Les problèmes de l'A.P.M.E.P.

Cette rubrique propose des problèmes choisis pour l'originalité de leur caractère : esthétique, subtil, ingénieux, voire récréatif, dont la solution nécessite initiatives, démarche inventive, recherche, effort intellectuel.

Elle accueille tous ceux qui aiment inventer, chercher de "beaux problèmes"...si possible trouver des solutions, et les invite à donner libre cours à leur imagination créatrice.

Priorité est naturellement réservée aux énoncés composés par des collègues et au dialogue ouvert entre eux par le jeu des réponses et des solutions. Les auteurs sont priés de joindre les solutions aux propositions d'énoncés. Énoncés, réponses et solutions sont à envoyer à l'adresse suivante (réponse à des problèmes différents sur feuilles séparées S.V.P., sans oublier votre nom sur chaque feuille) :

François LO JACOMO
21 rue Juliette Dodu,
75010 PARIS.

ÉNONCÉS

ÉNONCÉ N°237(Charles NOTARI, Montaut)
Soient $ABCD$ et $AEFG$ deux carrés ayant un sommet commun A et des côtés de longueurs différentes. Soit P l'intersection de la droite (EF) avec la droite (CD). A quelle condition les droites (AP) et (CF) sont-elles perpendiculaires ?

ÉNONCÉ N° 238 (Jacques AMON, Limoges)
La surface d'équation $x^n + y^n + z^n = a^n$ contient-elle des droites, et si oui, lesquelles ?

ÉNONCÉ N°239 (Igor CHARIGUINE, Moscou)
A l'intérieur d'un triangle ABC, on trace un cercle de rayon a tangent aux côtés $[AB]$ et $[AC]$. A partir des sommets B et C, on trace deux tangentes à ce cercle, qui se coupent au point M.
Démontrer que le rayon ρ du cercle inscrit dans le triangle BCM peut se cal-

culer par la formule : $\rho = r_a\left(\frac{r-a}{r_a-a}\right)$ où r est le rayon du cercle inscrit dans le triangle ABC et r_a le rayon du cercle exinscrit, tangent au côté $[BC]$ et aux prolongements des côtés $[AB]$ et $[AC]$.

SOLUTIONS

ÉNONCÉ N° 219 (François LO JACOMO, Paris)

Trouver le plus possible de fonctions f, de **R** dans **R** (ou resp. de **C** dans **C**) vérifiant pour tout réel (resp. complexe) x et tout entier $n > 0$:

$$f(x) = \sum_{k=0}^{n-1} f\left(\frac{x+k}{n}\right).$$

SOLUTIONS proposées par Pierre SAMUEL (Bourg la Reine)

Il s'agit de trouver des fonctions f, de **R** dans **R** ou de **C** dans **C** qui, pour tout entier $n > 0$ et tout x, vérifient :

$$\text{A}(n,x) \qquad f(x) = \sum_{k=0}^{n-1} f\left(\frac{x+k}{n}\right)$$

En posant $x = nz$, A(n,x) équivaut à :

$$\text{B}(n,z) \qquad f(nz) = f(z) + f\left(z+\frac{1}{n}\right) + \ldots + f\left(z+\frac{n-1}{n}\right).$$

Ces fonctions seront appelées "solutions".

1 - QUELQUES REMARQUES ALGÉBRIQUES SIMPLES.

a) Les solutions forment un espace vectoriel sur **R** (ou **C**).

b) On a $f(\frac{1}{2}) = 0$ (appliquer B(2,0)).

c) Si f est un polynôme de terme dominant az^q ($a \neq 0$), les termes dominants des deux membres de B(n,z) sont $an^q z^q$ et naz^q. L'égalité n'est possible que pour $q = 1$. Pour un tel polynôme $f(z) = az + b$, la condition B(n,z) équivaut à

$$anz + b = naz + \frac{a}{n}\left(1 + 2 + \ldots + (n-1)\right) + nb \quad , \quad \text{c'est-à-dire} \quad \text{à}$$

$(1-n)\,b = \frac{a}{n} \times \frac{1}{2} n\,(n-1)$, ou encore $b = -\frac{1}{2}a$. *Les seules solutions polynômiales* sont donc de la forme $f(z) = a\left(z - \frac{1}{2}\right)$.

d) Un calcul analogue montre que les fonctions complexes de la forme $f(z) = az + b\bar{z} - \frac{1}{2}(a+b)$ sont aussi des solutions.

2 - DÉTERMINATION DES SOLUTIONS CONTINUES DIFFÉRENTIABLES

En faisant la différence de A(n, z + 1) et de A(n,z), on obtient, pour tout entier $n>0$, $f(x+1) - f(x) = f\left(\frac{x+n}{n}\right) - f\left(\frac{x}{n}\right)$. En supposant f *continue*, on fait tendre n vers l'infini et on obtient $f(z+1) - f(z) = f(1) - f(0)$ pour tout z. Remplaçons f par la fonction g définie par $g(z) = f(z) - f\left(\frac{3}{2}\right)\left(z - \frac{1}{2}\right)$ qui est aussi une solution par (1.c), de sorte que $g(z+1) - g(z)$ est encore une constante. Or celle-ci est nulle car $g\left(\frac{3}{2}\right) = g\left(\frac{1}{2}\right) = 0$ (cf.1.b). Donc g est *périodique de période* 1.

Traitons directement le cas d'une solution périodique g définie sur **C**. Pour $z = x + iy$ (x,y réels), posons $g(z) = G(x,y)$ et supposons G continûment différentiable. Alors B(n,z) s'écrit:

$$(1) \qquad G(nx,ny) = G(x,y) + G\left(x + \frac{1}{n}, y\right) + \ldots + G\left(x + \frac{n-1}{n}, y\right).$$

D'où, en dérivant par rapport à x, et en divisant par n,

$$G'_x(nx,ny) = \frac{1}{n}\left(G'_x(x,y) + G'_x\left(x + \frac{1}{n}, y\right) + \ldots + G'_x\left(x + \frac{n-1}{n}, y\right)\right).$$

Si n tend vers l'infini, le second membre tend vers $\int_x^{x+1} G'_x(x+t,y)\,dt$ car G'_x est continue. Comme G est une primitive de G'_x, l'intégrale vaut $G(x+1,y) - G(x,y) = g(z+1) - g(z)$ et est nulle d'après la périodicité. Ainsi $G'_x(nx,ny)$ tend vers 0. Or on a le lemme suivant:

Lemme - Soit $h : \mathbf{R} \to \mathbf{C}$ une fonction continue et périodique de période 1. Si, pour tout x réel, la suite $(h(nx))$ $(n \in \mathbf{N})$ tend vers 0, alors h est nulle.

