \sum_{\text{sym.}} &\left(4x^5y - x^4y^2 - 3x^3y^3\right) + \left(4xy^5 - x^2y^4 - 3x^3y^3\right) \\ &+ \left(2x^4yz - 2x^3y^2z - 2x^3yz^2 + 2x^2y^2z^2\right) \geqslant 0, \end{aligned}$$

où $\sum_{\text{sym.}}$ désigne la somme sur toutes les permutations circulaires de x, y, z.

D'après l'inégalité de Schur, on a :

$$x(x-y)(x-z) + y(y-z)(y-x) + z(z-x)(z-y) \geqslant 0,$$

ce qui donne en multipliant par $2xyz$:

$$\sum_{\text{sym.}} 2x^4yz - 2x^3y^2z - 2x^3yz^2 + 2x^2y^2z^2 \geqslant 0.$$

D'un autre côté, on a d'après l'inégalité du réordonnement :

$$\sum_{\text{sym.}} x^5y \geqslant \sum_{\text{sym.}} x^4y^2, \quad \sum_{\text{sym.}} x^5y \geqslant \sum_{\text{sym.}} x^3y^3,$$

ce qui donne

$$\sum_{\text{sym.}} 4x^5y - x^4y^2 - 3x^3y^3 \geqslant 0,$$

et de même,

$$\sum_{\text{sym.}} 4xy^5 - x^2y^4 - 3x^3y^3 \geqslant 0,$$

ce qui permet de conclure.

---

34. On pose $x + y = c^2$, $y + z = a^2$, $z + x = b^2$, avec $a, b, c > 0$ et quitte à faire une permutation circulaire, on peut supposer que $a \geqslant b, c$. On a alors

$$x = \frac{-a^2 + b^2 + c^2}{2}, \quad y = \frac{a^2 - b^2 + c^2}{2}, \quad z = \frac{a^2 + b^2 - c^2}{2},$$

et l'inégalité devient

$$\frac{-a^2 + b^2 + c^2}{c} + \frac{a^2 - b^2 + c^2}{a} + \frac{a^2 + b^2 - c^2}{b} \leqslant \frac{5}{2\sqrt{2}}\sqrt{a^2 + b^2 + c^2},$$

Si $b+c-\dfrac{176}{27}bc \leqslant 0$, l'inégalité de la moyenne donne $F(a,b,c,d) \leqslant bc(a+d) \leqslant (1/3)^3 = 1/27$, et l'inégalité est démontrée dans ce cas. On a égalité si et seulement si $b=c=1/3$ et $(a=0,\ d=1/3)$ ou $(a=1/3,\ d=0)$.

Si $b+c-\dfrac{176}{27}bc > 0$, alors

$$\begin{aligned} F(a,b,c,d) &\leqslant bc(a+d)+\Big(\frac{a+d}{2}\Big)^2\Big(b+c-\frac{176}{27}bc\Big) \\ &= F\Big(\frac{a+d}{2},b,c,\frac{a+d}{2}\Big). \end{aligned}$$

On considère les quadruplets :

$$P_0=(a,b,c,d),\ P_1=\Big(\frac{a+d}{2},b,c,\frac{a+d}{2}\Big),\ P_2=\Big(\frac{a+d}{2},\frac{b+c}{2},\frac{b+c}{2},\frac{a+d}{2}\Big),$$
$$P_3=\Big(\frac{1}{4},\frac{1}{4},\frac{b+c}{2},\frac{a+d}{2}\Big),\ P_4=\Big(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4}\Big).$$

L'argument précédent montre que $F(P_i)\leqslant 1/27$ ou $F(P_i)\leqslant F(P_{i+1})$. Comme $F(P_4)=1/27$, le résultat s'ensuit immédiatement.

Par ailleurs, on a égalité si et seulement si un nombre est égal à 0, les trois autres étant égaux à $1/3$, ou si les quatre nombres sont égaux à $1/4$.

---

36. Considérons des entiers naturels $x_1,x_2,\ldots,x_n$ dont la somme est égale à un entier fixé N (l'exercice correspond au cas particulier où $N=1976$).

Si l'un des x_i est égal à 1, et si j est un indice quelconque différent de i alors, en supprimant x_i et en remplaçant x_j par x_j+1, on remarque que le produit des $n-1$ nombres obtenus est plus grand que le produit initial des n nombres considérés.

Si maintenant $x_i=4$, on ne modifie ni le produit, ni la somme en remplaçant x_i par $2+2$.

Si enfin $x_i>4$, on décompose x_i sous la forme $x_i=(x_i-2)+2$. Le nouveau produit est alors supérieur au précédent car $2(x_i-2)>x_i$.

En conclusion, on peut supposer, dans la recherche du produit maximal que l'on peut former, que les entiers considérés sont tous égaux à 2 ou à 3. Mais comme $2^3<3^2$, on aura intérêt à remplacer les groupes de 3 nombres égaux à 2 par des groupes de 2 nombres égaux à 3. On est donc amené à distinguer trois cas :

- Si $N=3p$ ($p\in\mathbb{N}$), alors la valeur maximale est 3^p.
- Si $N=3p+1=3(p-1)+2$ ($p\in\mathbb{N}$) , alors la valeur maximale est $4\times 3^{p-1}$.
- Si $N=3p+2$ ($p\in\mathbb{N}$), alors la valeur maximale est 2×3^p.

En particulier, puisque $1976 = 3\times 658+2$, le produit maximal constitué d'entiers dont la somme est égale à 1976 est 2×3^{658}.

---

37. 1ère solution. On note $|V_x|=a,\ \ |V_y|=b,\ \ |V_z|=c$. On raisonne par récurrence sur $|V|$: le résultat est évidemment vrai si $|V|=1$. Si on suppose le résultat acquis pour tout ensemble V tel que $|V| < n$, et soit un ensemble V tel que $|V| = n$. Il est clair qu'il existe un plan parallèle à un plan des coordonnées ne contenant aucun point de V, et divisant V en deux sous-ensembles non vides V_1 et V_2, de telle sorte que $n = |V_1| + |V_2|$, $|V_1| < n$ et $|V_2| < n$. D'après l'hypothèse de récurrence

$$|V_1| \leqslant a_1 b_1 c_1, \quad |V_2| \leqslant a_2 b_2 c_2.$$

Supposons le plan que l'on vient d'introduire parallèle au plan xy. On a alors

$$a_1 + a_2 = a, \quad b_1 + b_2 = b, \quad c_1 \leqslant c, \quad c_2 \leqslant c.$$

D'après l'inégalité de Cauchy-Schwarz,

$$\begin{aligned} |V|^2 = \left(|V_1| + |V_2|\right)^2 \leqslant \left(\sqrt{a_1 b_1 c_1} + \sqrt{a_2 b_2 c_2}\right)^2 &\leqslant \left(\sqrt{a_1 b_1} + \sqrt{a_2 b_2}\right)^2 c \\ &\leqslant c(a_1 + b_1)(a_2 + b_2) = abc, \end{aligned}$$

ce qui termine la preuve.

2$^{\text{ème}}$ solution. On va utiliser un raisonnement combinatoire. On note V_{ij} l'ensemble des points de V de la forme (x, i, j), i.e., l'ensemble des points de V qui se projettent sur le plan yz au point (i, j).

On a alors $V = \bigcup_{(i,j)\in V_x} V_{ij}$, d'où

$$|V| \leqslant \sum_{(i,j)\in V_x} |V_{ij}|,$$

et d'après l'inégalité de Cauchy-Schwarz

$$|V|^2 \leqslant \sum_{(i,j)\in V_x} 1^2 \cdot \sum_{(i,j)\in V_x} |V_{ij}|^2 = |V_x| \cdot \sum_{(i,j)\in V_x} |V_{ij}|^2.$$

On cherche un ensemble X tel que $|X| = \sum_{(i,j)\in V_{ij}} |V_{ij}|^2$. Il est clair que l'ensemble

$$X = \bigcup_{(i,j)\in V_x} (V_{ij} \times V_{ij})$$

convient.

Par ailleurs, l'application $f \colon X \to V_y \times V_z$ définie par

$$f((x, i, j), (x', i, j)) = ((x, j), (x', i))$$

est injective, et donc $|X| \leqslant |V_y| \cdot |V_z|$, d'où le résultat.

5

ANALYSE COMBINATOIRE

Les problèmes de combinatoire apparaissent fréquemment dans les compétitions mathématiques, et notamment dans les olympiades internationales. Ce chapitre aborde l'essentiel des connaissances et techniques requises dans la résolution de ce type de problèmes.

On introduit également la notion de graphe et on l'étudie en connexion avec les problèmes de dénombrement. On verra ainsi comment les idées introduites dans ce cadre permettent de développer une méthode d'analyse simplificatrice.

On finira ce chapitre par une digression sur les fonctions génératrices. Il s'agit d'un thème assez technique, mais dont l'application en combinatoire s'avère très efficace.

5.1. Dénombrement d'ensembles finis

5.1.1. Arrangements. Permutations. Soient E et F des ensembles finis non vides de cardinaux respectifs p et n.

On établit sans difficulté qu'il existe $n \times n \times \cdots \times n = n^p$ applications de E dans F. Parmi ces applications, $n \times (n-1) \times \cdots \times (n-p+1)$ sont injectives.

On appelle *arrangement* de p éléments de F toute application injective du sous-ensemble $\{1, 2, \ldots, p\}$ de $\mathbb{N}^*$ dans F. Un arrangement est donc aussi bien un p-uplet de F.

D'après ce qui précède, le nombre de ces arrangements est

$$\boxed{A_n^p = \frac{n!}{(n-p)!} = n(n-1)\cdots(n-p+1).} \tag{5.1}$$

On appelle *permutation* de l'ensemble F toute bijection de F sur lui-même. Une permutation de F est donc aussi bien un réordonnement des n éléments de F. Le nombre de ces permutations est

$$\boxed{A_n^n = n(n-1)\cdots 1 = n!.} \tag{5.2}$$

♦ **Exemples.**

1. Le nombre de suites finies de longueur n et à valeurs dans l'ensemble $\{0,1\}$ est égal à 2^n : en effet, c'est le nombre d'applications de l'ensemble $\{1,2,\ldots,n\}$ dans l'ensemble $\{0,1\}$.

2. Quel est le nombre de manières d'asseoir n couples mariés mari-épouse autour d'une table ronde de $2n$ places de telle sorte que les maris et épouses soient alternés ?

Il y a $2(n!)$ façons d'asseoir les n maris. Pour chacune de ces possibilités, il y a $n!$ façons d'asseoir les n épouses. Il s'ensuit que le nombre recherché est $2(n!)^2$.

3. Quel est le nombre minimal de tours permettant de contrôler toutes les cases inoccupées d'un échiquier $n \times n$? De combien de façons ceci peut-il être réalisé ?

Note. Au jeu d'échecs, une pièce contrôle les cases où elle peut se déplacer. Une tour contrôle donc la ligne et la colonne où elle se trouve.

Il est impossible de contrôler toutes les cases inoccupées d'un échiquier $n \times n$ à l'aide de moins de n tours. D'un autre côté, on peut toujours placer n tours de telle manière à contrôler toutes les cases inoccupées d'un échiquier $n \times n$:

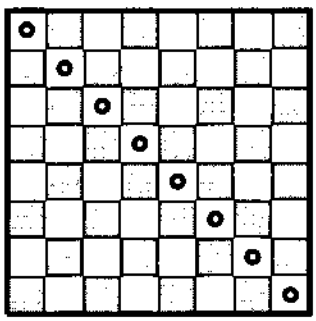


FIG. 5.1.

On doit placer au moins une tour par ligne. On peut placer la tour de la première ligne dans l'une quelconque des n colonnes, la tour de la deuxième ligne dans l'une quelconque des $n-1$ colonnes, autre que la colonne déjà choisie, etc...

Il s'ensuit qu'il existe $n!$ façons de disposer n tours dans un échiquier $n \times n$ de manière à contrôler toutes les cases inoccupées de l'échiquier.

5.1.2. Combinaisons. On appelle *combinaison* de p éléments d'un ensemble non vide E toute partie à p éléments de E. Si E possède n éléments, alors le nombre des combinaisons de p éléments de E, nombre qui est désigné par $\binom{n}{p}$, ou parfois C_n^p, a pour valeur

$$\boxed{\binom{n}{p} = \frac{A_n^p}{p!} = \frac{n!}{p!(n-p)!}, \quad p = 0,1,\ldots,n,} \tag{5.3}$$

où $\binom{n}{0} = \binom{n}{n} = 1$ $(0! = 1)$.

Les nombres $\binom{n}{p}$ sont appelés coefficients binomiaux, et il s'ensuit de la définition que

$$\binom{n}{p} = \binom{n}{n-p}, \quad p = 0, 1, \ldots, n. \tag{5.4}$$

♦ **Exemples.**

1. Quel est le nombre des points d'intersection des diagonales d'un polygone convexe à n sommets situés à l'intérieur de ce polygone sachant que trois quelconques de ses diagonales ne sont pas concourantes en un même point ?

On numérote les n sommets du polygone dans le sens trigonométrique en commençant par l'un quelconque d'entre eux : $A_1, A_2, \ldots, A_n$. À tout ensemble de 4 sommets A_i, A_j, A_k, A_l $(i < j < k < l)$, correspond un point M où A_iA_k et A_jA_l se recoupent.

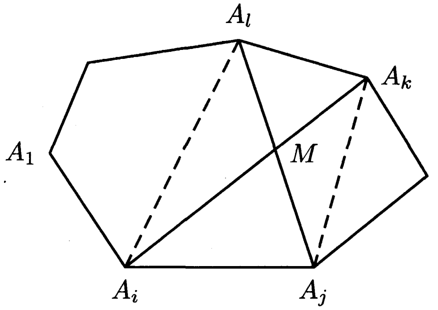


FIG. 5.2.

Réciproquement, à chaque point d'intersection de deux diagonales situé à l'intérieur du polygone correspond un ensemble de 4 sommets. Il s'ensuit qu'il existe

$$\binom{n}{4} = \frac{n(n-1)(n-2)(n-3)}{4!}$$

points d'intersection des diagonales du polygone situés en son intérieur.

2. Quel est le nombre de m-uplets $(x_1, x_2, \ldots, x_m)$ de $(\mathbb{N}^*)^m$ vérifiant

$$x_1 + x_2 + \cdots + x_m = n?$$

On considère un segment $[A_0A_n]$ de longueur n. Toute solution dans $(\mathbb{N}^*)^m$ de l'équation $x_1+x_2+\cdots+x_m = n$ équivaut au choix de $m-1$ points $B_1, B_2, \ldots, B_{m-1}$ parmi les points $A_1, A_2, \ldots, A_{n-1}$.

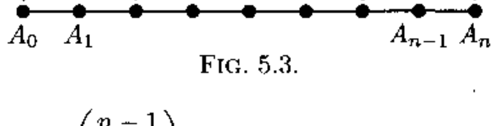


FIG. 5.3.

Il s'ensuit qu'il existe $\binom{n-1}{m-1}$ m-uplets d'entiers strictement positifs dont la somme vaut n.

5.1.3. Applications d'un ensemble fini dans un ensemble fini. Soit f une application de E fini dans F fini. On a alors :

$$|f(E)| \leqslant \min\big(|E|, |F|\big)$$

car l'image par f de n points distincts est constituée de n points distincts ou confondus.

En particulier, si f est injective $\|E\| \leqslant \|F\|$; si elle est surjective $\|F\| \leqslant \|E\|$ et si elle est bijective $\|F\| = \|E\|$.

♦ **Exemples.**

1. On considère la grille rectangulaire de $\mathbb{N} \times \mathbb{N}$:

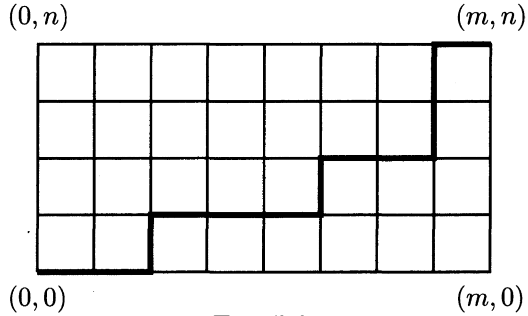


FIG. 5.4.

Quel est le nombre de façons d'aller de $(0,0)$ à (m,n) par un chemin où à chaque pas l'une des coordonnées augmente d'une unité ?

Soit E l'ensemble des chemins menant de $(0,0)$ à (m,n). Si on désigne par un « 0 » un déplacement horizontal et par un « 1 » un déplacement vertical, il apparaît que tout élément de E peut être uniquement représenté par une suite finie de longueur $m+n$ et à valeurs dans l'ensemble $\{0,1\}$ comportant exactement m « 0 ». Si F désigne l'ensemble de ces suites, alors

$$|F| = \binom{m+n}{m} = \binom{m+n}{n},$$

et comme E et F sont en bijection, il s'ensuit que :

Le nombre de façons d'aller de $(0,0)$ à (m,n) par un chemin où à chaque pas l'une des coordonnées augmente d'une unité est

$$|E| = \binom{m+n}{m} = \binom{m+n}{n}.$$

2. Quel est le nombre de sous-ensembles à k éléments de $\{1,2,\ldots,n\}$ ne contenant pas d'entiers consécutifs ?

On va construire une bijection entre l'ensemble de ces parties, et l'ensemble des parties à k éléments de $\{1,2,\ldots,n+1-k\}$.

Pour tout sous-ensemble $A = \{a_1, a_2, \dots, a_k\}$ de $\{1, 2, \dots, n\}$ dont les éléments sont indexés de telle sorte que $a_1 < a_2 < \cdots < a_k$ et où aucun a_i ne succède à a_{i-1}, $i = 2, 3, \dots, k$, on pose

$$f(A) = \{a_1, a_2 - 1, \dots, a_k - (k-1)\}.$$

Il est alors clair que tous les éléments de $f(A)$ sont distincts, et que $f(A)$ est une partie à k éléments de $\{1, 2, \dots, n+1-k\}$. Il s'ensuit que l'application f est bien définie.

D'un autre côté, f est visiblement injective, et si $B = \{b_1, b_2, \dots, b_k\}$ est une partie à k éléments de $\{1, 2, \dots, n+1-k\}$ dont les éléments sont indexés de telle sorte que $b_1 < b_2 < \cdots < b_k$, alors

$$A = \{b_1, b_2 + 1, \dots, b_k + (k-1)\}$$

est l'image réciproque de B par f. On en déduit que f est bijective et donc :

Le nombre de sous-ensembles à k éléments de $\{1, 2, \dots, n\}$ ne contenant pas d'entiers consécutifs est

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

5.1.4. Dénombrement par récurrence. Nous nous contenterons ici de fournir quelques exemples illustrant cette technique :

1. Soit $n > 1$ un entier. Trouver le nombre de permutations $(a_1, a_2, \dots, a_n)$ de l'ensemble $\{1, 2, \dots, n\}$ telles qu'il existe un et un seul indice $i \in \{1, 2, \dots, n-1\}$ vérifiant $a_i > a_{i+1}$.

(Olympiades bulgares-1995)

On note p_n le nombre recherché, et soit $(a_1, a_2, \dots, a_{n+1})$ une permutation de l'ensemble $\{1, 2, \dots, n+1\}$ telle qu'il existe un et un seul indice $i \in \{1, 2, \dots, n\}$ vérifiant $a_i > a_{i+1}$. Distinguons alors les deux cas :

a) $a_{n+1} = n+1$, auquel cas correspondent p_n permutations ;

b) il existe $i \in \{1, 2, \dots, n\}$ tel que $a_i = n+1$. Dans ce cas, il existe $\binom{n}{i-1}$ permutations convenables.

On en déduit que

$$p_{n+1} = p_n + \sum_{i=1}^{n} \binom{n}{i-1} = p_n + 2^n - 1$$

d'après la formule du binôme (voir paragraphe suivant). On a donc, compte tenu de $p_2 = 1$:

$$p_n = 2^n - n - 1.$$

2. On considère un entier $n > 1$ et on se donne $2n$ points autour d'un cercle. De combien de façons peut-on relier ces points, deux à deux, à l'aide de n cordes qui ne se recoupent pas à l'intérieur du cercle ?

Soit F_n le nombre recherché. On désigne par A_1 un des $2n$ points placés autour du cercle, et on numérote les autres points $2, 3, \ldots, 2n$ dans le sens trigonométrique : $A_2, A_3, \ldots, A_{2n}$.

Le point A_1 peut être relié à l'un quelconque des points $A_2, A_4, \ldots, A_{2n}$, et seulement à l'un de ces points : en effet, si A_1 est relié à un point A_k où k est impair, alors on aurait un nombre impair de points de part et d'autre de la corde A_1A_k, et une des n cordes construites doit nécessairement recouper la corde A_1A_k, ce qui est exclu.

Supposons donc le point A_1 relié au point A_{2k}. Il y a donc $2(k-1)$ points d'un côté de la corde A_1A_{2k} et $2(n-k)$ points de l'autre côté. Il s'ensuit qu'il existe $F_{k-1}F_{n-k}$ façons de relier les points $A_1, A_2, \ldots, A_{2n}$, deux à deux, tels que A_1 soit relié à A_{2k} et sans que les n cordes construites ne se recoupent à l'intérieur du cercle. Quitte à poser $F_0 = 1$, on obtient

$$F_n = \sum_{k=0}^{n-1} F_k F_{n-1-k} = F_0F_{n-1} + F_1F_{n-2} + \cdots + F_{n-1}F_0.$$

La solution de cette équation de récurrence, compte tenu de $F_0 = F_1 = 1$, est

$$F_n = \frac{1}{n+1}\binom{2n}{n} = c_n,$$

qui est la suite des nombres de Catalan[1]. Ceci sera établi ultérieurement grâce aux fonctions génératrices.

3. Soit, dans un plan, n droites $(D_1), (D_2), \ldots, (D_n)$ telles que deux quelconques d'entre elles ne soient pas parallèles ni trois quelconques concourantes en un même point. Déterminer le nombre R_n de régions que ces droites déterminent dans le plan.

On pourrait penser que le nombre R_n dépend de la position des droites (D_i), $i = 1, 2, \ldots, n$, mais le raisonnement ci-dessous montre qu'il n'en est rien.

En effet, supposons les $(n-1)$ droites $(D_1), (D_2), \ldots, (D_{n-1})$ déjà construites ; traçons alors la droite (D_n). Cette droite recoupe les droites (D_i), $i = 1, 2, \ldots, n-1$, en $n-1$ points distincts qui déterminent n parties sur la droite (D_n). Il s'ensuit que (D_n) entraîne l'introduction de n nouvelles régions. On a donc

$$R_n = [n + (n-1) + \cdots + 2] + 2 = \frac{n^2+n+2}{2}.$$

Ce nombre ne dépend que du nombre n des droites considérées.

5.2. Les identités combinatoires

5.2.1. Théorème. *(formule du binôme de Newton) Pour tout entier $n \geqslant 1$ et pour tous nombres complexes x et y, on a la formule suivante, dite formule du*

1. Eugène Charles Catalan (1814-1894), mathématicien belge.

binôme de Newton[2] :

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

♦ **Preuve.** En développant le produit

$$(x+y)^n = \underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ facteurs.}},$$

on obtient des termes de la forme $x^k y^{n-k}$, $k = 0, 1, 2, \ldots, n$.

Pour former le terme $x^k y^{n-k}$, on commence par choisir k facteurs $(x+y)$, puis on multiplie les « x » correspondant à ces facteurs par les « y » correspondant aux $(n-k)$ autres facteurs. Il s'ensuit qu'il y a exactement $\binom{n}{k}$ termes de la formes $x^k y^{n-k}$, d'où le résultat.

□

♦ **Exemples.**

1. En posant $x = y = 1$, on obtient immédiatement

$$\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n.$$

2. Prouver que, pour $n \geqslant 1$,

$$\sum_{k=0}^{n} k\binom{n}{k} = n \cdot 2^{n-1}.$$

On utilise le fait que si n, $k \geqslant 1$,

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

ce qui permet de conclure :

$$\sum_{k=0}^{n} k\binom{n}{k} = n \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} = n \cdot 2^{n-1}.$$

Une autre méthode consiste à dériver le polynôme

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

et considérer l'égalité pour $x = 1$.

2. Isaac Newton (1646-1727), mathématicien et physicien anglais.

5.2.2. Le triangle de Pascal. L'ensemble des coefficients binomiaux peut être représenté par une construction triangulaire dite triangle de Pascal[3] que l'on obtient comme suit : à l'intersection de la ligne n et du niveau k se situe le coefficient binomial $\binom{n}{k}$:

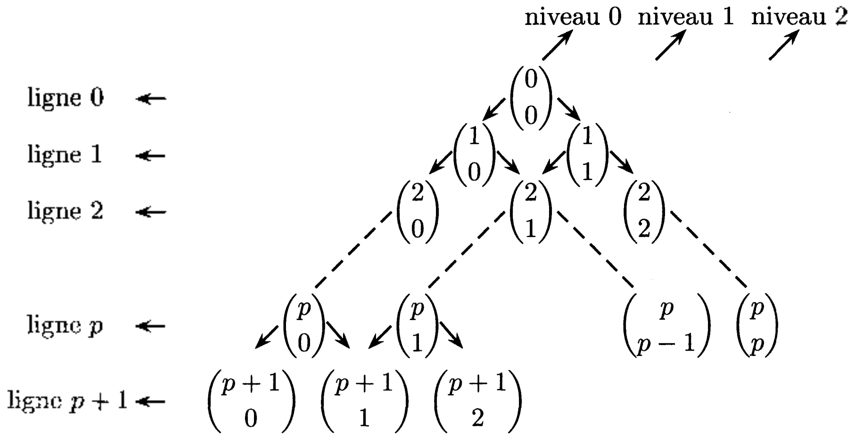


FIG. 5.5.

La relation $\binom{n}{k} = \binom{n}{n-k}$ exprime que le triangle ainsi construit est symétrique par rapport à la ligne verticale passant par $\binom{0}{0}$.

La représentation en triangle est justifiée par la relation suivante :

$$\boxed{\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},} \tag{5.5}$$

pour tous les entiers n et k tels que $n \geqslant k \geqslant 1$, dont on déduit par itération :

$$\boxed{\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{k}{k}.} \tag{5.6}$$

On peut aussi démontrer cette dernière identité sans avoir recours à la première : soit A_i l'ensemble des parties à $k+1$ éléments de $\{1, 2, \ldots, n+1\}$ dont le plus petit élément est i. Il est alors clair que

$$|A_i| = \binom{n+1-i}{k}, \quad i = 1, 2, \ldots, n+1-k.$$

D'un autre côté, $(A_i)_i$ constitue une partition de l'ensemble des parties à $k+1$ éléments de $\{1, 2, \ldots, n+1\}$. Il s'ensuit que

$$\binom{n+1}{k+1} = \sum_{i=1}^{n+1-k} \binom{n+1-i}{k} = \binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{k}{k}.$$

3. Blaise Pascal (1623-1662), mathématicien français.

5.2.3. Identité de Vandermonde[4]**.** *Si $k, m, n \in \mathbb{N}$ sont tels que $k \leqslant \min(m, n)$, alors*

$$\binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \cdots + \binom{n}{k}\binom{m}{0} = \binom{m+n}{k}. \tag{5.7}$$

♦ **Preuve.** En considérant l'identité

$$(1+x)^n(1+x)^m = (1+x)^{m+n},$$

il s'ensuit que le coefficient de x^k dans le développement de $(1+x)^{m+n}$ est égal à

$$\sum_{i=0}^{k}\binom{n}{i}\binom{m}{k-i} = \binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \cdots + \binom{n}{k}\binom{m}{0},$$

d'où le résultat.

□

L'idée de la démonstration précédente a un intérêt en soi, et peut être appliquée pour établir plusieurs identités combinatoires.

♦ **Exemples.**

1. Évaluer la somme suivante dans laquelle m et n sont deux entiers positifs vérifiant $m \leqslant n$ et $n > 1$:

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^m\binom{n}{m}.$$

La dernière somme est le coefficient de x^n dans le polynôme

$$x^n(1-x)^n + x^{n-1}(1-x)^n + \cdots + x^{n-m}(1-x)^n.$$

Or,

$$\begin{aligned} x^n(1-x)^n + x^{n-1}(1-x)^n + \cdots + x^{n-m}(1-x)^n &= x^{n-m}(1-x)^{n-1} - \\ &\quad x^{n+1}(1-x)^{n-1}. \end{aligned}$$

Il s'ensuit que

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^m\binom{n}{m} = \begin{cases} 0 & \text{si } m = n, \\ (-1)^m\binom{n-1}{m} & \text{si } m < n. \end{cases}$$

4. Alexandre Vandermonde (1735-1796), mathématicien français.

2. p et q étant deux entiers positifs, démontrer la relation suivante :

$$\sum_{0\leqslant k\leqslant q} \frac{1}{2^{p+k}}\binom{p+k}{k} + \sum_{0\leqslant k\leqslant p} \frac{1}{2^{q+k}}\binom{q+k}{k} = 2.$$

(Concours général français-1985)

En multipliant par 2^{p+q}, la relation à démontrer s'écrit :

$$\underbrace{\sum_{k=0}^{q} 2^{q-k}\binom{p+k}{p}}_{=S_1} + \underbrace{\sum_{k=0}^{p} 2^{p-k}\binom{q+k}{q}}_{=S_2} = 2^{p+q+1}.$$

L'expression S_1 est le coefficient de x^p dans le polynôme

$$(1+x)^{p+q} + 2(1+x)^{p+q-1} + \cdots + 2^q(1+x)^p.$$

D'un autre côté, si $x \neq 1$,

$$(1+x)^{p+q} + 2(1+x)^{p+q-1} + \cdots + 2^q(1+x)^p = \left[2^{q+1}(1+x)^p - (1+x)^{p+q+1}\right]\frac{1}{1-x},$$

et pour $|x| < 1$,

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots$$

Il s'ensuit donc que S_1 est le coefficient de x^p dans l'expression

$$\left[2^{q+1}(1+x)^p - (1+x)^{p+q+1}\right](1 + x + x^2 + \cdots).$$

Mais le coefficient de x^j dans l'expression $P(x)(1 + x + x^2 + \cdots)$, où $P(x) = \sum_{i=1}^{n} a_i x^i$ est un polynôme, est égal à $(a_0 + a_1 + \cdots + a_j)$, où l'on a posé $a_r = 0$ pour $r > n$. Il s'ensuit que

$$S_1 = 2^{q+1} \times 2^p - \sum_{k=0}^{p} \binom{p+q+1}{k}.$$

De manière analogue on trouve

$$S_2 = 2^{p+1} \times 2^q - \sum_{k=0}^{q} \binom{p+q+1}{k}.$$

On a donc finalement

$$S_1 + S_2 = 2^{p+q+2} - \sum_{k=0}^{p+q+1} \binom{p+q+1}{k} = 2^{p+q+1},$$

ce qu'il fallait démontrer.

5.2.4. Les preuves combinatoires. Dans les exemples qui suivent, la technique utilisée consiste à introduire un certain ensemble que l'on dénombre de deux manières différentes.

♦ **Exemples.**

1. On considère l'identité de Vandermonde :

$$\binom{n}{0}\binom{m}{k}+\binom{n}{1}\binom{m}{k-1}+\cdots+\binom{n}{k}\binom{m}{0}=\binom{m+n}{k},$$

où $k \leqslant \min(m,n)$.

Considérons un ensemble de m balles blanches et de n balles noires. Il y a $\binom{m+n}{k}$ façons de choisir k balles parmi ces $m+n$ balles. Chacun de ces choix correspond au choix de i balles blanches et $k-i$ balles noires. Il s'ensuit que

$$\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}=\binom{m+n}{k},$$

d'où le résultat.

2. Dans le même ordre d'idées, considérons la grille de la figure 5.4. Le nombre de façons d'aller de $(0,0)$ à (m,n) par un chemin où à chaque pas l'une des coordonnées augmente d'une unité est $\binom{m+n}{m}=\binom{m+n}{n}$.

Le produit $\binom{m}{k-i}\binom{n}{i}$, $i=0,1,\ldots,k$, est égal au nombre de façons d'aller de $(0,0)$ à $(n+m-k,k)$ en passant par le point $(m-k+i,k-i)$.

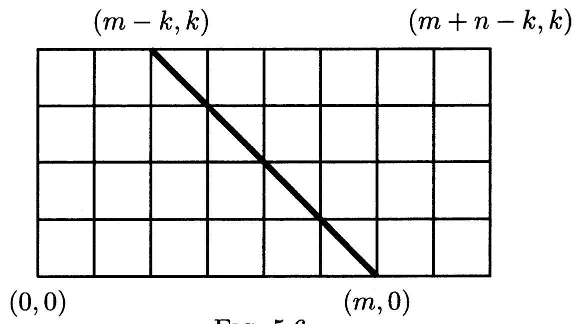


FIG. 5.6.

Comme tout chemin de $(0,0)$ à $(n+m-k,k)$ coupe la droite reliant les points $(m,0)$ et $(m-k,k)$ en un seul point, il s'ensuit que

$$\binom{n}{0}\binom{m}{k}+\binom{n}{1}\binom{m}{k-1}+\cdots+\binom{n}{k}\binom{m}{0}=\binom{m+n}{k},$$

qui est l'identité de Vandermonde.

3. p et q étant deux entiers positifs, démontrer la relation suivante :

$$\sum_{0\leqslant k\leqslant q} \frac{1}{2^{p+k}}\binom{p+k}{k} + \sum_{0\leqslant k\leqslant p} \frac{1}{2^{q+k}}\binom{q+k}{k} = 2.$$

(Concours général français-1985)

On partitionne l'ensemble $\{0,1\}^{p+q+1}$ en deux parties :

- la partie A formée des $(p+q+1)$-uplets possédant au moins $p+1$ fois le nombre 1,

- la partie B formée des $(p+q+1)$-uplets possédant au moins $q+1$ fois le nombre 0.

Si on dénombre l'ensemble A suivant la position du $(p+1)$-ième 1, alors

$$|A| = \sum_{k=0}^{q} 2^{q-k}\binom{p+k}{k}.$$

De même,

$$|B| = \sum_{k=0}^{p} 2^{p-k}\binom{q+k}{k},$$

et il s'ensuit que

$$\sum_{k=0}^{q} 2^{q-k}\binom{p+k}{k} + \sum_{k=0}^{p} 2^{p-k}\binom{q+k}{k} = 2^{p+q+1},$$

ce qui permet de conclure.

On démontre maintenant une formule qui permet de calculer la somme de certains termes d'une suite donnée.

5.2.5. Formule de multisection. *Soit $f(x) = a_0+a_1x+a_2x^2+\cdots$ un polynôme et soient deux entiers $m \in \mathbb{N}^*$ et $r \in \mathbb{N}$. On a*

$$\sum_{k\equiv r\,(\mathrm{mod}\ m)} a_k x^k = \frac{1}{m}\sum_{t=0}^{m-1} \omega^{-rt} f(\omega^t x), \tag{5.8}$$

où $\omega = e^{2i\pi/m}$.

♦ **Preuve.** La preuve de cette formule consiste simplement à comparer les coefficients de x^j, $j = 0, 1, \ldots$, dans les deux membres de la dernière équation.

Le coefficient de x^j dans l'expression

$$\frac{1}{m}\sum_{t=0}^{m-1} \omega^{-rt} f(\omega^t x)$$

est égal à :

$$c_j = \frac{1}{m}\sum_{t=0}^{m-1} a_j \omega^{t(j-r)} = \begin{cases} a_j & \text{si } j \equiv r \pmod{m}, \\ 0 & \text{sinon.} \end{cases}$$

□

À titre d'application, on désire exprimer $\displaystyle\sum_{k\equiv r \pmod{m}} \binom{n}{k}$ sous la forme d'une somme de m termes seulement. On pose alors

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

Il s'ensuit que

$$\begin{aligned} \sum_{k\equiv r \pmod{m}} \binom{n}{k} = \frac{1}{m}\sum_{t=0}^{m-1} \omega^{-rt} f(\omega^t) &= \frac{1}{m}\sum_{t=0}^{m-1} \omega^{-rt}(1+\omega^t)^n \\ &= \frac{1}{m}\sum_{t=0}^{m-1} \left[\sum_{k=0}^{n} \binom{n}{k} \omega^{(k-r)t}\right] \end{aligned}$$

D'un autre côté,

$$\Re e \left[\sum_{k=0}^{n} \binom{n}{k} \omega^{(k-r)t}\right] = 2^n \cos\left((n-2r)\frac{t\pi}{m}\right) \cos^n\left(\frac{t\pi}{m}\right).$$

En effet,

$$\cos^n\left(\frac{t\pi}{m}\right) = \left(\frac{e^{it\pi/m} + e^{-it\pi/m}}{2}\right)^n = \frac{1}{2^n}\sum_{k=0}^{n} \binom{n}{k} e^{i(2k-n)t\pi/m},$$

ce qui donne

$$\begin{aligned} 2^n \cos\left((n-2r)\frac{t\pi}{m}\right) \cos^n\left(\frac{t\pi}{m}\right) &= \Re e \left[\sum_{k=0}^{n} \binom{n}{k} e^{i(2k-n)t\pi/m} e^{i(n-2r)t\pi/m}\right] \\ &= \Re e \left[\sum_{k=0}^{n} \binom{n}{k} \omega^{(k-r)t}\right]. \end{aligned}$$

On en déduit que

$$\sum_{k\equiv r \pmod{m}} \binom{n}{k} = \frac{1}{m}\sum_{t=0}^{m-1} 2^n \cos\left((n-2r)\frac{t\pi}{m}\right) \cos^n\left(\frac{t\pi}{m}\right),$$

ce qui résout le problème.

5.3. Le principe d'inclusion et d'exclusion

5.3.1. Théorème. *(formule du crible ou principe d'inclusion et d'exclusion) Soient $A_1, A_2, \ldots, A_n$ des ensembles finis. On a alors*

$$\begin{aligned}|A_1 \cup A_2 \cup \ldots \cup A_n| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| + \cdots + \\ &\quad (-1)^{n-1} |A_1 \cap A_2 \cap \ldots \cap A_n|.\end{aligned} \tag{5.9}$$

♦ **Preuve.** Le théorème peut être démontré par récurrence sur n. On peut toutefois simplifier la démonstration en introduisant la notion de fonction caractéristique d'une partie A d'un ensemble E, considérée comme application de E dans $\mathbb{Z}$ (mais à valeurs dans $\{0, 1\}$) :

$$\chi_A(x) = \begin{cases} 0 & \text{si } x \notin A, \\ 1 & \text{si } x \in A. \end{cases}$$

En posant $E = A_1 \cup A_2 \cup \ldots \cup A_n$, on a, pour toute partie A de E :

$$|A| = \sum_{x \in E} \chi_A(x).$$

Or,

$$1 - \chi_{(\bigcup_{1 \leqslant i \leqslant n} A_i)} = \chi_{(\overline{\bigcup_{1 \leqslant i \leqslant n} A_i})} = \chi_{\bigcap_{1 \leqslant i \leqslant n} \overline{A_i}} = \prod_{1 \leqslant i \leqslant n} \chi_{\overline{A_i}} = \prod_{1 \leqslant i \leqslant n} (1 - \chi_{A_i}),$$

où $\overline{A}$ désigne le complémentaire de la partie A dans E.

Comme

$$\prod_{1 \leqslant i \leqslant n} (1 - \chi_{A_i}) = 1 - \sum_{i=1}^{n} \chi_{A_i} + \sum_{1 \leqslant i < j \leqslant n} \chi_{A_i} \cdot \chi_{A_j} - \cdots + (-1)^n \prod_{i=1}^{n} \chi_{A_i},$$

on obtient

$$\chi_{(\bigcup_{1 \leqslant i \leqslant n} A_i)} = \sum_{i=1}^{n} \chi_{A_i} - \sum_{1 \leqslant i < j \leqslant n} \chi_{A_i \cap A_j} + \cdots + (-1)^{n-1} \chi_{\bigcap_{1 \leqslant i \leqslant n} A_i},$$

ce qui donne, en faisant la somme des valeurs de ces fonctions en tout point x de E,

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| + \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \ldots \cap A_n|.$$

□

♦ **Exemples.**

1. Une permutation σ de l'ensemble $\{1, 2, \dots, n\}$ est dite être un dérangement si elle ne possède aucun point fixe, en ce sens que, pour tout $i \in \{1, 2, \dots, n\}$, $\sigma(i) \neq i$. Trouver le nombre de dérangements de $\{1, 2, \dots, n\}$.

Soit A_i, $i = 1, 2, \dots, n$, l'ensemble des permutations σ de $\{1, 2, \dots, n\}$ telles que $\sigma(i) = i$. On a alors

$$|A_1 \cup A_2 \cup \dots \cup A_n| = n(n-1)! - \binom{n}{2}(n-2)! + \cdots + (-1)^{n-1}.$$

Ainsi, le nombre de dérangements de $\{1, 2, \dots, n\}$ vaut :

$$\sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^n}{n!}\right].$$

2. Soit $S = \{z \in \mathbb{C} \mid |z| = 1\}$. Pour toute application $f : S \longrightarrow S$ et $k \in \mathbb{N}$, on désigne par $f^k : S \longrightarrow S$ l'itérée k-ième de f. On dit qu'un élément $\omega \in S$ est un point périodique de période n ($n \in \mathbb{N}$) si

$$f^i(\omega) \neq \omega \quad \forall i = 1, 2, \dots, n-1, \text{ et } \quad f^n(\omega) = \omega.$$

Si f est définie par $f(z) = z^m$ ($m \in \mathbb{N}$), trouver le nombre des points périodiques de f de période 1989.

(Olympiades chinoises-1989)

Soit $\mathcal{E}_n$ l'ensemble des $z \in S$ tels que $f^n(z) = z$. Dans le cas de la fonction $f(z) = z^m$ ($m \in \mathbb{N}$), l'ensemble $\mathcal{E}_n$ consiste en les racines $(m^n - 1)$-ièmes de l'unité, d'où $|\mathcal{E}_n| = m^n - 1$.

Si $z \in \mathcal{E}_n$ est un point de période k, alors k divise n : en effet, si $n = qk + r$ avec $0 < r < k$, alors $z = f^n(z) = f^r(z)$, ce qui est absurde.

Puisque $1989 = 3^2 \times 13 \times 17$, il s'ensuit que les points périodiques de période 1989 sont ceux appartenant à $\mathcal{E}_{1989}$ mais à aucun des ensembles $\mathcal{E}_{1989/3}$, $\mathcal{E}_{1989/13}$ et $\mathcal{E}_{1989/17}$. On pense alors au principe d'inclusion et d'exclusion, mais que vaut $|\mathcal{E}_s \cap \mathcal{E}_t|$?

Montrons que $\mathcal{E}_s \cap \mathcal{E}_t = \mathcal{E}_{(s,t)}$: d'une part, comme (s,t) divise s, on a $\mathcal{E}_{(s,t)} \subseteq \mathcal{E}_s$, et de même $\mathcal{E}_{(s,t)} \subseteq \mathcal{E}_t$, d'où $\mathcal{E}_{(s,t)} \subseteq \mathcal{E}_s \cap \mathcal{E}_t$. Sinon, écrivons $s = qt + r$ avec $0 < r < t$; si $z \in \mathcal{E}_s \cap \mathcal{E}_t$, alors $z = f^s(z) = f^r(z)$, ce qui montre que $z \in \mathcal{E}_t \cap \mathcal{E}_r$. Il s'ensuit (algorithme d'Euclide) que $(\mathcal{E}_s \cap \mathcal{E}_t) \subseteq (\mathcal{E}_t \cap \mathcal{E}_r) \subseteq \ldots \subseteq \mathcal{E}_{(s,t)}$.

Le principe d'inclusion et d'exclusion permet finalement de trouver le nombre des points périodiques de période 1989 :

$$m^{1989} - m^{663} - m^{153} - m^{117} + m^{51} + m^{39} + m^9 - m^3.$$

5.3.2. L'indicatrice d'Euler. Pour $n \geqslant 1$, on rappelle que l'indicatrice d'Euler de n, notée $\varphi(n)$, est le nombre des entiers au plus égaux à n et premiers avec n. Le principe d'inclusion et d'exclusion nous permettra de retrouver la formule explicite de $\varphi(n)$.

Si la décomposition de n en facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, appelons A_i l'ensemble des multiples de p_i qui sont $\leqslant n$. On a donc :

$$|A_1 \cup A_2 \cup \ldots \cup A_k| = \sum_{i=1}^{k} \frac{n}{p_i} - \sum_{1 \leqslant i < j \leqslant k} \frac{n}{p_i p_j} + \cdots + (-1)^{k-1} \frac{n}{p_1 p_2 \cdots p_k}.$$

Il s'ensuit que

$$\varphi(n) = n\Big[1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{1 \leqslant i < j \leqslant k} \frac{1}{p_i p_j} + \cdots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k}\Big] = n \prod_{i=1}^{k} \Big(1 - \frac{1}{p_i}\Big).$$

5.3.3. Les applications surjectives. On se propose de déterminer le nombre $F(n,m)$, $(n, m \in \mathbb{N}^*)$ des applications surjectives de $\{1, 2, \ldots, n\}$ vers $\{1, 2, \ldots, m\}$. Soit E l'ensemble des applications de $\{1, 2, \ldots, n\}$ dans $\{1, 2, \ldots, m\}$, et F le sous-ensemble de E constitué par les applications surjectives. Soit maintenant B_i l'ensemble des applications $f \in E$ qui n'atteignent pas i, i.e. $i \notin f(\{1, 2, \ldots, n\})$. On a alors $F = \overline{B_1} \cap \overline{B_2} \cap \ldots \cap \overline{B_m}$, et le principe d'inclusion et d'exclusion permet alors d'écrire :

$$|F| = m^n - \binom{m}{1}(m-1)^n + \binom{m}{2}(m-2)^n - \cdots + (-1)^m \binom{m}{m}(m-m)^m.$$

5.3.4. Le problème des ménages. Ce problème a été posé, résolu et popularisé par Édouard Lucas[5]. En voici l'énoncé : quel est le nombre de manières d'asseoir n ménages (= couples mariés mari-épouse) autour d'une table ronde de $2n$ places, les maris et épouses étant alternés de telle sorte qu'aucune épouse ne soit à côté de son mari ?

Ce problème se résout par application du principe d'inclusion et d'exclusion, mais on aura besoin du lemme suivant :

Lemme de Kaplansky[6]. *Les nombres $1, 2, \ldots, m$ $(m \geqslant 3)$ sont placés autour d'un cercle. Pour $1 \leqslant k \leqslant \lfloor m/2 \rfloor$, soit $\alpha(k)$ le nombre de sous-ensembles à k éléments de $\{1, 2, \ldots, m\}$ ne contenant pas deux éléments adjacents sur le cercle. On a alors :*

$$\alpha(k) = \frac{m}{k}\binom{m-k-1}{k-1}, \quad 1 \leqslant k \leqslant \lfloor m/2 \rfloor.$$

En effet, soit α_i le nombre de tels sous-ensembles qui contiennent i, $i = 1, 2, \ldots, m$. On a alors, par raison de symétrie, $\alpha_1 = \alpha_2 = \cdots = \alpha_m$.

Si maintenant A est un tel sous-ensemble contenant 1, alors $2, m \notin A$, et les $k-1$ autres éléments de A doivent être choisis dans l'ensemble $\{3, \ldots, m-1\}$ de telle sorte que les $k-1$ éléments choisis ne soient pas adjacents (les nombres $3, 4, \ldots, m-1$ étant placés sur une même ligne). On a donc (cf. l'exemple 2 du

5. Édouard Lucas (1842-1891), mathématicien français.

6. Irving Kaplansky (1917-2006), mathématicien américain d'origine polonaise.

paragraphe 5.1.3)

$$\alpha_1 = \binom{(m-3)-(k-1)+1}{k-1} = \binom{m-k-1}{k-1}.$$

Comme $\sum_{i=1}^m \alpha_i = k\alpha(k)$ (tout sous-ensemble à k éléments est compté k fois dans la somme $\sum_{i=1}^m \alpha_i$), il s'ensuit que

$$\alpha(k) = \frac{1}{k}\sum_{i=1}^m \alpha_i = \frac{m}{k}\binom{m-k-1}{k-1}.$$

□

Supposons les épouses déjà placées (2(n!) possibilités), et numérotons-les dans le sens trigonométrique, à partir de l'une d'entre elles : $E_1, E_2, \ldots, E_n$. Affectons à chaque siège libre le numéro de l'épouse assise à droite : $S_1, S_2, \ldots, S_n$.

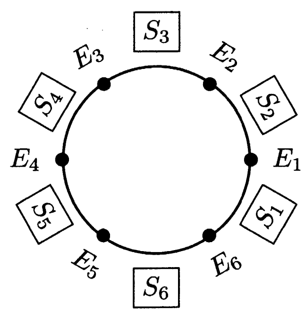


FIG. 5.7.

Le problème équivaut à compter le nombre $\mu(n)$ des affectations de sièges convenables aux maris. Le nombre total de placements des ménages est alors $2(n!)\mu(n)$. Il s'agit donc de calculer le nombre de permutations σ de $\{1, 2, \ldots, n\}$ telles que : $\sigma(i) \neq i, i+1$ pour $i \in \{1, 2, \ldots, n\}$, avec la convention $n+1 = 1$. Posons donc

$$A_{2i} = \{\sigma \mid \sigma(i) = i+1\}, \quad i \in \{1, 2, \ldots, n\},$$
$$A_{2i-1} = \{\sigma \mid \sigma(i) = i\}, \quad i \in \{1, 2, \ldots, n\}.$$

On a alors, en appliquant le principe d'inclusion et d'exclusion,

$$\mu(n) = |\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_{2n}}| = n! + \sum_{\beta \subseteq \{1,2,\ldots,2n\},\ \beta \neq \varnothing} (-1)^{|\beta|}|A_\beta|,$$

où l'on a posé par définition $A_\beta = \cap_{i\in\beta} A_i$. Il est important de noter à ce stade que $|A_\beta| = 0$ si β contient deux éléments consécutifs (les nombres $1, 2, \ldots, 2n$ étant placés autour d'un cercle). On applique alors le lemme de Kaplansky :

$$\begin{aligned}\mu(n) &= n! + \sum_{k=1}^n (-1)^k \frac{2n}{k}\binom{2n-k-1}{k-1}(n-k)! \\ &= \sum_{k=0}^n (-1)^k \frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!.\end{aligned}$$

5.4. Notions sur les graphes

Un graphe $\mathcal{G}$ est formé de deux ensembles : un ensemble fini non vide X, appelé ensemble des sommets de $\mathcal{G}$, et un ensemble A de paires de sommets, appelé ensemble des arêtes de $\mathcal{G}$. Ainsi, A est un sous-ensemble de l'ensemble des parties de X ayant deux éléments. On écrit souvent $\mathcal{G} = \big(X(\mathcal{G}), A(\mathcal{G})\big)$.

Dans la pratique, un graphe se représente par une figure plane contenant des traits reliant entre eux un ensemble fini de points. Le nombre d'arêtes issues d'un point x est appelé le degré de x, couramment désigné par $d(x)$. Un sous-graphe $\mathcal{H}$ de $\mathcal{G}$ est un graphe tel que $X(\mathcal{H}) \subseteq X(\mathcal{G})$ et $A(\mathcal{H}) \subseteq A(\mathcal{G})$.

On appelle graphe complet d'ordre $n \geqslant 2$ le graphe $\mathcal{G}_n$ de n sommets, ayant pour arêtes tous les segments déterminés par ces points. Ainsi, $\mathcal{G}_n$ a $\binom{n}{2}$ arêtes.

5.4.1. Proposition. *(lemme des poignées de mains) Soit $\mathcal{G} = (X, A)$ un graphe quelconque, alors*

$$\sum_{x \in X} d(x) = 2|A|. \tag{5.10}$$

En effet, dans la somme de gauche, chaque arête est comptée exactement deux fois, puisqu'elle a deux extrémités.

On en déduit en particulier que le nombre de sommets de degré impair dans $\mathcal{G}$ est un entier pair.

5.4.2. Les arbres. Dans un graphe $\mathcal{G} = (X, A)$, une chaîne est une suite finie de sommets, $x_0, x_1, \ldots, x_m$, telle que, pour tout $i \in \{0, 1, \ldots, m-1\}$, $\{x_i, x_{i+1}\} \in A$. L'entier m s'appelle la longueur de la chaîne en question. Lorsque $x_0 = x_m$, on dit que la chaîne est fermée et on l'appelle un cycle.

Un graphe $\mathcal{G}$ est dit connexe si, pour tout $(x, y) \in X^2$, il existe une chaîne reliant x à y. On est maintenant en mesure de définir ce qu'est un arbre : un arbre est un graphe $\mathcal{G} = (X, A)$ connexe, sans cycle, comportant au moins deux sommets.

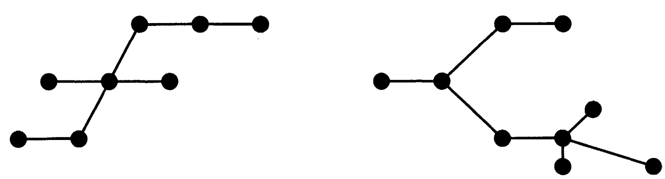


FIG. 5.8.

Dans l'arbre $\mathcal{G} = (X, A)$, le sommet x est dit pendant si $d(x) = 1$ (un arbre contient forcément au moins deux tels sommets).

Proposition. *Soit $\mathcal{G} = (X, A)$ un arbre; on a alors*

$$|A| = |X| - 1. \tag{5.11}$$

♦ **Preuve.** On prouve le résultat par récurrence sur $|X| = n$. Si $n = 2$, alors $|X| = 2$ et $|A| = 1$ et le résultat est immédiat.

Supposons que pour tout arbre $\mathcal{G} = (X, A)$ à $k \geqslant 2$ sommets, on ait $|A| = k-1$. Soit alors un arbre $\mathcal{H} = (X', A')$ à $k+1$ sommets, et soit x un sommet pendant de $\mathcal{H}$. Il est alors immédiat que $\mathcal{H} \setminus \{x\}$ est un arbre ayant k sommets. En appliquant l'hypothèse de récurrence à cet arbre, il apparaît que $\mathcal{H}$ possède $(k-1)+1 = k$ arêtes.

□

♦ **Exemples.**

1. Si $\mathcal{G} = (X, A)$ est un graphe connexe ayant éventuellement des cycles, alors $|A| \geqslant |X| - 1$. Si par contre $\mathcal{G} = (X, A)$ est un graphe sans cycles non nécessairement connexe (une forêt), alors $|A| \leqslant |X| - 1$.

2. Quelles sont les valeurs de l'entier $n > 9$ pour lesquelles il est possible pour n enfants de se partager équitablement 9 barres de chocolat sans avoir à couper une barre en plus de deux morceaux ?

On considère un graphe à n sommets, où les sommets représentent les n enfants, et on dessine une arête entre deux sommets si les enfants correspondant à ces sommets se partagent une barre de chocolat. Si ce graphe contenait un cycle passant par k sommets, alors les k enfants en question auraient bénéficié au total de k barres de chocolat au minimum. Or, ceci ne peut se réaliser car $n > 9$ et le partage est supposé équitable. Il s'ensuit que le graphe étudié est une forêt. Comme le partage est équitable, les arbres constituant cette forêt doivent contenir le même nombre d'arêtes et de sommets. Si t désigne le nombre d'arbres dans cette forêt, alors t doit diviser le nombre total d'arêtes dans le graphe, à savoir 9. Si $t = 1$, l'arbre obtenu a 9 arêtes et 10 sommets. Si $t = 3$, chaque arbre a 3 arêtes et 4 sommets. Si $t = 9$, chaque arbre a une seule arête et 2 sommets. Ceci conduit aux valeurs $n = 10, 12$ et 18, lesquelles conviennent parfaitement comme on peut facilement vérifier.

5.4.3. Cycles euleriens. Un cycle eulerien (resp. une chaîne eulerienne) dans un graphe $\mathcal{G}$ est un cycle (resp. une chaîne) contenant chaque arête de $\mathcal{G}$ une et une seule fois.

Un graphe pourra donc être parcouru sans lever le crayon et en ne passant qu'une seule fois sur chaque trait s'il admet une chaîne eulerienne. On aimerait bien caractériser de telles graphes.

Si $\mathcal{G}$ est un graphe admettant un cycle eulerien $\mathcal{C}$, et si x est un sommet de $\mathcal{G}$, alors $\mathcal{C}$ arrive à x autant de fois qu'il en part. Il s'ensuit que tout sommet de $\mathcal{G}$ est de degré pair.

D'un autre côté, si tous les sommets d'un graphe $\mathcal{G}$ sont de degré pair, peut-on affirmer qu'il existe un cycle eulerien ? Il faut déjà clairement que le graphe $\mathcal{G}$ soit connexe. Euler a démontré en 1766 le théorème suivant :

Théorème. *Un graphe connexe $\mathcal{G} = (X, A)$ est eulerien si et seulement si $d(x)$ est pair pour tout sommet $x \in X$.*

♦ **Preuve.** Considérons un graphe connexe $\mathcal{G} = (X, A)$ où tous les sommets sont de degré pair. Montrons que $\mathcal{G}$ est réunion de cycles disjoints. Prenons $x_0 \in X$ et choisissons, en partant de x_0, aussi longtemps que possible, des arêtes non encore parcourues de sorte à former une chaîne. Les sommets étant tous de degré pair, cette chaîne est en fait un cycle $\mathcal{C}_1$ qui se referme en x_0. Si, en supprimant les arêtes de ce cycle, il reste encore des arêtes, alors on choisit un sommet x_1 par lequel passe $\mathcal{C}_1$ et tel que dans le graphe partiel $\mathcal{G} \setminus \mathcal{C}_1$ on ait $d(x_1) > 0$. Ceci est possible car $\mathcal{G}$ est connexe. Dans la composante connexe de $\mathcal{G} \setminus \mathcal{C}_1$ contenant x_1, construisons un nouveau cycle $\mathcal{C}_2$ de x_1 à x_1. Comme le nombre d'arêtes dans $\mathcal{G}$ est fini, ce procédé s'arrêtera lorsqu'on aura obtenu un ensemble de cycles disjoints en arêtes dont la réunion est $\mathcal{G}$ tout entier. Or, on peut rallonger $\mathcal{C}_1$ en insérant en x_1 le cycle $\mathcal{C}_2$ et ainsi de suite jusqu'à aboutir au cycle eulerien recherché.

□

De manière analogue, un graphe $\mathcal{G} = (X, A)$ admet une chaîne eulerienne si et seulement si il a zéro ou deux sommets impairs. Dans ce dernier cas, la chaîne en question aura les deux sommets impairs comme extrémités. La figure planaire représentée ci-dessous peut donc être tracée sans lever le crayon et en ne passant qu'une seule fois sur chaque trait.

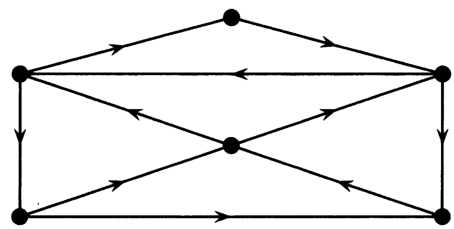


FIG. 5.9.

5.4.4. Cycles hamiltoniens. Dans un graphe $\mathcal{G}$, un cycle est dit hamiltonien s'il passe une et une seule fois par chaque sommet de $\mathcal{G}$.

Il n'y a pas de bonne caractérisation des graphes admettant des cycles hamiltoniens. Par contre, il est intéressant de se demander si un graphe donné est la réunion de cycles hamiltoniens disjoints en arêtes. En particulier, le graphe complet $\mathcal{G}_n$ peut-il être décomposé en cycles hamiltoniens disjoints ? On peut déjà vérifier que $\mathcal{G}_5$ peut être décomposé en deux tels cycles. Qu'en est-il de $\mathcal{G}_4$?

Théorème. *$\mathcal{G}_n$ est réunion de cycles hamiltoniens disjoints si et seulement si n est impair.*

♦ **Preuve.** Le graphe $\mathcal{G}_n$ possède $\binom{n}{2} = \frac{n(n-1)}{2}$ arêtes. Tout cycle hamiltonien en utilise n ; on a donc besoin de $(n-1)/2$ cycles. En particulier, n doit être impair.

Si $n = 2m + 1$ est impair, construisons m cycles hamiltoniens disjoints de la façon suivante : on place $2m$ des sommets du graphe $\mathcal{G}_{2m+1}$ autour d'un cercle de manière à avoir un polygone régulier à $2m$ sommets et plaçons le dernier sommet au centre de ce polygone. Numérotons ensuite, dans le sens trigonométrique les $2m$ sommets en question : $1, 2, \ldots, 2m$.

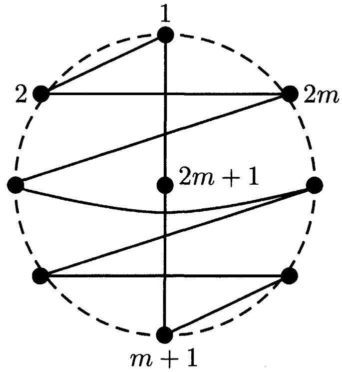


FIG. 5.10.

Le cycle représenté dans la figure ci-dessous est hamiltonien. Celui-ci donne lieu par des rotations d'angles $k\pi/m$, $k = 0, 1, \ldots, m-1$, à m cycles hamiltoniens disjoints.

□

5.5. Les problèmes de type Ramsey

Dans ce paragraphe, on va appliquer le principe des tiroirs à l'étude d'une classe de problèmes. Cette étude nous mènera à l'introduction d'une suite de nombres dont le calcul et l'estimation demeurent actuellement encore parmi les problèmes les plus fascinants de l'analyse combinatoire.

5.5.1. Les nombres de Ramsey bicolores. Étant donné un graphe complet $\mathcal{G}_n$, on appelle k-clique tout sous-graphe de $\mathcal{G}_n$ à k sommets. Le problème que l'on cherche à résoudre est le suivant : si p et q sont deux entiers $\geqslant 2$, existe-t-il un plus petit entier $n = R(p, q)$ tel que, pour toute coloration de $\mathcal{G}_n$ à l'aide de deux couleurs : rouge et vert (une couleur pour chaque arête), il y ait toujours au moins une p-clique rouge ou une q-clique verte ?

Ce problème a été résolu par Ramsey[7] en 1928 qui a prouvé l'existence des nombres $R(p, q)$ pour tous entiers $p, q \geqslant 2$. Les nombres $R(p, q)$ sont appelés les nombres de Ramsey bicolores, et ils vérifient, compte tenu de leur définition, l'égalité : $R(p, q) = R(q, p)$. On a aussi, pour tout $p \geqslant 2$, $R(p, 2) = p$.

♣ **Calcul de R(3, 3).** Il s'agit de construire un graphe ayant le plus grand nombre de sommets qui, pour une coloration convenable, ne contienne aucune 3-clique rouge, ni de 3-clique verte.

7. Frank Ramsey (1903-1930), philosophe et mathématicien anglais.

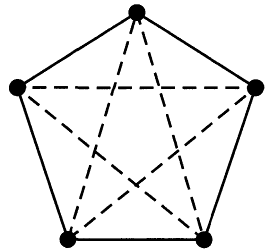


FIG. 5.11.

La figure ci-dessus donne une coloration de $\mathcal{G}_5$ sans aucun triangle (3-clique) monochromatique.

D'un autre côté, soient A, B, C, D, E et F les sommets d'un graphe complet $\mathcal{G}_6$.

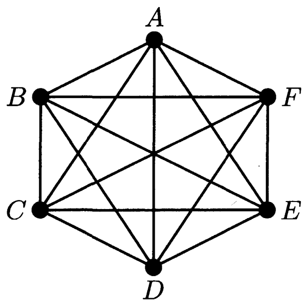


FIG. 5.12.

D'après le principe des tiroirs, une des deux couleurs, rouge par exemple, est utilisée pour colorier trois au moins des segments AB, AC, AD, AE et AF. Sans perte de généralité, on peut supposer les segments AB, AC et AD coloriés en rouge. Considérons maintenant les trois segments BC, CD et BD. Si un de ces segments est colorié en rouge, par exemple BC, le triangle ABC est alors rouge. Si par contre les trois segments sont coloriés en vert, alors le triangle BCD est vert.

Il s'ensuit que

$$\boxed{R(3,3) = 6.} \tag{5.12}$$

Ce résultat (en fait $R(3,3) \leqslant 6$ suffirait) permet de résoudre la question suivante : dans une réunion de six personnes, il y a au moins trois personnes se connaissant mutuellement, ou trois personnes complètement étrangères l'une à l'autre.

♣ **Quelques estimations.** On ne connaît actuellement, malgré la puissance de calcul actuelle des ordinateurs, que 7 nombres de Ramsey bicolores lorsque p et q sont $\geqslant 3$: $R(3,3) = 6$, $R(3,4) = 9$, $R(3,5) = 14$, $R(3,6) = 18$, $R(3,7) = 23$, $R(4,4) = 18$ et dernièrement $R(4,5) = 25$. Cependant, plusieurs estimations de ces nombres ont été trouvées, dont la majoration suivante due aux deux mathématiciens Erdös[8] et Szekeres[9] :

Théorème. *Pour tous les entiers $p, q \geqslant 2$,*

$$R(p,q) \leqslant R(p-1,q) + R(p,q-1). \tag{5.13}$$

♦ **Preuve.** En effet, si on pose $n = R(p-1,q) + R(p,q-1)$, il nous suffirait de prouver que, pour toute coloration de $\mathcal{G}_n$ en rouge et vert, il existe au moins une p-clique verte ou une q-clique rouge.

Si on fixe un sommet x de $\mathcal{G}_n$, alors celui-ci est l'extrémité de $n-1 = R(p-1,q) + R(p,q-1) - 1$ arêtes dans $\mathcal{G}_n$. Il y a donc au moins $R(p-1,q)$ arêtes vertes ou $R(p,q-1)$ arêtes rouges parmi ces $n-1$ arêtes, et l'on peut supposer, par raison de symétrie, que l'on ait la première possibilité.

Si A désigne l'ensemble des sommets de $\mathcal{G}_n$, autres que x, qui sont l'extrémité de l'une de ces $R(p-1,q)$ arêtes vertes, alors $|A| = R(p-1,q)$. Par définition des nombres de Ramsey bicolores, on en déduit que le graphe complet engendré par les sommets appartenant à A contient soit une $(p-1)$-clique verte, soit une q-clique rouge.

Il s'ensuit que le graphe complet engendré par les sommets de $A \cup \{x\}$ contient au moins une p-clique verte ou une q-clique rouge.

□

Corollaire. *On a, pour tous les entiers $p, q \geqslant 2$,*

$$R(p,q) \leqslant \binom{p+q-2}{p-1}. \tag{5.14}$$

♦ **Preuve.** On raisonne par récurrence sur $p+q$: on sait que $\forall p \geqslant 2,\ R(p,2) = R(2,p) = p = \binom{p}{p-1}$. Supposons donc l'inégalité vraie pour tous $p, q \geqslant 3$ tels que $p+q = n$. Si maintenant p et q sont deux entiers tels que $p+q = n+1$, alors

$$R(p,q) \leqslant R(p-1,q) + R(p,q-1) \leqslant \binom{p+q-3}{p-2} + \binom{p+q-3}{p-1} = \binom{p+q-2}{p-1}.$$

□

Théorème. *Pour tous les entiers $p, q \geqslant 2$ tels que $R(p-1,q)$ et $R(p,q-1)$ soient pairs,*

$$R(p,q) \leqslant R(p-1,q) + R(p,q-1) - 1. \tag{5.15}$$

♦ **Preuve.** On pose $n = R(p-1,q) + R(p,q-1) - 1$, et on fixe un sommet x de $\mathcal{G}_n$. Le sommet x est alors l'extrémité de $n-1$ arêtes dans $\mathcal{G}_n$. Si $R(p-1,q)$ au

8. Pal Erdös (1913-1996), mathématicien hongrois.

9. George Szekeres (1911-2005), mathématicien hongrois.

moins de ces arêtes sont vertes, ou $R(p, q-1)$ au moins des arêtes sont rouges, le problème est résolu comme vu dans la démonstration précédente. Si par contre, il y a exactement $R(p-1, q) - 1$ arêtes vertes et $R(p, q-1) - 1$ arêtes rouges et ceci pour tous les sommets x de $\mathcal{G}_n$, alors $\mathcal{G}_n$ contient au total

$$\frac{n}{2}[R(p-1, q) - 1]$$

arêtes vertes, ce qui est impossible car ce nombre n'est pas un entier.

□

♣ **Calcul de R(3, 4).** On sait déjà que $R(2,4) = 4$ et que $R(3,3) = 6$. On a donc, d'après le théorème qui vient d'être démontré,

$$R(3,4) \leqslant 4 + 6 - 1 = 9.$$

D'un autre côté, la figure ci-dessous montre une coloration de $\mathcal{G}_8$ sans aucune 3-clique rouge, ni de 4-clique verte :

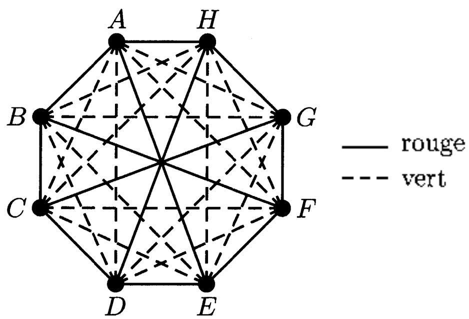


FIG. 5.13.

On prouve de façon analogue que $R(4,4) = 18$ et que $R(3,5) = 14$. Cependant, si on essaie de majorer $R(3,6)$ en utilisant cette méthode

$$R(3,6) \leqslant R(2,6) + R(3,5) = 20,$$

on s'aperçoit que la majoration obtenue n'est pas une égalité ($R(3,6) = 18$).

5.5.2. Les nombres de Ramsey multicolores. Dans la définition des nombres de Ramsey donnée jusqu'à présent, on avait supposé que deux couleurs seulement étaient utilisées pour colorier les arêtes du graphe complet $\mathcal{G}_n$; d'où le qualitatif « bicolore ».

De manière naturelle, on peut définir, pour $k \geqslant 3$, le nombre de Ramsey multicolore $R(p_1, p_2, \ldots, p_k)$ comme étant le plus petit entier positif n tel que, pour toute coloration du graphe complet $\mathcal{G}_n$ à l'aide de k couleurs : couleur 1, couleur 2, ..., couleur k, il existe au moins une couleur i et une p_i-clique colorée à l'aide de la couleur i.

♣ **Calcul de R(3, 3, 3).** On commence par prouver que $R(3,3,3) \leqslant 17$, majoration qui a fait l'objet de l'exercice suivant posé aux olympiades internationales de 1964 : parmi 17 scientifiques chacun est en correspondance avec tous les autres. Dans leurs échanges de lettres ils ne traitent que trois sujets et on suppose que deux scientifiques ne traitent qu'un seul sujet dans leurs correspondances mutuelles. Démontrer qu'il y a au moins trois scientifiques qui traitent entre eux un seul et même sujet.

On représente les 17 scientifiques par les 17 sommets d'un graphe complet dont on colorie les arêtes à l'aide de trois couleurs : rouge, vert et bleu, chaque couleur représentant un des trois sujets. D'après les données de l'énoncé, chaque arête est coloriée par une seule couleur.

On fixe maintenant un sommet A du graphe précédemment construit, et on considère les 16 arêtes issues de A. Il y a au moins six parmi ces arêtes qui sont coloriées par la même couleur, rouge par exemple. Désignons alors par B, C, D, E, F et G les six autres extrémités de ces arêtes, et distinguons deux cas :

- le sous-graphe complet de $\mathcal{G}_{17}$ ayant B, C, D, E, F et G comme sommets est coloré en vert et bleu uniquement. Ce sous-graphe contient alors un triangle monochromatique ($R(3,3) = 6$) ;

- il y a une arête rouge, BC par exemple, parmi les arêtes reliant les points B, C, D, E, F et G entre eux. Le triangle ABC est alors un triangle rouge.

On a donc finalement $R(3,3,3) \leqslant 17$, et il s'agit maintenant de trouver une coloration de $\mathcal{G}_{16}$ à l'aide des trois couleurs : rouge, vert et bleu, sans aucun triangle (3-clique) monochromatique pour établir que $R(3,3,3) = 17$.

Affectons à chaque sommet de $\mathcal{G}_{16}$ la valeur d'un élément de l'ensemble $(\mathbb{Z}/2\mathbb{Z})^4$, deux sommets distincts ayant des affectations différentes. Il s'agit maintenant de trouver une partition $\{A_1, A_2, A_3\}$ de $(\mathbb{Z}/2\mathbb{Z})^4 \setminus \{0\}$ telle qu'aucune des parties A_i, $i = 1,2,3$, ne contienne trois éléments de la forme $x, y, x + y$. Une telle partition est donnée ci-dessous :

$$\begin{aligned}
A_1 &= \{(\bar{1},\bar{0},\bar{0},\bar{0}),\ (\bar{0},\bar{1},\bar{0},\bar{0}),\ (\bar{0},\bar{0},\bar{1},\bar{0}),\ (\bar{0},\bar{0},\bar{0},\bar{1}),\ (\bar{1},\bar{1},\bar{1},\bar{1})\},\\
A_2 &= \{(\bar{1},\bar{1},\bar{0},\bar{0}),\ (\bar{1},\bar{0},\bar{1},\bar{0}),\ (\bar{0},\bar{0},\bar{1},\bar{1}),\ (\bar{1},\bar{1},\bar{1},\bar{0}),\ (\bar{0},\bar{1},\bar{1},\bar{1})\},\\
A_3 &= \{(\bar{0},\bar{1},\bar{1},\bar{0}),\ (\bar{1},\bar{0},\bar{0},\bar{1}),\ (\bar{0},\bar{1},\bar{0},\bar{1}),\ (\bar{1},\bar{0},\bar{1},\bar{1}),\ (\bar{1},\bar{1},\bar{0},\bar{1})\}.
\end{aligned}$$

On colorie les arêtes de $\mathcal{G}_{16}$ de la façon qui suit : l'arête (x, y), $x, y \in (\mathbb{Z}/2\mathbb{Z})^4$, est coloriée en rouge, vert ou bleu suivant que $x + y$ est dans A_1, A_2 ou A_3. La coloration obtenue ne contient aucun triangle monochromatique, car si le triangle (x, y, z) était monochromatique, alors $x + y$, $y + z$ et $z + x$ appartiendraient à un même A_i alors que $(x+y)+(y+z) = (x+z)$, ce qui est impossible, d'où le résultat.

♣ **Une majoration de $\mathbf{R(3,3\ldots,3)}$.** Soit k un entier $\geqslant 3$. On pose

$$R_k = R(\underbrace{3,3,\ldots,3}_{k \text{ fois.}}).$$

Théorème. *Pour tout entier $k \geqslant 2$,*

$$R_k \leqslant \lfloor k!e \rfloor + 1. \tag{5.16}$$

♦ **Preuve.** On commence d'abord par prouver l'inégalité, valable pour tout $k \geqslant 3$,

$$R_k \leqslant k(R_{k-1} - 1) + 2.$$

En effet, on pose $n = k(R_{k-1} - 1) + 2$, et on fixe un sommet x dans le graphe complet $\mathcal{G}_n$. Celui-ci est l'extrémité de $n - 1 = k(R_{k-1} - 1) + 1$ arêtes dans $\mathcal{G}_n$. Si le graphe $\mathcal{G}_n$ est coloré à l'aide de k couleurs : couleur 1, couleur 2, ..., couleur k, il existe au moins une couleur i qui est utilisée pour colorier au moins $(R_{k-1}-1)+1 = R_{k-1}$ de ces $n-1$ arêtes. Si A désigne l'ensemble des R_{k-1} extrémités de ces arêtes, autres que x, alors on a l'une des deux possibilités suivantes :

- le sous-graphe complet engendré par A contient une arête de couleur i, auquel cas correspond un triangle de couleur i.

- le sous-graphe engendré par A ne contient aucune arête de couleur i. Il contient donc un triangle monochromatique compte tenu de la définition de R_{k-1}.

Dans tous les cas, $\mathcal{G}_n$ contient un triangle monochromatique, et on a donc bien :

$$\forall k \geqslant 3, \quad R_k \leqslant k(R_{k-1} - 1) + 2,$$

soit encore, pour $k \geqslant 3$ fixé,

$$\frac{R_p - 1}{p!} \leqslant \frac{R_{p-1} - 1}{(p-1)!} + \frac{1}{p!}, \quad p = 3, 4, \ldots, k.$$

On obtient donc, en sommant les $k-2$ dernières inégalités et en tenant compte de $R_2 = R(3,3) = 6$

$$\frac{R_k - 1}{k!} \leqslant 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{k!}.$$

Mais on sait déjà que e est la limite commune des deux suites adjacentes :

$$u_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}, n \geqslant 1, \quad v_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \frac{1}{n \cdot n!}, n \geqslant 1,$$

d'où le résultat.

□

♦ **Exemples.**

1. Une société internationale a ses membres dans six pays différents. La liste de ses membres contient 1978 noms qui sont numérotés 1, 2, ..., 1978. Montrer qu'il y a au moins un membre de cette société dont le numéro est, soit la somme des numéros de deux membres de la société appartenant au même pays que lui, soit le double du numéro d'un membre de la société appartenant au même pays que lui.

(Olympiades internationales-1978/6)

On va prouver un résultat plus général : si $k \in \mathbb{N}^*$ et $\{S_1, S_2, \ldots, S_k\}$ est une partition quelconque de l'ensemble $\{1, 2, \ldots, n-1\}$, où $n = R_k$, alors il existe $i \in \{1, 2, \ldots, k\}$, et des entiers x, y, z (non nécessairement distincts) appartenant à S_i tels que $x + y = z$.

En effet, numérotons les sommets de $\mathcal{G}_n$: $1, 2, \ldots, n$. On colorie alors les arêtes de $\mathcal{G}_n$ à l'aide de k couleurs : couleur 1, couleur 2, ..., couleur k, l'arête (x, y), $x, y \in \{1, 2, \ldots, n\}$, étant coloriée avec la couleur i si $|x - y| \in S_i$. Par définition de R_k, la configuration obtenue contient au moins un triangle monochromatique. Si $x < y < z$ sont les sommets de ce triangle, alors $y - x, z - y$ et $z - x$ appartiennent à un même S_i, et on a manifestement

$$(z - y) + (y - x) = (z - x).$$

□

Dans l'exercice proposé, on demande de prouver que toute partition $\{S_1, S_2, \ldots, S_6\}$ de l'ensemble $\{1, 2, \ldots, 1978\}$ est telle qu'il existe $i \in \{1, 2, \ldots, 6\}$, et des nombres $x, y, z \in S_i$ tels que $x + y = z$. Or, on a déjà prouvé que

$$R_6 \leqslant \lfloor 6! \times e \rfloor + 1 = 1958,$$

et on peut donc remplacer le nombre 1978 par le nombre plus petit 1957.

Cette solution n'était pas celle qu'on attendait des candidats. Une autre solution est présentée ci dessous :

Soit $\{S_1, S_2, \ldots, S_6\}$ une partition de l'ensemble $\{1, 2, \ldots, 1957\}$. Par raison de symétrie, on peut supposer que S_1 possède au moins $\lfloor 1957/6 \rfloor + 1 = 327$ éléments. Si l'une des différences

$$b_1 = a_{327} - a_{326},\ b_2 = a_{327} - a_{325}, \ldots,\ b_{326} = a_{327} - a_1,$$

où $a_1 < a_2 < \cdots < a_{327}$ sont les éléments de S_1, est dans S_1, alors le problème serait résolu car alors pour un certain i,

$$a_{327} - a_i = a_j \in S_1 \quad \Longrightarrow \quad a_i + a_j = a_{327} \in S_1.$$

Supposons donc que les b_i n'appartiennent pas à S_1. Comme ils sont distincts deux à deux, on peut supposer que S_2 possède au moins $\lfloor 326/5 \rfloor + 1 = 66$ éléments. Prenons alors les différences

$$c_1 = b'_{66} - b'_{65},\ c_2 = b'_{66} - b'_{64}, \ldots,\ c_{65} = b'_{66} - b'_1,$$

où $b'_1 < b'_2 < \cdots < b'_{66}$ appartiennent à S_2, et sont de la forme $a_{327} - a_i$, $i = 1, 2, \ldots, 326$.

Comme auparavant, on suppose que les c_i n'appartiennent pas à S_2 sinon le problème serait résolu, mais comme ils sont de la forme $a_k - a_l$, où $1 \leqslant a_l < a_k \leqslant 1957$, on suppose de même qu'ils n'appartiennent pas non plus à S_1. Comme les c_i sont distincts deux à deux et, on peut supposer que S_3 en possède au moins $\lfloor 65/4 \rfloor + 1 = 17$ éléments $c'_1 < c'_2 < \cdots < c'_{17}$. On suppose de nouveau que les différences

$$d_1 = c'_{17} - c'_{16},\ d_2 = c'_{17} - c'_{15}, \ldots,\ d_{16} = c'_{17} - c'_1,$$

n'appartiennent ni à S_1, ni à S_2 ni à S_3, et l'on peut supposer que S_4 en possède au moins $\lfloor 16/3 \rfloor + 1 = 6$ éléments $d'_1 < d'_2 < \cdots < d'_6$. On suppose de nouveau que les différences

$$e_1 = d'_6 - d'_5,\ e_2 = d'_6 - d'_4, \ldots,\ e_5 = d'_6 - d'_1,$$

appartiennent soit à S_5 soit à S_6. Si trois parmi eux, $e'_1 < e'_2 < e'_3$, appartiennent disons à S_5, alors

$$f_1 = e'_3 - e'_1, \ f_2 = e'_3 - e'_2,$$

appartiennent à S_6, mais alors $g = f_2 - f_1 < 1957$ appartient à un des S_i, $i = 1, 2, \ldots, 6$, ce qui termine la démonstration.

5.6. Les fonctions génératrices

5.6.1. Fonction génératrice d'une suite. Si $(a_n)_{n\in\mathbb{N}}$ est une suite de nombres, alors la fonction G définie par :

$$\boxed{G(x) = \sum_{k=0}^{+\infty} a_k x^k}$$

est appelée fonction génératrice de la suite $(a_n)_{n\in\mathbb{N}}$.

Comme seuls nous intéressent les coefficients a_k, $k = 0, 1, 2, \ldots$, on ne se préoccupera pas des problèmes de convergence. On effectuera nos calculs sur les fonctions génératrices comme si on avait affaire à des polynômes.

On introduit la notation

$$\boxed{a_n = a_n[G]}$$

pour signifier que a_n est le coefficient de x^n dans la fonction G.

♦ **Exemples.**

1. La fonction génératrice de la suite $(1, 1, \ldots)$ est

$$1 + x + x^2 + \cdots = \frac{1}{1-x}.$$

Plus généralement, la fonction génératrice de la suite

$$\binom{n-1}{0}, \binom{1+n-1}{1}, \ldots, \binom{k+n-1}{k}, \ldots$$

est

$$\sum_{k=0}^{+\infty} \binom{k+n-1}{k} x^k = \frac{1}{(1-x)^n}. \tag{5.17}$$

En effet, c'est vrai pour $n = 1$ et si

$$\sum_{k=0}^{+\infty} \binom{k+n-2}{k} x^k = \frac{1}{(1-x)^{n-1}},$$

alors

$$\frac{1}{(1-x)^n} = \left[\sum_{k=0}^{+\infty} x^k\right] \left[\sum_{k=0}^{+\infty} \binom{k+n-2}{k} x^k\right] = \sum_{k=0}^{+\infty} c_k x^k,$$

où
$$c_k = \sum_{i=0}^{k} \binom{i+n-2}{i} = \binom{k+n-1}{k},$$
et le résultat s'ensuit par récurrence sur n.

Cette formule reste valable pour tout $\alpha \in \mathbb{R}$:
$$(1-x)^{\alpha} = \sum_{k=0}^{+\infty} \binom{k-\alpha-1}{k} x^k, \tag{5.18}$$
où l'on a posé par définition
$$\binom{\alpha}{r} = \frac{\alpha(\alpha-1)\cdots(\alpha-r+1)}{r!}$$
pour tout $\alpha \in \mathbb{R}$ et pour tout $r \in \mathbb{N}$.

2. Trouver la fonction génératrice de la suite de Fibonacci $(F_n)_{n\in\mathbb{N}^*}$ définie par :
$$\begin{cases} F_1 = F_2 = 1, \\ F_n = F_{n-1} + F_{n-2} \quad (n \geqslant 3). \end{cases}$$

On pose $G(x) = \sum_{n=1}^{+\infty} F_n x^n$; on a alors
$$G(x) = x + x^2 + \sum_{n\geqslant 3} (F_{n-1} + F_{n-2})x^n = x + x^2 + x(G(x) - x) + x^2 G(x),$$
et il s'ensuit que
$$G(x) = \frac{x}{1-x-x^2}. \tag{5.19}$$

Ceci permet de retrouver la formule de Binet :
$$G(x) = \frac{1}{\sqrt{5}} \left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x} \right) = \frac{1}{\sqrt{5}} \sum_{k=1}^{+\infty} (\alpha^k - \beta^k) x^k,$$
où $\alpha = (1+\sqrt{5})/2$ et $\beta = (1-\sqrt{5})/2$, d'où
$$F_n = a_n[G] = \frac{\alpha^n - \beta^n}{\sqrt{5}}, \quad n \geqslant 1.$$

5.6.2. Les suites 0-1. Soit A un ensemble de suites finies prenant leurs valeurs dans l'ensemble $\{0,1\}$. On note a_n, $n = 0, 1, \ldots$, le nombre d'éléments de A dont la longueur est n (en posant $a_0 = 1$), et on pose :
$$G_A(x) = \sum_{n=0}^{+\infty} a_n x^n.$$

Si A est constitué de toutes les suites finies qui se décomposent, de façon unique, en un bloc $b \in B$ suivi d'un bloc $c \in C$, alors
$$G_A(x) = G_B(x) G_C(x)$$

car on a $a_n[G_A] = \sum_{i=0}^{n} a_i[G_B]a_{n-i}[G_C]$.