Soit $\frac{p}{q}$ (p et q entiers et $q > 0$) un nombre rationnel quelconque. Prenons $x = \frac{1}{q}$ et faisons tendre n vers l'infini dans la progression arithmétique $p + \mathbf{N}q$. Alors $h\left(n.\frac{1}{q}\right) = h\left(\frac{p}{q}\right)$ est un nombre indépendant de n. Comme sa limite est nulle, il est nul. Ainsi h est nulle sur $\mathbf{Q}$ donc sur $\mathbf{R}$ par continuité.

Remarque : Par changement linéaire de variable, la conclusion reste vraie pour une période quelconque. On aurait pu aussi utiliser le fait que, pour x irrationnel, l'ensemble des nx est dense modulo 1.

Le lemme montre que la restriction de G'_x à $\mathbf{R}$ est nulle. Ainsi la restriction de G à $\mathbf{R}$ est constante, donc *nulle* par (1.c).

Cela règle le cas des *solutions continûment dérivables définies sur* $\mathbf{R}$: ce sont les polynômes $f(x) = a\left(x - \frac{1}{2}\right)$.

Revenons aux fonctions définies sur C. En divisant par n la formule (1), on voit que $\frac{g(nz)}{n} = \frac{G(nx,ny)}{n}$ tend vers l'intégrale $\int_x^{x+1} G(t,y)\,dt$ qui, par périodicité, vaut $\int_0^1 G(t,y)\,dt$. Cette intégrale ne dépend que de y; notons-la $c(y)$. Ainsi $\frac{g(nz)}{n}$ tend vers $c(y)$.

Soient alors p et q deux entiers positifs. Les limites des deux membres de $\frac{g(n.pz)}{n} = \frac{pg(np.z)}{np}$ sont respectivement $c(py)$ et $pc(y)$, d'où $c(py) = pc(y)$; de même, $c(y) = q.c\left(\frac{y}{q}\right)$ et $p.c(y) = q.c\left(\frac{py}{q}\right)$. Ainsi, $c(ry) = rc(y)$ pour tout nombre rationnel $r > 0$. Comme c est continue (en tant qu'intégrale d'une fonction $G(t,y)$ qui dépend continûment du paramètre y), on a $c(ay) = ac(y)$ pour tout a réel positif, d'où $c(a) = ac(1)$, de sorte que $c(y)$ est de la forme ky, k constante, pour $y \geq 0$. De même $c(y) = k'y$ pour $y \leq 0$. Comme $c(y) = \int_0^1 G(t,y)\,dt$ est dérivable, on en déduit $k' = k$ et $c(y) = ky$ pour tout y réel.

Or la fonction $z = xi + y \mapsto y$ est une solution, car elle vaut $\frac{1}{2} i(\bar{z} - z)$ (cf.1,d). Pour elle, $k = 1$. Par linéarité, on peut donc supposer $k = 0$.

Comme ci-dessus pour G'_x, on voit que $G'_y(nx,ny)$ tend vers $\int_0^1 G'_y(t,y)\,dt$. Par dérivation par rapport à y de l'égalité $ky = c(y) = \int_0^1 G(t,y)\,dt$, cette limite vaut $k = 0$. Donc $G'_y(nx,ny)$ tend vers 0 et le lemme montre que la restriction de G'_y à $\mathbf{R}$ est nulle.

On suppose alors que G'_y est dérivable par rapport à y et que sa dérivée G''_{yy} a son module borné par un nombre $M>0$ dans la bande $|y| \leq 1$; par périodicité, c'est vrai si G''_{yy} est continue. Dans la formule de Taylor

$$G(x,y) = G(x,0) + y\,G'_y(x,0) + R(x,y) = R(x,y)$$

le reste $R(x, y)$ a son module borné par $\frac{My^2}{2}$. D'où $|G(x,y)| \leq \frac{1}{2} My^2$ pour $|y| \leq 1$ et $x \in \mathbf{R}$. Soient u et v deux réels. Dans la formule $G(u,v) = \sum_{k=0}^{n-1} G\left(\frac{u+k}{n}, \frac{v}{n}\right)$, les modules des termes du second membre sont, pour n assez grand, tous bornés par $\frac{Mv^2}{2n^2}$. On a donc $|G(u,v)| \leq \frac{Mv^2}{2n}$, d'où $G(u,v) = 0$ en faisant tendre n vers l'infini. D'où le théorème :

> ***Théorème :*** Les solutions sur C, $f(z) = F(x,y)$ $(z = x + iy)$, où F est deux fois continûment différentiable, sont toutes de la forme $f(z) = az + b\bar{z} - \frac{1}{2}(a + b)$.

En fait, seules l'existence et la continuité de F'_x, F'_y et F''_{yy} ont été utilisées.

3 - D'AUTRES SOLUTIONS, D'ORDINAIRE TRES DISCONTINUES.

Soit E une partie de $\mathbf{R}$ ou de C, vérifiant la condition :

(S) Si $z \in \mathbf{E}$, $r \in \mathbb{Q}$ et si n est un entier >0, alors $z + r$ et nz sont dans E.

Alors, si $z \in$ E, toutes les variables figurant dans $B(n,z)$ sont dans E, de sorte

qu'une vérification algébrique de B(n,z) dans E suffit.

Donnons-nous alors une *partition* (finie ou infinie) de **R** en parties E_i vérifiant chacune (S), et pour chaque i, un nombre réel a_i. Alors la fonction f définie par $f(x) = a_i\left(x - \frac{1}{2}\right)$ pour $x \in E_i$ est une solution. Par exemple, on peut prendre $f(x) = 2x - 1$ pour x rationnel et $f(x) = 0$ pour x irrationnel.

Dans le cas des fonctions de **C** dans **C**, on se donne une partition de **C** en parties E_i vérifiant (S), et pour chaque i des nombres complexes a_i et b_i. Alors la fonction f définie par $f(z) = a_i z + b_i \bar{z} - \frac{1}{2}(a_i + b_i)$ pour $z \in E_i$ est une solution.

Exemples de telles partitions.

1) Considérons une suite croissante (finie ou transfinie) $F_1 \subset F_2 \subset \ldots \subset F_i \subset \ldots$ de sous **Q**-espaces vectoriels de **R** ou **C** telle que $\mathbf{Q} \subset F_1$ et posons $E_1 = F_1$, $E_i = F_i - F_{i-1}$ (complémentaire) pour $i \geq 2$. Les E_i forment une partition et chacun vérifie (S) car

➡ $z \in E_i$ et $r \in \mathbf{Q}$ donnent $z + r \in F_i$; et $z + r \in F_{i-1}$ est impossible, car impliquant $z \in F_{i-1}$ ($i \geq 2$).

➡ $z \in E_i$ et n entier >0 donnent $nz \in F_i$; et $nz \in F_{i-1}$ est impossible, car impliquant $z \in F_{i-1}$ ($n \neq 0$).