D'un autre côté, si A est constitué de toutes les suites finies qui sont obtenues, de façon unique, en juxtaposant un certain nombre (pouvant être nul) d'éléments d'un ensemble A', alors

$$G_A(x) = 1 + \underbrace{G_{A'}(x)}_{\text{un bloc de } A'} + \underbrace{[G_{A'}(x)]^2}_{\text{2 blocs de } A'} + \cdots = \frac{1}{1 - G_{A'}(x)}.$$

Par exemple, si A désigne l'ensemble de toutes les suites finies prenant leurs valeurs dans l'ensemble $\{0, 1\}$, tout élément dans A se décompose, de façon unique, sous la forme :

$$\underbrace{(00\ldots0)}_{\geqslant 0.} \ \{\text{des blocs de } A'\} \ \underbrace{(11\ldots1)}_{\geqslant 0.},$$

où A' est le sous-ensemble de A formé par les suites de la forme :

$$\underbrace{(11\ldots1)}_{\geqslant 1.} \ \underbrace{(00\ldots0)}_{\geqslant 1.}.$$

On en déduit que

$$G_A(x) = (1 + x + x^2 + \cdots)\frac{1}{1 - G_{A'}(x)}(1 + x + x^2 + \cdots),$$

où

$$G_{A'}(x) = (x + x^2 + \cdots)(x + x^2 + \cdots) = \frac{x^2}{(1-x)^2}.$$

Il en résulte que

$$G_A(x) = \frac{1}{1 - 2x} = \sum_{n=0}^{+\infty} 2^n x^n,$$

et on retrouve ainsi le nombre de suites 0-1 de longueur n, à savoir 2^n.

La méthode exposée ici va permettre de calculer rapidement le nombre de suites 0-1 auxquelles on a imposé certaines conditions, et c'est bien là que réside tout son intérêt.

♦ **Exemples.**

1. Quel est le nombre de suites de longueur n prenant leurs valeurs dans l'ensemble $\{0, 1\}$ et ne possédant pas deux zéros consécutifs ?

Soit A l'ensemble des suites 0-1 ne possédant pas deux zéros consécutifs. Tout élément de A se décompose sous la forme :

$$\{\text{un ou aucun zéro}\} \ \{\text{des blocs de } A'\} \ \underbrace{(11\ldots1)}_{\geqslant 0.},$$

où A' est l'ensemble des suites 0-1 de la forme :

$$\underbrace{(11\ldots1)}_{\geqslant 1.} \ 0.$$

Il s'ensuit que

$$G_A(x) = (1+x)\frac{1}{1-\left(\dfrac{x^2}{1-x}\right)}\left(\frac{1}{1-x}\right) = \frac{1+x}{1-x-x^2}.$$

Comme

$$\frac{1+x}{1-x-x^2} = \sum_{n=0}^{+\infty}(F_n + F_{n+1})x^n \quad (F_0 = 0),$$

il s'ensuit que le nombre recherché est $F_n + F_{n+1} = F_{n+2}$.

2. Trouver le nombre de suites de longueur n prenant leurs valeurs dans l'ensemble $\{0, 1\}$ et sans aucun bloc de zéros de longueur impaire situé entre deux blocs non vides de 1.

Soit A l'ensemble formé par toutes les suites 0-1 vérifiant la condition précédente. Tout élément de A se met, de façon unique, sous l'une des deux formes :

$$\underbrace{(11\ldots1)}_{\geqslant 0.}\ \{\text{des blocs de } A'\}\ \underbrace{(00\ldots0)}_{\geqslant 0.},$$

ou

$$\underbrace{(00\ldots0)}_{\substack{\text{un nombre}\\ \text{impair} \geqslant 1.}}\ \underbrace{(11\ldots1)}_{\geqslant 1.}\ \{\text{des blocs de } A'\}\ \underbrace{(00\ldots0)}_{\geqslant 0.},$$

où A' est l'ensemble des suites 0-1 de la forme :

$$\underbrace{(00\ldots0)}_{\substack{\text{un nombre}\\ \text{pair} \neq 0.}}\underbrace{(11\ldots1)}_{\geqslant 1.}.$$

Il s'ensuit que :

$$\begin{aligned} G_A(x) &= \frac{1}{(1-x)^2} \times \frac{1}{1-\left(\dfrac{x^2}{1-x^2}\times\dfrac{x}{1-x}\right)} + \\ &\quad \frac{x}{1-x^2}\times\frac{x}{1-x}\times\frac{1}{1-\left(\dfrac{x^2}{1-x^2}\times\dfrac{x}{1-x}\right)}\times\frac{1}{1-x} \\ &= \frac{1}{(1-x)(1-x-x^2)}, \end{aligned}$$

ce qui donne :

$$a_n[G_A] = F_1 + F_2 + \cdots + F_{n+1} = F_{n+3} - 1.$$

5.6.3. Résolution d'équations de récurrence. Si $(a_n)_{n\in\mathbb{N}}$ est une suite définie par une relation de récurrence, il est efficace de rechercher sa fonction génératrice, que l'on obtient à l'aide de l'équation de récurrence après quelques manipulations algébriques. Le terme a_n est alors le coefficient de x^n dans le développement de G.

♦ **Exemples.**

1. Trouver l'expression explicite de la suite $(a_n)_{n\in\mathbb{N}}$ définie par

$$\begin{cases} a_0 = 1, \\ a_n - 3a_{n-1} = 4^n. \end{cases}$$

Si G est la fonction génératrice de $(a_n)_{n\in\mathbb{N}}$, alors

$$(1-3x)G(x) = 1 + 4x + 4^2x^2 + \cdots = \frac{1}{1-4x},$$

et par conséquent

$$G(x) = \frac{1}{(1-3x)(1-4x)} = \frac{\alpha}{1-3x} + \frac{\beta}{1-4x},$$

où $\alpha = -3$ et $\beta = 4$. On en déduit que

$$a_n = a_n[G] = 4^{n+1} - 3^{n+1}, \quad n \geqslant 0.$$

2. Trouver l'expression explicite de la suite $(a_n)_{n\in\mathbb{N}}$ définie par

$$\begin{cases} a_0 = 1, \\ a_n = \displaystyle\sum_{k=1}^{n-1} a_k a_{n-1-k}. \end{cases}$$

Si G est la fonction génératrice de $(a_n)_{n\in\mathbb{N}}$, alors

$$\begin{aligned} G(x) &= 1 + \sum_{n=1}^{+\infty}\Big(\sum_{k=0}^{n-1} a_k a_{n-1-k}\Big)x^n \\ &= 1 + (a_0a_0)x + (a_0a_1 + a_1a_0)x^2 + \cdots = 1 + x[G(x)]^2, \end{aligned}$$

et il s'ensuit que

$$G(x) = \frac{1}{2x}\left(1 \pm \sqrt{1-4x}\right).$$

Comme

$$\sqrt{1-4x} = \sum_{n=1}^{+\infty}\binom{n-3/2}{n}4^n x^n,$$

où

$$4^n\binom{n-3/2}{n} = 4^n\frac{(n-3/2)(n-3/2-1)\cdots(-1/2)}{n!} = \frac{-2}{n}\binom{2n-2}{n-1},$$

on a

$$a_n[G] = a_n\left[\left(\frac{1}{2x}\{1-\sqrt{1-4x}\}\right)\right] = \frac{1}{n+1}\binom{2n}{n},$$

et on reconnaît la suite des nombres de Catalan.

EXERCICES

1. Soient $n \in \mathbb{N}^*$, et $a_0, a_1, \ldots, a_n \in \{1, 2, \ldots, 2n\}$ deux à deux distincts. Montrer qu'il existe $(i, j) \in \{0, 1, \ldots, n\}^2$ tel que : $i \neq j$ et $a_i \mid a_j$.

---

2. Quelle est la somme des plus grands diviseurs impairs des entiers $1, 2, 3, \ldots, 2^n$, où $n \in \mathbb{N}$?

(Olympiades allemandes-1982)

---

3. Les nombres $1, 2, \ldots, 2n-1, 2n$ sont répartis en deux ensembles $\{a_1, a_2, \ldots, a_n\}$ et $\{b_1, b_2, \ldots, b_n\}$ tels que $a_1 < a_2 < \cdots < a_n$ et $b_1 > b_2 > \cdots > b_n$. Démontrer que

$$|a_1 - b_1| + |a_2 - b_2| + \cdots + |a_n - b_n| = n^2.$$

---

4. On considère un tableau carré $n \times n$ dont toutes les cases sont remplies comme suit : à l'intersection de la ligne i et de la colonne j se trouve le nombre $i + j - 1$. Quel est le plus petit produit de n nombres de ce tableau tels qu'il n'y ait pas deux de ces nombres sur la même ligne ou sur la même colonne ?

---

5. On désigne par $p_n(k)$ le nombre de permutations de l'ensemble $\{1, 2, \ldots, n\}$ ayant exactement k points fixes. Prouver que :

$$\sum_{k=0}^{n} k p_n(k) = n!.$$

(Olympiades internationales-1987/1)

---

6. Soit $f(n)$ le nombre de zéros dans la représentation décimale de l'entier positif n. Quelle est la valeur de la somme :

$$S = 2^{f(1)} + 2^{f(2)} + \cdots + 2^{f(99\ldots9)},$$

où le dernier nombre contient 10 fois le chiffre 9 ?

(Olympiades hongroises-1981)

---

7. a) Soit A un ensemble de cardinal n ($n \geqslant 2$). On désigne par $S(n, k)$ le nombre de partitions de A en k parties ($k \geqslant 2$). Démontrer que

$$S(n, k) = S(n-1, k-1) + kS(n-1, k).$$

b) Démontrer que le nombre de partitions de l'ensemble $\{1, 2, \ldots, n\}$ en k parties telles qu'aucune de ces parties ne contienne deux entiers consécutifs est égal à $S(n-1, k-1)$.

---

8. Dans une suite finie de nombres réels, la somme de sept termes consécutifs quelconques est négative et la somme de onze termes consécutifs quelconques est positive. Déterminer le nombre maximum de termes de la suite.

(Olympiades internationales-1977/2)

---

9. Soient I une partie finie et non vide de $\mathbb{Z}$ et f et g deux fonctions définies sur I. Soit m le nombre de couples (x, y) vérifiant $f(x) = g(y)$, n le nombre de couples (x, y) vérifiant $f(x) = f(y)$ et k le nombre de couples (x, y) vérifiant $g(x) = g(y)$. Démontrer que

$$2m \leqslant n + k.$$

---

10. On se donne n points dans un plan. Montrer qu'il existe au moins $\binom{n-3}{2}$ quadrilatères convexes ayant leurs sommets parmi ces points. On suppose $n > 4$ et que trois points ne sont pas alignés.

(Olympiades internationales-1969/5)

---

11. Soit k un entier tel que $1 \leqslant k < n$. On considère toutes les suites finies d'entiers positifs dont la somme vaut n. Trouver $T(n, k)$, le nombre total de termes égaux à k dans toutes ces suites.

(proposé à l'OIM-1988)

---

12. Soient n et r deux entiers ($1 \leqslant r \leqslant n$). On forme tous les sous-ensembles à r éléments de l'ensemble $\{1, 2, \ldots, n\}$ et on considère pour chacun de ces sous-ensembles son plus petit élément. On appelle $f(n, r)$ la moyenne arithmétique de tous les nombres ainsi obtenus. Prouver que

$$f(n, r) = \frac{n+1}{r+1}.$$

(Olympiades internationales-1981/2)

---

13. Il y a 1988 villes connectées entre elles grâce à un réseau de 4000 routes. Prouver qu'il existe un parcours fermé passant par moins de 20 villes.

(Tournoi international des villes-1988)

---

14. Dans un groupe de n personnes, il y a q paires d'amis et dans chaque ensemble de trois personnes, il y a au moins une paire d'ennemis. On suppose que deux éléments quelconques du groupe sont soit des amis, soit des ennemis.

Prouver qu'il existe au moins une personne dont l'ensemble des ennemis contient au plus $q(1-4q/n^2)$ paires d'amis.

(Olympiades des États-Unis-1995)

---

15. Les pentagones convexes $A_1A_2A_3A_4A_5$ et $B_1B_2B_3B_4B_5$ appartiennent à des plans parallèles dans l'espace. Chaque côté de ces deux pentagones ainsi que chaque segment A_iB_j pour i et j vérifiant $1 \leqslant i, j \leqslant 5$, est coloré soit en rouge, soit en vert.

On suppose que tout triangle dont les trois sommets sont des sommets de ces deux pentagones et dont les trois côtés sont colorés a deux côtés de couleurs différentes. Montrer que les dix côtés des deux pentagones sont tous de la même couleur.

(Olympiades internationales-1979/2)

---

16. Prouver que l'ensemble des suites finies de longueur n prenant leurs valeurs dans l'ensemble $\{0, 1\}$ et contenant le bloc 01 exactement m fois est $\binom{n+1}{2m+1}$.

(Olympiades britanniques-1982)

---

17. Une matrice carrée à n lignes et n colonnes, à éléments dans l'ensemble $S = \{1, 2, \ldots, 2n-1\}$, est appelée une matrice d'argent si, pour tout $i = 1, \ldots, n$, la réunion de la i-ième ligne et de la i-ième colonne contient tous les éléments de S. Montrer que :

a) il n'existe pas de matrice d'argent pour $n = 1997$;

b) il existe des matrices d'argent pour une infinité de valeurs de n.

(Olympiades internationales-1997/4)

---

18. Pour quelles valeurs de l'entier positif n existe-t-il un tableau $n \times n$ de nombres égaux à $-1, 0$ ou 1 tel que les $2n$ sommes obtenues en sommant les éléments d'une même colonne et d'une même ligne soient deux à deux distinctes ?

(proposé à l'OIM-1988)

---

19. Soit n un entier strictement positif : $A_1, A_2, \ldots, A_{2n+1}$ sont $2n+1$ sous-ensembles d'un ensemble B. On suppose vérifiées les propriétés suivantes :

a) chaque ensemble A_i contient exactement $2n$ éléments ;

b) pour tout (i, j), $1 \leqslant i < j \leqslant 2n+1$, $A_i \cap A_j$ contient exactement un élément ;

c) tout élément de B appartient à au moins deux des ensembles A_i.

Pour quelles valeurs de n est-il possible d'associer à tout élément de B la valeur 0 ou 1 de telle sorte que, dans chaque ensemble A_i, on trouve exactement n éléments affectés de la valeur 0 ?

(Olympiades internationales-1988/2)

---

20. On se donne une famille de s sous-ensembles $A_1, A_2, \ldots, A_s$ de l'ensemble $\{1, 2, \ldots, M\}$ tels que $|A_i| = a_i$, $i = 1, 2, \ldots, s$. On suppose aussi que deux quelconques de ces sous-ensembles ne sont pas inclus l'un dans l'autre (une telle famille est dite de Sperner, ou spernerienne). Prouver alors l'inégalité :

$$\sum_{i=1}^{s} \frac{1}{\binom{M}{a_i}} \leqslant 1.$$

(Olympiades russes-1987)

---

21. On définit la suite $(a_n)_{n \in \mathbb{N}^*}$ par

$$\sum_{d|n} a_d = 2^n.$$

Prouver que n divise a_n pour tout $n \in \mathbb{N}^*$.

(proposé à l'OIM-1989)

---

22. On considère deux entiers strictement positifs k et n et un ensemble S de n points du plan tels que :

a) trois points quelconques de S ne sont pas alignés ;

b) pour tout point P de S, il existe au moins k points distincts dans S situés à une même distance de P.

Démontrer que $k \leqslant 1/2 + \sqrt{2n}$.

(Olympiades internationales-1989/3)

---

23. Chaque case d'un échiquier $n \times n$ ($n \geqslant 2$) est numérotée à l'aide d'un élément de l'ensemble $\{1, 2, \ldots, n^2\}$, deux cases différentes n'ayant pas la même numérotation. Prouver qu'il existe deux cases voisines dont les numéros diffèrent d'une quantité $\geqslant n$.

(proposé à l'OIM-1988)

---

24. Soit A un ensemble fini d'entiers naturels non nuls. Prouver qu'il existe un ensemble fini B tel que $A \subseteq B \subseteq \mathbb{N}^*$ et

$$\prod_{x\in B} x = \sum_{x\in B} x^2.$$

(Olympiades iraniennes-1995)

---

25. Soit $S = \{1, 2, \ldots, 280\}$. Trouver la plus petite valeur de l'entier n pour que chaque sous-ensemble de n éléments de S contienne au moins 5 nombres deux à deux premiers entre eux.

(Olympiades internationales-1991/3)

---

26. Soit $Z_{m,n}$ l'ensemble de tous les couples (i, j), où $i \in \{1, 2, \ldots, m\}$ et $j \in \{1, 2, \ldots, n\}$, et soit $a_{m,n}$ le nombre de sous-ensembles de $Z_{m,n}$ ne contenant pas de couples (i_1, j_1), (i_2, j_2) tels que $|i_1 - i_2| + |j_1 - j_2| = 1$. Prouver alors, pour tous entiers strictement positifs m et k, que

$$a_{m,2k}^2 \leqslant a_{m,2k-1}a_{m,2k+1}.$$

(proposé à l'OIM-1988)

---

27. Sur un cercle on se donne un ensemble de $2n - 1$ points distincts (n est un entier supérieur ou égal à 3). Si exactement k de ces points sont coloriés en noir, cette coloration est dite « bonne » s'il existe au moins une paire de points noirs telle que l'un des deux arcs ouverts formés par ces deux points contienne exactement n points de E.

Trouver la plus petite valeur de k pour laquelle toute coloration en noir d'exactement k points de E est « bonne ».

(Olympiades internationales-1990/2)

---

28. Soit S un ensemble de m couples (a, b) d'entiers positifs vérifiant $1 \leqslant a < b \leqslant n$. Prouver qu'il existe au moins

$$4m\frac{m - n^2/4}{3n}$$

triplets (a, b, c) tels que (a, b), (a, c) et (b, c) appartiennent à S.

(Olympiades hongroises-1987)

---

29. Soit n un entier naturel non nul. On dit qu'une permutation $(x_1, x_2, \ldots, x_{2n})$ de l'ensemble $\{1, 2, \ldots, 2n\}$ possède la propriété P si $|x_i - x_{i+1}| = n$ pour au moins un i dans l'ensemble $\{1, 2, \ldots, 2n-1\}$.

Démontrer que, pour chaque n, il y a plus de permutations possédant la propriété P que de permutations ne la possédant pas.

(Olympiades internationales-1989/6)

---

30. Soient n, p et q des entiers positifs tels que $n > p + q$. Soient $x_0, x_1, \ldots, x_n$ des entiers vérifiant les deux conditions suivantes :

a) $x_0 = x_n = 0$;

b) Pour tout entier i tel que $1 \leqslant i \leqslant n$, on a soit $x_i - x_{i-1} = p$, soit $x_i - x_{i-1} = -q$.

Montrer qu'il existe une paire (i, j) d'indices avec $i < j$ et $(i, j) \neq (0, n)$ telle que $x_i = x_j$.

(Olympiades internationales-1996/6)

---

31. Pour tout entier strictement positif n, $f(n)$ désigne le nombre de façons de représenter n comme une somme de puissances de 2 à exposants entiers positifs ou nuls.

Deux représentations qui ne diffèrent que par l'ordre des termes de la somme sont considérées comme les mêmes. Par exemple $f(4) = 4$ car le nombre 4 peut être représenté par les quatre façons suivantes : 4 ; $2+2$; $2+1+1$; $1+1+1+1$.

Montrer que, pour tout entier $n \geqslant 3$:

$$2^{n^2/4} < f(2^n) < 2^{n^2/2}.$$

(Olympiades internationales-1997/6)

---

32. On se donne 9 points dans l'espace dont quatre quelconques ne sont pas coplanaires. Trouver la plus petite valeur de l'entier positif n pour laquelle il existe un triangle monochromatique pour chaque coloriage en bleu et rouge de n arêtes quelconques dessinées entre les neuf points considérés.

(Olympiades internationales-1992/3)

---

33. Soit p un nombre premier impair. Trouver le nombre de sous-ensembles A de $\{1, 2, \ldots, 2p\}$ tels que :

a) A possède exactement p éléments, et

b) la somme des éléments de A est divisible par p.

(Olympiades internationales-1995/6)

SOLUTIONS

1. Tout entier $\geqslant 1$ s'écrit, d'une façon unique, sous la forme $2^\alpha(2\beta+1)$, $(\alpha,\beta)\in\mathbb{N}^2$. Ainsi, pour chaque $i\in\{0,1,\ldots,n\}$, il existe $(\alpha_i,\beta_i)\in\mathbb{N}^2$ tel que $a_i=2^{\alpha_i}(2\beta_i+1)$. Les $n+1$ entiers $\beta_0,\beta_1,\ldots,\beta_n$ sont dans $\{0,1,\ldots,n-1\}$, qui est de cardinal n ; il existe donc $(i,j)\in\{0,1,\ldots,n\}^2$ tel que $i\neq j$ et $\beta_i=\beta_j$. On a alors $a_i\mid a_j$ ou $a_j\mid a_i$ suivant que $\alpha_i\leqslant\alpha_j$ ou $\alpha_j\leqslant\alpha_i$.

---

2. Tout entier parmi les entiers $2^{n-1}+1, 2^{n-1}+2,\ldots,2^n$ s'écrit sous la forme $2^\alpha(2\beta+1)$ où $(\alpha,\beta)\in\mathbb{N}^2$. Le plus grand diviseur impair d'un tel entier est alors $2\beta+1$. Réciproquement, si $2\beta+1$ est un entier impair $\leqslant 2^n$, alors il existe un unique entier dans l'ensemble $\{2^{n-1}+1,2^{n-1}+2,\ldots,2^n\}$ dont $2\beta+1$ soit le plus grand diviseur impair. On a donc la relation de récurrence :

$$a_n=a_{n-1}+(1+3+\cdots+2\times 2^{n-1}-1)=a_{n-1}+4^{n-1},\quad n\geqslant 2.$$

On en déduit immédiatement que

$$a_n=a_1+4+\cdots+4^n=\frac{1}{3}(4^n+2).$$

---

3. Désignons par a_k et b_k les éléments vérifiant les relations

$$n\leqslant a_k<\cdots<a_n,\quad b_1>b_2>\cdots>b_k\geqslant n.$$

Ainsi, les $n+1$ nombres $b_1,b_2,\ldots,b_k,a_k,a_{k+1},\ldots,a_n$ sont compris entre n et $2n$. Posons $m_i=\min(a_i,b_i)$ et $M_i=\max(a_i,b_i)$. Tous les M_i sont donc compris entre $n+1$ et $2n$, et tous les m_i sont compris entre 1 et n ; par conséquent,

$$\begin{aligned}
&|a_1-b_1|+|a_2-b_2|+\cdots+|a_n-b_n|\\
=\;&(M_1-m_1)+(M_2-m_2)+\cdots+(M_n-m_n)\\
=\;&(M_1+M_2+\cdots+M_n)-(m_1+m_2+\cdots+m_n)\\
=\;&[(n+1)+(n+2)+\cdots+2n]-[1+2+\cdots+n]\\
=\;&n^2.
\end{aligned}$$

---

4. Démontrons que la plus petite valeur que l'on peut atteindre est $1\times 3\times\cdots\times(2n-1)$. C'est la valeur du produit des n nombres situés sur la diagonale principale du tableau.

Supposons $n\geqslant 2$ et choisissons n nombres tels qu'il n'y ait pas deux de ces nombres sur la même ligne ou sur la même colonne. À moins que les nombres choisis ne soient tous situés sur la diagonale principale du tableau, il doit exister deux nombres $i+i'-1$ (celui situé à l'intersection de la ligne i et de la colonne i') et $j+j'-1$ (celui situé à l'intersection de la ligne j et de la colonne j') tels que $i<j$ et $i'>j'$. Considérons alors les nombres $i+j'-1$ et $i'+j-1$ au lieu des nombres $i+i'-1$ et $j+j'-1$ et laissons les $n-2$ autres nombres inchangés. On a alors

$$(i+j'-1)(i'+j-1)-(i+i'-1)(j+j'-1)=(i-j)(i'-j')<0.$$

Le nouveau produit est donc plus petit que le produit des n nombres choisis, d'où le résultat.

---

5. 1$^{\text{ère}}$ solution. Le nombre de permutations de $\{1,2,\ldots,n\}$ à k points fixes s'obtient en choisissant de toutes les façons possibles les $n-k$ points non fixes et en les permutant de toutes les façons qui ne les laissent pas fixes. Autrement dit, $p_n(k)=\binom{n}{k}p_{n-k}(0)$. D'où, pour tout $k=1,2,\ldots,n$,

$$kp_n(k)=k\binom{n}{k}p_{n-k}(0)=n\binom{n-1}{k-1}p_{(n-1)-(k-1)}(0)=np_{n-1}(k-1).$$

Ainsi,

$$\sum_{k=0}^{n}kp_n(k)=n\sum_{k=1}^{n}p_{n-1}(k-1)=n(n-1)!=n!,$$

car $\sum_{k=1}^{n}p_{n-1}(k-1)$ représente le nombre de toutes les permutations de $n-1$ objets.

2$^{\text{ème}}$ solution. On raisonne par récurrence sur n. Les cas $n=1$ et $n=2$ ne posent aucun problème. Pour établir le passage de n à $n+1$, on commence d'abord par remarquer que $p_n(k)=\binom{n}{k}p_{n-k}(0)$. D'un autre côté, le principe d'inclusion et d'exclusion nous permet d'écrire

$$p_n(0)=n!-\left[n(n-1)!-\binom{n}{2}(n-2)!+\cdots+(-1)^{n-1}\right]=n!\left[\frac{1}{2!}-\frac{1}{3!}+\cdots+\frac{(-1)^n}{n!}\right]$$

pour $n\geqslant 2$; $p_n(n-1)=0$ et $p_n(n)=1$.

Il en résulte que $p_{n+1}(k)=(n+1)p_n(k)+\binom{n+1}{k}(-1)^{n-k+1}$, pour tout k, $0\leqslant k\leqslant n-2$, mais elle reste également vérifiée pour $k=0,1,\ldots,n$. Il s'ensuit que :

$$\begin{aligned}\sum_{k=1}^{n+1}kp_{n+1}(k) &= n+1+\sum_{k=1}^{n}kp_{n+1}(k)\\ &= \sum_{k=1}^{n}k(n+1)p_n(k)+(n+1)+\sum_{k=1}^{n}(-1)^{n-k+1}k\binom{n+1}{k}\\ &= (n+1)!+\sum_{k=1}^{n+1}(-1)^{n-k+1}k\binom{n+1}{k},\end{aligned}$$

or,

$$\begin{aligned}\sum_{k=1}^{n+1}(-1)^{n-k+1}k\binom{n+1}{k} &= \sum_{k=1}^{n+1}(-1)^{n-k+1}(n+1)\binom{n}{k-1}\\ &= (n+1)\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k} = (n+1)(1-1)^n = 0.\end{aligned}$$

---

6. On calcule le nombre des entiers compris entre 1 et $10^{10}-1$ ayant k zéros dans leur représentation décimale. Pour former un tel nombre constitué de l chiffres ($k < l$), il faut placer k zéros dans $l-1$ positions possibles, puis il faut choisir $l-k$ chiffres différents de zéro. Ainsi, le nombre des entiers compris entre 1 et $10^{10}-1$ ayant k zéros dans leur représentation décimale est :

$$\sum_{l=k+1}^{10}\binom{l-1}{k}9^{l-k}.$$

La somme S vaut donc :

$$\sum_{l=1}^{10}\sum_{k=0}^{l-1}\binom{l-1}{k}9^{l-k}\times 2^k = \sum_{l=1}^{10}9^l\times\left(\frac{11}{9}\right)^{l-1} = \frac{9}{10}(11^{10}-1).$$

Note. Plus généralement, soit $f(n)$ le nombre de zéros dans l'écriture en base b, $b \geqslant 2$, de l'entier positif n. On peut calculer la somme :

$$S_m = \sum_{k=1}^{b^m-1}2^{f(k)},$$

où $m \in \mathbb{N}^*$. On trouve :

$$S_m = (b-1)\frac{(b+1)^m-1}{b}.$$

---

7. a) Soit x un élément de l'ensemble A de cardinal n. L'ensemble G des partitions de A en k parties est une réunion disjointe des deux ensembles suivants :

E : l'ensemble des partitions de A formé des partitions de $A\setminus\{x\}$ en $k-1$ parties et du singleton $\{x\}$.

F : l'ensemble des partitions de A en k parties telles que x appartienne à l'une de ces parties. Tout élément de F s'obtient à partir d'une partition de $A\setminus\{x\}$ en k parties en adjoignant x à l'une d'entre elles. On a donc

$$|G| = |E| + |F|,$$

i.e.,

$$S(n,k) = S(n-1,k-1) + kS(n-1,k).$$

b) Soit $\gamma(n,k)$ le nombre de partitions de l'ensemble $\{1,2,\ldots,n\}$ en k parties telles qu'aucune de ces parties ne contienne deux entiers consécutifs. On a :

$$\gamma(n,2) = 1, \quad \gamma(n,k) = \gamma(n-1,k-1) + (k-1)\gamma(n-1,k).$$

En effet, on raisonne de manière analogue à celle de a) en prenant $n = x$ et en tenant compte du fait que n peut constituer une partie ou être adjoint à une partie ne contenant pas son prédécesseur. Ainsi, les deux suites $\{\gamma(n,k)\}_{k\geqslant 2}$ et $\{S(n-1,k-1)\}_{k\geqslant 2}$ coïncident pour tout $n \geqslant 2$ (récurrence sur n par exemple), et on a alors l'égalité :

$$\gamma(n,k) = S(n-1,k-1).$$

---

8. Il y a au plus 16 termes dans cette suite : en effet, s'il y en avait davantage, on pourrait écrire les inégalités suivantes :

$$\begin{gathered} x_1 + x_2 + \cdots + x_{11} > 0, \\ x_2 + x_3 + \cdots + x_{12} > 0, \\ \ldots \\ x_7 + x_8 + \cdots + x_{17} > 0. \end{gathered}$$

Or, la somme des éléments d'une même colonne est négative, et la somme de ces inégalités conduit à une contradiction.

D'un autre côté, il existe une suite de 16 termes vérifiant les conditions de l'énoncé. Par exemple

$$(5,\ 5,\ -13,\ 5,\ 5,\ 5,\ -13,\ 5,\ 5,\ -13,\ 5,\ 5,\ 5,\ -13,\ 5,\ 5).$$

En conclusion, le nombre maximum de termes dans une suite vérifiant les conditions de l'énoncé est 16.

---

9. Soit a_1 une des valeurs prises par la fonction f et soit n_{a_1} le nombre des x vérifiant $f(x) = a_1$ et soit k_{a_1} le nombre des x vérifiant $g(x) = a_1$. Le nombre de couples (x,y) tels que $f(x) = a_1$ et $g(y) = a_1$ est alors $n_{a_1}k_{a_1}$, celui des couples (x,y) tels que $f(x) = a_1$ et $f(y) = a_1$ est $n_{a_1}^2$ et celui des couples (x,y) tels que $g(x) = a_1$ et $g(y) = a_1$ est $k_{a_1}^2$. Si les valeurs prises par f sont $a_1, a_2, \ldots, a_p$ alors

$$\begin{aligned} m &= n_{a_1}k_{a_1} + n_{a_2}k_{a_2} + \cdots + n_{a_p}k_{a_p}, \\ n &= n_{a_1}^2 + n_{a_2}^2 + \cdots + n_{a_p}^2, \\ k &= k_{a_1}^2 + k_{a_2}^2 + \cdots + k_{a_p}^2, \end{aligned}$$

et en utilisant l'inégalité $2ab \leqslant a^2 + b^2$, on obtient le résultat demandé.

---

10. On raisonne par récurrence sur $n \geqslant 5$, et on commence par prouver la base de la récurrence : si les 5 points forment un pentagone convexe, le problème est résolu. Si l'enveloppe convexe des 5 points est un quadrilatère, le problème est encore résolu. Si maintenant l'enveloppe convexe des 5 points est un triangle ABC, la droite (DE) coupe deux côtés du triangle que l'on suppose par symétrie égaux à $[BA]$ et $[BC]$. Le quadrilatère $ADEC$ est alors convexe.

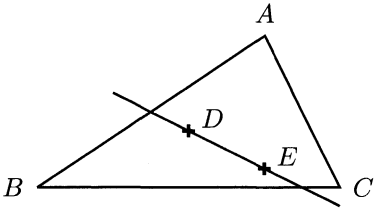


FIG. 5.14.

Étudions le cas $n > 5$; on a $\binom{n}{5}$ sous-ensembles de 5 points. Pour chaque sous-ensemble, on a au moins un quadrilatère convexe (cas $n = 5$). Le nombre $f(n)$ de quadrilatères convexes est alors, puisque chaque quadrilatère est compté $n-4$ fois, au moins égal à $\binom{n}{5} \Big/ (n-4)$. Il suffirait pour conclure de démontrer que pour $n > 5$,

$$\frac{\binom{n}{5}}{n-4} \geqslant \binom{n-3}{2}.$$

Pour $n = 6$, les deux nombres sont égaux à 3. Par ailleurs

$$r = \frac{\binom{n}{5}}{n-4} \times \frac{1}{\binom{n-3}{2}} = \frac{n(n-1)(n-2)}{60(n-4)} = \frac{n^2+n+6}{60} + \frac{2}{5(n-4)},$$

d'où, pour $n \geqslant 7$, $r \geqslant 1$, ce qui achève la démonstration.

---

11. On place n points sur une même ligne. Ils déterminent $n-1$ espaces intérieurs. Des barres verticales peuvent être insérées dans ces espaces avec 2^{n-1} façons produisant toutes les suites possibles de somme n. Pour trouver le nombre $T(n,k)$, on dessine n points sur une même ligne, et on encadre un bloc de k points consécutifs :

$$\ldots \ | \ . \ | \ \ldots \ | \ \boxed{k \text{ points}} \ | \ \ldots$$

1er cas. Les points encadrés ne contiennent ni le premier ni le dernier point. Il y a $(n-k-1)$ façons pour placer le cadre, et 2^{n-k-2} façons pour placer les barres verticales dans les $(n-k-2)$ espaces disponibles. Ceci définit une suite avec un terme égal à k.

2ème cas. Les points encadrés contiennent le premier ou le dernier point. Il y a alors deux façons pour placer le cadre, et 2^{n-k-1} façons pour disposer les barres verticales dans les $(n-k-1)$ espaces disponibles. On obtient ainsi :

$$T(n,k) = (n-k-1)\cdot 2^{n-k-2} + 2\cdot 2^{n-k-1} = (n-k+3)\cdot 2^{n-k-2}.$$

---

12. $1^{\text{ère}}$ solution. Il y a deux questions qui se posent. D'abord, quels éléments de l'ensemble $\{1,2,\ldots,n\}$ peuvent être les plus petits dans un sous-ensemble à r éléments de $\{1,2,\ldots,n\}$? Ensuite, quelle est la contribution de chacun de ces plus petits éléments à la somme ?

Pour $m = 1,2,\ldots,n-r+1$, le nombre de sous-ensembles à r éléments de $\{1,2,\ldots,n\}$ dont m est le plus petit élément est égal à $\binom{n-m}{r-1}$. Ainsi, la somme S des plus petits éléments de chaque sous-ensemble à r éléments de $\{1,2,\ldots,n\}$ est donnée par

$$\begin{aligned} S &= 1\binom{n-1}{r-1} + 2\binom{n-2}{r-1} + \cdots + (n-r+1)\binom{r-1}{r-1} \\ &= \left[\binom{n-1}{r-1} + \binom{n-2}{r-1} + \cdots + \binom{r-1}{r-1}\right] + \\ &\qquad\qquad \left[\binom{n-2}{r-1} + \cdots + \binom{r-1}{r-1}\right] + \cdots + \binom{r-1}{r-1}. \end{aligned}$$

On a donc

$$S = \binom{n}{r} + \binom{n-1}{r} + \cdots + \binom{r}{r} = \binom{n+1}{r+1}.$$

Puisque le nombre de sous-ensembles à r éléments de $\{1,2,\ldots,n\}$ est $\binom{n}{r}$, il s'ensuit que

$$f(n,r) = \binom{n+1}{r+1} \bigg/ \binom{n}{r} = \frac{n+1}{r+1}.$$

$2^{\text{ème}}$ solution. Afin d'alléger les notations, on fera usage du langage de la théorie des graphes. On considère un graphe où les sommets coloriés en blanc sont les sous-ensembles à r éléments de $\{1,2,\ldots,n\}$ et les sommets coloriés en noir sont les sous-ensembles à $r+1$ éléments de $\{0,1,\ldots,n\}$. Un sommet noir X est alors relié à un sommet blanc Y si Y est obtenu en supprimant à X son plus petit élément. Le degré d'un sommet blanc est alors égal à son plus petit élément. Par ailleurs, le graphe précédemment défini contient $\binom{n}{r}$ sommets blancs, et $\binom{n+1}{r+1}$ arêtes. Il s'ensuit donc que

$$f(n,r) = \binom{n+1}{r+1} \bigg/ \binom{n}{r} = \frac{n+1}{r+1}.$$

---

13. On dessine un graphe dont les villes sont les sommets et les routes constituent les arêtes. On va montrer qu'il existe un sous-graphe dont les sommets sont tous de degré $\geqslant 3$: en effet, on supprime successivement les sommets de degré $\leqslant 2$. Au total, on aura supprimé au plus 2×1988 arêtes, ce qui prouve qu'à la fin du procédé précédent, on se retrouvera avec un sous-graphe dont les sommets sont de degrés $\geqslant 3$. Tous nos raisonnements seront appliqués à ce sous-graphe.

Raisonnons par l'absurde en supposant que toute chaîne ait une longueur $\geqslant 21$. Choisissons donc un sommet x_0, et considérons toutes les suites finies de sommets $(x_1, \ldots, x_k)$ telles que $k \leqslant 10$ et chaque paire $\{x_i, x_{i+1}\}$, $0 \leqslant i \leqslant k-1$, soit une arête. Un sommet sera dit dans le niveau k si k arêtes le séparent de x_0.

Tout sommet dans le niveau k ($k \leqslant 9$) donne lieu à deux nouveaux sommets au minimum car on a supposé que toute chaîne avait une longueur $\geqslant 21$. On a ainsi l'arbre suivant :

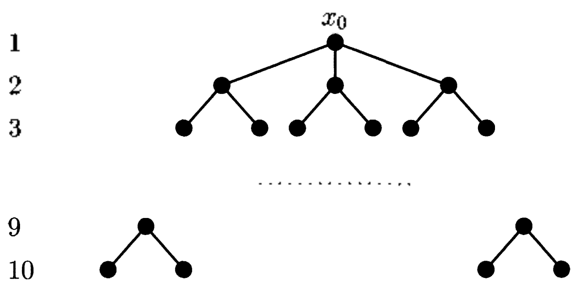


FIG. 5.15.

Dans le niveau $k \leqslant 10$, il y a au moins $3 \times 2^{k-1}$ sommets, et par conséquent, l'arbre précédent contient au moins $3+3\times 2+3\times 2^2+\cdots+3\times 2^9 = 3(2^{10}-1) = 3069$ sommets, d'où la contradiction.

---

14. Le problème est de prouver que dans un graphe à n sommets et q arêtes ne contenant aucun triangle, il existe toujours un sommet x tel que le nombre d'arêtes reliant les sommets non connectés avec x ne dépasse pas $q(1-4q/n^2)$.

Si $d(x)$ désigne le degré du sommet x, et A l'ensemble des arêtes du graphe considéré, alors

$$\sum_x d(x) = 2q, \qquad \sum_{(x,y)\in A} d(x)+d(y) = \sum_x d(x)^2,$$

puisque chaque $d(x)$ est compté $d(x)$ fois dans la dernière somme.

D'un autre côté, l'absence de triangles dans le graphe étudié se traduit par le fait que le nombre d'ennemis de toute paire $\{x,y\}$ est égal à $(n-2)-[d(x)-1]-[d(y)-1] = n-d(x)-d(y)$. Le nombre de sous-ensembles $\{A,B,C\}$, où A, B et C sont des sommets reliés par une seule arête, est égal à

$$\sum_{(x,y)\in A} n-d(x)-d(y)$$

mais également à

$$\sum_x F(x),$$

où $F(x)$ désigne le nombre d'arêtes reliant les sommets non connectés avec x. On a ainsi

$$\sum_x F(x) = qn - \sum_x d(x)^2 \leqslant qn - \frac{1}{n}\left[\sum_x d(x)\right]^2 = qn - \frac{4q^2}{n}.$$

Il existe donc un sommet x_0 tel que $F(x_0) \leqslant q - 4q^2/n^2 = q(1 - 4q/n^2)$.

---

15. On va montrer que les deux pentagones sont monochromatiques, puisqu'ils sont tous les deux de la même couleur.

Raisonnons par l'absurde, et supposons que le pentagone $A_1A_2A_3A_4A_5$ ne soit pas monochromatique. Il contient donc deux côtés consécutifs avec des couleurs différentes. Sans perte de généralité, on peut supposer que A_1A_2 soit rouge et que A_2A_3 soit vert. Comme il y a 5 segments colorés partant de A_2 vers un sommet du pentagone $B_1B_2B_3B_4B_5$, le principe des tiroirs implique que 3 parmi ces segments sont de la même couleur ; rouge par exemple. Mais alors deux de ces 3 segments partent vers une paire de sommets consécutifs de $B_1B_2B_3B_4B_5$. Sans perte de généralité, on peut supposer être dans le cas de la figure suivante :

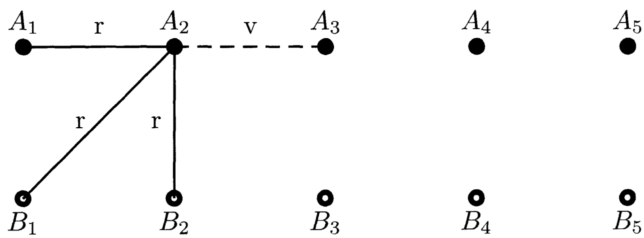


FIG. 5.16.

Comme le triangle $A_1B_1B_2$ n'est pas monochromatique, il doit posséder un côté rouge, ce qui constitue une contradiction car alors on aurait un triangle monochromatique. Il s'ensuit que le pentagone $A_1A_2A_3A_4A_5$, et similairement $B_1B_2B_3B_4B_5$ sont tous les deux monochromatiques.

Supposons donc que le pentagone $A_1A_2A_3A_4A_5$ soit coloré en rouge, et que $B_1B_2B_3B_4B_5$ soit coloré en vert. Si, à partir d'un sommet A_i, plus de trois segments verts partent vers un sommet du pentagone $B_1B_2B_3B_4B_5$, il résultera un triangle monochromatique, car 2 au moins parmi ces 3 segments partiraient vers une paire de sommets consécutifs. Ainsi, un sommet A_i n'est pas l'extrémité de plus de 2 segments verts, et donc 10 segments au plus parmi les segments A_iB_j, $1 \leqslant i, j \leqslant 5$, sont colorés en vert. En considérant le même raisonnement appliqué aux sommets du pentagone $B_1B_2B_3B_4B_5$, on déduit que 10 segments au plus parmi les segments A_iB_j, $1 \leqslant i, j \leqslant 5$, sont colorés en rouge. Ceci mène à une contradiction puisque le nombre des segments A_iB_j, $1 \leqslant i, j \leqslant 5$ est en fait 25, ce qui achève la démonstration.

Note. Le même raisonnement s'applique si on remplace les pentagones par des polygones à $2n+1$ côtés. Par contre, le résultat est mis en défaut si l'on considère des polygones à $2n$ côtés : en effet, on colorie les segments A_iA_{i+1} $(i = 1, 2, \ldots, 2n)$

en rouge, les segments B_iB_{i+1} ($i = 1, 2, \ldots, 2n$) en vert puis les segments A_iB_j ($1 \leqslant i, j \leqslant 2n$) en rouge si $i - j$ est pair, et en vert si $i - j$ est impair.