2) En particulier, on peut prendre pour suite (F_i) une suite croissante de *sous-corps* de **R** ou **C**. Ainsi la fonction f définie par $f(z) = 6z - 3$ pour z rationnel, $f(z) = z + 5\bar{z} - 3$ pour z algébrique non rationnel, et $f(z) = \bar{z} - \frac{1}{2}$ pour x transcendant est une solution.

3) La partition : axe réel, demi-plan $y>0$, demi-plan $y<0$ de **C** (avec $z = x + iy$). Celle-ci peut donner lieu à des solutions continues non dérivables.

Remarque : Donnons-nous deux partitions (E_i) et (F_j) dont tous les termes vérifient (S) et, pour chacune, une solution f et g. Toute combinaison linéaire de f et g est une solution par (1.a)). Mais elle peut être construite à partir de la partition $(E_i \cap F_j)$ par le procédé ci-dessus.

AUTRES SOLUTIONS

Charles NOTARI (Montaut) suggère de chercher en outre parmi les fonctions trigonométriques en signalant que pour tout $\theta \in \mathbf{R}$, $\prod_{k=0}^{n-1}\left(2\sin\left(\theta+\frac{k\pi}{n}\right)\right)=2\sin(n\theta)$ car si l'on applique l'identité:

$\forall z \in \mathbf{C}, z^n-1=\prod_{k=0}^{n-1}\left(z-e^{\frac{-2ki\pi}{n}}\right)$ à $z = e^{2i\theta}$, on obtient à gauche :

$z^n-1=2i\sin(n\theta)e^{in\theta}$ et à droite : $z-e^{-\frac{2ki\pi}{n}}=e^{i\left(\theta+\frac{\pi}{2}-\frac{k\pi}{n}\right)}\left(2\sin\left(\theta+\frac{k\pi}{n}\right)\right)$

Malheureusement, la fonction $f(x) = \ln|2\sin(\pi x)|$ n'est pas définie sur $\mathbf{Z}$, et il n'est pas possible de la prolonger sur $\mathbf{Z}$ de sorte que notre relation soit satisfaite pour tout x réel. En effet, pour $x = 0$, il faudrait que l'on ait : $\sum_{k=1}^{n-1} f\left(\frac{k}{n}\right)=0$ donc $\prod_{k=1}^{n-1}\left(2\sin\frac{k\pi}{n}\right)=1$ alors que, d'après l'identité précédente, $\forall z \in \mathbf{C}, \prod_{k=1}^{n-1}\left(z-e^{-\frac{2ki\pi}{n}}\right)=\left(z^{n-1}+z^{n-2}+\ldots+z+1\right)$, ce qui donne pour $z = 1$: $\prod_{k=1}^{n-1}\left(2\sin\frac{k\pi}{n}\right)=n$ D'ailleurs, on n'a même pas $f\left(\frac{1}{2}\right)=0$!

Je n'ai pas reçu d'autres réponses à cet énoncé, mais j'avais moi-même pensé à une fonction simple, celle qui a suggéré l'énoncé : la fonction partie entière $x \mapsto E(x)$.
Effectivement, si $x \in [pn + q, pn + q + 1[$ ($p \in \mathbf{Z}$ et q entier : $0 \le q < n$), $E\left(\frac{x+k}{n}\right)$ vaudra $p + 1$ pour les q valeurs de $k \ge n - q$ et vaudra p sinon.

On peut même varier sur ce thème, choisir six constantes complexes arbitraires $a_1, a_2, \ldots a_6$ et considérer la fonction g de $\mathbf{C} \to \mathbf{C}$ définie par:

- si $y = 0$ et $x \ge 0$, $g(x + iy) = a_1 E(x)$
- si $y > 0$ et $x \ge 0$, $g(x + iy) = a_2 E(x)$
- si $y < 0$ et $x \ge 0$, $g(x + iy) = a_3 E(x)$
- si $y = 0$ et $x < 0$, $g(x + iy) = a_4 E(x)$
- si $y > 0$ et $x < 0$, $g(x + iy) = a_5 E(x)$
- si $y < 0$ et $x < 0$, $g(x + iy) = a_6 E(x)$

qui satisfait bien la relation.

On peut aussi faire appel à la fonction h de $\mathbf{C} \to \mathbf{C}$, définie par:

- si x entier ≥ 1, $h(x + iy) = b_1$
- si x entier ≤ 0, $h(x + iy) = b_2$
- si $x \notin \mathbb{Z}$ $h(x + iy) = 0$

qui convient également, quelles que soient les constantes b_1 et b_2.

Peut-on en trouver d'autres qui ne se ramènent pas à celles de Pierre SAMUEL ou à celles-ci?

ÉNONCÉ N° 220 (M.ROUSSELET, Herblay)

Soit ABC un triangle quelconque. Déterminer le plus grand triangle équilatéral inscrit dans le triangle ABC.

SYNTHÈSE DES SOLUTIONS REÇUES

Suscité par un simple exercice posé en atelier de recherche de Troisième (ABC étant un triangle quelconque, peut-on y inscrire un triangle équilatéral?), cet énoncé a donné lieu à des développements multiples et intéressants qui je vais m'efforcer de résumer ici.

Edgard DELPLANCHE (Créteil) présente une étude savante de la famille des triangles équilatéraux IJK inscrits ou exinscrits dans le triangle ABC ($I \in (BC)$, $J \in (CA)$, $K \in (AB)$).

Cette même étude vaut pour toute famille de triangles IJK semblables à un triangle donné. Dans le cas des triangles équilatéraux, la démonstration de Charles NOTARI (Montant) s'en rapproche.

On remarque tout d'abord que les cercles circonscrits aux triangles AJK, BKI et CIJ se coupent en un point P (étudier les angles $\widehat{KPJ}$, $\widehat{IPK}$ et $\widehat{JPI}$), lequel est indépendant du triangle de la famille dans la mesure où les trois angles $\widehat{APB}$, $\widehat{BPC}$ et $\widehat{CPA}$ valent respectivement $\hat{C} + \hat{K}$, $\hat{B} + \hat{J}$ et $\hat{A} + \hat{I}$: il suffit d'étudier $\widehat{AJK} + \widehat{KIB} = \widehat{APB}$, etc... pour s'en convaincre. Si l'on appelle I_0, J_0 et K_0 les projections orthogonales de ce point pivot P sur (BC), (CA) et (AB) respectivement, $I_0J_0K_0$ appartient à la famille: les cercles circonscrits à AJ_0K_0, BK_0I_0 et CI_0J_0 ont même pour diamètres respectifs $[AP]$, $[BP]$ et $[CP]$. Le triangle $I_0J_0K_0$ est le plus petit triangle de la famille, les autres s'en déduisent par une similitude de centre P, d'angle φ et de rapport $\frac{1}{\cos \varphi}$. C'est donc pour φ maximum que l'on trouvera la solution de notre problème.

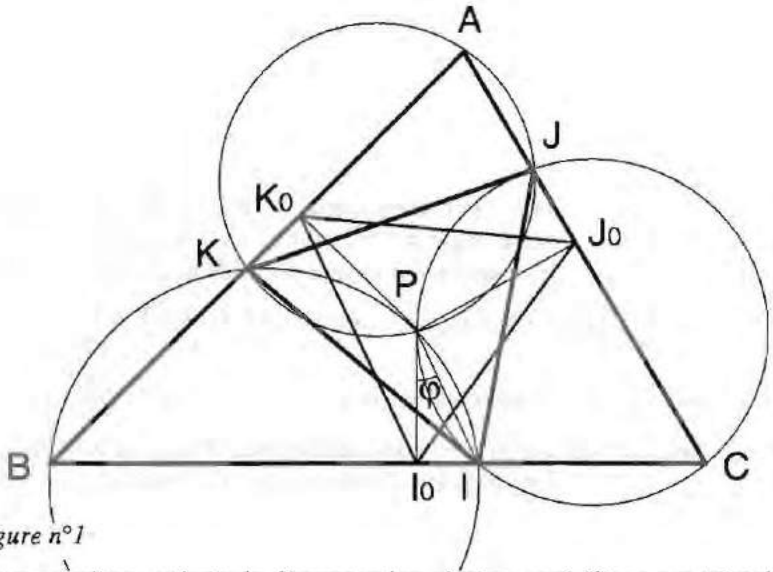


figure n°1

Cette première partie de la démonstration n'est pas spécifique aux triangles équilatéraux IJK, mais dans le cas particulier de la famille des triangles équilatéraux, on peut en dire plus : dans le cercle circonscrit à AJ_0K_0, dont $[AP]$ est un diamètre, $J_0K_0 = AP.\sin\widehat{A}$ et de même $K_0I_0 = BP.\sin\widehat{B}$, $I_0J_0 = CP.\sin\widehat{C}$, de sorte que si $I_0J_0K_0$ est équilatéral, $\frac{PA}{PB} = \frac{\sin\widehat{B}}{\sin\widehat{A}} = \frac{CA}{CB}$, P appartient donc au cercle d'Apollonius passant par C et les pieds des bissectrices intérieure et extérieure de $\widehat{C}$. Par symétrie, P appartient aux trois cercles d'Apollonius, mais ces trois cercles d'Apollonius se coupent en deux points (ils sont orthogonaux au cercle circonscrit à ABC).

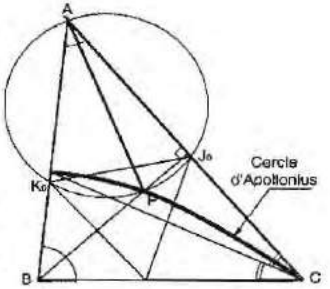


figure 2

René BENOIST (Palaiseau) et Michel BIGOT (Equeurdreville) s'efforcent, à partir d'un triangle équilatéral donné, d'en construire géométriquement un plus grand, alors que Marie-Laure CHAILLOUT opte délibérément pour le calcul trigonométrique. René MANZONI (Le Havre)

détermine analytiquement K comme intersection de (AB) avec la transformée de (AC) par la rotation de centre I et d'angle $\pi/3$. Son étude débouche sur deux cas, incitant à se demander : le point pivot P de la démonstration d'Edgard DELPLANCHE peut-il être en I? Bien sûr! il suffit que $\widehat{A} = \frac{2\pi}{3}$ et que I soit le pied de la bissectrice intérieure de $\widehat{A}$. D'une part, parce qu'alors la rotation de centre I et d'angle $\pi/3$ transforme (AC) en (AB), donc tout point J de la droite (AC) en un point K de la droite (AB) tel que IJK soit équilatéral. D'autre part, parce que, comme $\sin\frac{\pi}{3} = \sin\frac{2\pi}{3}$, $\frac{IB}{IA} = \frac{CB}{CA}$ et $\frac{IC}{IA} = \frac{BC}{BA}$, ce qui signifie que I appartient aux trois cercles d'Apollonius.

Je m'attarderai davantage sur la démonstration de Raymond RAYNAUD (Digne), qui met en avant trois idées intéressantes. La première, c'est qu'il est possible de retourner le problème en recherchant non pas le plus grand triangle équilatéral IJK inscrit dans ABC, mais le plus petit triangle semblable à ABC circonscrit à un triangle équilatéral donné IJK. La seconde, c'est que si l'on admet que $I \in [BC]$, $J \in [CA]$ et $K \in [AB]$, un tel triangle peut être explicitement construit à l'aide des arcs capables, l'un de centre a qui voit $[JK]$ sous l'angle $\widehat{A}$, un autre de centre b qui voit $[KI]$ sous l'angle $\widehat{B}$ et un troisième de centre c voyant $[IJ]$ sous l'angle $\widehat{C}$. Une droite quelconque ou presque passant par K coupera deux de ces arcs capables en A et B. (AJ) et (BI) se couperont en C, qui appartient au troisième arc capable puisqu'il voit $[IJ]$ sous l'angle $\widehat{C}$. Ces arcs capables sont d'ailleurs les cercles circonscrits à AJK, BKI et CIJ de la démonstration d'Edgard DELPLANCHE.

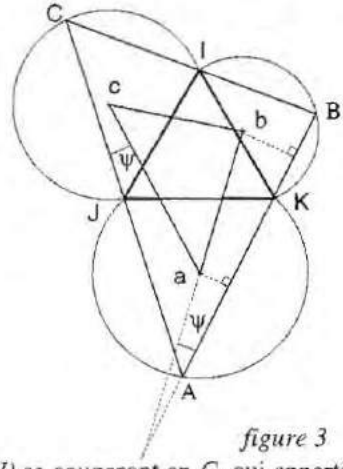


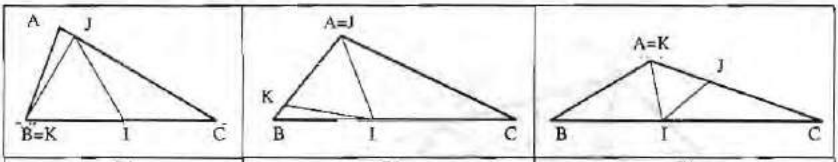
figure 3

La troisième idée, c'est que a et b étant les centres des arcs capables contenant A et B, la projection orthogonale de a sur $[AK]$ (donc sur $[AB]$) est le milieu de $[AK]$, et la projection orthogonale de b sur $[BK]$ (donc sur $[AB]$)

est le milieu de $[BK]$, si bien que $AB = 2ab \cos \psi$, ψ étant l'angle que fait (AB) avec (ab). Il en résulte que c'est pour ψ maximum qu'on trouvera la solution de notre problème, alors que $\psi = 0$ ((AB) parallèle à (ab)) nous donne le plus grand triangle semblable à ABC circonscrit au triangle IJK donné. A noter que le fait que IJK soit équilatéral ne joue aucun rôle dans la démonstration, et que, par ailleurs, le triangle abc est nécessairement semblable à ABC.