---

16. 1ère solution. Une suite finie de longueur n contient le bloc 01 exactement m fois si et seulement si elle est de la forme :

$$(11\ldots1)\underbrace{(0\ldots01\ldots1)\ldots(0\ldots01\ldots1)}_{m \text{ blocs.}}(00\ldots0).$$

Une telle suite S contient le bloc 10 m, $(m-1)$ ou $(m+1)$ fois. Cependant, si on considère la suite finie de longueur $n+2$: $1\{S\}0$, on est sûr d'avoir $m+1$ fois le bloc 10, d'où $2m+1$ passages 01 ou 10. Réciproquement, une suite finie de longueur $n+2$ de la forme $1\{S\}0$ contenant $2m+1$ passages 01 ou 10 donne lieu à une suite S de longueur n contenant exactement m fois le bloc 01. De telles suites sont au nombre de $\binom{n+1}{2m+1}$ car il y a $n+1$ possibilités pour choisir les emplacements des points de passage parmi les espaces intérieurs disponibles.

2ème solution. Comme dans la première solution, on commence par remarquer que toute suite finie contenant le bloc 01 exactement m fois est de la forme :

$$(11\ldots1)\underbrace{(0\ldots01\ldots1)\ldots(0\ldots01\ldots1)}_{m \text{ blocs.}}(00\ldots0).$$

La fonction génératrice du nombre de ces suites est alors

$$G(x) = (1 + x + x^2 + \cdots)\left[(x + x^2 + \cdots)\right]^m (1 + x + x^2 + \cdots)$$

qui se calcule directement $G(x) = x^{2m}(1-x)^{-2m-2}$.

Le nombre recherché est donc

$$N = a_n[G] = a_{n-2m}\left[(1-x)^{-2m-2}\right] = (-1)^{n-2m}\binom{-2m-2}{n-2m},$$

avec

$$\binom{-2m-2}{n-2m} = \frac{(-2m-2)(-2m-3)\ldots(-n-1)}{(n-2m)!} = (-1)^{n-2m}\binom{n+1}{n-2m},$$

d'où finalement

$$N = \binom{n+1}{n-2m} = \binom{n+1}{2m+1}.$$

---

17. a) Soit n un entier impair $\geqslant 2$, et supposons qu'il existe une matrice d'argent à n lignes et n colonnes. On va montrer qu'alors tout nombre $x = 1, 2, \ldots, 2n-1$ doit apparaître au moins une fois sur la diagonale de la matrice A : en effet, fixons un nombre $x \in \{1, 2, \ldots, 2n-1\}$ et désignons par A_k, $k = 1, 2, \ldots, n$, l'ensemble de la k-ième ligne et de la k-ième colonne. Il y a un x dans chaque A_k, $k = 1, 2, \ldots, n$, soit au total (avec répétition) n. D'un autre côté, si aucun x n'est situé sur la diagonale de A, tout x appartient à deux A_k. Comme n est impair, ceci ne peut se réaliser.

Ainsi, tout $x \in \{1, 2, \ldots, 2n-1\}$ doit apparaître sur la diagonale de la matrice A, mais il n'y a que n positions possibles, d'où la contradiction.

b) Pour $n = 2$, la matrice

$$A_1 = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$$

est une matrice d'argent. Pour $n = 4$, la matrice

$$A_2 = \begin{pmatrix} 1 & 2 & 5 & 6 \\ 3 & 1 & 7 & 5 \\ 4 & 6 & 1 & 2 \\ 7 & 4 & 3 & 1 \end{pmatrix}$$

convient.

La construction de A_2 à partir de A_1 peut être généralisée : en effet, si A_k est une matrice $2^k \times 2^k$ qui est une matrice d'argent, alors on considère la matrice A_{k+1} à 2^{k+1} lignes et 2^{k+1} colonnes définie par :

$$A_{k+1} = \begin{pmatrix} A_k & B_k \\ C_k & A_k \end{pmatrix},$$

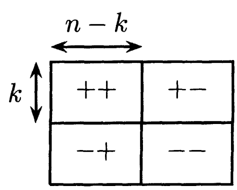
où B_k est la matrice obtenue en rajoutant à chaque élément de A_k le nombre 2^{k+1} et C_k est la matrice obtenue en substituant aux éléments de la diagonale de B_k le nombre 2^{k+1}. Il est alors immédiat que la matrice A_{k+1} est une matrice d'argent.

---

18. *Condition nécessaire*. On considère un tableau vérifiant les conditions de l'énoncé, et on désigne par l_i, c_j, $i, j = 1, 2, \ldots, n$, les sommes des éléments de la i-ième ligne et de la j-ième colonne respectivement. On a alors

$$\sum_{i=1}^{n} |l_i| + \sum_{j=1}^{n} |c_j| \geqslant \left(\sum_{k=-n}^{n} |k| \right) - n = n^2.$$

Comme il y a exactement une seule valeur de l'ensemble $\{-n, -n+1, \ldots, n\}$ qui n'est pas prise par les l_i et les c_j, on peut choisir n sommes positives ou nulles telles que les autres sommes soient négatives ou nulles. On réordonne alors les lignes et les colonnes de manière à placer dans les k premières lignes et les $n-k$ premières colonnes les sommes positives.



On a ainsi :

$$\sum_{i=1}^{n}|l_i|+\sum_{j=1}^{n}|c_j| \;=\; (l_1+\cdots+l_k)-(l_{k+1}+\cdots+l_n)+ (c_1+\cdots+c_{n-k})-(c_{n-k+1}+\cdots+c_n).$$

Dans la dernière somme, les éléments de type $++$ ou $--$ sont comptés deux fois, et les éléments de type $+-$ sont éliminés. On a donc

$$\sum_{i=1}^{n}|l_i|+\sum_{j=1}^{n}|c_j| \leqslant 2k(n-k)+2k(n-k)=4k(n-k),$$

d'où $(n-2k)^2 \leqslant 0$, c'est-à-dire $n=2k$, i.e. n est pair.

Condition suffisante. Pour montrer que la tâche peut être effectuée si n est pair, on peut raisonner par récurrence, ou même fournir une solution explicite. Une telle solution s'obtient en disposant des $+1$ en dessous de la diagonale principale, des -1 en dessus de la diagonale principale et en alternant $+1$ et 0 le long de la diagonale :

$$\begin{bmatrix} +1 & -1 & -1 & \cdots \\ +1 & 0 & -1 & \cdots \\ +1 & +1 & +1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Les sommes des éléments d'une même ligne sont donc : $4k-n-2, 4k-n-1$, $k=1,2,\ldots,n/2$, et les sommes des éléments d'une même colonne sont : $n-4k, n-4k-3$, $k=0,1,\ldots,n/2-1$. Ces deux familles de nombres recouvrent l'ensemble $\{-n,-n+1,\ldots,n\}$. (Les lignes donnent tous les nombres $\equiv n+2$ ou $n+3 \pmod 4$ et les colonnes donnent tous les nombres $\equiv n$ ou $n+1 \pmod 4$).

---

19. 1ère solution. *Condition nécessaire.* On construit un tableau à $2n$ lignes et $2n$ colonnes de la manière suivante : à l'intersection de la i-ième ligne et de la j-ième colonne on place le nombre, 0 ou 1, appartenant à $A_i \cap A_j$ si $i \neq j$, et le nombre, 0 ou 1, appartenant à $A_i \cap A_{2n+1}$ si $i=j$.

Le nombre total de zéros dans le dernier tableau est égal à $2n^2$ puisque chaque ligne en contient n. Par ailleurs, il y a n zéros sur la diagonale principale du tableau. Mais celui-ci est symétrique par rapport à cette diagonale. Il s'ensuit que $2n^2-n$ est pair, et donc que n est lui-même pair.

Condition suffisante. Il suffit de construire un tableau symétrique à $2n$ lignes et $2n$ colonnes avec n zéros dans chaque ligne et sur la diagonale principale : en effet, en prenant $B=\{(i,j) \mid 1 \leqslant i \leqslant j \leqslant 2n\}$, $A_i=\{(k,i) \mid k \leqslant i\} \cup \{(i,k) \mid k \geqslant i\}$, $i=1,2,\ldots,2n$ et enfin $A_{2n+1}=\{(i,i) \mid 1 \leqslant i \leqslant 2n\}$, on constate que la famille $(A_i)_i$ vérifie les conditions de l'énoncé.

Une solution possible est donnée par ailleurs ci-dessous :

$$\begin{bmatrix} 0 & 1 & 0 & 1 & \dots \\ 1 & 0 & 1 & 0 & \dots \\ 0 & 1 & 1 & 0 & \dots \\ 1 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

$2^{\text{ème}}$ solution. *Condition nécessaire.* On considère le graphe complet $\mathcal{G}_{2n+1}$ où les sommets représentent les ensembles A_i, $i = 1, 2, \dots, 2n+1$. On affecte à chacune des arêtes $\{A_i, A_j\}$ le nombre, 0 ou 1, appartenant à $A_i \cap A_j$, et on supprime ensuite toutes les arêtes affectées du nombre 1. Le degré de tout sommet dans le graphe résultant est alors n, et comme il y a un nombre impair de sommets, il s'ensuit que n doit être pair.

Condition suffisante. Comme $2n+1$ est impair, $\mathcal{G}_{2n+1}$ peut être décomposé en n cycles hamiltoniens disjoints. Si n est pair, choisissons $n/2$ cycles arbitraires parmi ces n cycles et affectons les arêtes de ces cycles du nombre 0, puis affectons les autres arêtes du nombre 1. Ainsi, chaque A_i contient exactement n éléments affectés de la valeur 0.

---

20. Appelons chaîne toute famille de sous-ensembles $B_1, B_2, \dots, B_i$ de l'ensemble $\{1, 2, \dots, M\}$ vérifiant $B_1 \subset B_2 \subset \dots \subset B_i$, les inclusions étant strictes. Une chaîne est dite maximale si elle a le plus grand nombre possible de sous-ensembles, soit M. Se donner une chaîne maximale équivaut à se donner une permutation $(x_1, x_2, \dots, x_M)$ de $\{1, 2, \dots, M\}$, à savoir $B_1 = \{x_1\}$, $B_2 \setminus B_1 = \{x_2\}, \dots,$ $B_M \setminus B_{M-1} = \{x_M\}$. Il y a donc $M!$ chaînes maximales. Observons alors que le caractère spernerien d'une famille $\mathcal{S}$ équivaut à ce que toute chaîne maximale $\mathcal{C}$ satisfasse à $|\mathcal{C} \cap \mathcal{S}| = 0$ ou 1. Par ailleurs, le nombre de chaînes maximales $B_1 \subset B_2 \subset \dots \subset B_M = \{1, 2, \dots, M\}$ telles que $|B_i| = i$, $i = 1, 2, \dots, M$ et $B_{a_k} = A_k$ est égal à $a_k!(M - a_k)!$. On a ainsi

$$a_1!(M - a_1)! + a_2!(M - a_2)! + \dots + a_s!(M - a_s)! \leqslant M!,$$

ce qui est équivalent à l'inégalité en question.

Note. Ce résultat permet de prouver un théorème dû à Emmanuel Sperner : le nombre maximum de blocs d'une famille de Sperner de $\{1, 2, \dots, M\}$ vaut $\dbinom{M}{\lfloor M/2 \rfloor}$.

En effet, si $\mathcal{S}$ est une famille spernerienne, on vient d'établir que

$$\sum_{B \in \mathcal{S}} \frac{1}{\dbinom{M}{|B|}} \leqslant 1.$$

Comme $\dbinom{M}{k} \leqslant \dbinom{M}{\lfloor M/2 \rfloor}$ pour tout $k \in \{0, 1, \dots, M\}$, il s'ensuit que

$$\sum_{B \in \mathcal{S}} \frac{1}{\dbinom{M}{|B|}} \geqslant \sum_{B \in \mathcal{S}} \frac{1}{\dbinom{M}{\lfloor M/2 \rfloor}} = \frac{|\mathcal{S}|}{\dbinom{M}{\lfloor M/2 \rfloor}},$$

ce qui donne $|S| \leqslant \binom{M}{\lfloor M/2 \rfloor}$. Ce majorant est atteint par la famille des parties à $\lfloor M/2 \rfloor$ éléments de $\{1, 2, \dots, M\}$, qui est évidemment spernerienne.

---

21. 1ère solution. Appelons une suite finie s de longueur n et à valeurs dans l'ensemble $\{0,1\}$ répétitive si, pour un entier positif d divisant n, s peut être divisée en d blocs identiques. Il est clair que toute suite finie de longueur n peut être reproduite en répétant son unique bloc non répétitif de longueur maximale.

On obtient ainsi une formule de récurrence pour le nombre de suites finies non répétitives de longueur n identique à celle de l'énoncé. Ainsi, a_n n'est autre que le nombre de suites finies non répétitives de longueur n.

La conclusion est alors une conséquence du fait qu'une suite finie non répétitive de longueur n produit n suites distinctes non répétitives qui se déduisent l'une de l'autre par permutation circulaire.

2ème solution. On raisonne par récurrence sur n. Pour $n = 1$, il n'y a rien à prouver. Supposons donc que $k \,|\, a_k$ pour $k < n$. Il suffit donc de prouver que si $p^\alpha \,|\, n$, où p est premier, alors $p^\alpha \,|\, a_n$. Posons $n = p^\alpha m$, où m n'est pas divisible par p. On a alors

$$2^n = \sum_{d|p^\alpha m} a_d = \sum_{d|p^{\alpha-1}m} a_d + \sum_{d|m} a_{p^\alpha d} = 2^{p^{\alpha-1}m} + a_{p^\alpha m} + \sum_{\substack{d|m \\ d<m}} a_{p^\alpha d},$$

ce qui donne

$$a_n = 2^{p^\alpha m} - 2^{p^{\alpha-1}m} - \sum_{\substack{d|m \\ d<m}} a_{p^\alpha d}.$$

Comme, par hypothèse de récurrence, $a_{p^\alpha d}$ est divisible par p^α pour $d < m$, il s'ensuit que

$$a_n \equiv 2^{p^{\alpha-1}m}\left(2^{p^{\alpha-1}(p-1)m} - 1\right) \pmod{p^\alpha}.$$

Si $p = 2$, alors $p^{\alpha-1}m \geqslant \alpha$, ce qui implique que $2^{p^{\alpha-1}m} \equiv 0 \pmod{p^\alpha}$.

Si par contre $p > 2$, alors le théorème d'Euler s'applique :

$$2^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha},$$

i.e.,

$$2^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha},$$

ce qui donne de nouveau $a_n \equiv 0 \pmod{p^\alpha}$.

---

22. Dans chacune des deux solutions proposées ici, la technique consiste à introduire une quantité que l'on dénombre de deux manières différentes. La deuxième solution montre cependant que la condition a) est superflue.

1ère solution. Soit l le nombre de triplets (A, B, C) tels que $A \neq B$ et $AC = BC$. La condition b) de l'énoncé implique que

$$l \geqslant 2n\binom{k}{2}.$$

Cependant, si l'on se donne deux points A et B de S, il existe au plus deux points C_1 et C_2 tels que (A, B, C_1) et (A, B, C_2) soient de tels triplets : en effet, s'il y avait un autre tel point C_3, les points C_1, C_2, C_3 seraient alignés et la condition a) ne serait plus respectée. On a donc

$$l \leqslant 2n(n-1).$$

Il s'ensuit que $k^2 - k - 2(n-1) \leqslant 0$, ce qui donne

$$k \leqslant \frac{1+\sqrt{1+8(n-1)}}{2} < \frac{1}{2} + \frac{1}{2}\sqrt{8n} = \frac{1}{2} + \sqrt{2n}.$$

2ème solution. Soit l le nombre de segments déterminés par les n points considérés. On a alors

$$l = \binom{n}{2}.$$

D'un autre côté, si P est un point de S, alors la condition b) nous assure de l'existence d'un cercle de centre P contenant au moins k points de S. Ces points forment au moins $\binom{k}{2}$ segments. Puisque S contient n points, le nombre total de ces segments, comptés plusieurs fois éventuellement, est au moins $n\binom{k}{2}$.

Mais, un segment est compté plus d'une seule fois s'il est une corde commune à au moins 2 cercles. Comme il n'y a que n cercles, le nombre de cordes communes, comptées plusieurs fois éventuellement, ne dépasse pas $\binom{n}{2}$. On a ainsi

$$l \geqslant n\binom{k}{2} - \binom{n}{2},$$

ce qui mène de nouveau à

$$k^2 - k - 2(n-1) \leqslant 0.$$

Note. De tels ensembles existent bien : en effet, pour $k = 2$ par exemple, on peut prendre pour S les trois sommets d'un triangle équilatéral.

---

23. Supposons que les numéros de deux cases voisines quelconques diffèrent d'au plus $n - 1$. Pour $k = 1, 2, \ldots, n^2 - n$, soient A_k l'ensemble des cases numérotées à l'aide des éléments $1, 2, \ldots, k$, B_k l'ensemble des cases numérotées à l'aide des éléments $k + n, \ldots, n^2$ et C_k l'ensemble des cases restantes. Par l'hypothèse de départ, A_k et B_k n'ont pas de côté en commun ; C_k contient seulement $n-1$ cases. Par conséquent, il existe une ligne et une colonne de cases ne contenant aucune case de C_k, et donc une ligne et une colonne de cases appartenant toutes soit à A_k, soit à B_k.

Mais, cette situation n'est possible ni pour A_1, ni pour B_{n^2-n}. Ainsi, il existe un indice $k \in \{1, 2, \ldots, n^2-n-1\}$ tel que $B_1, B_2, \ldots, B_k$ contiennent chacun une ligne et une colonne de cases tandis que B_{k+1} ne possède pas cette propriété. Il s'ensuit que A_{k+1} contient une ligne et une colonne de cases et donc possède des cases en commun avec B_k, d'où la contradiction.

---

24. On note $S(X)$ et $P(X)$ respectivement la somme des carrés et le produit des éléments de l'ensemble fini X.

Il suffit de résoudre le problème pour $A = \{1, 2, \ldots, n\}$, $n \geqslant 1$. D'ailleurs, on supposera $n \geqslant 5$ de sorte que $S(A) < P(A)$. Si on rajoute à l'ensemble A suffisamment de nombres 1, on obtient une collection X de nombres entiers naturels non nuls telle que $S(X) = P(X)$.

Choisissons un 1 parmi les nombres 1 redondants. 1 est une racine du trinôme $x^2 - P(X)x + S(X) - 1 = 0$. Si on enlève le 1 sélectionné de la collection X et on met à sa place la deuxième racine de ce trinôme, à savoir $P(X) - 1$, on obtient une nouvelle collection X' telle que $S(X') = P(X')$ et contenant moins de redondances (il est clair que $P(X) - 1$ est trop grand, de sorte qu'on n'introduit pas ainsi de nouvelles redondances).

En répétant ce processus, on aboutit au bout d'un nombre fini d'opérations à un ensemble B qui convient.

---

25. Soient $A_1 = \{k \in S \mid 2 \text{ divise } k\}$, $A_2 = \{k \in S \mid 3 \text{ divise } k\}$, $A_3 = \{k \in S \mid 5 \text{ divise } k\}$, $A_4 = \{k \in S \mid 7 \text{ divise } k\}$ et $A = A_1 \cup A_2 \cup A_3 \cup A_4$. On a alors $|A_1| = 140$, $|A_2| = 93$, $|A_3| = 56$, $|A_4| = 40$. On calcule de même

$$\begin{gathered}
|A_1 \cap A_2| = 46, \quad |A_1 \cap A_3| = 28, \quad |A_1 \cap A_4| = 20, \\
|A_2 \cap A_3| = 18, \quad |A_2 \cap A_4| = 13, \quad |A_3 \cap A_4| = 8, \\
|A_1 \cap A_2 \cap A_3| = 9, \quad |A_1 \cap A_2 \cap A_4| = 6, \\
|A_1 \cap A_3 \cap A_4| = 4, \quad |A_2 \cap A_3 \cap A_4| = 2, \\
|A_1 \cap A_2 \cap A_3 \cap A_4| = 1.
\end{gathered}$$

Le principe d'inclusion et d'exclusion nous permet alors d'écrire

$$|A| = (140+93+56+40) - (46+28+20+18+13+8) + (9+6+4+2) - 1 = 216.$$

Il est clair que parmi 5 éléments quelconques appartenant à A, 2 au moins appartiennent à un même A_i $(1 \leqslant i \leqslant 4)$, et donc ne sont pas premiers entre eux. Il s'ensuit que $n > 216$.

Soit P l'ensemble de tous les nombres premiers appartenant à S (1 inclus). Chaque nombre composé appartenant à S est soit dans l'ensemble $A \setminus \{2, 3, 5, 7\}$, soit dans l'ensemble $\{11^2, 11\times 13, 11\times 17, 11\times 19, 11\times 23, 13^2, 13\times 17, 13\times 19\}$, ce qui donne $|P| = 280 - (212+8) = 60$.

Soit T un sous-ensemble de S à 217 éléments. On montre que T contient 5 nombres deux à deux premiers entre eux. Il est alors évident qu'il suffit de se restreindre au cas $|T\cap P| \leqslant 4$. On a alors $|T\cap (S\setminus P)| \geqslant 217-4 = 213$, i.e., parmi tous les nombres composés appartenant à S, il y a au plus 7 éléments qui ne sont pas dans T. Soient maintenant les ensembles $M_1, M_2, \ldots, M_8$ définis par :

$$\begin{aligned}
M_1 &= \{2\times 23, 3\times 19, 5\times 17, 7\times 13, 11\times 11\}\\
M_2 &= \{2\times 29, 3\times 23, 5\times 19, 7\times 17, 11\times 13\},\\
M_3 &= \{2\times 31, 3\times 29, 5\times 23, 7\times 19, 11\times 17\},\\
M_4 &= \{2\times 37, 3\times 31, 5\times 29, 7\times 23, 11\times 19\},\\
M_5 &= \{2\times 41, 3\times 37, 5\times 31, 7\times 29, 11\times 23\},\\
M_6 &= \{2\times 43, 3\times 41, 5\times 37, 7\times 31, 13\times 17\},\\
M_7 &= \{2\times 47, 3\times 43, 5\times 41, 7\times 37, 13\times 19\},\\
M_8 &= \{2^2, 3^2, 5^2, 7^2, 13^2\}.
\end{aligned}$$

Évidemment $M_i \subsetneq S\setminus P$, $i = 1, 2, \ldots, 8$. D'après le principe des tiroirs, il existe i_0, $1 \leqslant i_0 \leqslant 8$, tel que $M_{i_0} \subseteq T$. Les cinq éléments de M_{i_0} sont alors deux à deux premiers entre eux, d'où $n = 217$.

---

26. On désigne par $\mathcal{A}_m$ la famille des sous-ensembles de $\{1, 2, \ldots, m\}$ qui ne contiennent pas deux éléments i_1, i_2 tels que $|i_1 - i_2| = 1$. De plus, pour tout ensemble $A \in \mathcal{A}_m$, soit $a_{m,n,A}$ le nombre de sous-ensembles de $Z_{m,n}$ ne contenant pas de couples (i_1, j_1), (i_2, j_2) tels que

$$|i_1 - i_2| + |j_1 - j_2| = 1$$

et dont les seuls éléments de la forme (i, n) sont tels que $i \in A$.

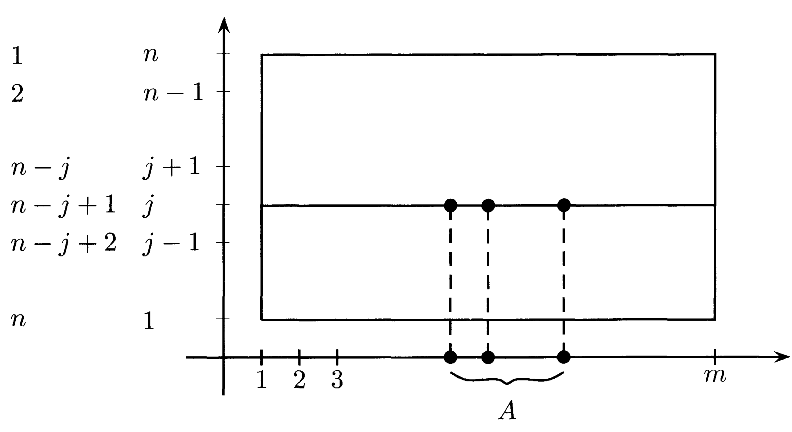


FIG. 5.17.

Il s'ensuit donc que, pour tout j tel que $1 \leqslant j \leqslant n$,

$$a_{m,n} = \sum_{A \in \mathcal{A}_m} a_{m,j,A} a_{m,n-j+1,A}.$$

En particulier, si $n = 2k$, $j = k$,

$$a_{m,2k} = \sum_{A \in \mathcal{A}_m} a_{m,k,A} a_{m,k-1,A},$$

si $n = 2k - 1$, $j = k$,

$$a_{m,2k-1} = \sum_{A \in \mathcal{A}_m} a_{m,k,A} a_{m,k,A}$$

et si $n = 2k + 1$, $j = k$,

$$a_{m,2k+1} = \sum_{A \in \mathcal{A}_m} a_{m,k+1,A} a_{m,k+1,A}.$$

D'après l'inégalité de Cauchy-Schwarz, il s'ensuit que $a_{m,2k}^2 \leqslant a_{m,2k-1} a_{m,2k+1}$.

---

27. Relions deux points de E s'il existe exactement n points sur l'un des deux arcs ouverts qu'ils définissent. Appelons cycle toute suite $(A_1, A_2, \ldots, A_r)$ de r points ($r \geqslant 3$) telle que A_i et A_{i+1} soient reliés par un segment pour $i = 1, 2, \ldots, r$, les indices étant pris modulo r. On se propose de démontrer que E est composé de cycles disjoints. En effet, soit A_1 un point de E et supposons construite une suite $(A_1, A_2, \ldots, A_r)$ telle que A_i et A_{i+1} soient reliés par un segment pour $i = 1, 2, \ldots, r-1$, et A_r soit relié à un point A_i, $1 \leqslant i \leqslant r-1$. Comme un point de E n'est l'extrémité que de deux segments, A_r ne peut être relié à un point autre que A_1. Il s'ensuit que A_1 appartient à un unique cycle de E.

Orientons le cercle, et notons les points de E dans le sens trigonométrique $A_1, A_2, \ldots, A_{2n-1}$. En prenant comme d'habitude les indices modulo $2n-1$, le cycle $\left(A_1, A_{1+(n+1)}, \ldots, A_{1+p(n+1)}\right)$ se referme sur A_1 pour un certain entier p. On a alors

$$p(n+1) = q(2n-1)$$

pour un certain $q \in \mathbb{N}$.

D'un autre côté, $l = (n+1, 2n-1) = (n+1, 3n) = 3$ ou 1. On distingue alors deux cas :

- $l = 1$, on a alors $p = 2n-1$, d'où un unique cycle. Comme l'ensemble $\{A_1, A_3, \ldots, A_{2n-1}\}$ ne contient aucune paire de points reliés entre eux, il s'ensuit que $k > n-1$. Mais tout sous-ensemble de $\{A_1, A_2, \ldots, A_{2n-1}\}$ à n éléments contient une paire de points reliés entre eux, ce qui implique que $k = n$.

- $l = 3$, on a alors $p = (2n-1)/3$, d'où trois cycles disjoints. Dans tout cycle, on peut choisir une partie à $\left\lfloor \left(\dfrac{2n-1}{3}\right) \Big/ 2 \right\rfloor$ éléments ne contenant aucune paire de points reliés entre eux. On a donc

$$k = 3 \left\lfloor \left(\frac{2n-1}{3}\right) \Big/ 2 \right\rfloor + 1 = n - 1.$$

Finalement, la plus petite valeur de k est $n-1$ ou n suivant que 3 divise ou ne divise pas $n+1$.

---

28. On dessine un graphe dont les sommets sont les entiers $1, 2, \ldots, n$, avec une arête entre x et y si et seulement si (x, y) ou (y, x) appartient à S. Le problème est alors de trouver une minoration du nombre de triangles contenus dans le graphe ainsi construit.

On note $d(x)$ le degré du sommet x. Si x et y sont reliés par une arête, alors $d(x) + d(y) - 2$ arêtes ont des extrémités parmi les $n-2$ autres sommets, et donc au moins $d(x) + d(y) - 2 - (n-2)$ sommets sont reliés à x et à y simultanément. Ainsi, au moins $d(x) + d(y) - n$ triangles contiennent à la fois x et y. Il s'ensuit que le nombre total de triangles est au moins

$$\sum_{(x,y)\in S} \frac{d(x) + d(y) - n}{3}$$

puisque chaque triangle est compté trois fois dans la somme précédente. Or,

$$\sum_{(x,y)\in S} [d(x) + d(y)] = \sum_{x=1}^{n} d(x)^2$$

car chaque $d(x)$ est compté $d(x)$ fois dans la dernière somme. Ainsi,

$$\sum_{(x,y)\in S} \frac{d(x) + d(y) - n}{3} = \frac{1}{3}\left[\sum_{x=1}^{n} d(x)^2 - nm\right],$$

et puisque

$$\sum_{x=1}^{n} d(x)^2 \geqslant \frac{1}{n}\left[\sum_{x=1}^{n} d(x)\right]^2,$$

il s'ensuit que

$$\sum_{(x,y)\in S} \frac{d(x) + d(y) - n}{3} \geqslant \frac{1}{3}\left[\frac{1}{n} \times (2m)^2 - nm\right] = \frac{4m(m - n^2/4)}{3n}.$$

---

29. $1^{\text{ère}}$ solution. Pour chaque $i \in \{1, 2, \ldots, n\}$, notons A_i l'ensemble des permutations de $\{1, 2, \ldots, 2n\}$ où i et $i+n$ occupent des positions voisines. L'ensemble $A = \bigcup_{i=1}^{n} A_i$ est l'ensemble des permutations de $\{1, 2, \ldots, 2n\}$ ayant la propriété P. Le principe d'inclusion et d'exclusion nous permet d'écrire

$$|A| = \sum_{i=1}^{n} |A_i| - \sum_{1\leqslant i<j\leqslant n} |A_i \cap A_j| + \cdots$$

Une récurrence sur le nombre des ensembles considérés permet d'établir la majoration $|A| \leqslant \sum_{i=1}^{n} |A_i|$. De même, on peut obtenir la minoration

$$|A| \geqslant \sum_{i=1}^{n} |A_i| - \sum_{1\leqslant i<j\leqslant n} |A_i \cap A_j|.$$

Il y a exactement $2(2n-1)$ possibilités pour placer i et $i+n$ dans des emplacements voisins. Pour chacune de ces possibilités, il y a $(2n-2)!$ permutations de l'ensemble $\{1, 2, \ldots, 2n\}$ maintenant i et $i+n$ dans les emplacements fixés. Ainsi $|A_i| = 2(2n-1)!$, $i = 1, 2, \ldots, n$.

Maintenant, il s'agit de déterminer $|A_i \cap A_j|$ pour i, j tels que $1 \leqslant i < j \leqslant n$. Il est clair que les premiers à apparaître dans la permutation $(x_1, x_2, \ldots, x_{2n})$ parmi i et $i+n$ d'une part, et j et $j+n$ d'autre part ne peuvent pas avoir des emplacements voisins. Supposons d'abord que i précède $i+n$, et que j précède $j+n$. Les couples d'indices (i, j) tels que $j > i+1$ et $j \leqslant 2n-1$ sont au nombre de

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

On a donc $(2n-3)(2n-2)$ manières de placer i et j conformément aux restrictions précédentes. À chacun de ces cas correspondent $(2n-4)!$ permutations de l'ensemble $\{1, 2, \ldots, 2n\}$. En tenant compte des cas où l'ordre de i et $i+n$, ou de j et $j+n$ est inversé, on obtient $|A_i \cap A_j| = 2 \times 2 \times (2n-2)! = 2^2(2n-2)!$, $(i, j) \in \{1, 2, \ldots, n\}^2$, $i < j$.

On a donc finalement

$$|A| \geqslant \sum_{i=1}^{n} 2(2n-1)! - \sum_{1 \leqslant i < j \leqslant n} 2^2(2n-2)! = (2n)! - \binom{n}{2} 2^2(2n-2)! > \frac{(2n)!}{2}.$$

Comme le nombre de permutations de $\{1, 2, \ldots, 2n\}$ est égal à $(2n)!$, il apparaît qu'il y a plus de permutations possédant la propriété P que de permutations ne la possédant pas.

2$^{\text{ème}}$ solution. Deux éléments distincts $x, y \in \{1, 2, \ldots, 2n\}$ seront dits jumeaux si $|x-y| = n$. Une permutation $(x_1, x_2, \ldots, x_{2n})$ de $\{1, 2, \ldots, 2n\}$ (ou, plus généralement, d'un ensemble à $2n$ éléments composé de n paires de jumeaux) est dite de type T_k si $|x_i - x_{i+1}| = n$ se produit exactement k fois. On note alors $F_k(n)$ le nombre de permutations de $\{1, 2, \ldots, 2n\}$ de type T_k.

Soit $(x_1, x_2, \ldots, x_{2n})$ une permutation de type T_0. On supprime x_{2n} et son jumeau. Ce qui reste est alors une permutations de $2n-2$ éléments ($n-1$ paires de jumeaux), qui est de type T_0 ou de type T_1. Puisque x_{2n} peut prendre $2n$ valeurs et puisque, dans le premier cas, son jumeau peut occuper $2n-2$ positions, tandis que dans le deuxième cas, la position du jumeau est déterminée par la permutation de type T_1 obtenue, on a la relation de récurrence qui suit :

$$F_0(n) = 2n\big[(2n-2)F_0(n-1) + F_1(n-1)\big]. \tag{1}$$

Maintenant, soit $(x_1, x_2, \ldots, x_{2n})$ une permutation de type T_1 et soit (x_j, x_{j+1}) l'unique paire de jumeaux adjacents. On supprime cette paire pour ainsi obtenir une permutation de $2n-2$ éléments ($n-1$ paires de jumeaux), qui est de type T_0 ou de type T_1. Un raisonnement analogue au précédent nous conduit à la deuxième relation de récurrence :

$$F_1(n) = 2n\big[(2n-1)F_0(n-1) + F_1(n-1)\big]. \tag{2}$$

En soustrayant (1) de (2), on obtient

$$F_1(n) = F_0(n) + 2nF_0(n-1)$$

et en remplaçant dans (1), on aboutit à

$$F_0(n) = 2n\big[(2n-1)F_0(n-1) + (2n-2)F_0(n-2)\big].$$

En posant $P(n) = F_0(n)/(2n)!$, la dernière relation se réécrit

$$P(n) = P(n-1) + \frac{P(n-2)}{(2n-3)(2n-1)},$$

soit encore

$$P(n) - P(n-1) < \frac{1}{(2n-3)(2n-1)} = \frac{1}{2}\left(\frac{1}{2n-3} - \frac{1}{2n-1}\right).$$

Puisque $P(1) = 0$, on obtient

$$P(n) = \sum_{k=2}^{n}\big[P(k) - P(k-1)\big] < \frac{1}{2}\left(1 - \frac{1}{2n-1}\right) < \frac{1}{2},$$

d'où le résultat.

3$^{\text{ème}}$ solution. La solution suivante, due à un candidat chinois, a le mérite d'éviter tous les calculs.

Le cas $n = 1$ est trivial. Supposons $n \geqslant 2$. Soit A (resp. B) l'ensemble des permutations de $\{1, 2, \ldots, 2n\}$ ne possédant pas (resp. possédant) la propriété P. Pour montrer que $|B| > |A|$, il suffit de construire une injection $f\colon A \to B$ qui ne soit pas surjective.

Soit $\alpha = (x_1, x_2, \ldots, x_{2n})$ un élément de A. Comme α ne possède pas la propriété P, le jumeau de x_1 (l'élément x_i tel que $|x_i - x_1| = n$) est x_r avec $3 \leqslant r \leqslant 2n$. Maintenant on pose

$$f(\alpha) = (x_2, x_3, \ldots, x_{r-1}, x_1, x_r, x_{r+1}, \ldots, x_{2n}).$$

L'application $f\colon A \to B$ est bien définie. Montrons qu'elle est injective. Soient $\alpha = (x_1, x_2, \ldots, x_{2n})$, $\beta = (y_1, y_2, \ldots, y_{2n})$ deux éléments de A où le jumeau de x_1 est x_r et celui de y_1 est y_s, où $3 \leqslant r, s \leqslant 2n$. On suppose que $f(\alpha) = f(\beta)$, i.e.,

$$(x_2, x_3, \ldots, x_{r-1}, x_1, x_r, \ldots, x_{2n}) = (y_2, y_3, \ldots, y_{s-1}, y_1, y_s, \ldots, y_{2n}).$$

Comme $\{x_1, x_r\}$ (resp. $\{y_1, y_s\}$) est l'unique paire de jumeaux dans $f(\alpha)$ (resp. $f(\beta)$), on doit avoir $r = s$, $x_1 = y_1$ et $x_r = y_r$, ce qui implique aussi $x_i = y_i$ pour tout $i = 1, 2, \ldots, 2n$, d'où l'injectivité.

D'un autre côté, il est clair que f n'est pas surjective car B contient des permutations possédant plusieurs paires de jumeaux tandis que $f(A)$ ne contient que des permutations avec une unique paire de jumeaux, ce qui achève la démonstration.

---

30. Remarquons d'abord que l'on peut supposer $(p, q) = 1$: en effet, si $p = p'd$ et $q = q'd$ avec $(p', q') = 1$, on pose $X_i = x_i/d$. Les nombres X_i, $i = 0, 1, \ldots, n$, sont alors des entiers, et on a $X_{i+1} - X_i = p'$ ou $X_i - X_{i+1} = q'$.

Posons maintenant $\Delta_{i+1} = x_{i+1} - x_i$ $(i = 0, 1, \ldots, n-1)$, ce qui donne $\Delta_i = p$ ou $\Delta_i = -q$, et si l'égalité $\Delta_i = p$ se produit k fois alors

$$\begin{aligned} x_n - x_0 &= (x_n - x_{n-1}) + (x_{n-1} - x_{n-2}) + \cdots + (x_1 - x_0) \\ &= \Delta_n + \Delta_{n-1} + \cdots + \Delta_1 = kp - (n-k)q. \end{aligned}$$

Ainsi, $kp = (n-k)q$, et il s'ensuit qu'il existe $m \in \mathbb{N}$ tel que $k = mq$ et $n - k = mp$, ce qui donne $n = m(p+q)$, avec $m > 1$ puisque $n > p + q$.

Étudions le problème dans une grille rectangulaire $(qm) \times (pm)$ comme dans la figure 5.18. :

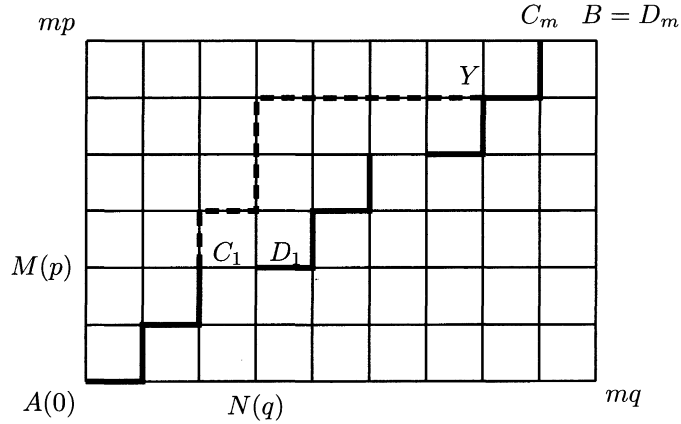


FIG. 5.18.

On commence au point A, et on se déplace d'une unité vers la droite si $\Delta_i = p$, et d'une unité vers le haut si $\Delta_i = -q$. À la fin, on aura effectué pm déplacements vers le haut et qm déplacements vers la droite, ce qui nous mènera au point B.

Maintenant, considérons le point X où la courbe de mouvement sur la grille rectangulaire recoupe le rectangle AMD_1N pour la première fois :

- Si $X = D_1$ alors $x_{p+q} = \Delta_{p+q} + \Delta_{p+q-1} + \cdots + \Delta_1 + x_0 = p \times (-q) + q \times (+p) + x_0 = x_0$ et le problème est résolu.

- Si $X = C_1$ appartient au côté $[MD_1]$ du rectangle, alors on considère les translatés D_1D_2, $D_2D_3, \ldots$, $D_{m-1}B$ du rectangle AD_1. On aura ainsi une courbe discontinue représentée en gras dans la figure ci-dessus. La courbe réelle du mouvement (celle représentée avec des pointillés) qui est en dessus de la courbe en gras au début passera de l'autre côté de la courbe pour pouvoir finir en B. Si on rajoute à la courbe en gras les segments $[C_1D_1], [C_2D_2], \ldots, [C_mD_m]$, alors le théorème des valeurs intermédiaires nous assure de l'existence d'un point commun à cette courbe et à la courbe réelle du mouvement. Soit Y le premier point où ces deux courbes se recoupent.

Si Y appartient à un des segments $[C_iD_i]$, $i = 1, 2, \ldots, m$, et $Y \neq C_i, D_i$, alors le point de $[C_iD_i]$ situé avant Y n'appartient pas à la courbe réelle du mouvement qui a donc rejoint Y après un déplacement $[ZY]$ vers le haut, mais alors cette courbe qui était en dessus de la nouvelle courbe en C_1 est devenue en dessous de cette même courbe en Z, ce qui contredit l'hypothèse de minimalité imposée à Y. Ainsi, Y appartient à la courbe initiale représentée en gras.

Si Y est l'image d'un point Y_0 à l'intérieur du rectangle AMD_1N, alors il existe $t \in \mathbb{N}$ tel que $x(Y) - x(Y_0) = tq$ et $y(Y) - y(Y_0) = tp$, ce qui implique que si Y_0 représente x_i alors Y représente $x_{i+t(p+q)}$, et on a

$$x_{i+t(p+q)} = \Delta_{i+t(p+q)} + \cdots + \Delta_{i+1} + x_i = tp \times (-q) + tq \times (+p) + x_i = x_i$$

et le problème est encore résolu puisque $i + t(p+q) \neq n$.

- Le cas où X appartient au côté $[ND_1]$ du rectangle AMD_1N se traite de manière identique.

---

31. 1$^{\text{ère}}$ solution. Si $n = 2k+1$ est un entier impair > 1. Toute représentation de n contient au moins un « 1 ». En supprimant ce dernier, on se retrouve avec une représentation de $2k$. Réciproquement, en adjoignant un « 1 » à une représentation de $2k$, on obtient une représentation de $2k+1$. Cette correspondance étant bijective, on obtient la formule :

$$f(2k+1) = f(2k), \quad k = 1, 2, \ldots \tag{1}$$

D'un autre côté, si $n = 2k$ est un entier pair > 0, alors on peut partitionner l'ensemble des représentations de n en deux sous-ensembles : celles contenant un « 1 » au moins une fois, et celles ne contenant aucun « 1 ». Il y a $f(2k-1)$ représentations du premier type. Par ailleurs, une représentation du deuxième type peut être associée à la représentation de k obtenue en divisant tous les sommants par 2 et cette correspondance est bijective. On obtient donc la deuxième relation de récurrence :

$$f(2k) = f(2k-1) + f(k), \quad k = 1, 2, \ldots \tag{2}$$

On en déduit que f est croissante et que :

$$f(2k) - f(2k-2) = f(k), \quad k = 1, 2, \ldots,$$

avec la convention $f(0) = 1$, ce qui implique que :

$$f(2n) = f(0) + f(1) + \cdots + f(n), \quad n = 1, 2, \ldots$$

La majoration demandée est facile à obtenir : on a par croissance de f,

$$f(2^n) = f(2^{n-1}) + f(2^{n-1} - 1) + \cdots + f(2) + f(2) < 2^{n-1} f(2^{n-1}), n \geqslant 3,$$

ce qui donne

$$f(2^n) < 2^{n-1} \times 2^{n-2} \times \cdots \times 2^1 \times f(2) = 2 \times 2^{n(n-1)/2}.$$

La majoration en découle aussitôt puisque $2 \times 2^{n(n-1)/2} < 2^{n^2/2}$ pour $n \geqslant 3$.