Cette démonstration peut être utilisée pour trouver le plus grand triangle équilatéral circonscrit à un triangle ABC donné. Les centres des arcs capables voyant $[AB]$, $[BC]$ et $[AC]$ sous un angle $\pi/3$ sont les points C', A' et B' tels que les triangles $AC'B$, $BA'C$ et $CB'A$ soient isocèles avec $\widehat{C'} = \widehat{B'} = \widehat{A'} = \frac{2\pi}{3}$. On reconnaît là une situation classique où l'on démontre que le triangle $A'B'C'$ est équilatéral. Le plus grand triangle équilatéral circonscrit à ABC a ses côtés parallèles à ceux de $A'B'C'$: si T est l'intersection des trois cercles contenant les arcs capables (T est le point de Toricelli du triangle ABC où l'on voit les trois côtés sous l'angle $2\pi/3$ ou $-\pi/3$), l'homothétie de centre T et de rapport 2 transforme $A'B'C'$ en $A''B''C''$, solution de notre problème: $[A''B'']$est bien parallèle à $[A'B']$ et de longueur double et il passe par C car $[TA'']$ et $[TB'']$ étant des diamètres de leurs cercles respectifs, $\widehat{TCA''}$ et $\widehat{TCB''}$ sont des angles droits. Le même résultat pouvait être atteint par la méthode d'Edgard DELPLANCHE sous réserve de retourner le problème (chercher le plus petit triangle semblable à ABC inscrit dans le triangle $A''B''C''$ donné), et Charles NOTARI nous informe qu'il a été obtenu par FASHBENDER en 1846.

Toutes ces méthodes conduisent au même résultat: le plus grand triangle équilatéral IJK tel que $I \in [BC]$, $J \in [CA]$ et $K \in [AB]$ a un sommet confondu avec un sommet du triangle ABC, et deux sommets appartenant à un même côté de ABC. Suivant les cas, on obtient :*(figure 4)*



Si	Si	Si
$\widehat{A} \geq \widehat{B} \geq \pi/3 \geq \widehat{C}$	$2\pi/3 \geq \widehat{A} \geq \pi/3 \geq \widehat{B} \geq \widehat{C}$	$\widehat{A} \geq 2\pi/3 \geq \widehat{B} \geq \widehat{C}$

Mais la question que l'on peut raisonnablement ou déraisonnablement se poser, c'est : pourquoi faut-il se limiter aux triangles équilatéraux ayant un sommet sur [*BC*], un sur [*CA*] et un sur [*AB*]? Peut-être est-ce la définition d'un triangle inscrit dans un autre, mais alors, n'existe-t-il pas d'autres triangles équilatéraux plus grands que ceux de la figure 4 n'ayant aucun sommet à l'extérieur de *ABC*, et quel est le plus grand d'entre eux?

La question a été envisagée sous cet angle par Charles NOTARI et Marguerite PONCHAUX (Lille), et le raisonnement ci-dessous est très proche de la démonstration de Marguerite PONCHAUX.

Considérons un triangle équilatéral *IJK* n'ayant aucun sommet à l'extérieur de *ABC*. S'il ne touche aucun côté, il existe une homothétie de centre *I* et de rapport strictement supérieur à 1 qui le transforme en un triangle touchant au moins un côté (en *J* ou en *K*). S'il ne touche qu'un seul côté, par exemple en *J* ou bien en *J* et *K*, il existe une homothétie de centre *J* et de rapport strictement supérieur à 1 qui le transforme en un triangle plus grand touchant au moins deux côtés (le deuxième en *I* ou en *K*). Et s'il touche deux côtés distincts, par exemple [*AB*] et [*AC*], il existe une homothétie de centre *A* et de rapport supérieur à 1 qui le transforme en un triangle touchant les trois côtés.

De sorte que le plus grand triangle équilatéral n'ayant aucun sommet extérieur à *ABC* touche obligatoirement les trois côtés du triangle *ABC*. Mais cela ne signifie aucunement qu'il a un sommet sur [*BC*], un sur [*CA*] et un sur [*AB*] : il peut avoir un sommet confondu avec *A*, *B* ou *C* et toucher le côté opposé. Et c'est même exclusivement parmi ces derniers triangles qu'il faut rechercher la solution de notre problème.

Supposons en effet qu'un triangle *IJK* équilatéral vérifie : $I \in]BC[$, $J \in]CA[$ et $K \in]AB[$, et supposons que l'angle $\widehat{A}$ soit le plus grand des trois (au sens large), ce qui entraîne que $\widehat{B}$ et $\widehat{C}$ sont strictement inférieurs à $\pi/2$, la droite

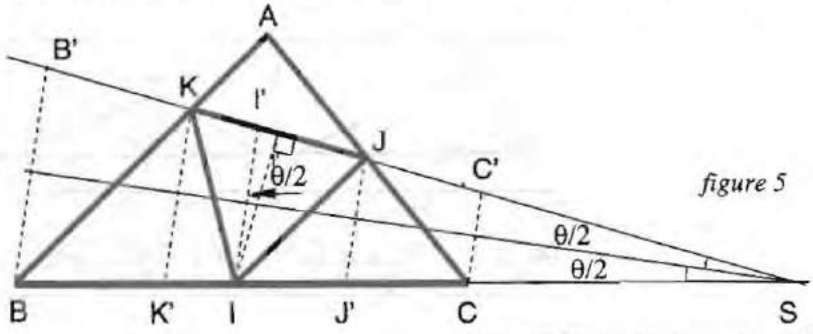


figure 5

(KJ) fait avec la droite *(BC)*, qu'elle coupe en *S*, un angle θ. *S* est extérieur au triangle *ABC*, on peut le supposer à droite de *C* (le cas : θ = 0 et *S* à l'infini ne posant pas de problème particulier). $\theta < \pi/3$, car $\widehat{JSI} + \widehat{SIJ} = \widehat{KJI} = \pi/3$. La symétrie par rapport à la bissectrice de $\widehat{S}$ transforme *C* en *C'* et *B* en *B'* : *C'* est extérieur à *ABC*, car $\widehat{SCC'} \leq \pi/2 < \widehat{SCA}$ et *B'* également, car

$$\widehat{BKJ} > \widehat{BAJ} \geq \widehat{CBA} \Rightarrow \widehat{SBA} < \widehat{SBB'} = \frac{1}{2}\left(\widehat{SBA} + \widehat{BKS}\right).$$

Donc cette symétrie transforme *K* et *J*, qui appartiennent à]*B'C'*[, en *K'* et *J'* appartenant à]*BC*[. Et elle transforme *I* en *I'* ∈]*KJ*[, car la droite *(II')* fait avec l'axe du triangle équilatéral passant par *I* un angle $\theta/2 < \pi/6$.
Elle transforme donc le triangle équilatéral *IJK* en un triangle équilatéral isométrique *I'J'K'* dont aucun sommet n'est extérieur à *ABC*, et qui n'est pas de taille maximale, car il ne touche qu'un seul côté du triangle.

Si, maintenant, l'un des sommets *J* ou *K* est en *A*, et que *I* ∈ [*BC*],on doit avoir $\widehat{A} \geq \frac{\pi}{3}$, mais on ne suppose plus que $\widehat{A}$ est le plus grand des trois angles. Plaçons un repère orthonormé de sorte que *B* et *C* appartiennent à $\overrightarrow{Ox}$ et *A* à $\overrightarrow{Oy}$, d'ordonnée 1. La distance de *A* à un point *I* de [*BC*], d'abscisse *x*, est une fonction convexe $\sqrt{1+x^2}$ de *x*. Elle n'atteint donc son maximum qu'en l'une des extrémités de l'intervalle où peut se trouver *I*, et ces extrémités sont atteintes lorsque celui des points *J* ou *K* qui n'est pas confondu avec *A* touche lui aussi un côté, [*AB*], [*AC*] ou [*BC*]. En d'autres termes, le triangle solution a obligatoirement deux sommets sur un même côté de *ABC*, et un sommet confondu avec *A*, *B* ou *C*, et il touche les trois côtés de *ABC*. Combien existe-t-il de tels triangles ? Trois ! Un ayant deux sommets sur [*AB*], un autre ayant deux sommets sur [*BC*] et un troisième ayant deux sommets sur [*CA*]. C'est seulement dans le cas trivial où *ABC* est équilatéral qu'ils sont tous trois confondus, mais deux d'entre eux sont confondus dès lors que l'un des angles de *ABC* vaut π/3. Parmi ces trois triangles, il y a la solution proposée par la majorité des lecteurs *(figure 4)*, qui en outre a un sommet sur [*AB*], un sur [*BC*] et un sur [*CA*], mais ce n'est pas toujours le plus grand des trois : si $\widehat{A} \geq \widehat{B} \geq \frac{\pi}{3} > \widehat{C} > \widehat{A} - \frac{\pi}{3}$ le plus grand a pour côté

[AB], et si $\widehat{A} > \frac{\pi}{3} > \widehat{B} \geq \widehat{C}$, le plus grand a deux sommets sur]BC[.

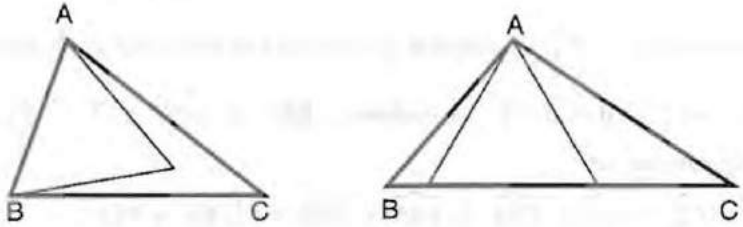


Figure 6

ÉNONCÉ N°221 (M.DELEHAM, Reims).

Soit p un entier ≥ 3 ; montrer que p est premier si et seulement si le nombre de quadruplets (a,b,c,d) d'entiers ≥ 0 tels que $(p-1) = a(a+1) + b(b+1) + c(c+1) + d(d+1)$ est égal à $(p+1)$.

SOLUTION

Remarquons tout d'abord que deux quadruplets qui ne diffèrent que par l'ordre des éléments sont considérés comme distincts. Ainsi, pour $p = 7$, on a :

$6 = 2+2+2+0 = 2+2+0+2 = 2+0+2+2 = 0+2+2+2$
$= 6+0+0+0 = 0+6+0+0 = 0+0+6+0 = 0+0+0+6,$

ce qui donne bien huit décompositions. Par contre, on impose aux entiers d'être positifs ou nuls, ce qui n'est pas le cas des théorèmes traditionnels sur ce genre de questions.

Car, seconde remarque préliminaire, les solutions que j'ai reçues de Marie-Laure CHAILLOUT (Sarcelles) et Edgard DELPLANCHE (Créteil) s'appuient sur un théorème connu de ceux qui le connaissent et dont il me semble honnête de dire un mot à l'intention de ceux qui ne le connaissent pas, avant de présenter la solution de Marie-Laure CHAILLOUT. Il s'agit du nombre de décompositions d'un entier en somme de carrés. Car il est clair que la décomposition proposée équivaut à :

$$4p = (2a+1)^2 + (2b+1)^2 + (2c+1)^2 + (2d+1)^2$$

qui, d'ailleurs, n'admet de solutions qui si p est impair. Mais admet-elle toujours des solutions et combien ?

Tout d'abord, de combien de manières peut-on décomposer un entier n en somme de deux carrés ? Dans certains cas, zéro : par exemple si $n \equiv 3 \pmod 4$. Mais le résultat fondamental est que tout nombre premier

$p \equiv 1 \pmod 4$ peut être décomposé d'une et d'une seule manière en somme de deux carrés. On s'appuie, pour prouver cela, sur l'anneau des entiers de Gauss, $a + bi$, avec $(a,b) \in \mathbf{Z}^2$, qui est euclidien et possède donc les mêmes propriétés que $\mathbf{Z}$ en matière de décomposition en facteurs premiers. Un nombre $p \equiv 1 \pmod 4$ premier dans $\mathbf{Z}$, n'est pas premier dans $\mathbf{Z}[i]$, car il existe des entiers $q \in \mathbf{Z}$ tels que p divise $1 + q^2 = (1 + iq)(1 - iq)$: si p était premier dans $\mathbf{Z}[i]$, il diviserait soit $1 + iq$, soit $1 - iq$.

Par contre, un nombre $a + ib$ tel que $a^2 + b^2 = p$ est premier dans $\mathbf{Z}[i]$, sinon p ne serait pas premier dans $\mathbf{Z}$. Et la recherche du nombre de décompositions d'un entier n en somme de deux carrés se ramène à regrouper de toutes les manières possibles les facteurs premiers de n dans $\mathbf{Z}[i]$ sous forme $n = d\bar{d}$: c'est là qu'il faut procéder proprement en considérant comme distinctes des décompositions qui ne diffèrent que par l'ordre des éléments ou le signe de ces éléments. Au lieu de dire que 5 se décompose d'une seule manière en somme de deux carrés, on en trouvera huit décompositions distinctes :

$$5 = 1^2 + 2^2 = (-1)^2 + 2^2 = \ldots = 2^2 + 1^2 = (-2)^2 + 1^2 = \ldots$$

afin d'avoir un résultat simple qui s'applique aussi bien au nombre de décompositions de 2 ou de 25 en somme de carrés. Et ce résultat, c'est :

> Le nombre de décompositions d'un entier >0 en somme de deux carrés est égal à quatre fois le nombre de ses diviseurs $\equiv 1 \pmod 4$ moins quatre fois le nombre de ses diviseurs $\equiv 3 \pmod 4$.