Passons maintenant à la minoration : on commence d'abord par remarquer que si m et n sont de même parité, alors :

$$f(m+1) - f(m) \leqslant f(n+1) - f(n)$$

si $m \leqslant n$. Il s'ensuit que

$$f(2^n + 2k) - f(2^n) \geqslant f(2^n + 1) - f(2^n - 2k + 1),$$

i.e.,

$$f(2^n + 2k) + f(2^n - 2k) \geqslant 2f(2^n),$$

pour tous $n, k \in \mathbb{N}$ tels que $2k \leqslant 2^n$.

On en déduit que pour $n \geqslant 3$:

$$\begin{aligned} f(2^n) = f(2^{n-1}) + f(2^{n-1} - 1) + \cdots + f(1) + f(0) &\geqslant 2 \times 2 \times 2^{n-3} f(2^{n-2}) \\ &= 2^{n-1} f(2^{n-2}), \end{aligned}$$

mais cette estimation reste valable pour $n = 2$.

Il s'ensuit que :

$$f(2^n) > \begin{cases} 2^{n-1} \times 2^{n-3} \times \cdots \times 2^1 \times f(2^0) = 2^{n^2/4} & \text{si } n \text{ est pair,} \\ 2^{n-1} \times 2^{n-3} \times \cdots \times 2^2 \times f(2^1) > 2^{n^2/4} & \text{si } n \text{ est impair,} \end{cases}$$

et on remarque que cette minoration reste valable pour $n \geqslant 1$.

2ème solution. Cette solution fait appel à des notions avancées d'analyse. Cependant, elle a le mérite de fournir un meilleur encadrement ainsi que de pouvoir se généraliser à des entiers autres que les puissances de 2.

Le problème revient à dénombrer les solutions $(x_0, x_1, \ldots, x_n) \in \mathbb{N}^{n+1}$ de l'équation $x_0 + 2x_1 + \cdots + 2^n x_n = 2^n$, ou, ce qui revient au même, les solutions $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ de l'inéquation $2x_1 + 2^2 x_2 + \cdots + 2^n x_n \leqslant 2^n$.

Oublions pour le moment l'unique solution pour laquelle $x_n = 1$, et associons à chaque $(n-1)$-uplet $(x_1, x_2, \ldots, x_{n-1}) \in \mathbb{N}^{n-1}$ tel que $2x_1 + 2^2 x_2 + \cdots + 2^{n-1} x_{n-1} \leqslant 2^n$ l'hypercube $\{(y_1, y_2, \ldots, y_{n-1}) \in \mathbb{R}^{n-1} \mid \forall i \in \{1, 2, \ldots, n-1\},\ x_i \leqslant y_i \leqslant x_i + 1\}$. On cherche donc à encadrer la somme des volumes de ces hypercubes. Or, celle-ci est encadrée par les volumes des domaine $\Gamma_1 = \{(y_1, y_2, \ldots, y_{n-1}) \in \mathbb{R}^{n-1} \mid \sum_{i=1}^{n-1} 2^i y_i \leqslant 2^n\}$ et $\Gamma_2 = \{(y_1, y_2, \ldots, y_{n-1}) \in \mathbb{R}^{n-1} \mid \sum_{i=1}^{n-1} 2^i (y_i - 1) \leqslant 2^n\}$.

Or, la formule de Fubini permet de calculer le volume d'un domaine $\Lambda_n = \{(y_1, y_2, \ldots, y_n) \in \mathbb{R}^n \mid \sum_{i=1}^{n} a_i y_i \leqslant A\}$, $a_1, a_2, \ldots, a_n$, $A \in \mathbb{R}_+^*$. En étudiant les cas $n = 1, 2$, on conjecture, ce que l'on vérifie par récurrence, que le volume de Λ_n vaut $\dfrac{1}{n!} \dfrac{A^n}{a_1 a_2 \cdots a_n}$.

Il s'ensuit que

$$1+\frac{2^{n(n-1)/2}}{(n-1)!} \leqslant f(2^n) \leqslant 1+\frac{\left(2^{n+1}-2\right)^{n-1}}{2^{n(n-1)/2}(n-1)!} < 1+\frac{2^{n(n+1)/2}}{2(n-1)!},$$

ce qui est, dans le cas où $n \geqslant 8$, un meilleur encadrement que celui que l'on demande.

De plus, pour tout entier A compris entre 2^{n-1} et $2^n - 1$, on a :

$$\frac{1}{(n-1)!}\frac{A^{n-1}}{2^{n(n-1)/2}} \leqslant f(A) \leqslant \frac{1}{(n-1)!}\frac{(2^n+2-A)^{n-1}}{2^{n(n-1)/2}}.$$

Note. Géza Kos, ex-candidat hongrois aux olympiades internationales, propose la généralisation suivante : il existe des constantes positives a et b telles que pour tout entier $n \geqslant 1$:

$$2^{n^2/2-n\ln(n)-an} \leqslant f(2^n) \leqslant 2^{n^2/2-n\ln(n)+bn}.$$

---

32. Il est clair que, si deux points quelconques sont reliés par une arête, il y a au total $\binom{9}{2} = 36$ arêtes. Par ailleurs, si on considère un sous-graphe contenant 33 arêtes, on peut choisir 6 points reliés entre eux deux à deux : en effet, on peut choisir 3 points distincts qui soient extrémités des trois arêtes manquantes. Les six autres points sont alors deux à deux reliés entre eux. Le nombre de Ramsey $R(3,3) = 6$ est bien connu. Il s'ensuit que le sous-graphe considéré contient au moins un triangle monochromatique, et donc $n \leqslant 33$.

On se propose de construire un exemple de sous-graphe contenant 32 arêtes sans aucun triangle monochromatique. On commence avec le graphe complet $\mathcal{G}_5$. Il est facile de le colorier à l'aide de deux couleurs sans que la figure obtenue contienne de triangles monochromatiques.

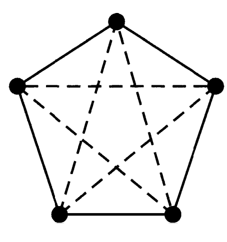


Fig. 5.19.

Maintenant, on part d'un graphe $\mathcal{H}$ sans aucun triangle monochromatique et on applique la construction suivante : on choisit un sommet A du graphe $\mathcal{H}$ et on rajoute un nouveau sommet B.

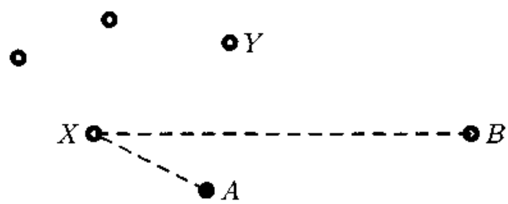


FIG. 5.20.

On relie B à tous les sommets de $\mathcal{H}$ à l'exception de A, et on colorie BX avec la même couleur de AX. Le nouveau triangle BXY n'est pas monochromatique car le triangle AXY ne l'était pas. En appliquant cette construction quatre fois à $\mathcal{G}_5$:

$$\mathcal{G}_5 \longrightarrow \mathcal{G}_6 \longrightarrow \mathcal{G}_7 \longrightarrow \mathcal{G}_8 \longrightarrow \mathcal{G}_9,$$

on obtient un sous-graphe de $\mathcal{G}_9$ contenant $10 + 4 + 5 + 6 + 7 = 32$ arêtes, et sans aucun triangle monochromatique. Concrètement, on peut donner l'exemple suivant :

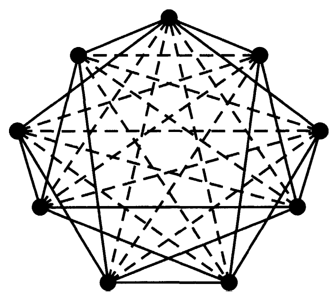


FIG. 5.21.

Le nombre minimal satisfaisant les conditions de l'énoncé est donc $n = 33$.

---

33. 1ère solution. Le choix d'un sous-ensemble à p éléments de $\{1, 2, \ldots, 2p\}$ dont la somme est $\equiv 0 \pmod p$ est équivalent au choix de q éléments de $\{1, 2, \ldots, p\}$ dont la somme est $\equiv r \pmod p$ et de $p - q$ éléments de $\{p+1, p+2, \ldots, 2p\}$ dont la somme est $\equiv -r \pmod p$.

Si on note $R_\alpha(\beta)$ le nombre de sous-ensembles à α éléments de $\{0, 1, \ldots, p-1\}$ dont la somme est $\equiv \beta \pmod p$, le problème est alors de trouver

$$S = \sum_{q=0}^{p} \sum_{r=0}^{p-1} R_q(r) R_{p-q}(-r).$$

Comme la somme des éléments de $\{0, 1, \ldots, p-1\}$ est $\equiv 0 \pmod p$, il s'ensuit que $R_q(r) = R_{p-q}(-r)$. On a donc

$$S = \sum_{q=0}^{p} \sum_{r=0}^{p-1} R_q(r)^2.$$

Le cas où $q = 0$ ou $q = p$ est trivial : on a $R_q(0) = 1$ et $R_q(r) = 0$ pour $1 \leqslant r \leqslant p-1$. Il s'ensuit que :

$$S = 2 + \sum_{q=1}^{p-1} \sum_{r=0}^{p-1} R_q(r)^2.$$

On se propose de démontrer que pour $1 \leqslant q \leqslant p-1$, $R_q(r) = R_q(0)\ \forall r$. Étant donné un sous-ensemble à q éléments de $\{0, 1, \ldots, p-1\}$ dont la somme est $\equiv 0 \pmod p$, on cherche à construire un ensemble de q entiers consécutifs dont la somme serait $\equiv r \pmod p$. Une idée qui semble naturelle serait de décaler tous les éléments de l'ensemble considéré d'une constante A/q où A est un multiple de q et où $A \equiv r \pmod p$. Or, une telle constante existe d'après le théorème chinois. Réciproquement, étant donné un sous-ensemble à q éléments de $\{0, 1, \ldots, p-1\}$ dont la somme est $\equiv r \pmod p$, on obtient un sous-ensemble à q éléments de $\{0, 1, \ldots, p-1\}$ dont la somme est $\equiv 0 \pmod p$ en retranchant A/q de chaque élément (et en réduisant modulo p). On a donc finalement

$$S = 2 + p \sum_{q=1}^{p-1} R_q(0)^2.$$

D'un autre côté, $R_q(0) + R_q(1) + \cdots + R_q(p-1) = \binom{p}{q}$, d'où $p\, R_q(0) = \binom{p}{q}$. On a finalement :

$$S = 2 + \frac{1}{p}\Big\{ \binom{2p}{p} - 2 \Big\},$$

où l'on a utilisé l'identité de Vandermonde.

2ème solution. On considère le polynôme de deux variables

$$F(x, y) = \prod_{j=1}^{2p} (1 + xy^j).$$

Le coefficient de $x^a y^b$ dans le développement de $F(x, y)$ est le nombre de sous-ensembles à a éléments de $\{1, 2, \ldots, 2p\}$ dont la somme des éléments est b. Le nombre N recherché peut donc s'écrire

$$N = \sum_{\sigma \equiv 0 \pmod p} [x^p y^\sigma] F(x, y),$$

où $[x^p y^\sigma] F(x, y)$ est le coefficient de $x^p y^\sigma$ dans le développement de $F(x, y)$. Il ne reste plus qu'à trouver une expression explicite de N. D'après la formule de multisection, on déduit que

$$N = a_p \Big[\frac{1}{p} \sum_{j=0}^{p-1} F(x, \omega^j) \Big],$$

où $\omega = e^{2i\pi/p}$. On a ainsi

$$\begin{aligned} N &= a_p\Big[\frac{1}{p}\sum_{j=0}^{p-1}(1+x\omega^j)(1+x\omega^{2j})\cdots(1+x\omega^{2pj})\Big] \\ &= a_p\Big[\frac{1}{p}\sum_{j=0}^{p-1}(1+x)^2(1+x\omega^j)^2\cdots(1+x\omega^{(p-1)j})^2\Big]. \end{aligned}$$

Mais puisque $(1, \omega^j, \omega^{2j}, \ldots, \omega^{(p-1)j})$ est une permutation de l'ensemble $\{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$ pour $j = 1, 2, \ldots, p-1$ (car p est premier), il s'ensuit que

$$N = a_p\Big[\frac{1}{p}\left[(1+x)^{2p} + (p-1)(1+x^p)^2\right]\Big]$$

car $(1+x)(1+\omega x)\cdots(1+\omega^{p-1}x) = 1+x^p$. On a donc finalement

$$N = \frac{1}{p}\Big\{\binom{2p}{p} + 2(p-1)\Big\} = \frac{1}{p}\Big\{\binom{2p}{p} - 2\Big\} + 2.$$

Note. Un candidat américain, Jacob Lurie, a eu le courage (et le temps!) pendant l'épreuve pour établir une généralisation intéressante : si n est un entier strictement positif quelconque, alors le nombre de sous-ensembles de $\{1, 2, \ldots, 2n\}$ à n éléments dont la somme est divisible par n est donné par la formule :

$$\frac{(-1)^n}{n}\sum_{d\,|\,n}\varphi\Big(\frac{n}{d}\Big)\binom{2d}{d}(-1)^d.$$

En effet, N est toujours donné par la formule :

$$N = a_n\Big[\frac{1}{n}\sum_{j=0}^{n-1}(1+x)^2(1+x\omega^j)^2\cdots(1+x\omega^{(n-1)j})^2\Big],$$

où $\omega = e^{2i\pi/n}$.

Pour tout j, $0 \leqslant j \leqslant n-1$, il existe un plus petit entier $k > 0$ tel que $\omega^{jk} = 1$. Cet entier est appelé l'ordre de ω^j et vaut $\delta = \dfrac{n}{d}$, où $d = (n, j)$. Ceci étant, on a

$$(1+x)^2(1+x\omega^j)^2\cdots(1+x\omega^{(n-1)j})^2 = \Big[\underbrace{(1+x)(1+x\omega^j)\cdots(1+x\omega^{(\delta-1)j})}_{=1+x^\delta(-1)^{\delta-1}}\Big]^{2d}.$$

Pour chaque diviseur d de n, il existe $\varphi\Big(\dfrac{n}{d}\Big)$ entiers j compris entre 0 et $n-1$ tels que $(n, j) = d$, et il s'ensuit que

$$N = \frac{1}{n}\sum_{d\,|\,n}\varphi\Big(\frac{n}{d}\Big)\binom{2d}{d}(-1)^{\delta d-d} = \frac{(-1)^n}{n}\sum_{d\,|\,n}\varphi\Big(\frac{n}{d}\Big)\binom{2d}{d}(-1)^d.$$

$3^{\text{ème}}$ **solution.** Cette solution a valu un prix spécial à Nikolay Nikolov, candidat bulgare participant alors pour la quatrième fois aux olympiades internationales.

On pose $\omega = e^{2i\pi/p}$. On a alors :

$$\prod_{k=1}^{2p}(x-\omega^k) = (x^p-1)^2 = x^{2p} - 2x^p + 1.$$

On définit maintenant la quantité :

$$t(\omega) = \sum_{1\leqslant j_1<j_2<\cdots<j_p\leqslant 2p} \omega^{j_1}\omega^{j_2}\cdots\omega^{j_p}.$$

On a donc $t(\omega) = 2$. Par ailleurs, si l'on écrit $t(\omega) = \sum a_j\omega^j$, alors a_j représente le nombre de sous-ensembles $\{j_1, j_2, \ldots, j_p\}$ de $\{1, 2, \ldots, 2p\}$ tels que $j_1+j_2+\cdots+j_p \equiv j \pmod p$, et on peut écrire :

$$(a_0-2) + a_1\omega + \cdots + a_{p-1}\omega^{p-1} = 0.$$

Comme le polynôme minimal de ω sur $\mathbb{Q}[X]$ est $1+x+\cdots+x^{p-1}$, il s'ensuit que

$$a_0 - 2 = a_1 = a_2 = \cdots = a_{p-1}.$$

Comme par ailleurs $a_0 + a_1 + \cdots + a_{p-1} = \binom{2p}{p}$, on conclut immédiatement que :

$$a_0 = \frac{1}{p}\left\{\binom{2p}{p} - 2\right\} + 2.$$

Note. On dit qu'un nombre $a \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ s'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(a) = 0$. Si tel est le cas, on appelle polynôme minimal de a sur $\mathbb{Q}[X]$ le polynôme unitaire de $\mathbb{Q}[X]$ de degré minimal annulant a.

Tout polynôme non nul de $\mathbb{Q}[X]$ dont a est une racine est alors divisible par ce polynôme (ceci découle de la condition de minimalité imposée au degré du polynôme minimal).

Dans notre cas, il s'agit de prouver que le polynôme minimal de $\omega = e^{2i\pi/p}$ sur $\mathbb{Q}[X]$ est $P(x) = 1+x+\cdots+x^{p-1}$. Remarquons tout de suite que ω est racine de ce polynôme. Il suffit donc de prouver que ce polynôme est irréductible dans $\mathbb{Q}[X]$ [10].

---

10. Ceci a été déjà vu en page 88.

6

GÉOMÉTRIE

Si ce chapitre est là, c'est parce qu'on a voulu que ce livre puisse servir d'outil complet de préparation aux olympiades internationales où la géométrie est omniprésente. En fait, le passage en revue de tous les éléments de géométrie plane rencontrés au collège et au lycée nécessiterait un volume équivalent à celui de ce livre. Il ne s'agit donc pas ici d'un cours à proprement parler mais plutôt d'un rappel de certains théorèmes et résultats pouvant s'avérer indispensables pour résoudre les problèmes d'olympiades.

6.1. Formules fondamentales dans un triangle

Soit ABC un triangle. On note $a = BC$; $b = CA$; $c = AB$; $\widehat{A} = \widehat{CAB}$; $\widehat{B} = \widehat{ABC}$; $\widehat{C} = \widehat{BCA}$.

6.1.1. Théorème. *(Loi des sinus) Si R désigne le rayon du cercle circonscrit au triangle ABC alors :*

$$\frac{a}{\sin \widehat{A}} = \frac{b}{\sin \widehat{B}} = \frac{c}{\sin \widehat{C}} = 2R. \tag{6.1}$$

♦ **Preuve.** Soit $\mathcal{C}$ le cercle circonscrit au triangle ABC. Si $\widehat{A} = 90°$, alors $[BC]$ est un diamètre de $\mathcal{C}$, et on a $a = 2R$. Si $\widehat{A} \neq 90°$, considérons le point D diamétralement opposé de B sur $\mathcal{C}$:

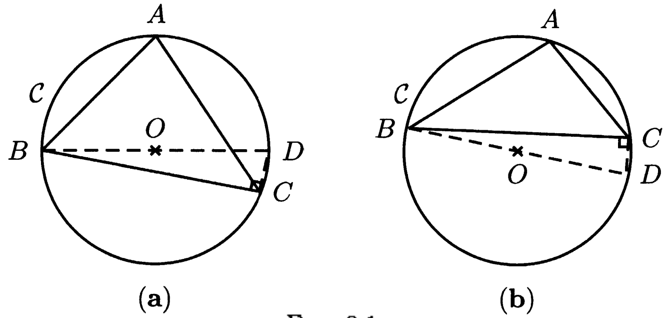


FIG. 6.1.

On a alors $\sin \widehat{A} = \sin \widehat{BDC} = \dfrac{a}{2R}$. De même, on montre que $\sin \widehat{B} = \dfrac{b}{2R}$ et $\sin \widehat{C} = \dfrac{c}{2R}$.

□

♦ **Remarques.**

1. Comme la surface S du triangle ABC peut s'écrire $S = \dfrac{1}{2}ab\sin \widehat{C} = \dfrac{1}{2}bc\sin \widehat{A} = \dfrac{1}{2}ca\sin \widehat{B}$, il s'ensuit que

$$\boxed{\frac{a}{\sin \widehat{A}} = \frac{b}{\sin \widehat{B}} = \frac{c}{\sin \widehat{C}} = \frac{abc}{2S} = 2R,} \tag{6.2}$$

soit, en particulier,

$$\boxed{S = \frac{abc}{4R}.} \tag{6.3}$$

2. Comme $\dfrac{b}{\sin \widehat{B}} \times \dfrac{c}{\sin \widehat{C}} = \dfrac{a^2}{\sin^2 \widehat{A}}$, il s'ensuit que

$$\boxed{S = \frac{a^2}{2} \times \frac{\sin \widehat{B} \sin \widehat{C}}{\sin \widehat{A}} = \frac{a^2}{2} \times \frac{\sin \widehat{B} \sin \widehat{C}}{\sin (\widehat{B} + \widehat{C})}.} \tag{6.4}$$

3. Soit I_1 le point où la bissectrice intérieure de $[\widehat{BAC}]$ coupe la droite (BC). On retrouve en appliquant la loi des sinus dans les triangles ABI_1 et ACI_1 l'identité :

$$\boxed{\frac{I_1B}{I_1C} = \frac{c}{b}.} \tag{6.5}$$

6.1.2. Théorème. *(Formule d'Al Kashi[1]) On a la formule :*

$$a^2 = b^2 + c^2 - 2bc\cos \widehat{A}. \tag{6.6}$$

1. Masûd Al Kashi (1390-1450), mathématicien perse.

♦ **Preuve.** On a $a^2 = BC^2 = (\overrightarrow{AC} - \overrightarrow{AB})^2 = b^2 + c^2 - 2bc\cos\widehat{A}$.

□

♦ **Remarques.**

1. Dans le cas d'un triangle rectangle en A, on retrouve le théorème de Pythagore[2].

2. Soit m_a la longueur de la médiane issue du sommet A et soit I le milieu du segment $[BC]$.

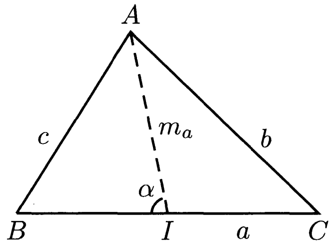


FIG. 6.2.

En appliquant la formule d'Al Kashi dans les triangles AIB et AIC, on trouve : $c^2 = \frac{a^2}{4} + m_a^2 - 2m_a \times \frac{a}{2} \times \cos\alpha$; $b^2 = \frac{a^2}{4} + m_a^2 - 2m_a \times \frac{a}{2} \times \cos(\pi - \alpha)$, ce qui conduit à la formule dite de la médiane :

$$\boxed{4m_a^2 + a^2 = 2b^2 + 2c^2.} \tag{6.7}$$

6.1.3. Théorème. *(Formule de Héron[3]) L'aire S du triangle ABC est donnée par la formule :*

$$S = \sqrt{p(p-a)(p-b)(p-c)}, \tag{6.8}$$

où $p = (a+b+c)/2$ est le demi périmètre du triangle ABC.

♦ **Preuve.** Des formules $S = \frac{1}{2}bc\sin\widehat{A}$, $\cos\widehat{A} = \frac{b^2+c^2-a^2}{2bc}$ et $\sin^2\widehat{A} + \cos^2\widehat{A} = 1$, on trouve :

$$16S^2 = 4b^2c^2 - (b^2+c^2-a^2)^2 = 16p(p-a)(p-b)(p-c).$$

□

♦ **Exemples.**

1. Les longueurs des côtés d'un triangle acutangle (i.e., dont tous les angles sont aigus) sont des entiers et le diamètre de son cercle circonscrit est $6,25$. Calculer les longueurs des côtés de ce triangle.

On peut supposer $a \leqslant b \leqslant c$. Comme c est un entier, $c \leqslant 6$. D'un autre côté, si s désigne la longueur du côté d'un triangle équilatéral inscrit dans le

2. Pythagore de Samos (569 av. J.-C.-475 av. J.-C.), mathématicien grec.

3. Héron d'Alexandrie (10-75), géomètre et physicien grec.

cercle circonscrit au triangle de côtés a, b, c alors $c \geqslant s$. Or, par la loi des sinus, $s = 6,25 \times \sin \pi/3 > 5$, ce qui donne $5 < c \leqslant 6$, soit $c = 6$.

On a donc $\sin \widehat{C} = 6/6,25 = 24/25$, soit encore $\cos \widehat{C} = 7/25$. D'après la formule d'Al Kashi, on obtient donc $a^2 + b^2 - 36 = \dfrac{14}{25}ab$, ce qui impose $25 \mid ab$. Or, $a \leqslant 6$ et $b \leqslant 6$, ce qui donne $a = b = 5$.

Réciproquement, on vérifie sans peine que les mesures trouvées réalisent les conditions demandées.

2. Existe-t-il un triangle d'aire entière et dont les côtés sont des nombres premiers ?

Si $a \leqslant b \leqslant c$ sont les longueurs des côtés d'un tel triangle et S son aire on a d'après la formule de Héron $16S^2 = (a - b + c)(a + b - c)(a + c - b)(b + c - a)$.

Les quatre facteurs du $2^{\text{ème}}$ membre sont de la même parité, donc ils sont nécessairement pairs. Deux cas sont alors possibles :

- a, b et c sont pairs, et comme ils sont premiers $a = b = c = 2$.

- $a = 2$ et b et c sont impairs, avec par inégalité triangulaire $c < 2 + b$, donc $c = b$.

Or, dans les deux cas S ne peut être un nombre entier.

6.1.4. Théorème. *(Inégalité d'Euler) Soient R et r les rayons respectifs des cercles circonscrit et inscrit dans le triangle ABC. On a alors l'inégalité dite d'Euler :*

$$R \geqslant 2r. \tag{6.9}$$

Plus précisément, si O et I désignent les centres respectifs des cercles circonscrit et inscrit dans le triangle ABC, alors :

$$OI^2 = R^2 - 2Rr. \tag{6.10}$$

♦ **Preuve.** L'égalité $OI^2 = R^2 - 2Rr$ est équivalente à $2Rr = R^2 - OI^2$. Or, $R^2 - OI^2 = IU \cdot IV = IA \cdot IM$ (le lecteur familiarisé avec la notion de puissance reconnaîtra la puissance du point I par rapport au cercle circonscrit au triangle ABC), où M est le deuxième point d'intersection de (AI) avec le cercle circonscrit au triangle ABC.

Soit D le projeté orthogonal de I sur (AC). On a alors $r = ID$. Soit enfin M' le point diamétralement opposé de M sur le cercle circonscrit au triangle ABC.

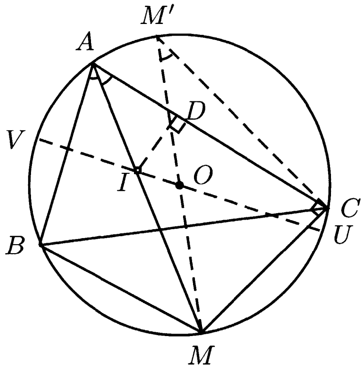


FIG. 6.3.

Les triangles AID et $M'MC$ sont semblables donc $\dfrac{IA}{MM'} = \dfrac{ID}{MC}$, c'est-à-dire $IA \cdot MC = MM' \cdot ID = 2Rr$. Or, $MC = MB = MI$: en effet $\widehat{MCI} = \dfrac{\widehat{A}}{2} + \dfrac{\widehat{C}}{2}$, et donc $\widehat{MIC} = \pi - \left(\widehat{B} + \dfrac{\widehat{A}}{2} + \dfrac{\widehat{C}}{2}\right) = \dfrac{\widehat{A}}{2} + \dfrac{\widehat{C}}{2} = \widehat{MCI}$.

On en déduit que $R^2 - OI^2 = IA \cdot MC = 2Rr$, d'où le résultat.

□

♦ **Remarques.**

1. On aurait pu démontrer l'inégalité d'Euler seule en utilisant les inégalités algébriques usuelles. Par exemple, en utilisant l'inégalité :

$$abc \geqslant (a+b-c)(b+c-a)(c+a-b),$$

que l'on obtient immédiatement par transformation de Ravi, on a $pabc \geqslant 8S^2$ (notations de la formule de Héron), c'est-à-dire $\dfrac{abc}{4S} \geqslant \dfrac{2S}{p}$.

Or, $\dfrac{abc}{4S} = R$ et $\dfrac{S}{p} = r$ (identité souvent utile et facile à retrouver), d'où $R \geqslant 2r$.

2. Réciproquement, si la distance OI des centres de deux cercles $\mathcal{C}(O,R)$ et $\mathcal{C}'(I,r)$ vérifie l'égalité $OI^2 = R^2 - 2Rr$, alors il existe une infinité de triangles inscrits dans le cercle $\mathcal{C}$ et dont le cercle inscrit est le cercle $\mathcal{C}'$.

En effet, considérons un point quelconque $A \in \mathcal{C}$ et construisons les points $B, C \in \mathcal{C}$ où les deux tangentes menées de A au cercle $\mathcal{C}'$ viennent recouper le cercle $\mathcal{C}$.

Soit M le point, autre que A, où la droite (AI) coupe le cercle $\mathcal{C}$. On a alors $AI \cdot IM = R^2 - OI^2 = 2Rr$. Or (notations de la figure 6.3) les triangles AID et $M'MC$ sont semblables, d'où $AI \cdot CM = 2Rr$, par conséquent $IM = CM$.

Or, cette dernière égalité caractérise le centre du cercle inscrit dans le triangle ABC, d'où le résultat.

6.2. Les transversales

On appelle *transversale* du triangle ABC toute droite coupant respectivement les droites (BC), (CA), (AB), en des points M, N, P distincts des sommets A, B, C.

6.2.1. Théorème. *(Théorème de Menelaüs[4]) Soit ABC un triangle. Soient M, N, P trois points appartenant respectivement aux droites (BC), (CA), (AB) et distincts des sommets A, B, C du triangle ABC.*

Une condition nécessaire et suffisante pour que les points M, N, P soient alignés est :

$$\frac{\overline{MB}}{\overline{MC}} \times \frac{\overline{NC}}{\overline{NA}} \times \frac{\overline{PA}}{\overline{PB}} = +1. \tag{6.11}$$

♦ **Preuve.** Si M, N, P sont alignés, considérons le point $D \in (AC)$ tel que $(BD) \parallel (MN)$.

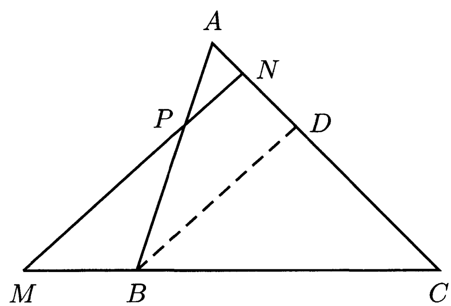


FIG. 6.4.

On a alors (théorème de Thalès[5]) : $\dfrac{\overline{MB}}{\overline{MC}} = \dfrac{\overline{ND}}{\overline{NC}}$ et $\dfrac{\overline{PA}}{\overline{PB}} = \dfrac{\overline{NA}}{\overline{ND}}$, ce qui donne :

$$\frac{\overline{MB}}{\overline{MC}} \times \frac{\overline{NC}}{\overline{NA}} \times \frac{\overline{PA}}{\overline{PB}} = +1.$$

Réciproquement, si les points M, N, P vérifient la dernière égalité, considérons le point K où la droite (MN) coupe (AB) (si (MN) était parallèle à (AB), on déduirait de la relation vérifiée par M, N, P que $\dfrac{\overline{PA}}{\overline{PB}} = +1$, ce qui est impossible) ; on a alors, d'après le théorème direct,

$$\frac{\overline{PA}}{\overline{PB}} = \frac{\overline{KA}}{\overline{KB}},$$

ce qui montre que les points P et K coïncident.

□

4. Menelaüs d'Alexandrie (70-130), mathématicien grec.
5. Thalès de Milet (624 av. J.-C.-547 av. J.-C.), mathématicien grec.

♦ **Exemples.**

1. Les trois bissectrices extérieures des angles d'un triangle ABC coupent les côtés opposés en trois points alignés (quand ces trois points existent).

En effet, soient U, V, W les points où les bissectrices extérieures des angles $[\widehat{BAC}]$, $[\widehat{ABC}]$, $[\widehat{BCA}]$ respectivement coupent les côtés opposés.

On a alors $(AB = c,\ BC = a,\ CA = b)$:

$$\frac{\overline{UB}}{\overline{UC}} = \frac{c}{b}, \quad \frac{\overline{VC}}{\overline{VA}} = \frac{a}{c}, \quad \frac{\overline{WA}}{\overline{WB}} = \frac{b}{a},$$

et le résultat s'ensuit d'après la réciproque du théorème de Menelaüs.

2. Soit ABC un triangle et $\mathcal{C}$ son cercle circonscrit. Soient L le point où la tangente au cercle $\mathcal{C}$ en A coupe (BC), M le point où la tangente au cercle $\mathcal{C}$ en B coupe (AC) et N le point où la tangente au cercle $\mathcal{C}$ en C coupe (AB). Les points L, M, N sont alignés.

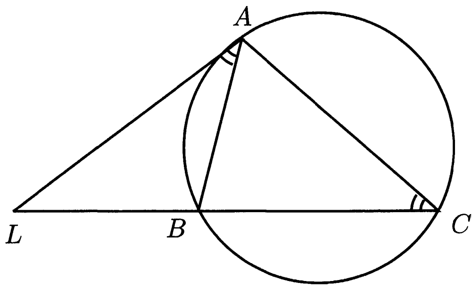


FIG. 6.5.

En effet, les triangles ALB et CLA étant semblables, on a $\dfrac{AL}{CL} = \dfrac{AB}{CA}$ et $AL^2 = BL \cdot CL$, donc $(AB = c,\ BC = a,\ CA = b)$:

$$\frac{\overline{LB}}{\overline{LC}} = \frac{c^2}{b^2},$$

et de manière analogue :

$$\frac{\overline{MC}}{\overline{MA}} = \frac{a^2}{c^2}, \quad \frac{\overline{NA}}{\overline{NB}} = \frac{b^2}{a^2},$$

ce qui permet de conclure.

6.2.2. Théorème. *(Théorème de Ceva) Soit ABC un triangle. Soient A', B', C' trois points appartenant respectivement aux droites (BC), (CA), (AB) et distincts des sommets A, B, C du triangle ABC.*

Une condition nécessaire et suffisante pour que les droites (AA'), (BB'), (CC') soient parallèles ou concourantes est :

$$\frac{\overline{A'B}}{\overline{A'C}} \times \frac{\overline{B'C}}{\overline{B'A}} \times \frac{\overline{C'A}}{\overline{C'B}} = -1. \tag{6.12}$$

♦ **Preuve.** Supposons les droites (AA'), (BB'), (CC') parallèles ou concourantes.

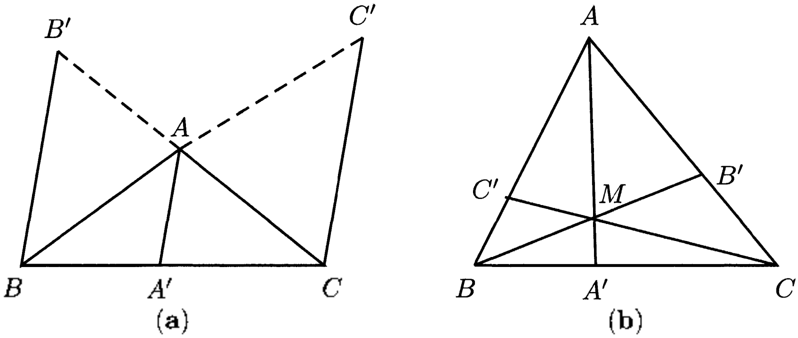


FIG. 6.6.

Si $(AA') \parallel (BB') \parallel (CC')$ (figure 6.6.a), alors, d'après le théorème de Thalès :

$$\frac{\overline{B'C}}{\overline{B'A}} \times \frac{\overline{C'A}}{\overline{C'B}} = \frac{\overline{BC}}{\overline{BA'}} \times \frac{\overline{CA'}}{\overline{CB}} = -\frac{\overline{A'C}}{\overline{A'B}}.$$

Si (AA'), (BB'), (CC') sont concourantes en un point M (figure 6.6.b), alors appliquons le théorème de Menelaüs dans les triangles ACA' et ABA' en considérant respectivement les transversales (BMB') et (CMC') :

$$\frac{\overline{BA'}}{\overline{BC}} \times \frac{\overline{B'C}}{\overline{B'A}} \times \frac{\overline{MA}}{\overline{MA'}} = +1, \qquad \frac{\overline{CB}}{\overline{CA'}} \times \frac{\overline{MA'}}{\overline{MA}} \times \frac{\overline{C'A}}{\overline{C'B}} = +1,$$

ce qui donne la relation souhaitée en multipliant membre à membre les deux égalités.

Réciproquement, supposons que A', B', C' vérifient la relation :

$$\frac{\overline{A'B}}{\overline{A'C}} \times \frac{\overline{B'C}}{\overline{B'A}} \times \frac{\overline{C'A}}{\overline{C'B}} = -1.$$

Si $(AA') \parallel (BB')$, on considère le point $C_1 \in (AB)$ tel que $(CC_1) \parallel (AA') \parallel (BB')$. En appliquant le cas direct du théorème de Ceva[6], on trouve que $C_1 = C'$. De même, si (AA') et (BB') se coupent en un point M, on considère le point C_1 où la droite (CM) coupe (AB) et on déduit en appliquant le cas direct que $C_1 = C'$.

□

♦ **Exemples.**

1. On retrouve le fait que les bissectrices intérieures d'un triangle ABC sont concourantes en un point I (centre du cercle inscrit) et que les médianes sont concourantes en un point G (centre de gravité). De même, on peut retrouver le fait que les hauteurs d'un triangles ABC sont concourantes en un point H (orthocentre) :

6. Giovanni Ceva (1647-1734), mathématicien italien.

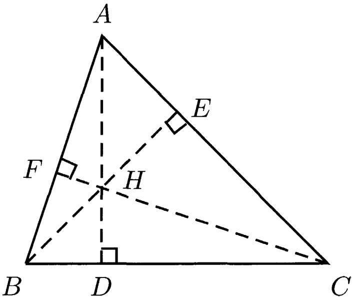


FIG. 6.7.

En effet, les triangles ACF et ABE sont semblables, d'où ($AB = c$, $BC = a$, $CA = b$) :

$$\frac{AE}{AF} = \frac{c}{b},$$

et de manière analogue

$$\frac{CD}{CE} = \frac{b}{a}; \quad \frac{BF}{BD} = \frac{a}{c}.$$

2. Les droites joignant les sommets A, B, C d'un triangle ABC aux points de contact du cercle inscrit dans ABC avec les côtés opposés sont concourantes en un point J appelé point de Gergonne[7] du triangle ABC : en effet, $CD = CE$, $AE = AF$, $BF = BD$.

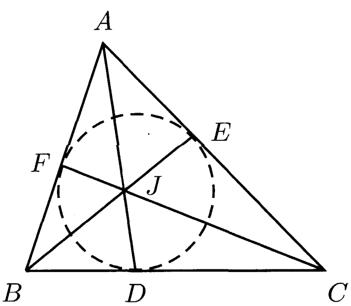


FIG. 6.8.

6.3. Les quadrilatères

6.3.1. Théorème. *(Inégalité de Ptolémée[8]) Soit $ABCD$ un quadrilatère. On a alors l'inégalité :*

$$AC \cdot BD \leqslant AB \cdot CD + BC \cdot DA, \tag{6.13}$$

avec égalité si et seulement si le quadrilatère $ABCD$ est convexe inscriptible (i.e., si les points A, B, C, D dans cet ordre sont cocycliques).

7. Joseph Diaz Gergonne (1771-1859), mathématicien français.

8. Claude Ptolémée (85-165), astronome et mathématicien grec.

♦ **Preuve.** On pose $AB = a$, $BC = b$, $CD = c$, $DA = d$, $AC = x$, $BD = y$. On considère la demi-droite symétrique de $[AD)$ par rapport à la bissectrice de l'angle $[\widehat{BAC}]$.

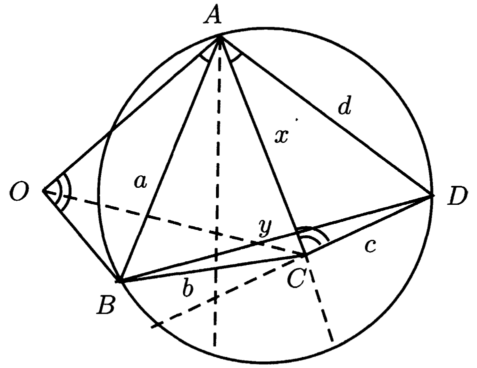


FIG. 6.9.

Sur cette demi-droite, considérons l'unique point O tel que $\widehat{AOB} = \widehat{ACD}$. Les deux triangles OAB et CAD sont donc semblables, et il s'ensuit que :

$$\frac{OB}{c} = \frac{OA}{AC} = \frac{AB}{AD} = \frac{a}{d} \quad \Longrightarrow \quad OB = \frac{ac}{d}. \tag{1}$$

D'un autre côté, $\widehat{OAC} = \widehat{BAD}$ et $OA/AB = AC/AD$, ce qui montre que les deux triangles OAC et BAD sont semblables. On en déduit que :

$$\frac{OC}{y} = \frac{x}{d} \quad \Longrightarrow \quad OC = \frac{xy}{d}. \tag{2}$$

L'inégalité de Ptolémée résulte donc de l'inégalité triangulaire dans le triangle OBC.

L'égalité a lieu si et seulement si le point B appartient au segment $[OC]$, ce qui revient à dire que $\widehat{ABC} = \pi - \widehat{ADC}$, i.e., le quadrilatère $ABCD$ est convexe inscriptible.

$\square$

♦ **Exemples.**

1. Soit C le cercle circonscrit à un triangle équilatéral ABC.

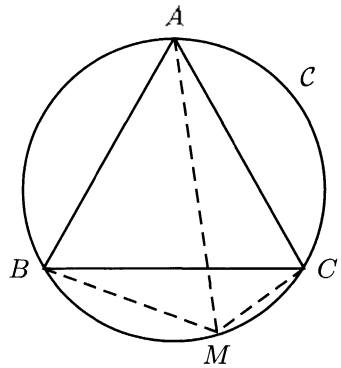


FIG. 6.10.

Pour tout point M appartenant à l'arc d'extrémités B et C ne contenant pas A, on a :

$$\boxed{AM = BM + CM.} \tag{6.14}$$

2. Construire un quadrilatère convexe inscriptible $ABCD$ connaissant les longueurs (dans cet ordre) a, b, c, d de ses côtés.

Choisissons sur une même droite les points O, B et C tels que $OB = ac/d$, $BC = b$ et $B \in [OC]$.

D'après (1), on a $OA/AC = a/d$. On en déduit que le point A appartient au lieu des points M tels que $OM/CM = a/d$ (on rappelle qu'il s'agit d'un cercle appelé cercle d'Apollonios[9]). La position du point A est alors déterminée par l'intersection de ce cercle et du cercle de centre B et de rayon a. Enfin, on construit le point D dont la position sur le cercle circonscrit au triangle ABC est fixée par $\widehat{ACD} = \widehat{AOB}$.

Les deux cercles dont l'intersection détermine le point A se coupent en deux points symétriques par rapport à (BC). On aurait pu choisir n'importe lequel des deux points d'intersection, mais les deux solutions obtenues sont symétriques l'une de l'autre. Le problème possède donc, à une isométrie près, une unique solution.