On remarquera que si $n \equiv 3 \pmod 4$, il a autant de diviseurs $\equiv 1 \pmod 4$ que de diviseurs $\equiv 3 \pmod 4$, le nombre obtenu est bien zéro, comme prévu.
Le détail de ces démonstrations peut être trouvé par exemple dans : G.H.HARDY and E.M.WRIGHT, *An introduction to the theory of numbers* (Oxford, third edition : 1954).

Pour passer de ce résultat à celui que l'on cherche; on fait appel aux séries: Si l'on élève au carré la série $S(x) = \sum_{k=0}^{k=\infty} a_k x^k$ (série formelle ou série convergente, peu importe), le coefficient de x^n dans $S^2(x)$ sera $b_n = \sum_{k=0}^{n} a_k a_{n-k}$. Supposons que a_k soit le nombre de décompositions de k en somme de deux carrés, b_n sera le nombre de décompositions de n en somme de quatre carrés, sous réserve de considérer comme distinctes celles qui ne diffèrent que par le signe ou l'ordre des éléments. Or, le résultat précédent

permet d'écrire alors :

$$S(x) = 1 + 4\left(\frac{x}{1-x} - \frac{x^3}{1-x^3} + \frac{x^5}{1-x^5} - \frac{x^7}{1-x^7} + \dots\right),$$

car $\frac{x^k}{1-x^k} = \sum_{n \text{ divisible par } k} x^n$ et que toutes les conditions de convergence sont remplies, lorsque $|x| < 1$, pour permuter les sommations.

En posant $u_n = \frac{x^n}{1-x^n}$, on va chercher le carré de

$$L(x,\theta) = \frac{1}{4}\operatorname{cotan}\frac{\theta}{2} + \sum_{n=1}^{+\infty} u_n \sin n\theta.$$

L'identité

$$\frac{1}{2}\operatorname{cotan}\frac{\theta}{2}\sin n\theta = \frac{1}{2} + \cos\theta + \cos 2\theta + \dots + \cos(n-1)\theta + \frac{1}{2}\cos n\theta$$

permet d'écrire $L^2(x,\theta) = \left(\frac{1}{4}\operatorname{cotan}\frac{\theta}{2}\right)^2 + \sum_{k=0}^{+\infty} C_k \cos k\theta$ et à l'aide d'autres identités comme : $\sum_{n=1}^{+\infty} u_n(1+u_n) = \sum_{n=1}^{+\infty} n u_n$, on arrive finalement à :

$$L^2(x,\theta) = \left(\frac{1}{4}\operatorname{cotan}\frac{\theta}{2}\right)^2 + \sum_{k=1}^{+\infty} u_k(1+u_k)\cos k\theta + \frac{1}{2}\sum_{k=1}^{+\infty} k u_k(1-\cos k\theta)$$

qui se ramène, lorsque $\theta = \pi/2$, à : $S^2(x) = 1 + 8\sum' m u_m$, la somme $\sum'$ s'étendant à tous les $m > 0$ non divisibles par 4 (du fait de l'influence de $(1 - \cos k\theta)$ pour $\theta = \pi/2$).
On redéveloppe alors les $u_m(x)$ pour aboutir au résultat cherché :

> Le nombre de décompositions d'un entier p comme somme de quatre carrés, en considérant comme distinctes deux décompositions qui ne diffèrent que par le signe ou l'ordre des éléments, est égal à huit fois la somme de ses diviseurs non multiples de 4.

Si p est impair, par exemple, à chaque diviseur d de p correspondent deux diviseurs de $4p$ non multiples de 4 : d et $2d$. La somme des diviseurs de $4p$ non multiples de 4 vaut donc trois fois la somme des diviseurs de p.
C'est là que je passe la parole à Marie-Laure CHAILLOUT :

p étant impair, le nombre de solutions dans $\mathbf{Z}^4$ de l'équation : $x^2 + y^2 + z^2 + t^2 = 4p$ est $24\sigma(p)$ où $\sigma(p)$ est la somme des diviseurs de p. Les quadruplets solutions sont soit éléments de $(2\mathbf{Z})^4$ soit éléments de $(2\mathbf{Z} + 1)^4$. Le nombre de solutions de cette équation éléments de $(2\mathbf{Z})^4$ est égal au nombre de solutions dans $\mathbf{Z}^4$ de l'équation $x^2 + y^2 + z^2 + t^2 = p$, soit $8\sigma(p)$.

Par conséquent, le nombre de solutions dans $(2\mathbf{Z} + 1)^4$ de l'équation $x^2 + y^2 + z^2 + t^2 = 4p$ est $16\sigma(p)$.

Donc le nombre de solutions de cette équation dans $(2\mathbf{Z} + 1)^4$ est $\sigma(p)$.

Donc le nombre de solutions dans $\mathbf{N}^4$ de l'équation :

$$p - 1 = a(a + 1) + b(b + 1) + c(c + 1) + d(d + 1)$$

est : 0 si p est pair et $\sigma(p)$ si p est impair.

Ce nombre est $p + 1$ si et seulement si p est un nombre premier impair.

En conclusion, je voudrais profiter de cet exercice pour plonger un peu dans l'univers des quaternions, car c'est là que l'on trouve la preuve la plus simple que tout entier naturel est la somme de quatre carrés, même si cela ne suffit pas à dire de combien de manières.

Cette remarquable algèbre de dimension 4 sur $\mathbf{R}$ ou de dimension 2 sur $\mathbf{C}$ est, rappelons-le, l'ensemble H des $t + xi + yj + zk$ muni d'une multiplication définie par : $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ et $ki = -ik = j$. C'est un exemple exceptionnel de corps non commutatif, le seul de dimension finie sur $\mathbf{R}$, qui possède néanmoins quelques points communs avec le corps des nombres complexes, comme les notions de conjugué et de norme.

Le groupe des unités de H n'est autre que la sphère unité de $\mathbf{R}^4$, donc l'ensemble des : $q = \cos\theta + \sin\theta(xi + yj + zk)$ avec $x^2 + y^2 + z^2 = 1$. Il existe un morphisme de ce groupe des unités dans le groupe des rotations de $\mathbf{R}^3$, de noyau $\{1, -1\}$, qui à q associe la rotation d'angle 2θ autour de $\vec{u} = (x,y,z)$, et l'image réciproque par ce morphisme du groupe des rotations du tétraèdre (resp. de l'icosaèdre) sont deux des plus beaux hypersolides réguliers : l'hypergranatoèdre (24 sommets, 24 hyperfaces octaédriques) et resp. l'hypericosaèdre (120 sommets, 600 hyperfaces tétraédriques).