3. Soit $ABCD$ un quadrilatère convexe inscriptible. On a alors la relation :

$$\boxed{\frac{x}{y} = \frac{ad + bc}{ab + cd},} \tag{6.15}$$

où l'on a conservé les mêmes notations qu'à la figure 6.9.

On considère le point A', symétrique du point A par rapport à la médiatrice de $[BD]$, et le point D', symétrique du point D par rapport à la médiatrice de $[AC]$.

9. Apollonios de Perga (262 av. J.-C.-190 av. J.-C.), géomètre grec.

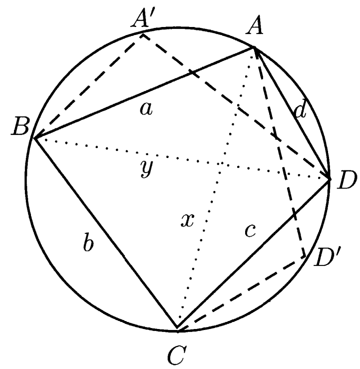


FIG. 6.11.

Le théorème de Ptolémée appliqué à chacun des deux quadrilatères convexes inscriptibles $A'BCD$ et $ABCD'$ donne alors :

$$y \cdot A'C = ab + cd, \quad x \cdot BD' = ad + bc.$$

Or, $A'C = BD'$ (deux cordes interceptant des arcs de même longueur), d'où la formule souhaitée.

6.3.2. Aire d'un quadrilatère inscriptible. *(formule de Brahmagupta[10]) Soit $ABCD$ un quadrilatère convexe inscriptible dont les longueurs des côtés sont notées a, b, c, d. Son aire est donnée par :*

$$\mathcal{A}(ABCD) = \sqrt{(p-a)(p-b)(p-c)(p-d)}, \tag{6.16}$$

où p est le demi périmètre de $ABCD$, i.e., $p = \frac{1}{2}(a+b+c+d)$.

♦ **Preuve.** Soient $\alpha = \widehat{ABC}$, $\beta = \widehat{CDA}$ et $f = AC$.

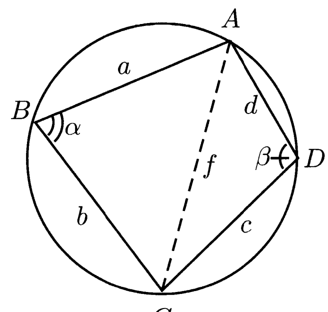


FIG. 6.12.

Comme le quadrilatère $ABCD$ est convexe, son aire s'écrit :

$$S = \mathcal{A}(ABCD) = \frac{1}{2}(ab\sin\alpha + cd\sin\beta),$$

10. Brahmagupta (598-670), mathématicien indien.

ce qui donne en élevant au carré :

$$16S^2 = 4a^2b^2\sin^2\alpha + 4c^2d^2\sin^2\beta + 8abcd\sin\alpha\sin\beta. \quad (1)$$

D'un autre côté, $a^2 + b^2 - 2ab\cos\alpha = f^2 = c^2 + d^2 - 2cd\cos\beta$, ce qui donne :

$$(a^2 + b^2 - c^2 - d^2)^2 = 4a^2b^2\cos^2\alpha + 4c^2d^2\cos^2\beta - 8abcd\cos\alpha\cos\beta. \quad (2)$$

En additionnant (1) et (2), on obtient

$$16S^2 + (a^2 + b^2 - c^2 - d^2)^2 = 4a^2b^2 + 4c^2d^2 - 8abcd\cos(\alpha + \beta). \quad (3)$$

Si alors $ABCD$ est inscriptible, $\cos(\alpha + \beta) = -1$, ce qui conduit à :

$$16S^2 = 4(ab + cd)^2 - (a^2 + b^2 - c^2 - d^2)^2 = 16(p - a)(p - b)(p - c)(p - d), \quad (4)$$

d'où le résultat.

□

♦ **Remarques.**

1. La formule (3) est valable pour un quadrilatère convexe quelconque.

2. Il est possible de déformer un quadrilatère convexe « articulé » $ABCD$ dont les côtés ont des longueurs fixées $AB = a$, $BC = b$, $CD = c$, $DA = d$. On voit d'après la formule (3) que l'aire obtenue est maximale lorsque le quadrilatère est inscriptible (le problème de la construction d'un quadrilatère convexe inscriptible connaissant les longueurs de ses côtés (dans cet ordre) a, b, c, d a été étudié à l'exemple 2 du point précédent).

6.3.3. Quadrilatères circonscriptibles. *Un quadrilatère convexe est dit circonscriptible si ses côtés sont tangents à un même cercle.*

Une condition nécessaire et suffisante pour qu'un quadrilatère convexe $ABCD$ soit circonscriptible est que :

$$AB + CD = AD + BC. \quad (6.17)$$

♦ **Preuve.** Il est facile de constater que dans un quadrilatère convexe circonscriptible $ABCD$, on a $AB + CD = AD + BC$.

Étudions la réciproque. Soit $ABCD$ un quadrilatère convexe dans lequel $AB + CD = AD + BC$. Si ce quadrilatère contient deux côtés adjacents égaux, les deux autres côtés sont eux aussi égaux et la preuve est facile à achever.

Supposons donc par exemple $AB > BC$; on a alors $AB - BC = AD - CD > 0$. On considère maintenant les points $P \in [AB]$ et $Q \in [DA]$ tels que : $BP = BC$, $DQ = DC$.

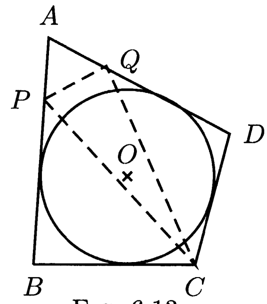


FIG. 6.13.

Le triangle APQ est donc isocèle de sommet A. La bissectrice intérieure de l'angle $[\widehat{BAD}]$ est donc portée par la médiatrice du segment $[PQ]$. De même, les bissectrices intérieures des angles $[\widehat{CBA}]$ et $[\widehat{ADC}]$ sont respectivement portées par les médiatrices des segments $[CP]$ et $[CQ]$.

Il s'ensuit que ces trois bissectrices intérieures se recoupent en un point O (le centre du cercle circonscrit au triangle PQC) qui est donc équidistant des côtés du quadrilatère $ABCD$ (et situé à l'intérieur de $ABCD$ convexe), d'où le résultat.

□

6.4. Puissance d'un point par rapport à un cercle

6.4.1. Théorème. *(Puissance d'un point par rapport à un cercle) Soit $\mathcal{C}$ un cercle de centre O et de rayon R et soit M un point quelconque du plan. Si une droite passant par M coupe $\mathcal{C}$ en A et B alors :*

$$\overline{MA} \cdot \overline{MB} = OM^2 - R^2. \tag{6.18}$$

Le réel $\overline{MA} \cdot \overline{MB}$, égal à $OM^2 - R^2$, est appelé puissance du point M par rapport au cercle $\mathcal{C}$.

♦ **Preuve.** Soit A' le point diamétralement opposé de A sur $\mathcal{C}$.

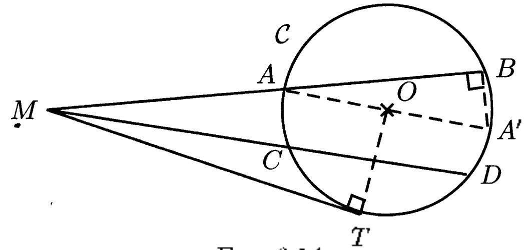


FIG. 6.14.

On a :

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

□

♦ **Remarques.**

1. La puissance d'un point M par rapport à un cercle $\mathcal{C}$ est un réel positif, nul ou négatif suivant que M est à l'extérieur, sur ou à l'intérieur du cercle $\mathcal{C}$.

2. Si M est à l'extérieur du cercle $\mathcal{C}$, et si T est l'un des deux points de contact du cercle $\mathcal{C}$ et des tangentes au cercle $\mathcal{C}$ menées à partir de M, alors $OM^2 - R^2 = MT^2$ est la puissance du point M par rapport au cercle $\mathcal{C}$.

3. Réciproquement, soient A, B, C, D quatre points deux à deux distincts n'appartenant pas à une même droite. Si (AB) et (CD) se coupent en un point M tel que $\overline{MA} \cdot \overline{MB} = \overline{MC} \cdot \overline{MD}$ alors les points A, B, C, D sont cocycliques.

En effet, supposons A, B, C non alignés et soit D_1 le point où la droite (MC) recoupe le cercle circonscrit au triangle ABC. On a alors $\overline{MA} \cdot \overline{MB} = \overline{MC} \cdot \overline{MD_1}$, soit encore ($\overline{MC} \neq 0$) $\overline{MD} = \overline{MD_1}$, d'où $D = D_1$.

6.4.2. Théorème. *Le lieu géométrique des points de même puissance par rapport à deux cercles donnés $\mathcal{C}$ et $\mathcal{C}'$ de centres distincts O et O', est une droite perpendiculaire à la ligne des centres (OO'). Cette droite est appelée l'axe radical des deux cercles $\mathcal{C}$ et $\mathcal{C}'$.*

♦ **Preuve.** On désigne par R et R' les rayons respectifs des cercles $\mathcal{C}$ et $\mathcal{C}'$. La puissance d'un point M par rapport aux cercles $\mathcal{C}$ et $\mathcal{C}'$ est la même si et seulement si $OM^2 - R^2 = O'M^2 - R'^2$, c'est-à-dire $OM^2 - O'M^2 = 2\overline{OO'} \cdot \overline{IM_1} = R^2 - R'^2$, où I est le milieu de $[OO']$ et M_1 est le projeté orthogonal de M sur (OO'). Ainsi, l'ensemble des points M ayant la même puissance par rapport à $\mathcal{C}$ et $\mathcal{C}'$ est la droite perpendiculaire à (OO') et passant par le point $M_1 \in (OO')$ défini par :

$$\overline{IM_1} = \frac{R^2 - R'^2}{2\overline{OO'}}.$$

□

♦ **Remarques.**

1. Si $A \in \mathcal{C} \cap \mathcal{C}'$ alors A appartient à l'axe radical des cercles $\mathcal{C}$ et $\mathcal{C}'$ (car sa puissance par rapport aux deux cercles est zéro).

2. L'axe radical de deux cercles sécants en deux points distincts A et B est donc la droite (AB).

3. L'axe radical de deux cercles tangents en A est la tangente commune en A à ces deux cercles.

6.4.3. Définition. *Soient $\mathcal{C}$, $\mathcal{C}'$, $\mathcal{C}''$ trois cercles de centres respectifs O, O', O''. On suppose les trois centres O, O', O'' non alignés. Les axes radicaux de ces trois cercles pris deux à deux se coupent en un point. Ce point est appelé le centre radical des trois cercles. C'est le seul point du plan qui ait même puissance par rapport aux trois cercles.*

♦ **Exemples.**

1. Soit ABC un triangle. Soit I_1 le point où la bissectrice intérieure de $[\widehat{BAC}]$ coupe la droite (BC). On a alors :

$$\boxed{AI_1^2 = AB \cdot AC - BI_1 \cdot CI_1.} \tag{6.19}$$

En effet, soit M le point où la droite (AI_1) coupe le cercle circonscrit au triangle ABC.

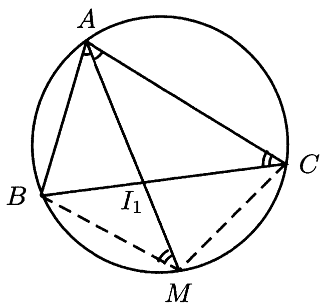


FIG. 6.15.

On a alors $BI_1 \cdot CI_1 = AI_1 \cdot MI_1$, ce qui donne $AI_1^2 + BI_1 \cdot CI_1 = AI_1 \cdot AM$. Or, les triangles ABM et AI_1C étant semblables, on obtient : $AB \cdot AC = AI_1 \cdot AM$.

2. On appelle inversion de centre O (ou de pôle O) et de rapport $k \in \mathbb{R}^*$ la transformation du plan qui à tout point M distinct de O associe le point $M' \in (OM)$ tel que $\overline{OM} \cdot \overline{OM'} = k$. Le point M' est alors appelé inverse du point M.

On démontre ici une des propriétés fondamentales de l'inversion : l'image d'un cercle $\mathcal{C}$ par une inversion de centre $O \notin \mathcal{C}$ est un cercle.

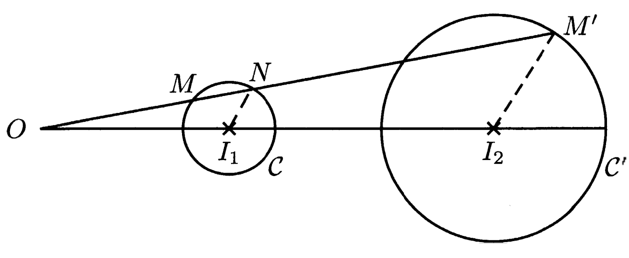


FIG. 6.16.

En effet, considérons un point $M \in \mathcal{C}$ et son inverse M'. Soit N le point du plan où la droite (OM) recoupe le cercle $\mathcal{C}$.

Si on note k le rapport de l'inversion considérée et p la puissance du point O par rapport au cercle $\mathcal{C}$, alors $\overline{OM} \cdot \overline{OM'} = k$ et $\overline{OM} \cdot \overline{ON} = p$, d'où $\overline{OM'}/\overline{ON} = k/p$.

Il s'ensuit que lorsque le point M décrit le cercle $\mathcal{C}$, le point M' décrit un cercle homothétique à $\mathcal{C}$, le point O et la constante k/p étant respectivement le centre et le rapport de l'homothétie en question.

Il est à noter que les centres de ces cercles ne sont pas inverse l'un de l'autre.

On va par exemple appliquer ce résultat pour établir l'assertion suivante : si $ABCD$ est un quadrilatère qui est à la fois inscriptible et circonscriptible, alors (avec les notations de la figure 6.17 ci-dessous) les droites (PR) et (QS) sont orthogonales.

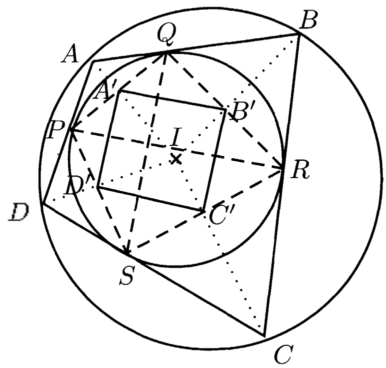


FIG. 6.17.

En effet, soit I le centre du cercle inscrit dans le quadrilatère $ABCD$. Soient A', B', C', D' les milieux respectifs des segments $[PQ]$, $[QR]$, $[RS]$, $[SP]$. Le quadrilatère $A'B'C'D'$ est alors un parallélogramme. Par ailleurs, on a $\overline{IA} \cdot \overline{IA'} = \overline{IB} \cdot \overline{IB'} = \overline{IC} \cdot \overline{IC'} = \overline{ID} \cdot \overline{ID'} = r^2$, où r est le rayon du cercle inscrit dans $ABCD$. Or, l'inverse du cercle circonscrit au quadrilatère $ABCD$ est un cercle, ce qui montre que $A'B'C'D'$ est inscriptible, c'est-à-dire que $A'B'C'D'$ est un rectangle. Il s'ensuit que $\left[(PR) \parallel (A'B')\right] \perp \left[(B'C') \parallel (QS)\right]$.

3. Construire l'axe radical (Δ) de deux cercles $\mathcal{C}$ et $\mathcal{C}'$ de centres respectifs O et O' $(O \neq O')$.

Il suffit de trouver un point appartenant à l'axe radical puisque celui-ci est perpendiculaire à la ligne des centres.

Seul le cas où les cercles $\mathcal{C}$ et $\mathcal{C}'$ n'ont pas de point commun nécessite une construction supplémentaire. Dans ce cas, on considère un cercle $\mathcal{C}''$ de centre $O'' \notin (OO')$ et qui coupe les cercles donnés $\mathcal{C}$ et $\mathcal{C}'$.

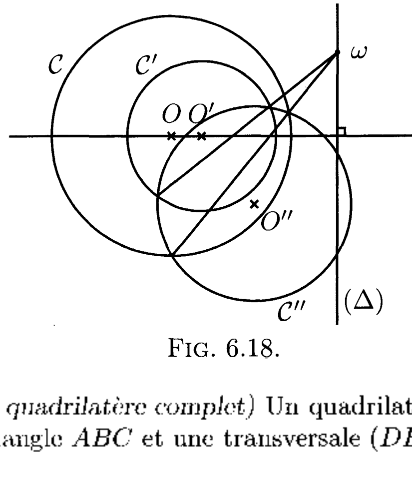


FIG. 6.18.

4. *(Une propriété du quadrilatère complet)* Un quadrilatère complet est la figure déterminée par un triangle ABC et une transversale (DEF) telle que $D \in (BC)$,

$E \in (CA)$, $F \in (AB)$. Les droites (AB), (BC), (CA), (DEF) sont alors dites côtés du quadrilatère complet de sommets A, B, C, D, E, F. Les trois segments $[AD]$, $[BE]$, $[CF]$ sont appelés diagonales du quadrilatère complet.

Soit H l'orthocentre du triangle ABC, A', B', C' les pieds des hauteurs :

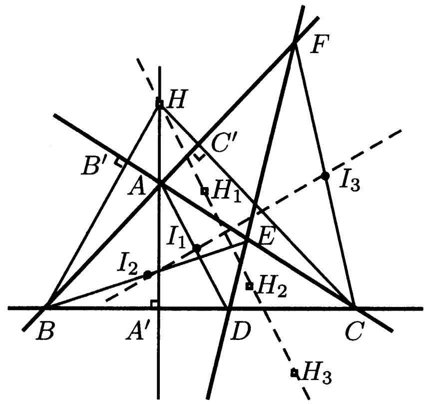


FIG. 6.19.

$\overline{HA} \cdot \overline{HA'}$ est la puissance du point H par rapport au cercle de diamètre $[AD]$, $\overline{HB} \cdot \overline{HB'}$ est la puissance du point H par rapport au cercle de diamètre $[BE]$, $\overline{HC} \cdot \overline{HC'}$ est la puissance du point H par rapport au cercle de diamètre $[CF]$.

Or, en considérant la puissance de H par rapport au cercle de diamètre $[AB]$, on a $\overline{HA} \cdot \overline{HA'} = \overline{HB} \cdot \overline{HB'}$. De même, en prenant le cercle de diamètre $[AC]$: $\overline{HA} \cdot \overline{HA'} = \overline{HC} \cdot \overline{HC'}$. Le même raisonnement peut être appliqué aux orthocentres des triangles AEF, CDE et BDF. Il s'ensuit que les trois cercles de diamètres $[AD]$, $[BE]$, $[CF]$, pris deux à deux, ont pour axe radical une droite qui porte les orthocentres ; par conséquent, les centres des cercles sont alignés.

La droite qui porte les milieux des diagonales $[AD]$, $[BE]$, $[CF]$ s'appelle droite de Newton[11] du quadrilatère complet. On a montré au passage que les quatre orthocentres des triangles formés par les côtés du quadrilatère pris trois à trois sont aussi alignés.

6.5. Géométrie dans le plan complexe

Tout point $M(x, y)$ dans un plan affine euclidien réel rapporté à un repère orthonormé direct $(O, \vec{\imath}, \vec{\jmath})$ peut être identifié au nombre complexe $z = x + iy$. Le nombre z est appelé affixe du point M et on parle alors abusivement de « plan complexe ».

De même, tout vecteur $\vec{u}(x, y)$ du plan peut être identifié au nombre complexe $z = x + iy$ appelé encore affixe du vecteur $\vec{u}$.

Tout problème de géométrie plane peut de cette manière être étudié dans le plan complexe. Ainsi, une translation de vecteur $\vec{u}$ dans le plan affine correspond

11. Isaac Newton (1643-1727), physicien et mathématicien anglais.

à la transformation $z \longmapsto z + a$ dans le plan complexe, où $a \in \mathbb{C}$ est l'affixe de $\vec{u}$. Une homothétie de centre A et de rapport $k \in \mathbb{R}$ correspond à la transformation $z \longmapsto k(z - a) + a$ dans le plan complexe, où $a \in \mathbb{C}$ est l'affixe du point A.

Les formules complexes associées à de nombreuses autres transformations usuelles sont à peine plus difficiles à obtenir. Il est par exemple facile de constater qu'une multiplication par le nombre complexe i fait tourner d'un angle $\pi/2$ autour de l'origine. Plus généralement, une multiplication par $e^{i\alpha}$, où $\alpha \in \mathbb{R}$, fait tourner d'un angle α autour de l'origine. Ainsi, une rotation de centre A et d'angle α correspond à la transformation $z \longmapsto e^{i\alpha}(z - a) + a$, où $a \in \mathbb{C}$ est l'affixe du point A.

Il est aussi simple d'exprimer des contraintes d'orthogonalité dans le plan complexe puisque pour $\vec{u}$, $\vec{v}$ vecteurs d'affixes respectives z et z', on a

$$\boxed{\vec{u} \cdot \vec{v} = \frac{1}{2}(z\overline{z'} + \overline{z}z').} \tag{6.20}$$

Enfin, l'angle orienté $(\widehat{\vec{u}, \vec{v}})$ est identifié à $\operatorname{Arg}(z'/z)$, où z et z' sont les affixes respectives de $\vec{u}$ et $\vec{v}$. Ainsi, trois points deux à deux distincts M_1, M_2, M_3 d'affixes respectives z_1, z_2, z_3 sont alignés si et seulement si $(z_3 - z_1)/(z_2 - z_1) \in \mathbb{R}$.

De même, quatre points deux à deux distincts M_1, M_2, M_3, M_4 d'affixes respectives z_1, z_2, z_3, z_4 sont cocycliques ou alignés si et seulement si

$$\boxed{\operatorname{Arg} \frac{z_4 - z_1}{z_3 - z_1} \equiv \operatorname{Arg} \frac{z_4 - z_2}{z_3 - z_2} \pmod{\pi},} \tag{6.21}$$

soit encore $\left(\dfrac{z_4 - z_1}{z_3 - z_1}\right) \Big/ \left(\dfrac{z_4 - z_2}{z_3 - z_2}\right) \in \mathbb{R}$. Cette dernière expression est appelée *birapport* de z_1, z_2, z_3, z_4.

♦ **Exemples.**

1. Le triangle ABC est équilatéral direct si et seulement si $a + jb + j^2c = 0$, où $j = \dfrac{-1}{2} + i\dfrac{\sqrt{3}}{2} = e^{2i\pi/3}$ et a, b, c sont les affixes respectives de A, B, C.

En effet, ABC est équilatéral direct si et seulement si $\overrightarrow{CA}$ se déduit de $\overrightarrow{CB}$ par la rotation d'angle $-\pi/3$, ce qui se traduit par $a - c = e^{-i\pi/3}(b - c) = -j(b - c)$, ce qui donne le résultat recherché puisque $1 + j + j^2 = 0$.

On peut utiliser le résultat que l'on vient de démontrer pour résoudre l'exercice suivant : soient A, B, C des points d'affixes respectives a, b, c. Le triangle ABC est équilatéral si et seulement si $a^2 + b^2 + c^2 - ab - bc - ca = 0$.

En effet, en factorisant : $a^2 + b^2 + c^2 - ab - bc - ca = (a + jb + j^2c)(a + j^2b + jc)$, on obtient les deux cas de figure : les triangles équilatéraux directs et indirects.

2. On considère quatre points deux à deux distincts A, B, C, D dans le plan affine euclidien. On a alors l'inégalité (de Ptolémée) :

$$AB \cdot CD + BC \cdot AD \geqslant AC \cdot BD,$$

avec égalité si et seulement si les points A, B, C, D, dans cet ordre, sont cocycliques ou appartiennent à une même droite.

En effet, fixons l'origine du repère orthonormé en A et notons z_1, z_2, z_3 les affixes respectives des points B, C, D. L'inégalité de Ptolémée est alors équivalente à :

$$|z_1| \cdot |z_3 - z_2| + |z_3| \cdot |z_2 - z_1| \geqslant |z_2| \cdot |z_3 - z_1|,$$

i.e.,

$$\left|\frac{1}{z_3} - \frac{1}{z_2}\right| + \left|\frac{1}{z_2} - \frac{1}{z_1}\right| \geqslant \left|\frac{1}{z_3} - \frac{1}{z_1}\right|,$$

ce qui est vrai (inégalité triangulaire).

L'égalité a lieu si et seulement si $\left(\frac{1}{z_2} - \frac{1}{z_1}\right) \Big/ \left(\frac{1}{z_3} - \frac{1}{z_2}\right) \in \mathbb{R}_+$, c'est-à-dire $\left(\frac{z_1}{z_3}\right) \Big/ \left(\frac{z_2 - z_1}{z_2 - z_3}\right) \in \mathbb{R}_-$, ce qui permet de conclure.

6.6. Les théorèmes isopérimétriques

On s'intéresse dans ce paragraphe à des questions du type : de tous les polygones vérifiant certaines propriétés, quel est celui de périmètre minimal ou maximal ? Quel est celui d'aire minimale ou maximale ?

6.6.1. Théorème. *De tous les triangles de même périmètre, le triangle équilatéral possède la plus grande surface.*

De tous les triangles de même surface, le triangle équilatéral possède le plus petit périmètre.

♦ **Preuve.** Pour un triangle de côtés a, b, c, de demi périmètre p et d'aire S, on a d'après la formule de Héron et l'inégalité de la moyenne :

$$S^2 = p(p-a)(p-b)(p-c) \leqslant p\left(\frac{p}{3}\right)^3.$$

Le théorème en résulte immédiatement.

□

6.6.2. Théorème. *De tous les quadrilatères convexes de même périmètre, le carré possède la plus grande surface.*

De tous les quadrilatères convexes de même surface, le carré possède le plus petit périmètre.

♦ **Preuve.** On a vu en remarque dans le point 6.3.2 que l'on peut déformer un quadrilatère jusqu'à l'inscrire dans un cercle, et qu'alors son aire s'en trouve augmentée. En appliquant la formule de Brahmagupta et l'inégalité de la moyenne à ce dernier quadrilatère (inscriptible), on obtient pour un quadrilatère quelconque de côtés a, b, c, d, de demi périmètre p et d'aire S :

$$S^2 \leqslant (p-a)(p-b)(p-c)(p-d) \leqslant \left(\frac{p}{2}\right)^4,$$

l'égalité ayant lieu si et seulement si $a = b = c = d$, ce qui permet de conclure.

□

6.6.3. Théorème. *Soit n un entier $\geqslant 3$. De tous les polygones à n côtés inscrits dans un cercle donné, le polygone régulier possède le plus grand périmètre et la plus grande surface.*

♦ **Preuve.** On peut distinguer deux cas de polygones inscrits dans un cercle donné $\mathcal{C}$, de centre O et de rayon R :

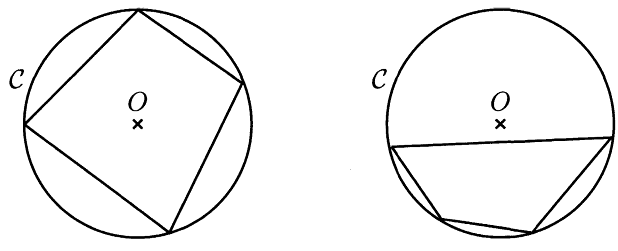


FIG. 6.20.

Si le point O n'est pas à l'intérieur du polygone considéré (figure 6.20.b), le périmètre de ce dernier est $\leqslant \pi R$ et son aire est $\leqslant \pi R^2/2$. Or, le périmètre d'un polygone régulier à n côtés inscrit dans le cercle $\mathcal{C}$ est $n \times 2R \sin \dfrac{\pi}{n}$ et son aire est égale à $n \times \dfrac{1}{2} R^2 \sin \dfrac{2\pi}{n}$. Il s'ensuit, après étude de la fonction $x \mapsto \sin x - x/2$ sur l'intervalle $[0, \pi/3]$, que le polygone régulier possède un plus grand périmètre et une plus grande surface que le polygone considéré.

On se place désormais dans le cas de la figure 6.20.a. Soit un polygone convexe $A_1A_2 \dots A_n$ inscrit dans le cercle $\mathcal{C}$ tel que le point O soit à son intérieur. Si on pose $\alpha_k = \widehat{A_kOA_{k+1}}$, avec $A_{n+1} = A_1$, alors le périmètre de ce polygone s'écrit $2R \times \sum_{i=1}^{n} \sin(\alpha_i/2)$ et sa surface s'écrit $R^2/2 \times \sum_{i=1}^{n} \sin \alpha_i$ avec $\sum_{i=1}^{n} \alpha_i = 2\pi$. Comme la fonction $x \mapsto \sin x$ est concave sur l'intervalle $[0, \pi]$, il s'ensuit que ces deux quantités sont maximales lorsque $\alpha_1 = \alpha_2 = \cdots = \alpha_n$ (inégalité de convexité), i.e., lorsque le polygone $A_1A_2 \dots A_n$ est régulier.

□

EXERCICES

1. Soit ABC un triangle dont tous les angles sont aigus. La bissectrice intérieure de l'angle A coupe le côté BC en L et recoupe le cercle circonscrit au triangle ABC en N. On désigne respectivement par K et M les projections orthogonales de L sur les côtés AB et AC. Prouver que l'aire du quadrilatère $AKNM$ et l'aire du triangle ABC sont égales.

(Olympiades internationales-1987/2)

---

2. ABC est un triangle non équilatéral. Pour tout point M à l'intérieur de ce triangle, on pose $S(M) = AC' + BA' + CB'$ où A', B' et C' sont les projections de M sur (BC), (AC) et (AB) respectivement.

Démontrer que si $S(M) = S(N)$ alors la droite (MN) est parallèle à la droite (OI), où O est le centre du cercle circonscrit à ABC et I est le centre de son cercle inscrit.

---

3. Soit $ABCD$ un trapèze isocèle de bases BC et AD. Le triangle $A'B'C$ est obtenu à partir du triangle ABC par rotation autour de C d'un certain angle α. Prouver que les milieux des segments $[A'D]$, $[BC]$, $[B'C]$ sont alignés.

(Olympiades russes-1989)

---

4. On considère un triangle $A_1A_2A_3$ et on appelle G son centre de gravité. Les droites (GA_1), (GA_2), (GA_3) recoupent le cercle circonscrit au triangle $A_1A_2A_3$ en A_1', A_2', A_3' respectivement. Prouver que :

$$GA_1 \cdot GA_2 \cdot GA_3 \leqslant GA_1' \cdot GA_2' \cdot GA_3'$$

et

$$\frac{1}{GA_1'} + \frac{1}{GA_2'} + \frac{1}{GA_3'} \leqslant \frac{1}{GA_1} + \frac{1}{GA_2} + \frac{1}{GA_3}.$$

---

5. Soit M le point d'intersection du cercle inscrit dans le triangle ABC avec le côté AB. On choisit un point arbitraire $T \neq B, C$ sur le côté BC. Prouver que les cercles inscrits dans les triangles BMT, MTA, ATC sont tangents à une même droite.

(Olympiades russes-1989)

---

6. On considère trois cercles isométriques, tangents deux à deux et tangents, tous les trois, intérieurement à un cercle $\mathcal{C}$. D'un point M de $\mathcal{C}$ on trace une tangente à chacun des trois cercles et on appelle A, B et C les points de contact.

Démontrer que l'une des longueurs MA, MB et MC est la somme des deux autres.

---

7. Soient a, b et c les longueurs des côtés d'un triangle de périmètre 1. Prouver alors l'inégalité :

$$a^2 + b^2 + c^2 + 4abc < \frac{1}{2}.$$

(Olympiades russes-1989)

---

8. On considère un point P à l'intérieur d'un triangle ABC. On désigne par x, y et z respectivement les distances de P aux points A, B et C, et par p, q et r respectivement les distances de P aux droites (BC), (CA) et (AB). Démontrer que

$$xyz \geqslant 8pqr.$$

---

9. On considère un point P à l'intérieur d'un triangle ABC. On désigne par x, y et z respectivement les distances de P aux points A, B et C, et par p, q et r respectivement les distances de P aux droites (BC), (CA) et (AB). Démontrer que :

$$x + y + z \geqslant 2(p + q + r).$$

---

10. On considère un polygone inscriptible $A_1A_2 \ldots A_n$ $(n \geqslant 2)$ et son centre de gravité G. On désigne par B_1, $B_2, \ldots$, B_n respectivement les points d'intersection des droites (A_1G), (A_2G),..., (A_nG) avec le cercle circonscrit dans le polygone. Prouver que :

$$\frac{A_1G}{GB_1} + \frac{A_2G}{GB_2} + \cdots + \frac{A_nG}{GB_n} = n.$$

---

11. L'angle A est le plus petit dans le triangle ABC. Les points B et C divisent le cercle circonscrit au triangle ABC en deux arcs. Soit $U \neq B, C$ un point appartenant à l'arc limité par B et C et ne contenant pas le point A. Les médiatrices des segments $[AB]$ et $[AC]$ coupent la droite (AU) aux points V et W respectivement. On appelle T le point d'intersection des droites (BV) et (CW). Prouver que $AU = TB + TC$.

(Olympiades internationales-1997/2)

---

12. Soit $ABCD$ un quadrilatère convexe. Sur les segments ouverts $]\,AB\,[$, $]\,BC\,[$, $]\,CD\,[$ et $]\,DA\,[$ on choisit respectivement les points M, N, P et Q tels que : $AQ = BM = CN = DP$.

Démontrer que si $MNPQ$ est un carré, alors $ABCD$ est aussi un carré.

(Olympiades roumaines-1995)

---

13. On désigne par m_a, m_b et m_c les longueurs des médianes d'un triangle de côtés de longueurs a, b et c. Prouver l'inégalité :

$$m_a(bc - a^2) + m_b(ca - b^2) + m_c(ab - c^2) \geqslant 0.$$

---

14. On considère un triangle ABC et on note a, b, c les longueurs des côtés $[BC]$, $[CA]$, $[AB]$ respectivement. Soient m_a, m_b et m_c les longueurs des médianes issues de A, B et C respectivement et soit d le diamètre du cercle circonscrit au triangle ABC. Prouver que :

$$\frac{a^2 + b^2}{m_c} + \frac{b^2 + c^2}{m_a} + \frac{c^2 + a^2}{m_b} \leqslant 6d.$$

---

15. Soit $ABCDE$ un pentagone convexe vérifiant la propriété (P) : $\mathcal{A}(ABC) = \mathcal{A}(BCD) = \mathcal{A}(CDE) = \mathcal{A}(DEA) = \mathcal{A}(EAB) = 1$.

Calculer l'aire du pentagone $ABCDE$. Montrer qu'il existe une infinité de pentagones non isométriques vérifiant la propriété (P).

(Olympiades des États-Unis-1972)

---

16. Les diagonales d'un quadrilatère inscriptible $ABCD$ se coupent en O. Prouver l'inégalité :

$$\frac{AB}{CD} + \frac{CD}{AB} + \frac{BC}{AD} + \frac{AD}{BC} \leqslant \frac{OA}{OC} + \frac{OC}{OA} + \frac{OB}{OD} + \frac{OD}{OB}.$$

(Olympiades russes-1987)

---

17. Pour tout point P intérieur au triangle ABC, on désigne respectivement par D, E et F les pieds des perpendiculaires abaissés de P sur $[BC]$, $[CA]$ et $[AB]$. Trouver les points P tels que

$$\frac{BC}{PD} + \frac{CA}{PE} + \frac{AB}{PF}$$

soit minimum.

(Olympiades internationales-1981/1)

---

18. Dans un triangle ABC on a $\widehat{A} = 2\widehat{B}$, l'angle $\widehat{C}$ est obtus et les mesures des côtés sont des entiers. Quel est le plus petit périmètre possible de ce triangle ?

---

19. $PQRS$ est un quadrilatère convexe à l'intérieur d'un triangle ABC. Prouver qu'il existe un triangle parmi les triangles PQR, PQS, PRS et QRS dont la surface est inférieure au $1/4$ de l'aire de ABC.

(Olympiades chinoises-1986)

---

20. On considère un cercle $\mathcal{C}$ et une tangente Δ à ce cercle. Soit M un point fixé de Δ. Déterminer le lieu géométrique des points P possédant la propriété suivante : il existe deux points Q et R sur la droite Δ tels que M soit le milieu du segment $[QR]$ et que $\mathcal{C}$ soit le cercle inscrit dans le triangle PQR.

(Olympiades internationales-1992/4)

---

21. Dans un plan on se donne deux cercles sécants $\mathcal{C}_1$ et $\mathcal{C}_2$; A est un de leurs points communs. Les points M_1 et M_2 parcourent respectivement, dans le même sens, les cercles $\mathcal{C}_1$ et $\mathcal{C}_2$, avec une même vitesse angulaire. À chaque tour les points M_1 et M_2 passent simultanément au point A. Montrer qu'il existe un point fixe du plan qui est constamment équidistant de M_1 et M_2.

(Olympiades internationales-1979/3)

---

22. Les diagonales AC et CE d'un hexagone régulier $ABCDEF$ sont divisées respectivement par des points intérieurs M et N de telle sorte que :

$$\frac{AM}{AC} = \frac{CN}{CE} = \lambda.$$

Déterminer λ lorsque B, M et N sont alignés.

(Olympiades internationales-1982/5)

---

23. Soit $ABCD$ un quadrilatère convexe inscrit dans un cercle de centre O. On désigne par P le point d'intersection de (AC) et (BD). Les cercles circonscrits aux triangles ABP et CDP se recoupent en Q. Si O, P et Q sont distincts, prouver que (OQ) est perpendiculaire à (PQ).

(Olympiades chinoises-1992)

---

24. Soit $\mathcal{C}$ un cercle dans le plan. Deux autres cercles, $\mathcal{C}_1$ et $\mathcal{C}_2$, passant par le centre O du cercle $\mathcal{C}$, se recoupent en un deuxième point M. On désigne par A et E les points d'intersection de $\mathcal{C}$ avec $\mathcal{C}_2$, et par C et D les points d'intersection de $\mathcal{C}$ avec $\mathcal{C}_1$. On suppose de plus que les droites (AD) et (CE) se recoupent en B. Prouver que $\widehat{BMO} = 90°$.

(Olympiades russes-1992)

---

25. ABC est un triangle rectangle en A et D est le pied de la hauteur issue de A. La droite joignant les centres des cercles inscrits dans les triangles ABD et ACD coupe respectivement $[AB]$ et $[AC]$ en K et L.

On désigne respectivement par S et T les aires des triangles ABC et AKL. Montrer que
$$S \geqslant 2T.$$

(Olympiades internationales-1988/5)

---

26. Soit ABC un triangle dont tous les angles sont aigus. Les bissectrices intérieures des angles A, B, C recoupent le cercle circonscrit au triangle ABC respectivement en A_1, B_1, C_1.

On appelle A_0 le point d'intersection de la bissectrice intérieure (AA_1) avec les bissectrices extérieures des angles B et C. Les points B_0 et C_0 sont définis de manière analogue. Prouver que :

a) l'aire du triangle $A_0B_0C_0$ est le double de l'aire de l'hexagone $AC_1BA_1CB_1$;

b) l'aire du triangle $A_0B_0C_0$ est supérieure ou égale à quatre fois l'aire du triangle ABC.

(Olympiades internationales-1989/2)

---

27. Dans le plan on se donne un polygone convexe à n côtés avec $n \geqslant 4$. On désigne par p le périmètre de ce polygone et par d la somme des longueurs de toutes ses diagonales. Prouver les inégalités :
$$n - 3 < \frac{2d}{p} < \left\lfloor \frac{n}{2} \right\rfloor \left\lfloor \frac{n+1}{2} \right\rfloor - 2.$$

(Olympiades internationales-1984/5)

---

28. On se donne un ensemble de segments dans le plan, de longueur totale égale à 1. Prouver qu'il existe une droite l telle que la somme des longueurs des projections des segments considérés sur cette droite soit $\leqslant \dfrac{\pi}{2}$.

(Proposé à l'OIM-1989)

---

29. Dans le plan on se donne un polygone convexe à n côtés. On désigne par a_k la mesure de son k-ième côté et par d_k la longueur de la projection du polygone sur la droite contenant le k-ième côté ($k = 1, 2, \ldots, n$). Prouver que

$$2 < \frac{a_1}{d_1} + \frac{a_2}{d_2} + \cdots + \frac{a_n}{d_n} \leqslant 4.$$

(Olympiades russes-1988)

---

30. Un cercle, dont le centre est situé sur le segment $[AB]$ d'un quadrilatère convexe $ABCD$ est tangent aux trois autres côtés. Prouver que, si le quadrilatère $ABCD$ est inscriptible, alors

$$AD + BC = AB.$$

(Olympiades internationales-1985/1)

---

31. On se donne quatre points A, B, C, D dans le plan, C et D étant dans un même demi-plan déterminé par la droite (AB). On suppose de plus que $AC \cdot BD = AD \cdot BC$ et $\widehat{ADB} = 90° + \widehat{ACB}$.

Calculer le rapport

$$\frac{AB \cdot CD}{AC \cdot BD}$$

et prouver que les cercles circonscrits aux triangles ACD et BCD sont orthogonaux (deux cercles sécants sont dits orthogonaux si les tangentes en leurs points d'intersection sont perpendiculaires l'une à l'autre).

(Olympiades internationales-1993/2)

---

32. Soit $ABCDEF$ un hexagone convexe tel que :

$$AB = BC = CD, \qquad DE = EF = FA, \qquad \widehat{BCD} = \widehat{EFA} = 60°.$$

Soient G et H deux points intérieurs à l'hexagone tels que $\widehat{AGB} = \widehat{DHE} = 120°$. Montrer que

$$AG + GB + GH + DH + HE \geqslant CF.$$

(Olympiades internationales-1995/5)

---

33. Soit P un point à l'intérieur du triangle ABC vérifiant

$$\widehat{APB} - \widehat{ACB} = \widehat{APC} - \widehat{ABC}.$$

Soient D et E les centres des cercles inscrits dans les triangles APB et APC respectivement. Montrer que les droites (AP), (BD) et (CE) sont concourantes.

(Olympiades internationales-1996/2)

---

34. $ABCD$ est un quadrilatère convexe tel que (AB) et (CD) ne sont pas parallèles. On considère un cercle passant par A et B et tangent à (CD) en P, et un cercle passant par C et D et tangent à (AB) en Q.

Prouver que la corde commune à ces deux cercles coupe $[PQ]$ en son milieu si et seulement si (AD) est parallèle à (BC).

(Olympiades chinoises-1990)

---

35. On se donne deux cercles concentriques dans le plan. On suppose le rayon d'un d'entre eux égal au double du rayon de l'autre. On considère un quadrilatère $ABCD$ inscrit dans le cercle de plus petit rayon, et on considère les points A_1, B_1, C_1 et D_1 où les demi-droites $[CD)$, $[DA)$, $[AB)$ et $[BC)$ recoupent le cercle de plus grand diamètre.

Prouver que le périmètre de $A_1B_1C_1D_1$ est supérieur ou égal au double du périmètre de $ABCD$, et déterminer quand l'égalité a lieu.

(Olympiades chinoises-1988)

---

36. On considère deux cercles concentriques de rayons respectifs R et R_1, où $R_1 > R$. $ABCD$ est un quadrilatère inscrit dans le cercle de rayon R et $A_1B_1C_1D_1$ est inscrit dans le cercle de rayon R_1, tel que A_1 est sur le prolongement de la demi-droite $[CD)$, B_1 est sur celui de $[DA)$, C_1 est sur celui de $[AB)$ et D_1 est sur celui de $[BC)$. Prouver que

$$\frac{\mathcal{A}(A_1B_1C_1D_1)}{\mathcal{A}(ABCD)} \geqslant \frac{R_1^2}{R^2},$$

où $\mathcal{A}(P)$ désigne l'aire du polygone P.

(Olympiades roumaines-1994)

---

37. Soit $ABCDEF$ un hexagone convexe tel que (AB) soit parallèle à (ED), (BC) soit parallèle à (FE) et (CD) soit parallèle à (AF).

Soient R_A, R_C et R_E les rayons des cercles circonscrits respectivement aux triangles FAB, BCD et DEF et soit p le périmètre de l'hexagone. Prouver que :

$$R_A + R_C + R_E \geqslant \frac{p}{2}.$$

(Olympiades internationales-1996/5)

SOLUTIONS

1. 1ère solution. On remarque que les triangles ABN et ALC sont semblables. Il s'ensuit que

$$\frac{AN}{AC} = \frac{AB}{AL}.$$

D'un autre côté,

$$\mathcal{A}(AKNM) = \frac{1}{2}AK \cdot AN \cdot \sin\frac{\widehat{A}}{2} + \frac{1}{2}AM \cdot AN \cdot \sin\frac{\widehat{A}}{2} = AK \cdot AN \cdot \sin\frac{\widehat{A}}{2}$$

car $AK = AM = AL\cos\frac{\widehat{A}}{2}$.

Comme $\mathcal{A}(ABC) = \frac{1}{2}AB \cdot AC \cdot \sin\widehat{A} = AB \cdot AC \cdot \sin\frac{\widehat{A}}{2}\cos\frac{\widehat{A}}{2}$, il s'ensuit que :

$$\mathcal{A}(ABC) = AK \cdot AL \cdot \sin\frac{\widehat{A}}{2} \cdot \cos\frac{\widehat{A}}{2} = AK \cdot AN \cdot \sin\frac{\widehat{A}}{2} = \mathcal{A}(AKNM).$$

2ème solution. On considère le point P de $[BC]$ où la parallèle à la droite (CN) passant par le point M coupe $[BC]$. Montrons qu'alors $(KP) \parallel (BN)$.

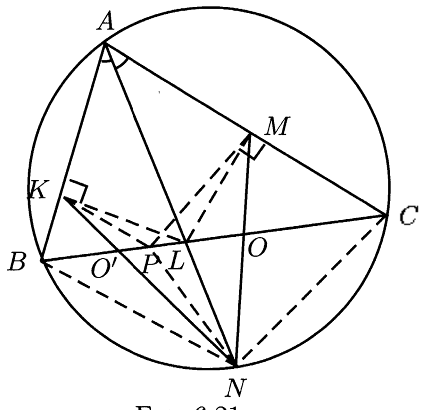


FIG. 6.21.

Comme $\widehat{MPC} = \widehat{PCN} = \widehat{BAN} = \widehat{LAC}$, il s'ensuit que le quadrilatère $APLM$ est inscriptible. Comme $AKLM$ l'est aussi, les points A, K, P, L et M sont cocycliques et on a donc $\widehat{KPL} = \pi - \frac{\widehat{A}}{2}$, ce qui implique que $\widehat{KPB} = \widehat{PBN}$, d'où $(KP) \parallel (BN)$.

Ainsi, $\mathcal{A}(MOC) = \mathcal{A}(OPN)$ et $\mathcal{A}(KO'B) = \mathcal{A}(O'PN)$, d'où le résultat demandé.

2.

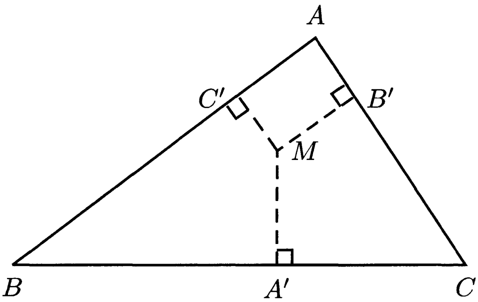


Fig. 6.22.

On pose $\vec{v_1} = \frac{\overrightarrow{BC}}{BC}$, $\vec{v_2} = \frac{\overrightarrow{AB}}{AB}$, $\vec{v_3} = \frac{\overrightarrow{CA}}{CA}$. On a alors

$$\begin{aligned} S(M) &= \overrightarrow{BM} \cdot \vec{v_1} + \overrightarrow{AM} \cdot \vec{v_2} + \overrightarrow{CM} \cdot \vec{v_3} \\ &= \overrightarrow{AM} \cdot (\vec{v_1} + \vec{v_2} + \vec{v_3}) + \overrightarrow{BA} \cdot \vec{v_1} + \overrightarrow{CA} \cdot \vec{v_3}. \end{aligned}$$

Si on pose $\vec{v} = \vec{v_1} + \vec{v_2} + \vec{v_3}$, alors $\vec{v} \neq \vec{0}$ (ABC est non équilatéral) et on a :

$$S(M) = S(N) \iff \left(\overrightarrow{AM} - \overrightarrow{AN}\right) \cdot \vec{v} = 0 \iff \overrightarrow{MN} \cdot \vec{v} = 0.$$

Si $M \neq N$ alors $\overrightarrow{MN} \perp \vec{v}$. Par ailleurs, on vérifie facilement que $S(O) = S(I) = p$ (p désigne le demi périmètre de ABC) et donc $\overrightarrow{OI} \perp \vec{v}$. On a donc $(MN) \parallel (OI)$, ce qu'il fallait démontrer.

3.

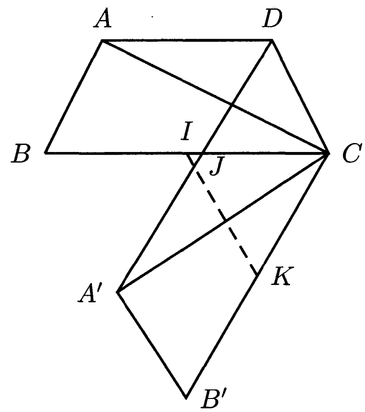


Fig. 6.23.

On désigne par I, J et K les milieux respectifs des segments $[BC]$, $[A'D]$ et $[B'C]$, et on étudie le problème dans le plan complexe d'origine I. Soient a, b et c des réels tels que B ait pour affixe $-a$, C ait pour affixe a, A ait pour affixe $b - ic$ et D ait pour affixe $b + ic$. Soit enfin $\varepsilon = e^{i\alpha}$ le nombre complexe qui, multiplié par un nombre complexe z, fait tourner le point d'affixe z d'un angle α autour de l'origine.

L'affixe du point K est donnée par

$$z_K = -a\varepsilon + a = a(1-\varepsilon),$$

et l'affixe du point J est donnée par

$$\begin{aligned} z_J &= \frac{1}{2}[z_D + z_{A'}] = \frac{1}{2}\big[(b+ic) + \big((-a-b+ic)\varepsilon + a\big)\big] \\ &= \frac{1}{2}\big[a(1-\varepsilon) + b(1-\varepsilon) + ic(1+\varepsilon)\big]. \end{aligned}$$

Comme $1+\varepsilon$ est perpendiculaire à $1-\varepsilon$, il s'ensuit que $i(1+\varepsilon)$ est un multiple réel de $1-\varepsilon$ et donc que z_J est un multiple réel de z_K, d'où le résultat.

Note. On arrive à résoudre l'exercice analytiquement, mais les calculs sont plus longs.

4.

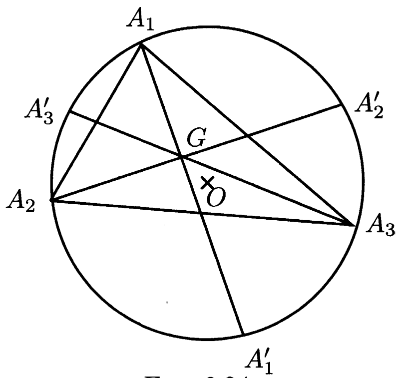


FIG. 6.24.

Soit O le centre du cercle circonscrit au triangle $A_1A_2A_3$. En utilisant la puissance d'un point par rapport à un cercle, on peut écrire pour tout i, $1 \leqslant i \leqslant 3$, $GA_i \cdot GA_i' = R^2 - OG^2$, où R est le rayon du cercle circonscrit au triangle $A_1A_2A_3$. Les inégalités à démontrer sont donc équivalentes à

$$\left(R^2 - OG^2\right)^3 \geqslant GA_1^2 \cdot GA_2^2 \cdot GA_3^2 \tag{1}$$

et

$$\left(R^2 - OG^2\right)\sum_{i=1}^{3}\frac{1}{GA_i} \geqslant \sum_{i=1}^{3} GA_i. \tag{2}$$

Afin de prouver ces inégalités, on remarque que

$$3\left(R^2 - OG^2\right) = \sum_{i=1}^{3} GA_i^2, \tag{3}$$

en effet,

$$\begin{aligned}\sum_{i=1}^{3} GA_i^2 &= \sum_{i=1}^{3} (\overrightarrow{GO} + \overrightarrow{OA_i})^2 = 3\big(OG^2 + R^2\big) - 2\overrightarrow{OG} \cdot \Big(\sum_{i=1}^{3} \overrightarrow{OA_i}\Big) \\ &= 3\big(R^2 - OG^2\big).\end{aligned}$$

L'inégalité (1) est donc une conséquence immédiate de l'inégalité entre les moyennes géométrique et arithmétique.

Pour démontrer l'inégalité (2), on écrit :

$$\frac{1}{3}\Big(\sum_{i=1}^{3} GA_i^2\Big)\Big(\sum_{i=1}^{3} \frac{1}{GA_i}\Big) \geqslant \frac{1}{9}\Big(\sum_{i=1}^{3} GA_i\Big)^2\Big(\sum_{i=1}^{3} \frac{1}{GA_i}\Big) \geqslant \sum_{i=1}^{3} GA_i,$$

ce qu'il fallait démontrer.

---

5. On considère la deuxième tangente commune aux cercles inscrits dans les triangles CMT et ATB. Cette droite coupe les segments $[MT]$ et $[AT]$ en N et L respectivement. Le résultat demandé sera donc acquis si on réussit à prouver qu'un cercle peut être inscrit dans le quadrilatère $AMNL$, i.e., si $MN + AL = NL + MA$ (caractérisation érigée en théorème dans le cours).

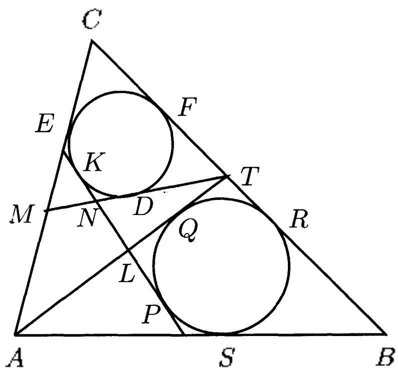


FIG. 6.25.

D'une part,

$$\begin{aligned} MN + AL - NL &= (MD - ND) + (AQ - LQ) - NL \\ &= (MD - NK) + (AQ - LP) - NL \\ &= MD + AQ - KP \\ &= ME + AS - KP.\end{aligned}$$

D'autre part,

$$KP = FR = BC - BE - CS.$$

Il s'ensuit que

$$MN + AL - NL = AB + AC - BC - AM,$$

et comme $AB + AC - BC = 2AM$, la démonstration est achevée.

6.

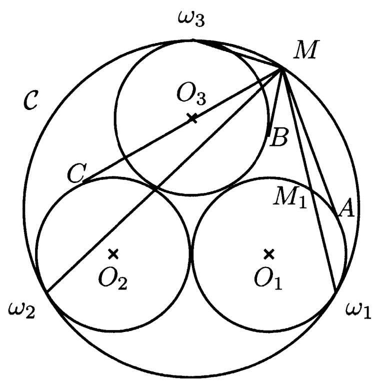


FIG. 6.26.

Désignons par R le rayon du cercle C et par r le rayon des trois cercles isométriques. Le cercle de centre O_1 est l'image du cercle $\mathcal{C}$ par l'homothétie de centre ω_1 et de rapport $\dfrac{r}{R}$. Il s'ensuit que

$$\omega_1 M_1 = \frac{r}{R}\omega_1 M, \text{ i.e., } MM_1 = \Big(1 - \frac{r}{R}\Big)\omega_1 M.$$

D'un autre côté, $MA^2 = MM_1 \cdot M\omega_1 = \Big(1 - \dfrac{r}{R}\Big)\omega_1 M^2$, d'où

$$\omega_1 M = \lambda MA, \quad \lambda = \sqrt{\frac{1}{1 - r/R}}.$$

De même on trouve $\omega_2 M = \lambda MC$ et $\omega_3 M = \lambda MB$.

En remarquant que le triangle $\omega_1\omega_2\omega_3$ est équilatéral et en appliquant le théorème de Ptolémée au quadrilatère $M\omega_1\omega_2\omega_3$, on trouve $M\omega_1 + M\omega_3 = M\omega_2$, d'où $MA + MB = MC$. Les autres cas de figure se traitent de manière identique.

---

7. a, b et c vérifient les inégalités triangulaires, d'où $a, b, c < \dfrac{1}{2}$. On examine le produit $\Big(\dfrac{1}{2} - a\Big)\Big(\dfrac{1}{2} - b\Big)\Big(\dfrac{1}{2} - c\Big)$; on a en développant :

$$\Big(\frac{1}{2} - a\Big)\Big(\frac{1}{2} - b\Big)\Big(\frac{1}{2} - c\Big) = \frac{1}{8} - \frac{1}{4}(a + b + c) + \frac{1}{2}(ab + bc + ca) - abc.$$

Or,

$$1 = (a + b + c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ca),$$

d'où :

$$\Big(\frac{1}{2} - a\Big)\Big(\frac{1}{2} - b\Big)\Big(\frac{1}{2} - c\Big) = \frac{1}{8} - \frac{1}{4}(a^2 + b^2 + c^2) - abc > 0,$$

ce qui fournit l'inégalité désirée.

Note. L'inégalité obtenue est la meilleure possible : en effet, si p, r et R désignent respectivement le demi périmètre, le rayon du cercle inscrit et le rayon du cercle circonscrit au triangle considéré, alors a, b, c sont les racines de l'équation :

$$x^3 - 2px^2 + (p^2 + r^2 + 4rR)x - 4prR = 0.$$

Il s'ensuit que :

$$a^2 + b^2 + c^2 = 2(p^2 - r^2 - 4Rr), \quad abc = 4prR.$$

Comme dans ce cas $p = 1/2$, on trouve

$$a^2 + b^2 + c^2 + 4abc = \frac{1}{2} - 2r^2,$$

ce qui peut être rendu aussi proche de $\frac{1}{2}$ que l'on veut, tout en préservant la contrainte $a + b + c = 1$.

8.

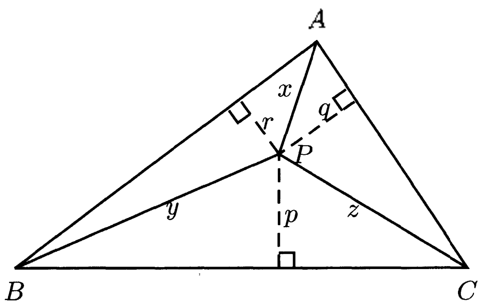


FIG. 6.27.

Soit h la mesure de la hauteur du triangle ABC issue de A. On a alors

$$\begin{aligned} \mathcal{A}(ABP) + \mathcal{A}(APC) &= \mathcal{A}(ABC) - \mathcal{A}(BPC) \\ &= \frac{1}{2}(h \cdot BC - p \cdot BC) \\ &\leqslant \frac{1}{2}xa \quad (\text{car } h \leqslant x + p). \end{aligned}$$

On a ainsi $cr + bq \leqslant xa$, et par symétrie $ap + bq \leqslant zc$ et $ap + cr \leqslant by$. L'inégalité de la moyenne donne alors : $cr + bq \geqslant 2\sqrt{crbq}$, $ap + bq \geqslant 2\sqrt{apbq}$ et $ap + cr \geqslant 2\sqrt{apcr}$. En multipliant membre à membre ces trois inégalités, on obtient $(8pqr) \times (abc) \leqslant (cr + bq)(ap + bq)(ap + cr) \leqslant (xyz) \times (abc)$, d'où le résultat.

---

9. On va s'inspirer de l'exercice précédent. On avait démontré l'inégalité $cr + bq \leqslant xa$. Or, si on considère le symétrique P' du point P par rapport à la bissectrice de l'angle A, et qu'on lui applique cette même inégalité, on obtient :

$$c \cdot \mathrm{d}\,(P', (AB)) + b \cdot \mathrm{d}\,(P', (AC)) \leqslant a \cdot \mathrm{d}\,(P', A),$$

ce qui donne $cq + br \leqslant xa$, et par symétrie $aq + bp \leqslant zc$ et $ar + cp \leqslant by$, d'où,

$$x + y + z \geqslant \underbrace{\left(\frac{b}{c} + \frac{c}{b}\right)}_{\geqslant 2} p + \underbrace{\left(\frac{c}{a} + \frac{a}{c}\right)}_{\geqslant 2} q + \underbrace{\left(\frac{a}{b} + \frac{b}{a}\right)}_{\geqslant 2} r \geqslant 2(p + q + r).$$

Note. Cette inégalité s'appelle l'inégalité d'Erdös-Mordell. C'est Erdös[12] qui l'a posée et Mordell[13] qui l'a démontrée en 1937.

---

10. On étudie le problème dans le plan complexe, et on suppose le cercle circonscrit au polygone $A_1A_2 \ldots A_n$ de rayon 1. Soient $a_1, a_2, \ldots, a_n$ les affixes des points $A_1, A_2, \ldots, A_n$ respectivement, et $b_1, b_2, \ldots, b_n$ celles des points $B_1, B_2, \ldots, B_n$ respectivement. Ainsi, G a pour affixe $g = \dfrac{a_1 + a_2 + \cdots + a_n}{n}$.

D'un autre côté, A_i, G et B_i étant alignés, on a, pour tout $i \in \{1, 2, \ldots, n\}$,

$$\frac{b_i - a_i}{\overline{b_i} - \overline{a_i}} = \frac{g - a_i}{\overline{g} - \overline{a_i}}. \tag{1}$$

Par ailleurs, $\overline{b_i} = \dfrac{1}{b_i}$ et $\overline{a_i} = \dfrac{1}{a_i}$, ce qui donne :

$$\frac{b_i - a_i}{\overline{b_i} - \overline{a_i}} = \frac{b_i - a_i}{1/b_i - 1/a_i} = -a_i b_i,$$

ce qui conduit, compte tenu de (1), à :

$$b_i = \frac{g - a_i}{1 - a_i \overline{g}}. \tag{2}$$

On en déduit que :

$$GA_i = |g - a_i| = \sqrt{(g - a_i)(\overline{g} - \overline{a_i})} = \sqrt{\frac{1}{a_i}(g - a_i)(a_i \overline{g} - 1)},$$

et,

$$GB_i = |g - b_i| = \sqrt{(g - b_i)(\overline{g} - \overline{b_i})} = (1 - g\overline{g})\sqrt{\frac{a_i}{(1 - a_i\overline{g})(a_i - g)}},$$

d'après (2).

Il s'ensuit que :

$$\begin{aligned}
\frac{GA_i}{GB_i} &= \frac{1}{1 - g\overline{g}} \sqrt{\frac{(a_i - g)(1 - a_i\overline{g})(g - a_i)(a_i\overline{g} - 1)}{a_i^2}} \\
&= \frac{(a_i\overline{g} - 1)(g - a_i)}{(1 - g\overline{g})a_i} \\
&= \frac{g\overline{g}}{1 - g\overline{g}} - \frac{a_i\overline{g}}{1 - g\overline{g}} - \frac{g\overline{a_i}}{1 - g\overline{g}} + \frac{1}{1 - g\overline{g}},
\end{aligned}$$

12. Pal Erdös (1913-1996), mathématicien hongrois.

13. Louis Joel Mordell (1888-1972), mathématicien anglais.

d'où :

$$\sum_{i=1}^{n}\frac{GA_i}{GB_i} = \frac{ng\overline{g}}{1-g\overline{g}} - \frac{(a_1+a_2+\cdots+a_n)\overline{g}}{1-g\overline{g}} - \frac{g\left(\dfrac{1}{a_1}+\dfrac{1}{a_2}+\cdots+\dfrac{1}{a_n}\right)}{1-g\overline{g}} + \frac{n}{1-g\overline{g}}$$

$$= \frac{-ng\overline{g}}{1-g\overline{g}} + \frac{n}{1-g\overline{g}} = n.$$

11. Soient X et Y les points où les droites (BV) et (CW) recoupent le cercle circonscrit au triangle ABC.

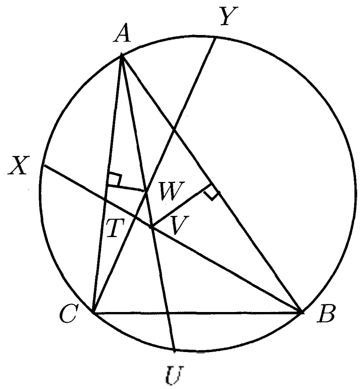


FIG. 6.28.

On oriente tous les arcs dans le sens trigonométrique. On a donc $\overset{\frown}{AU}=\overset{\frown}{YC}$ et $\overset{\frown}{AU}=\overset{\frown}{XB}$. Il s'ensuit que $\overset{\frown}{XB}=\overset{\frown}{YC}$ et donc que les segments $[BX]$ et $[YC]$ sont symétriques par rapport au diamètre contenant le point T. On en déduit que $TC = TX$, d'où $AU = BX = BT + TX = BT + CT$.

12.

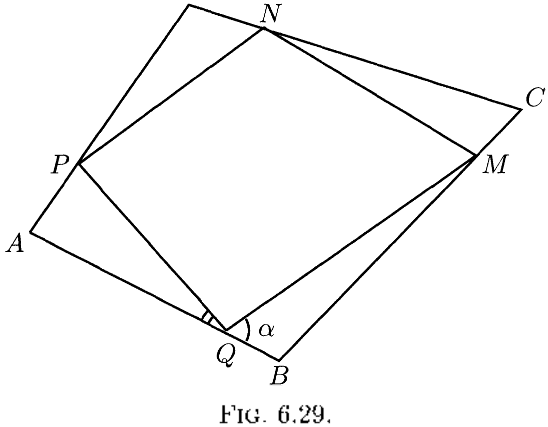


FIG. 6.29.

On pose $AQ = x$, $AD = d$, $PQ = u$ et $\widehat{MQB} = \alpha$. On a alors, dans le triangle APQ,

$$\begin{cases} PQ^2 = AP^2 + AQ^2 - 2AP \cdot AQ \cdot \cos\widehat{A}, \\ AP^2 = AQ^2 + PQ^2 - 2AQ \cdot PQ \cdot \cos\left(\frac{\pi}{2} - \alpha\right). \end{cases}$$

ce qui s'écrit :

$$\begin{cases} u^2 = x^2 + (d-x)^2 - 2x(d-x)\cos\widehat{A}, \\ (d-x)^2 = x^2 + u^2 - 2xu\sin\alpha, \end{cases}$$

ce qui implique, compte tenu du fait que $\dfrac{\sin\alpha}{x} = \dfrac{\sin\widehat{B}}{u}$, que

$$\cos\widehat{A} = \frac{x(1-\sin\widehat{B})}{d-x} \geqslant 0.$$

Il s'ensuit que $\widehat{A} \leqslant 90°$. On démontre de même que $\widehat{B} \leqslant 90°$, $\widehat{C} \leqslant 90°$ et $\widehat{D} \leqslant 90°$, ce qui implique que $\widehat{A} = \widehat{B} = \widehat{C} = \widehat{D} = 90°$, et donc $AB = BC = CD = DA$.

---

13. Soit G le centre de gravité du triangle en question, et soient I_a, I_b et I_c les milieux des côtés $[BC]$, $[CA]$ et $[AB]$ respectivement.

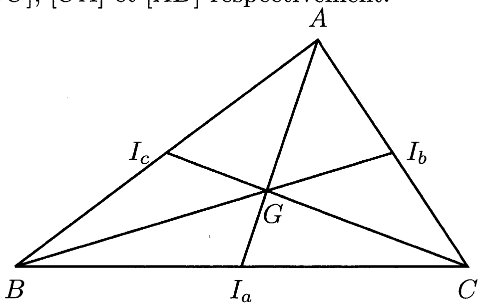


FIG. 6.30.

En appliquant l'inégalité de Ptolémée au quadrilatère BI_aGI_c, on obtient :

$$\frac{2m_b}{3} \times \frac{b}{2} \leqslant \frac{c}{2} \times \frac{m_a}{3} + \frac{a}{2} \times \frac{m_c}{3},$$

i.e.,

$$b^2 m_b \leqslant \frac{1}{2}(abm_c + bcm_a).$$

De même, on obtient :

$$c^2 m_c \leqslant \frac{1}{2}(bcm_a + cam_b), \quad a^2 m_a \leqslant \frac{1}{2}(cam_b + abm_c),$$

ce qui donne, en sommant, l'inégalité désirée.

---

14. Soient A_2, B_2, C_2 les milieux respectifs des segments $[BC]$, $[CA]$, $[AB]$, et A_1, B_1, C_1 les points où les droites (AA_2), (BB_2), (CC_2) respectivement viennent recouper le cercle circonscrit au triangle ABC.

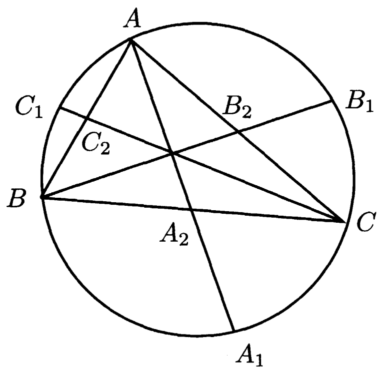


FIG. 6.31.

On a alors $AA_1 \leqslant d$, $BB_1 \leqslant d$ et $CC_1 \leqslant d$. Calculons A_1A_2 : on a $A_1A_2 \cdot AA_2 = BA_2 \cdot A_2C$, c'est-à-dire $A_1A_2 = \dfrac{a^2}{4m_a}$. De la même façon, on obtient $B_1B_2 = \dfrac{b^2}{4m_b}$ et $C_1C_2 = \dfrac{c^2}{4m_c}$. Il s'ensuit que

$$\frac{4m_a^2 + a^2}{4m_a} + \frac{4m_b^2 + b^2}{4m_b} + \frac{4m_c^2 + c^2}{4m_c} \leqslant 3d.$$

Par ailleurs, d'après la formule de la médiane, on a :

$$4m_a^2 + a^2 = 2(b^2 + c^2), \quad 4m_b^2 + b^2 = 2(c^2 + a^2), \quad 4m_c^2 + c^2 = 2(a^2 + b^2),$$

d'où le résultat demandé.

15.

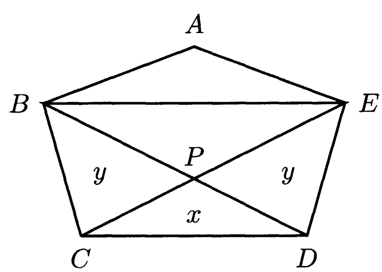


FIG. 6.32.

Puisque $\mathcal{A}(BCD) = \mathcal{A}(CDE)$, il s'ensuit que $(DC) \parallel (BE)$. De même, les autres diagonales sont parallèles à leurs côtés opposés. $ABPE$ est donc un parallélogramme et il en découle que $\mathcal{A}(PEB) = \mathcal{A}(EAB) = 1$.

Posons $x = \mathcal{A}(CPD)$ et $y = \mathcal{A}(CPB) = \mathcal{A}(EPD)$. On a donc $x + y = 1$ et

$$\frac{\mathcal{A}(EDP)}{\mathcal{A}(EPB)} = \frac{DP}{PB} = \frac{\mathcal{A}(CDP)}{\mathcal{A}(CPB)}, \text{ i.e., } \frac{y}{1} = \frac{x}{y}.$$

On en déduit que $y^2 + y - 1 = 0$, ce qui donne $y = \dfrac{\sqrt{5} - 1}{2}$ et $x = \dfrac{3 - \sqrt{5}}{2}$, d'où $\mathcal{A}(ABCDE) = y + x + y + 2 = \dfrac{5 + \sqrt{5}}{2}$.

Pour montrer qu'il existe une infinité de tels pentagones non isométriques, construisons un triangle PDC tel que $\mathcal{A}(PDC) = x$ (c'est-à-dire $\dfrac{3-\sqrt{5}}{2}$). Considérons ensuite les points E et B appartenant respectivement aux demi-droites $[CP)$ et $[DP)$ et tels que $\mathcal{A}(BCD) = \mathcal{A}(CDE) = 1$. Construisons enfin le quatrième sommet A du parallélogramme $EPBA$. Le pentagone ainsi construit vérifie la propriété (P).

---

16. On adopte les notations de la figure ci-dessous :

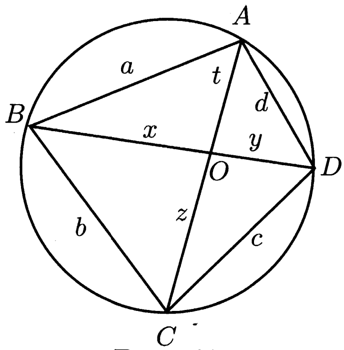


FIG. 6.33.

On démontre que $\dfrac{x}{y} = \dfrac{ab}{cd}$: en effet, on a d'une part

$$\frac{\mathcal{A}(ABC)}{\mathcal{A}(ACD)} = \frac{1/2 \times ab \sin \widehat{ABC}}{1/2 \times cd \sin \widehat{ADC}} = \frac{ab}{cd},$$

et d'autre part,

$$\frac{\mathcal{A}(ABC)}{\mathcal{A}(ACD)} = \frac{1/2 \times AC \cdot x \sin \widehat{AOB}}{1/2 \times AC \cdot y \sin \widehat{COD}} = \frac{x}{y}.$$

De même, on démontre que $\dfrac{t}{z} = \dfrac{ad}{bc}$, ce qui donne

$$\frac{x}{y} + \frac{t}{z} = \frac{a}{c}\left(\frac{b}{d} + \frac{d}{b}\right) \geqslant 2\frac{a}{c}.$$

De manière analogue, on obtient

$$\frac{y}{x} + \frac{z}{t} \geqslant 2\frac{c}{a}, \qquad \frac{x}{y} + \frac{z}{t} \geqslant 2\frac{b}{d}, \qquad \frac{y}{x} + \frac{t}{z} \geqslant 2\frac{d}{b},$$

ce qui donne

$$\frac{x}{y} + \frac{y}{x} + \frac{z}{t} + \frac{t}{z} \geqslant \frac{a}{c} + \frac{c}{a} + \frac{b}{d} + \frac{d}{b},$$

ce qu'il fallait démontrer.

---

17. On note a, b et c les mesures respectives des côtés opposés aux sommets A, B et C. On pose aussi $PD = x$, $PE = y$ et $PF = z$.

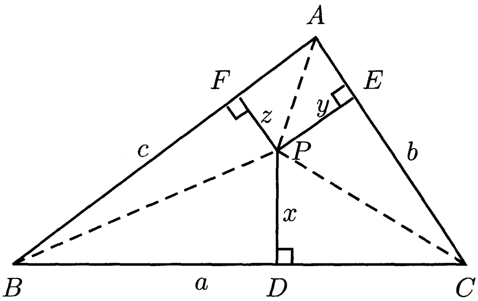


FIG. 6.34.

L'aire S du triangle ABC est donc :

$$2S = ax + by + cz.$$

On espère minimiser la quantité $\frac{a}{x} + \frac{b}{y} + \frac{c}{z}$. En appliquant l'inégalité de Cauchy-Schwarz, on obtient

$$\left(\frac{a}{x} + \frac{b}{y} + \frac{c}{z}\right) \underbrace{(ax + by + cz)}_{=2S} \geqslant (a + b + c)^2,$$

i.e.,

$$\frac{a}{x} + \frac{b}{y} + \frac{c}{z} \geqslant \frac{(a + b + c)^2}{2S},$$

avec égalité si et seulement si $x = y = z$. La valeur minimale est donc atteinte pour le centre du cercle inscrit dans le triangle ABC.

---

18. Désignons par a, b, c les mesures des côtés opposés aux sommets A, B, C respectivement. On a alors d'après la loi des sinus :

$$\frac{a}{b} = 2\cos\widehat{B}, \quad \frac{c}{b} = 4\cos^2\widehat{B} - 1,$$

ce qui implique que $a^2 = b(b + c)$.

Du fait que l'on cherche le périmètre minimum, on peut supposer que les entiers a, b et c sont premiers entre eux dans leur ensemble, ce qui entraîne que b et c sont premiers entre eux car $a^2 = b(b + c)$. Mais alors $b = m^2$ et $b + c = n^2$, d'où $a = mn$. On en déduit que $\frac{n}{m} = \frac{a}{b} = 2\cos\widehat{B}$.

Or, $\widehat{C} = \pi - 3\widehat{B}$ et comme $\widehat{C}$ est obtus, il s'ensuit que $0 < \widehat{B} < \pi/6$, ce qui donne $\sqrt{3} < \frac{n}{m} < 2$. La plus petite solution vérifiant cette inégalité est $m = 4$ et $n = 7$, ce qui donne $a = 28$; $b = 16$; $c = 33$.

Ainsi, le périmètre minimum du triangle ABC est 77.

---

19. Il existe deux cas de figure :

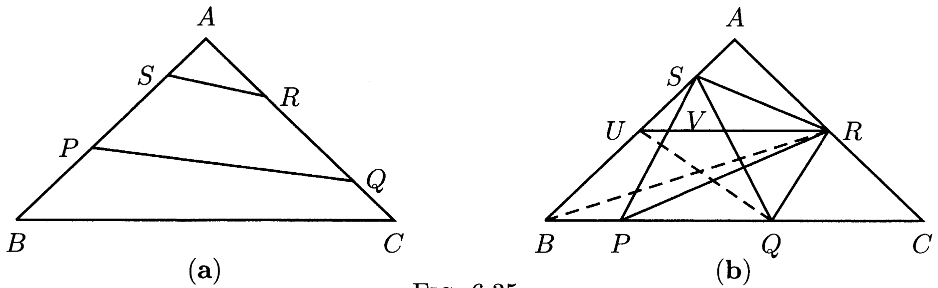


FIG. 6.35.

Nous traitons d'abord le cas (b). On peut toujours supposer $d(R, BC) \leqslant d(S, BC)$. La parallèle à (BC) passant par R coupe $[AB]$ en U et $[SP]$ en V. Puisque les triangles SQR et PQR ont la même base $[QR]$, on peut écrire :

$$\min\{\mathcal{A}(SQR), \mathcal{A}(PQR)\} \leqslant \mathcal{A}(VRQ) \leqslant \mathcal{A}(URQ) = \mathcal{A}(BUR).$$

Posons $x = \dfrac{BU}{AB}$; on a donc $\dfrac{\mathcal{A}(BUR)}{\mathcal{A}(BAR)} = x$, c'est-à-dire $\mathcal{A}(BUR) = x\mathcal{A}(BAR)$. Or,

$$\frac{\mathcal{A}(BAR)}{\mathcal{A}(ABC)} = \frac{AR}{AC} = 1 - \frac{RC}{AC} = 1 - x,$$

d'où $\mathcal{A}(BUR) = x(1-x)\mathcal{A}(ABC) \leqslant \dfrac{1}{4}\mathcal{A}(ABC)$ compte tenu de l'inégalité de la moyenne.

Le cas (a) se ramène au cas précédent en posant $B' = P$ et $C' = Q$ et en remarquant que $\mathcal{A}(AB'C') \leqslant \mathcal{A}(ABC)$.

Note. On a montré en particulier que si $PQRS$ est un parallélogramme à l'intérieur d'un triangle ABC, alors $\mathcal{A}(PQRS) \leqslant \dfrac{1}{2}\mathcal{A}(ABC)$.

---

20. Soit P un point dans le plan du cercle $\mathcal{C}$, et soient Q et R les points de rencontre de la droite Δ avec les tangentes au cercle $\mathcal{C}$ issues du point P. On désigne par O le centre du cercle $\mathcal{C}$, par A le point où la tangente Δ coupe le cercle $\mathcal{C}$ et par B le point diamétralement opposé au point A.

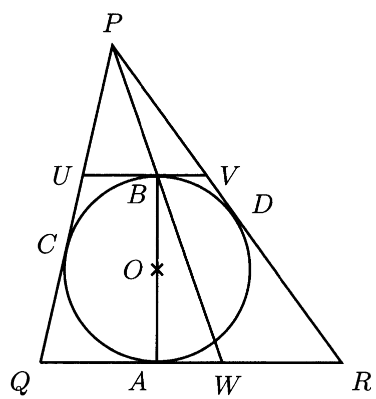


FIG. 6.36.

On montre que $QA = WR$. En effet, $PU + UB = PC = PD = PV + VB$ ce qui implique que $PV + VB$ est le demi périmètre du triangle PUV. Comme les deux triangles PUV et PQR sont homothétiques, il s'ensuit que $PR + RW$ est le demi périmètre p du triangle PQR. D'un autre côté, on a la relation classique $QA = p - PR$, d'où $QA = WR$.

Les points P avec la propriété en question sont donc les points du plan tels que M soit le milieu de $[AW]$, i.e., les points de la demi-droite d'origine B et de direction $\overrightarrow{MO}$.

---

21. On désigne par B le second point d'intersection des deux cercles $\mathcal{C}_1$ et $\mathcal{C}_2$ dont on note les centres O_1 et O_2 respectivement. La parallèle menée par A à la droite (O_1O_2) coupe le cercle $\mathcal{C}_1$ en E et le cercle $\mathcal{C}_2$ en F.

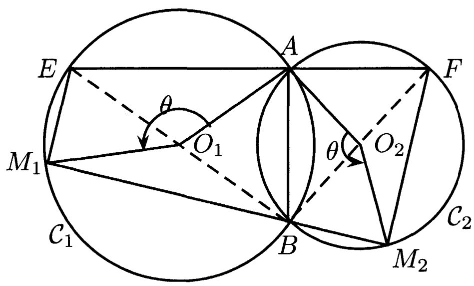


FIG. 6.37.

La droite (M_1M_2) passe toujours par le point B : en effet, soit θ l'angle parcouru par les deux points mobiles. On a alors $\widehat{ABM_1} = \dfrac{\theta}{2}$ et $\widehat{ABM_2} = \pi - \dfrac{\theta}{2}$, ce qui implique que $B \in (M_1M_2)$.

Remarquons maintenant que BE et BF sont des diamètres dans les cercles $\mathcal{C}_1$ et $\mathcal{C}_2$ respectivement. Il s'ensuit que $\widehat{BM_1E} = \widehat{BM_2F} = 90°$ et donc que les droites (M_1E) et (M_2F) sont parallèles. La médiatrice du segment $[M_1M_2]$ passe donc par le milieu du segment $[EF]$ qui est un point fixe du plan, d'où le résultat.

---

22. On suppose, ce que l'on peut toujours faire quitte à appliquer une homothétie, que l'hexagone régulier $ABCDEF$ a tous ses côtés de longueur 1. Considérons le point X où se coupent les deux droites (AC) et (BE).

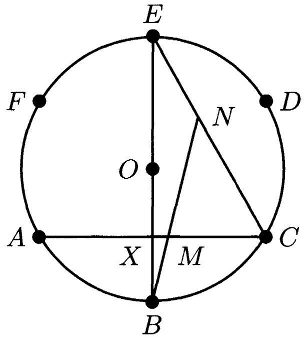


FIG. 6.38.

Si B, M et N sont alignés, on a d'après le théorème de Menelaüs :

$$\frac{CN}{NE} \times \frac{EB}{BX} \times \frac{XM}{MC} = 1.$$

Il ne reste plus qu'à exprimer toutes les distances intervenant dans la dernière égalité en fonction du rapport λ. On a $CE = 2\cos\widehat{BEC} = \sqrt{3}$. Il s'ensuit que $CN = \sqrt{3}\,\lambda$ et $NE = \sqrt{3}(1-\lambda)$. Par ailleurs $EB = 2$ et $BX = \frac{1}{2}$. Enfin, $MC = AC - AM = \sqrt{3}(1-\lambda)$ et $XM = \sqrt{3}\left(\lambda - \frac{1}{2}\right)$.

On a donc

$$\frac{\sqrt{3}\,\lambda}{\sqrt{3}(1-\lambda)} \times \frac{2}{1/2} \times \frac{\sqrt{3}\left(\lambda - \frac{1}{2}\right)}{\sqrt{3}(1-\lambda)} = 1,$$

ce qui donne $\lambda = \dfrac{1}{\sqrt{3}}$.

23.

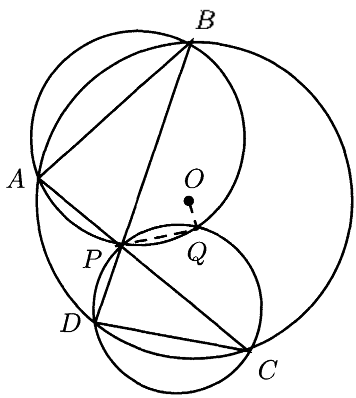


FIG. 6.39.

On a $\widehat{AQD} = \widehat{AQP} + \widehat{PQD} = \widehat{ABP} + \widehat{ACD} = 2\widehat{ABP} = \widehat{AOD}$.

Il s'ensuit que le quadrilatère $AOQD$ est inscriptible. Ainsi, $\widehat{OQP} = \widehat{OQA} + \widehat{AQP} = \widehat{ODA} + \widehat{ABD} = \widehat{ODA} + \frac{1}{2}\widehat{AOD} = 90°$.

---

24. Dans la figure ci-dessous, le point K désigne le milieu du segment $[CD]$.

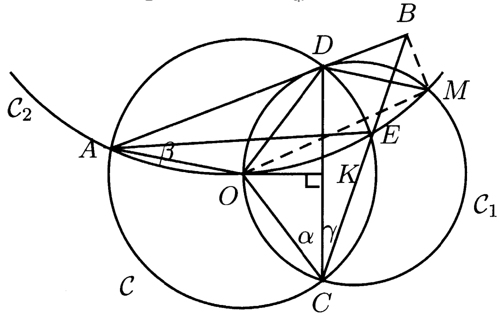


FIG. 6.40.

On a $\widehat{BMO} = \widehat{BMD} + \widehat{DMO}$. Or, $\widehat{DMO} = \widehat{DCO}$ et $\widehat{BED} = \pi - \widehat{CED} = \widehat{CAD} = \frac{1}{2}\widehat{COD} = \widehat{COK}$. Pour prouver que $\widehat{BMO} = \pi/2$, il suffit donc d'établir que $\widehat{BMD} = \widehat{BED}$, ce qui revient à dire que le quadrilatère $BMED$ est inscriptible.

Pour ce faire, on va démontrer que $\widehat{DME} = \widehat{DBE} = \alpha + \beta$ (voir la figure ci-dessus) : en effet, $\widehat{DME} = \widehat{DMO} + \widehat{OME} = \widehat{DCO} + \widehat{OAE} = \alpha + \beta$. D'un autre côté, $\widehat{DBE} = \pi - (\gamma + \widehat{CDB}) = \widehat{ADC} - \gamma$ et $\widehat{ADC} = \widehat{ADO} + \widehat{ODC} = \widehat{OAD} + \widehat{DCO} = (\beta + \gamma) + \alpha$, d'où le résultat recherché.

25.

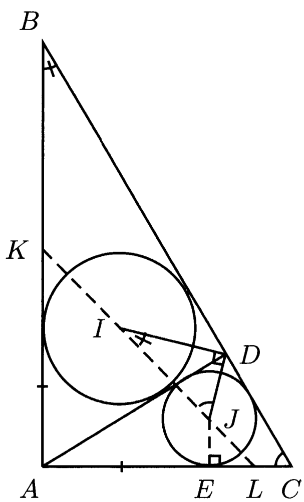


FIG. 6.41.

Une « bonne » figure incite à conjecturer que $AK = AL$ et que les triangles ABC et DIJ sont semblables.

On a d'une part $\widehat{IDJ} = \widehat{BAC} = \pi/2$. D'autre part, $\dfrac{DI}{DJ} = \dfrac{AB}{AC}$: en effet, posons $AB = c$; $BC = a$; $AC = b$ et soient r_1, r_2, r les rayons des cercles inscrits dans les triangles ABD, ADC et ABC respectivement. Comme ABC et DBA sont semblables, $\dfrac{r_1}{r} = \dfrac{c}{a}$, et comme ABC et DAC sont aussi semblables, on a aussi $\dfrac{r_2}{r} = \dfrac{b}{a}$. Il s'ensuit que $\dfrac{DI}{DJ} = \dfrac{r_1\sqrt{2}}{r_2\sqrt{2}} = \dfrac{c}{b} = \dfrac{AB}{AC}$ et que les triangles ABC et DIJ sont semblables.

On en déduit que $\widehat{KBD} + \widehat{DJK} = \dfrac{\pi}{2}$, soit encore $\widehat{BKJ} + \widehat{JDB} = \dfrac{3\pi}{2}$. Or, $\widehat{JDB} = \dfrac{3\pi}{4}$, d'où $\widehat{AKL} = \pi - \dfrac{3\pi}{4} = \dfrac{\pi}{4}$, ce qui prouve que $AK = AL$.

Considérons maintenant le point E, projeté orthogonal de J sur le côté $[BC]$. On a alors $EL = r_2 = r\dfrac{b}{a} = \left(\dfrac{b+c-a}{2}\right)\dfrac{b}{a}$. Par ailleurs, si E' désigne le projeté orthogonal du centre du cercle inscrit dans ABC sur le côté $[AB]$ alors $\dfrac{AE}{BE'} = \dfrac{b}{a}$ (car les triangles DAC et ABC sont semblables). Il s'ensuit que

$$AL = AE + EL = \frac{b}{a}\left(\frac{a+c-b}{2}\right) + \frac{b}{a}\left(\frac{b+c-a}{2}\right) = \frac{bc}{a},$$

d'où $T = \dfrac{1}{2}\left(\dfrac{bc}{a}\right)^2$. Or, $S = \dfrac{bc}{2}$, ce qui donne

$$\frac{T}{S} = \frac{bc}{a^2} = \frac{bc}{b^2+c^2} \leqslant \frac{1}{2},$$

l'égalité ayant lieu si et seulement si $b = c$.

---

26. a)

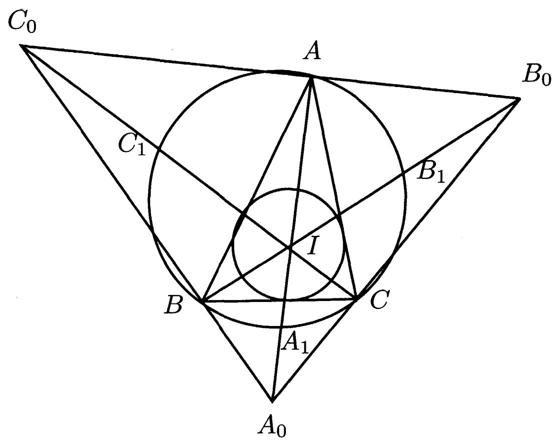


Fig. 6.42.

On démontre que A_1 est le milieu du segment $[IA_0]$: en effet, le triangle IBA_1 est isocèle de sommet A_1 puisque $\widehat{IA_1B} = \widehat{ACB}$ et $\widehat{A_1BI} = \dfrac{1}{2}(\widehat{ABC} + \widehat{BAC})$. Comme par ailleurs le triangle IBB_0 est rectangle en B, il en résulte que A_1 est le milieu de $[IA_0]$. De même, on démontre que B_1 est le milieu de $[IB_0]$ et que C_1 est le milieu de $[IC_0]$. On a donc

$$\begin{aligned}
\mathcal{A}(AB_1CA_1BC_1) &= \mathcal{A}(AB_1CI) + \mathcal{A}(CA_1BI) + \mathcal{A}(BC_1AI) \\
&= \frac{1}{2}\mathcal{A}(AB_0CI) + \frac{1}{2}\mathcal{A}(CA_0BI) + \frac{1}{2}\mathcal{A}(BC_0AI) \\
&= \frac{1}{2}\mathcal{A}(A_0B_0C_0)
\end{aligned}$$

b) Il suffit de prouver que l'aire de $AB_1CA_1BC_1$ est supérieure ou égale au double de l'aire du triangle ABC. Pour ce faire, remarquons que l'hexagone $AB_1CA_1BC_1$ est d'aire maximale parmi tous les hexagones inscrits dans le cercle circonscrit au triangle ABC et dont A, B et C sont des sommets non consécutifs. Ceci est vrai car A_1 est au milieu de l'arc $\overset{\frown}{BC}$, B_1 est au milieu de l'arc $\overset{\frown}{CA}$ et C_1 est au milieu de l'arc $\overset{\frown}{AB}$.

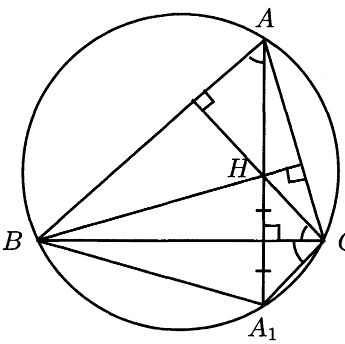


FIG. 6.43.

D'un autre côté, on peut trouver un tel hexagone d'aire exactement égale au double de $\mathcal{A}(ABC)$. Cet hexagone est obtenu en prenant pour A_1 l'intersection de la hauteur AH et du cercle circonscrit au triangle ABC, et en choisissant B_1 et C_1 de manière analogue.

Note. Le cercle circonscrit au triangle ABC est le cercle d'Euler du triangle $A_0B_0C_0$ d'où une autre façon de voir que A_1 est le milieu de $[IA_0]$.

---

27. On considère un polygone convexe $A_0A_1\ldots A_{n-1}$. Soit A_iA_j une diagonale ; on a alors par l'inégalité triangulaire,

$$A_iA_j + A_{i+1}A_{j+1} > A_iA_{i+1} + A_jA_{j+1}.$$

En additionnant membre à membre ces inégalités pour les $\binom{n}{2} - n = \dfrac{n(n-3)}{2}$ diagonales A_iA_j, chaque diagonale apparaît deux fois dans le terme de gauche et chaque côté apparaît $n-3$ fois dans le terme de droite si bien que $2d > (n-3)p$, soit

$$\frac{2d}{p} > n - 3.$$

Pour obtenir la majoration, considérons une diagonale A_iA_j. Comme elle est plus courte que toute ligne polygonale joignant A_i et A_j, on peut écrire :

$$A_iA_j < A_iA_{i+1} + \cdots + A_{j-1}A_j,$$
$$A_iA_j < A_jA_{j+1} + \cdots + A_{i-1}A_i.$$

Si n est impair, $n = 2k-1$, utilisons pour chaque diagonale A_iA_j celle des deux inégalités qui comporte le moins de termes à droite. En additionnant membre à membre ces $\dfrac{n(n-3)}{2}$ inégalités, on obtient d à gauche, et à droite une somme où chaque côté apparaît $2+3+\cdots+(k-1) = \dfrac{k(k-1)}{2} - 1$ fois. On a donc

$$d < \frac{p}{2}\big(k(k-1)-2\big) = \frac{p}{2}\Big(\frac{n^2-1}{4} - 2\Big).$$

Si n est pair, $n = 2k$, utilisons les mêmes inégalités que précédemment sauf pour les diagonales A_iA_{i+k} (même nombre de termes dans les deux inégalités) : pour ces « diamètres », on utilisera les inégalités $A_iA_{i+k} \leqslant \dfrac{p}{2}$. En sommant ces $\dfrac{n(n-3)}{2}$ inégalités, on obtient

$$d < k\frac{p}{2} + \frac{p}{2}\big(k(k-1)-2\big) = \frac{p}{2}\Big(\frac{n^2}{4} - 2\Big).$$

Finalement, il est très facile de vérifier que si n est pair, $\dfrac{n^2}{4} = \left\lfloor \dfrac{n}{2} \right\rfloor \left\lfloor \dfrac{n+1}{2} \right\rfloor$ et que si n est impair, $\dfrac{n^2-1}{4} = \left\lfloor \dfrac{n}{2} \right\rfloor \left\lfloor \dfrac{n+1}{2} \right\rfloor$.

---

28. On translate les n segments s_i $(1 \leqslant i \leqslant n)$ de façon à ce que leur milieu coïncide avec un même point origine V.

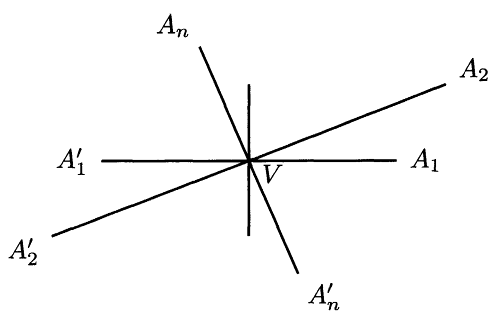


FIG. 6.44.

On désigne maintenant les $2n$ extrémités, dans le sens trigonométrique, par $A_1, A_2, \ldots, A_n, A_1', A_2', \ldots, A_n'$. Partant d'un point P_n' on trace un segment $[P_n'P_1]$ tel que $\overrightarrow{P_n'P_1} = \overrightarrow{VA_1}$, puis partant du point P_1 on trace un segment $[P_1P_2]$ tel que $\overrightarrow{P_1P_2} = \overrightarrow{VA_2}$, et ainsi de suite jusqu'à obtenir un polygone $P_1P_2\ldots P_nP_1'P_2'\ldots P_n'$.

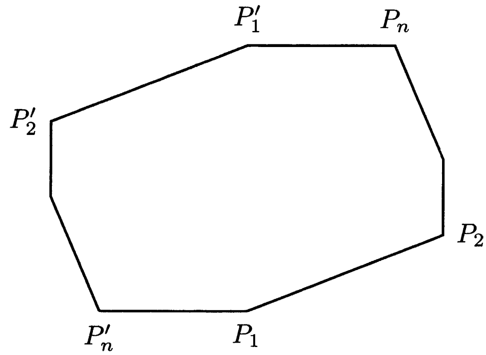


FIG. 6.45.

On choisit maintenant une paire de côtés parallèles dont la distance TT' est minimale. Il existe donc un cercle de diamètre TT' qui est intérieur au polygone $P_1P_2\dots P_nP'_1P'_2\dots P'_n$ si bien que

$$\pi \cdot TT' < \sum_{i=1}^{n} s_i = 1.$$

Or, la somme des longueurs des projections des segments s_i ($1 \leqslant i \leqslant n$) sur la droite (TT') est égale à $2TT' < \dfrac{2}{\pi}$, ce qu'il fallait démontrer.

---

29. La minoration est facile à démontrer : si D est le diamètre du polygone en question (la distance maximale entre deux sommets du polygone), alors $\sum_{i=1}^{n} a_i/d_i \geqslant \sum_{i=1}^{n} a_i/D$. Comme la ligne droite est le chemin le plus court entre deux points donnés, il s'ensuit que $\sum_{i=1}^{n} a_i > 2D$, d'où la minoration.

L'étape suivante sera d'établir la majoration pour les polygones convexes à n côtés possédant un centre de symétrie O :

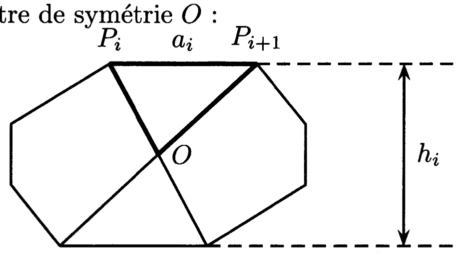


FIG. 6.46.

On appelle h_i la longueur de la projection du polygone sur une droite perpendiculaire au i-ième côté. On a donc $d_ih_i \geqslant \mathcal{A}$, $i = 1, 2, \dots, n$, où $\mathcal{A}$ désigne l'aire du polygone. Il s'ensuit que

$$\sum_{i=1}^{n} \frac{a_i}{d_i} \leqslant \sum_{i=1}^{n} \frac{a_ih_i}{\mathcal{A}} = \sum_{i=1}^{n} \frac{4\mathcal{A}(OP_iP_{i+1})}{\mathcal{A}} = 4.$$

Considérons maintenant un polygone convexe $A_1A_2\dots A_n$ et soit $\vec{v}_i = \overrightarrow{A_iA_{i+1}}$, $i = 1, 2, \dots, n$. Translatons ces vecteurs de manière à ce que leur origine coïncide avec un même point V, puis considérons les vecteurs $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n, -\vec{v}_1,$

$-\vec{v}_2, \ldots, -\vec{v}_n$, que l'on renumérote dans le sens trigonométrique : $\vec{u}_1 = \vec{v}_1, \vec{u}_2, \ldots, \vec{u}_{2n}$.

Partant d'un point P_{2n} on trace un segment $[P_{2n}P_1]$ tel que $\overrightarrow{P_{2n}P_1} = \vec{u}_1$, puis partant du point P_1 on trace un segment $[P_1P_2]$ tel que $\overrightarrow{P_1P_2} = \vec{u}_2$, et ainsi de suite jusqu'à obtenir un polygone $P_1P_2 \ldots P_{2n}$. Ce polygone possède un centre de symétrie. De plus, à chaque côté du polygone $A_1A_2 \ldots A_n$ correspondent deux côtés dans le polygone $P_1P_2 \ldots P_{2n}$ qui lui sont parallèles et égaux en longueur. Il s'ensuit que la projection de $P_1P_2 \ldots P_{2n}$ sur une droite quelconque dans le plan est exactement deux fois plus longue que celle de $A_1A_2 \ldots A_n$ (pourquoi ?). Ainsi, la quantité $\sum_{i=1}^{n} a_i/d_i$ est la même pour les deux polygones, ce qui nous ramène au cas précédemment étudié.

---

30. On note O le milieu du segment $[AB]$, qui représente aussi bien le centre du cercle circonscrit au quadrilatère $ABCD$. I, J et K étant les points de contact du cercle inscrit dans le quadrilatère $ABCD$, considérons la rotation transformant le triangle OJC au triangle OKH.

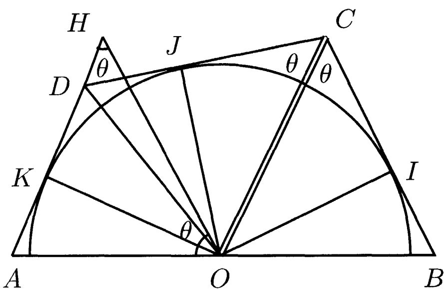


FIG. 6.47.

On a alors $\widehat{OHK} = \widehat{OCJ} = \theta$, et $\widehat{AOH} = \pi - (\widehat{OAH} + \theta)$. Mais puisque $ABCD$ est inscriptible, il s'ensuit que $\widehat{OAH} = \pi - 2\theta$, ce qui donne $\widehat{AOH} = \theta$. Ainsi, le triangle AOH est isocèle de sommet A. Il s'ensuit que

$$OA = AK + KH = AK + JC = AK + CI.$$

De même, on démontre que

$$OB = DJ + IB = DK + IB,$$

ce qui donne $AB = AD + BC$, ce qu'il fallait démontrer.

---

31. 1[ère] solution. On introduit le point auxiliaire E tel que $\widehat{EDB} = 90°$ et $DE = DB$.

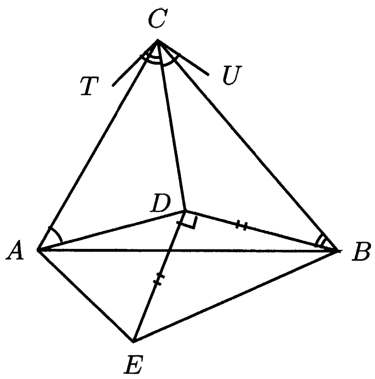


FIG. 6.48.

On a alors $\widehat{ADE} = \widehat{ACB}$ et

$$\frac{AD}{DE} = \frac{AD}{DB} = \frac{AC}{BC},$$

ce qui montre que les triangles ABC et AED sont semblables.

Il s'ensuit donc que $\widehat{CAB} = \widehat{DAE}$, c'est-à-dire $\widehat{CAD} = \widehat{BAE}$. Comme

$$\frac{AB}{AE} = \frac{AC}{AD},$$

il s'ensuit que les triangles ACD et ABE sont semblables. On en déduit que

$$\frac{AC}{AB} = \frac{AD}{AE} = \frac{CD}{BE} = \frac{CD}{\sqrt{2}\cdot BD},$$

ce qui implique que

$$\frac{AB\cdot CD}{AC\cdot BD} = \sqrt{2}.$$

Notons CU et CT les tangentes en C aux cercles circonscrits aux triangles ACD et BCD respectivement. On a donc $\widehat{UCD} = \widehat{CAD}$ et $\widehat{TCD} = \widehat{CBD}$. Montrons que $\widehat{CAD} + \widehat{CBD} = 90°$:

$$\begin{aligned}\widehat{CAD} + \widehat{DBC} &= \pi - (\widehat{ACB} + \widehat{DAB} + \widehat{DBA})\\ &= \pi - (\widehat{ADE} + \widehat{DAB} + \widehat{DBA}) = \pi - \left(\pi - \frac{\pi}{2}\right) = \frac{\pi}{2}.\end{aligned}$$

2ème solution. On résout le problème dans le plan complexe. Soient a, b, c et 0 les affixes respectives des points A, B, C et D. Posons

$$\lambda = \frac{AC}{AD} = \frac{BC}{BD}, \quad \widehat{CAD} = \alpha.$$

On a donc $a - c = \lambda e^{i\alpha}a$ et $c - b = \lambda i e^{i\alpha}b$: en effet, $\widehat{CBD} = 90° - \widehat{CAD}$ (voir la fin de la première solution). Il s'ensuit que $c = a(1-\lambda e^{i\alpha}) = b(1+i\lambda e^{i\alpha})$, d'où :

$$\begin{aligned}(a-b)c &= \lambda(e^{i\alpha}ac + ie^{i\alpha}bc)\\ &= \lambda\left[e^{i\alpha}(1+i\lambda e^{i\alpha}) + ie^{i\alpha}(1-\lambda e^{i\alpha})\right]ab\\ &= \lambda\, a\, b\, e^{i\alpha}(1+i).\end{aligned}$$

On a donc

$$AB \cdot CD = |a - b| \cdot |c| = \lambda\, |a| \cdot |b| \cdot \sqrt{2} = AC \cdot BD \cdot \sqrt{2},$$

et on continue comme dans la première solution.

32.

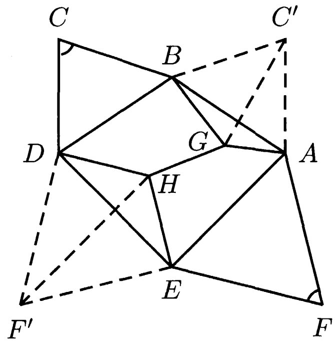


FIG. 6.49.

On remarque d'abord que BE est un axe de symétrie du quadrilatère $ABDE$. Construisons les deux points auxiliaires C', F', images respectives de C et F par la symétrie d'axe BE. Les points A, G, B, C' d'une part et les points E, H, D, F' d'autre part sont donc cocycliques. Il s'ensuit, par application du théorème de Ptolémée, que :

$$GA + GB = GC', \quad HE + HD = HF'.$$

On en déduit :

$$CF = C'F' \leqslant C'G + GH + HF' = AG + GB + GH + DH + HE,$$

avec égalité si et seulement si les points G et H se situent sur la droite $(C'F')$.

---

33. 1ère solution. On note M et N les points d'intersection de (AP) avec (BD) et (CE) respectivement.

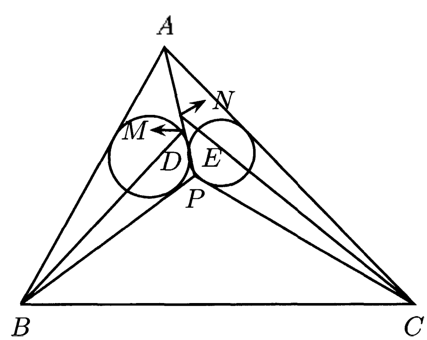


FIG. 6.50.

M et N sont confondus si et seulement si $\dfrac{MA}{MP} = \dfrac{NA}{NP}$, i.e., $\dfrac{AB}{AC} = \dfrac{BP}{CP}$. Considérons les points A', B', C' tels que $PA \cdot PA' = PB \cdot PB' = PC \cdot PC'$, autrement dit, les images de A, B et C par l'inversion de pôle P et de rapport 1.

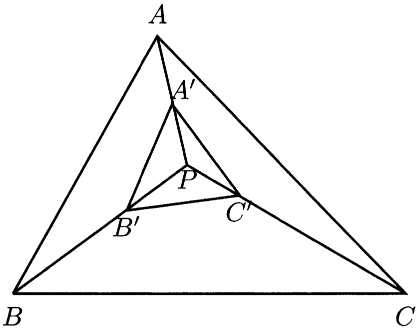


FIG. 6.51.

Les triangles PAB et $PA'B'$ sont alors semblables, d'où $\widehat{PA'B'} = \widehat{PBA}$, et de même $\widehat{PA'C'} = \widehat{PCA}$. Il s'ensuit que :

$$\begin{aligned}
\widehat{B'A'C'} &= \widehat{PBA} + \widehat{PCA} = (\widehat{B} - \widehat{PBC}) + (\widehat{C} - \widehat{PCB}) \\
&= (\pi - \widehat{A}) - (\pi - \widehat{BPC}) \\
&= \widehat{BPC} - \widehat{BAC},
\end{aligned}$$

et de même,

$$\widehat{A'C'B'} = \widehat{APB} - \widehat{ACB}, \qquad \widehat{A'B'C'} = \widehat{APC} - \widehat{ABC}.$$

Ainsi, la condition de l'énoncé implique que $A'B' = A'C'$. Or,

$$A'B' = \frac{PA'}{PB}AB = \frac{AB}{PB \cdot PA}, \qquad A'C' = \frac{PA'}{PC}AC = \frac{AC}{PA \cdot PC},$$

d'où le résultat.

2ème solution. Pour démontrer l'égalité $\dfrac{AB}{AC} = \dfrac{PB}{PC}$, on introduit deux points auxiliaires X et Y appartenant aux segments $[AB]$ et $[AC]$ respectivement et tels que :

$$\widehat{APX} = \widehat{ACB}, \qquad \widehat{APY} = \widehat{ABC}.$$

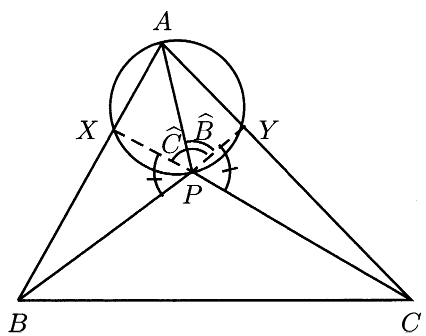


FIG. 6.52.

Il est alors clair que $AXPY$ est un quadrilatère inscriptible. Les triangles AXY et ABC sont donc semblables, et les droites (XY) et (BC) sont parallèles. D'un autre côté,

$$\frac{YC}{PC} = \frac{\sin\widehat{YPC}}{\sin\widehat{PYC}}, \qquad \frac{XB}{PB} = \frac{\sin\widehat{XPB}}{\sin\widehat{PXB}}.$$

Ainsi, $\dfrac{YC}{PC} = \dfrac{XB}{PB}$. (XY) et (BC) étant parallèles, on a $\dfrac{YC}{AC} = \dfrac{XB}{AB}$, soit enfin $\dfrac{AB}{AC} = \dfrac{PB}{PC}$, ce qu'il fallait démontrer.

---

34. La droite (PQ) coupe la corde commune $[EF]$ en K, le cercle circonscrit au triangle QCD en R et le cercle circonscrit au triangle PAB en S. On désigne par O le point d'intersection des droites (AB) et (CD).

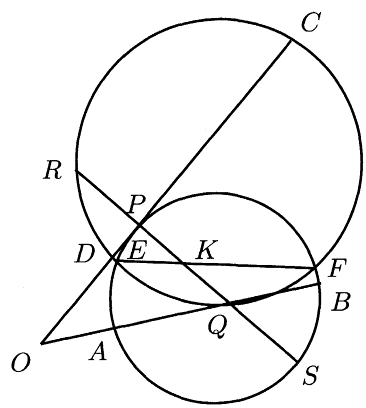


FIG. 6.53.

On pose $a = OA$, $b = OB$, $c = OC$, $d = OD$, $p = OP$ et $q = OQ$. En utilisant la puissance d'un point par rapport à un cercle, on obtient :

$$KP \cdot KS = KE \cdot KF = KQ \cdot KR,$$

ce qui permet d'écrire :

$$\frac{PR}{KP} = \frac{KR}{KP} - 1 = \frac{KS}{KQ} - 1 = \frac{QS}{KQ}.$$

Il s'ensuit que l'égalité $KP = KQ$ est équivalente à $PR = QS$, ou

$$CP \cdot DP = PR \cdot PQ = QS \cdot PQ = AQ \cdot BQ.$$

Or, $p^2 = ab$ et $q^2 = cd$, ce qui transforme l'égalité $(c-p)(p-d) = (q-a)(b-q)$ en l'égalité $(ac - bd)(bc - ad) = 0$. Comme $b > a$ et $c > d$, on a $ac - bd = 0$, c'est-à-dire $\dfrac{b}{a} = \dfrac{c}{d}$, ce qui équivaut à $(BC) \parallel (AD)$.

35.

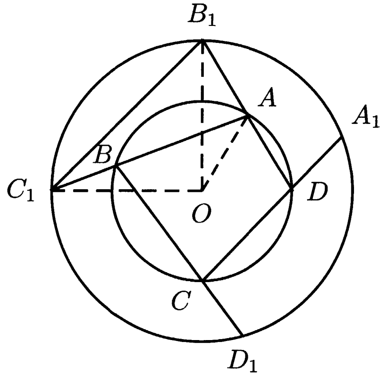


FIG. 6.54.

On désigne par O le centre commun des deux cercles. On applique alors l'inégalité de Ptolémée aux quadrilatères OAB_1C_1, OBC_1D_1, OCD_1A_1 et ODA_1B_1, ce qui donne :

$$\begin{aligned} 2AC_1 &\leqslant B_1C_1 + 2AB_1, \\ 2BD_1 &\leqslant C_1D_1 + 2BC_1, \\ 2CA_1 &\leqslant D_1A_1 + 2CD_1, \\ 2DB_1 &\leqslant A_1B_1 + 2DA_1. \end{aligned}$$

En additionnant ces inégalités, on arrive au résultat recherché. Pour que l'égalité ait lieu, il faut et il suffit que les quatre quadrilatères soient inscriptibles. Or, ceci implique que :

$$\widehat{OAC_1} = \widehat{OB_1C_1} = \widehat{OC_1B_1} = \widehat{OAD},$$

autrement dit, $[AO)$ est la bissectrice de l'angle $\widehat{BAD}$. De même, $[BO)$, $[CO)$ et $[DO)$ sont respectivement les bissectrices des angles $\widehat{ABC}$, $\widehat{BCD}$ et $\widehat{CDA}$. Il s'ensuit que O est le centre du cercle inscrit dans le quadrilatère $ABCD$, ce qui montre que $ABCD$ est un carré.

Réciproquement, si $ABCD$ est un carré, $A_1B_1C_1D_1$ est aussi un carré, et l'égalité a bien lieu.

---

36. On pose $a = AB$, $b = BC$, $c = CD$, $d = DA$, $x = B_1A$, $y = C_1B$, $z = D_1C$ et $\omega = A_1D$.

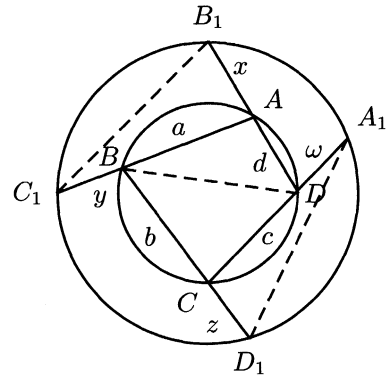


FIG. 6.55.

En utilisant la puissance d'un point par rapport à un cercle, on peut écrire : $x(x+d) = y(y+a) = z(z+b) = \omega(\omega+c) = R_1^2 - R^2$.

D'un autre côté, $\widehat{B_1AC_1} = \pi - \widehat{DAB} = \widehat{DCB} = \pi - \widehat{A_1CD_1}$. Il s'ensuit que :

$$\frac{\mathcal{A}(AB_1C_1)}{\mathcal{A}(ABCD)} = \frac{x(a+y)}{ad+bc}, \qquad \frac{\mathcal{A}(A_1CD_1)}{\mathcal{A}(ABCD)} = \frac{z(c+\omega)}{ad+bc},$$

et de la même façon, on obtient

$$\frac{\mathcal{A}(BC_1D_1)}{\mathcal{A}(ABCD)} = \frac{y(b+z)}{ab+cd}, \qquad \frac{\mathcal{A}(A_1B_1D)}{\mathcal{A}(ABCD)} = \frac{\omega(d+x)}{ab+cd}.$$

On a ainsi :

$$\begin{aligned}
\frac{\mathcal{A}(A_1B_1C_1D_1)}{\mathcal{A}(ABCD)} &= 1 + \frac{x(a+y)+z(c+\omega)}{ad+bc} + \frac{y(b+z)+\omega(d+x)}{ab+cd} \\
&= 1 + (R_1^2 - R^2)\left[\frac{x}{y(ad+bc)} + \frac{z}{\omega(ad+bc)} + \right. \\
&\qquad \left. \frac{y}{z(ab+cd)} + \frac{\omega}{x(ab+cd)}\right] \\
&\geqslant 1 + \frac{4(R_1^2 - R^2)}{\sqrt{(ad+bc)(ab+cd)}}.
\end{aligned}$$

Or,

$$\begin{aligned}
2\sqrt{(ad+bc)(ab+cd)} &\leqslant (ad+bc)+(ab+cd) = (a+c)(b+d) \\
&\leqslant \frac{1}{4}(a+b+c+d)^2 \leqslant 8R^2,
\end{aligned}$$

la dernière inégalité résultant du fait que parmi les quadrilatères inscrits dans un même cercle, le carré a le plus grand périmètre.

En conclusion, on a :

$$\frac{\mathcal{A}(A_1B_1C_1D_1)}{\mathcal{A}(ABCD)} \geqslant 1 + \frac{4(R_1^2 - R^2)}{4R^2} = \frac{R_1^2}{R^2}.$$

---

37. L'étape cruciale dans la solution de cet exercice consiste à considérer un rectangle contenant l'hexagone $ABCDEF$.

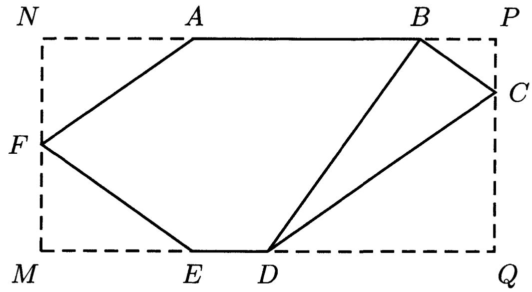


FIG. 6.56.

L'exercice est, semble-t-il, impossible sans cette manœuvre. Ceci explique en partie la raison pour laquelle le taux de réussite de cet exercice par les candidats ait été le plus bas dans toute l'histoire des olympiades internationales.

Dans le triangle BCD, on peut écrire :

$$4R_C = \frac{2BD}{\sin \widehat{C}} \geqslant \frac{NM + PQ}{\sin \widehat{C}} = \frac{NF + FM + PC + CQ}{\sin \widehat{C}}.$$

D'un autre côté,

$$NF = AF \sin \widehat{A}, \quad FM = FE \sin \widehat{E},$$
$$PC = BC \sin \widehat{B} = BC \sin \widehat{E}, \quad CQ = CD \sin \widehat{D} = CD \sin \widehat{A}.$$

Il s'ensuit que :

$$4R_C \geqslant AF\frac{\sin \widehat{A}}{\sin \widehat{C}} + FE\frac{\sin \widehat{E}}{\sin \widehat{C}} + BC\frac{\sin \widehat{E}}{\sin \widehat{C}} + CD\frac{\sin \widehat{A}}{\sin \widehat{C}},$$

et de même,

$$4R_A \geqslant CD\frac{\sin \widehat{C}}{\sin \widehat{A}} + ED\frac{\sin \widehat{E}}{\sin \widehat{A}} + AF\frac{\sin \widehat{C}}{\sin \widehat{A}} + AB\frac{\sin \widehat{E}}{\sin \widehat{A}},$$

et

$$4R_E \geqslant AB\frac{\sin \widehat{A}}{\sin \widehat{E}} + BC\frac{\sin \widehat{C}}{\sin \widehat{E}} + ED\frac{\sin \widehat{A}}{\sin \widehat{E}} + EF\frac{\sin \widehat{C}}{\sin \widehat{E}}.$$

Ceci donne finalement :

$$\begin{aligned}
4(R_A + R_C + R_E) &\geqslant FA\Big(\frac{\sin\widehat{A}}{\sin\widehat{C}} + \frac{\sin\widehat{C}}{\sin\widehat{A}}\Big) + EF\Big(\frac{\sin\widehat{C}}{\sin\widehat{E}} + \frac{\sin\widehat{E}}{\sin\widehat{C}}\Big)\\
&+ DE\Big(\frac{\sin\widehat{E}}{\sin\widehat{A}} + \frac{\sin\widehat{A}}{\sin\widehat{E}}\Big) + CD\Big(\frac{\sin\widehat{A}}{\sin\widehat{C}} + \frac{\sin\widehat{C}}{\sin\widehat{A}}\Big)\\
&+ BC\Big(\frac{\sin\widehat{C}}{\sin\widehat{E}} + \frac{\sin\widehat{E}}{\sin\widehat{C}}\Big) + AB\Big(\frac{\sin\widehat{E}}{\sin\widehat{A}} + \frac{\sin\widehat{A}}{\sin\widehat{E}}\Big),
\end{aligned}$$

soit encore :

$$4(R_A + R_C + R_E) \geqslant 2(FA + EF + DE + CD + BC + AB) = 2p,$$

d'où le résultat.

BIBLIOGRAPHIE

1. Akkar Mohammed, Akkar Marie-Thérèse, El Mossadeq Abdel Illah, Les mathématiques par les problèmes, Sochepress, Casablanca, 1985.

2. Boudine Jean-Pierre, Lo Jacomo François, Cuculière Roger, Olympiades Internationales de Mathématiques 1988-1997, Éditions du Choix, 1998.

3. Casiro Francis, Ferréol Robert, Olympiades Internationales et Concours Général 1983-1987, Éditions du Choix, 1989.

4. Casiro Francis, Cuculière Roger, Ferréol Robert, Olympiades Internationales et Concours Général 1988-1990, Éditions du Choix, 1991.

5. Chuan-Chong Chen, Khee-Meng Koh, Principles and Techniques in Combinatorics, World Scientific, 1992.

6. Comtet Louis, Analyse combinatoire, tomes I et II, Presses Universitaires de France, 1970.

7. Engel Arthur, Problem-Solving Strategies, Springer-Verlag, New York, 1998.

8. Fomin Dmitry, Genkin Sergey, Ilia Itenberg, Mathematical Circles, American Mathematical Society, 1996.

9. Fomin Dmitry, Kirichenko Alexey, Leningrad Mathematical Olympiads 1987-1991, MathPro Press, Westford, 1994.

10. Gerll Denis, Girard Georges, Les Olympiades Internationales de Mathématiques 1959-1975, Hachette, 1976.

11. Greitzer Samuel, International Mathematical Olympiads, 1959-1977, The Mathematical Association of America, 1977.

12. Hardy G. H., Littlewood Ernest, Pólya George, Inequalities, Cambridge University Press, 1952.

13. Hardy G. H., Wright E. M., An introduction to the theory of numbers, Oxford University Press, 1954.

14. Kazarinoff Nicholas, Geometric Inequalities, The Mathematical Association of America. Washington, DC, 1961.

15. Klamkin Murray, International Mathematical Olympiads, 1978-1985, The Mathematical Association of America, 1986.

16. Klamkin Murray, USA Mathematical Olympiads 1972-1986, The Mathematical Association of America, 1988.

17. Labelle Jacques, Théorie des graphes, Vuibert, Paris, 1982.

18. Liu Andy, Chinese Mathematics Competitions and Olympiads 1981-1993, Australian Mathematics Trust, 1998.

19. Lozansky Edward, Rousseau Cecil, Winning Solutions, Springer-Verlag, New York, 1996.

20. Nathan Altshiller-Court, College Geometry, Barnes & Noble, New York, 1952.

21. Sierpinski Waclaw, 250 problèmes de théorie élémentaire des nombres, Hachette, 1972.

22. Slinko Arkadii, USSR Mathematical Olympiads 1989-1992, Australian Mathematics Trust, 1997.

23. Soifer Alexandre, Les mathématiques par la résolution de problèmes, Éditions du Choix, 1995.

24. Sortais Yvonne, Sortais René, La géométrie du triangle, Hermann, 1987.

25. Steinhaus Hugo, Cent problèmes élémentaires de mathématiques, PWN-Gauthier-Villars, 1965.

NOTATIONS UTILISÉES

$\varnothing$: l'ensemble vide.

$\Longleftrightarrow$: si et seulement si.

$\Longrightarrow$: implique.

$\mathbb{N}$ (resp. $\mathbb{N}^*$) : ensemble des entiers naturels (resp. ensemble des entiers naturels non nuls).

$\mathbb{Z}$ (resp. $\mathbb{Z}^*$) : ensemble des entiers (resp. ensemble des entiers non nuls).

$\mathbb{Q}$ (resp. $\mathbb{Q}^*$) : ensemble des nombres rationnels (resp. ensemble des nombres rationnels non nuls).

$\mathbb{R}$ (resp. $\mathbb{R}^*$, resp. $\mathbb{R}_+$, resp. $\mathbb{R}_-$) : ensemble des nombres réels (resp. ensemble des nombres réels non nuls, resp. ensemble des nombres réels positifs, resp. ensemble des nombre réels négatifs).

$\mathbb{C}$ (resp. $\mathbb{C}^*$) : ensemble des nombres complexes (resp. ensemble des nombres complexes non nuls).

$|z|$: module du nombre complexe z.

$\operatorname{Arg}(z)$: argument du nombre complexe z.

$\Re e\,(z)$: partie réelle du nombre complexe z.

$\Im m\,(z)$: partie imaginaire du nombre complexe z.

$x \mid y$: x divise y.

$x \nmid y$: x ne divise pas y.

$x \equiv y \pmod{n}$: x est congru à y modulo n.

(x, y) : plus grand commun diviseur de x et y.

$[x, y]$: plus petit commun multiple de x et y.

$\lceil x \rceil$: plus petit entier supérieur ou égal à x.

$\lfloor x \rfloor$: plus grand entier inférieur ou égal à x (partie entière de x).

$\mathbb{Z}/n\mathbb{Z}$: ensemble des classes de résidus modulo n.

$\varphi(n)$: indicatrice d'Euler.

$(u_n)_{n\in\mathbb{N}}$: suite numérique indexée par $\mathbb{N}$.

$\mathbb{K}[X]$: ensemble des polynômes à coefficients dans le corps commutatif $\mathbb{K}$.

$|A|$ $\big($ou card$(A)\big)$: nombre d'éléments (cardinal) de l'ensemble fini A.

$x \in A$: x appartient à l'ensemble A.

$x \notin A$: x n'appartient pas à l'ensemble A.

$A \subseteq B$: A est un sous-ensemble de B.

$A \subset B$: A est un sous-ensemble strict de B.

$A \cap B$: l'intersection des deux ensembles A et B.

$A \cup B$: l'union des deux ensembles A et B.

$\displaystyle\binom{n}{p}$: nombre de sous-ensembles à p éléments d'un ensemble à n éléments.

$\mathcal{G}_n$: graphe complet à n sommets.

AB : distance des deux points A et B.

$\overline{AB}$: mesure algébrique du bipoint (A, B).

$\overrightarrow{AB}$: vecteur d'origine A et d'extrémité B.

(AB) : droite déterminée par les deux points distincts A et B.

$[AB]$: segment d'extrémités A et B.

$[AB)$: demi-droite d'origine A et passant par le point B, $B \neq A$.

$\hat{A}$, $\hat{B}$, $\hat{C}$: mesures des angles du triangle ABC.

$[\widehat{ABC}]$: angle (positif) déterminé par les deux demi-droites $[BA)$ et $[BC)$.

$\widehat{ABC}$: mesure (positive) en radians de l'angle déterminé par les deux demi-droites $[BA)$ et $[BC)$.

$(D) \parallel (\Delta)$: la droite (D) est parallèle à la droite (Δ).

$(D) \perp (\Delta)$: la droite (D) est perpendiculaire à la droite (Δ).

$\mathcal{A}(P)$: aire du polygone P.

$\vec{u} \cdot \vec{v}$: produit scalaire des vecteurs $\vec{u}$ et $\vec{v}$.

INDEX

A

B

C

D

E

F

Achevé d'imprimer en novembre 2007
dans les ateliers de Normandie Roto Impression s.a.s.
61250 Lonrai
N° d'impression : 07-3393
Dépôt légal : novembre 2007

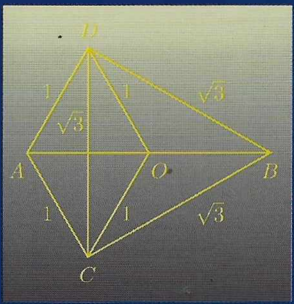
Imprimé en France

Les olympiades internationales de mathématiques ont connu un essor extraordinaire pendant les deux dernières décennies. En abordant les thèmes traditionnellement traités dans les olympiades nationales et internationales, ce livre met à la disposition du lecteur un outil complet de préparation à ce type de compétitions.

Chaque chapitre débute par une présentation des stratégies et techniques utiles et se poursuit par de nombreux exercices corrigés.

Ce livre peut être aussi utilisé pour préparer le concours général. Son contenu est d'un abord facile pour un élève courageux de terminale. Il pourra intéresser plus généralement tous ceux que les mathématiques passionnent.

Le lecteur trouvera ici :



- les stratégies utiles dans la résolution des problèmes d'olympiades ;
- les résultats que le candidat sérieux se doit de connaître ;
- des exemples choisis pour les idées instructives qu'ils contiennent ;
- plus de 150 problèmes tirés des olympiades nationales et internationales.

Préfaces de Claude Deschamps, leader de l'équipe de France aux olympiades internationales de mathématiques, et de Paul-Louis Hennequin, vice-président d'ANIMATH.

9 782729 836610

www.editions-ellipses.fr