Arrêtons-nous à l'hypergranatoèdre qui n'est autre que la réunion d'un hyperoctaèdre (8 sommets : $\pm 1, \pm i, \pm j, \pm k$ et 16 hyperfaces tétraédriques) et de son dual l'hypercube (16 sommets : $\frac{\pm 1 \pm i \pm j \pm k}{2}$ et 8 hyperfaces cubiques) lequel n'est autre que la réunion de deux hyperoctaèdres (tout comme le cube est la réunion de deux tétraèdres, obtenus en ne prenant

qu'un sommet sur deux). Notons au passage que tout hyperoctaèdre contenant le point 1 est un groupe, le plus petit groupe non commutatif après le groupe symétrique S_3.

Bref, le lien avec notre problème apparaît si l'on remarque que l'anneau D des quaternions demi-entiers ($a + bi + cj + dk$ avec $2a$, $2b$, $2c$ et $2d$ entiers, soit tous pairs soit tous impairs) possède des points communs avec l'anneau $\mathbf{Z}[i]$ des entiers de Gauss. Notamment, de la même manière dans les deux cas, on démontre l'existence d'une division euclidienne : $\forall\ (u,v) \in D^2$, $\exists\ (q,r) \in D^2$ et $\exists\ (q',r') \in D^2$ tels que $u = vq + r = q'v + r'$ avec $|r| < |v|$ et $|r'| < |v|$. Mais la non-commutativité empêche d'aller jusqu'à l'unicité de décomposition en facteurs premiers. Néanmoins, pour chacune des divisibilités (à gauche ou à droite), on a l'identité de Bézout et la notion de PGCD, d'où une forme affaiblie du théorème de Gauss :
Si $p \in \mathbf{Z}$ divise uv ($(u,v) \in D^2$) tout en étant premier à gauche avec u (c'est-à-dire : $\exists\ (\lambda,\mu) \in D^2$ tels que $\lambda p + \mu u = 1$), alors p divise v (car il commute avec tout quaternion). Comme pour tout nombre premier p, il existe a et b entier tels que p divise $1 + a^2 + b^2 = (1 + ai + bj)(1 - ai - bj)$, p n'est pas premier avec $1 + ai + bj$ et possède donc dans D un diviseur autre que les unités de D, permettant de l'écrire comme somme de quatre carrés. Mais, à la différence des entiers de Gauss, où commutativité implique unicité, dans D, il n'y a pas unicité.

Le groupe $\mathbf{U}$ des unités de D n'est autre que l'hypergranatoèdre, et la relation d'équivalence : $u \sim v \Leftrightarrow \exists\ \varepsilon \in \mathbf{U},\ u = \varepsilon v$ partitionne D en classes d'équivalences qui sont toutes des hypergranatoèdres. Si la norme des éléments d'un tel hypergranatoèdre est impaire, alors huit de ses éléments (soit un hyperoctaèdre) ont des composantes entières et les seize autres (soit deux hyperoctaèdres) ont des composantes non entières. A toute solution de $p = \left(a + \frac{1}{2}\right)^2 + \left(b + \frac{1}{2}\right)^2 + \left(c + \frac{1}{2}\right)^2 + \left(d + \frac{1}{2}\right)^2$ avec a, b, c, d, entiers ≥ 0, correspondent deux hyperoctaèdres conjugués de D : s'ils sont dans le même hypergranatoèdre, il leur correspondra huit éléments de D de coordonnées entières, donc huit solutions entières de $p = t^2 + x^2 + y^2 + z^2$ (en tenant compte cette fois-ci du signe de t, x, y, z), et s'ils sont dans deux hypergranatoèdres distincts (conjugués), il leur correspondra huit solutions entières de $p = t^2 + x^2 + y^2 + z^2$ dans chacun de ces hypergranatoèdres (donc seize en tout), mais ces seize mêmes solutions seront atteintes à partir d'une autre

solution de $p=\left(a+\frac{1}{2}\right)^2+\left(b+\frac{1}{2}\right)^2+\left(c+\frac{1}{2}\right)^2+\left(d+\frac{1}{2}\right)^2$ correspondant aux deux autres hyperoctaèdres non entiers de ces deux hypergranatoèdres.

Par exemple : $57=\left(\frac{13}{2}\right)^2+\left(\frac{7}{2}\right)^2+\left(\frac{3}{2}\right)^2+\left(\frac{1}{2}\right)^2$ définit deux hypergranatoèdres conjugués, l'un contenant $\frac{13}{2}+\frac{7}{2}i+\frac{3}{2}j+\frac{1}{2}k$ et l'autre, $\frac{13}{2}-\frac{7}{2}i-\frac{3}{2}j-\frac{1}{2}k$, de sorte que $\pm\frac{13}{2}\pm\frac{7}{2}i\pm\frac{3}{2}j\pm\frac{1}{2}k$ appartient au premier ou au second selon que le produit des signes vaut +1 ou −1. Dans le premier hypergranatoèdre,

$$\left(\frac{1+i+j+k}{2}\right)\left(\frac{13}{2}+\frac{7}{2}i+\frac{3}{2}j+\frac{1}{2}k\right)=\frac{1}{2}+\frac{5}{2}i+\frac{9}{2}j+\frac{11}{2}k$$

définissant une autre solution non entière : $57=\left(\frac{1}{2}\right)^2+\left(\frac{5}{2}\right)^2+\left(\frac{9}{2}\right)^2+\left(\frac{11}{2}\right)^2$

dont tous les représentants $\pm\frac{1}{2}\pm\frac{5}{2}i\pm\frac{9}{2}j\pm\frac{11}{2}k$ seront soit dans ce second hyperoctaèdre, soit dans son conjugué (inclus dans l'autre hypergranatoèdre). Et nous aurons un troisième hyperoctaèdre contenant : $\left(\frac{1+i+j+k}{2}\right)^2\left(\frac{13}{2}+\frac{7}{2}i+\frac{3}{2}j+\frac{1}{2}k\right)=-6+2i+j+4k$, donc huit solutions entières (en tenant compte des signes) déduites de $57=(-6)^2+2^2+1^2+4^2$, dont les huit conjuguées sont dans l'autre hypergranatoèdre. On tient compte du signe pour les solutions entières, car certains des entiers peuvent être nuls (par exemple : $1=1^2+0^2+0^2+0^2$), ce qui n'est pas le cas des demi-entiers, et il ne suffit pas nécessairement de changer les signes pour passer d'une solution entière à celles qui s'en déduisent.

Tout cela pour conclure qu'il existe, pour tout p impair, huit fois plus de solutions entières (en tenant compte du signe) de : $p=t^2+x^2+y^2+z^2$ que de solutions demi-entières positives :

$$p=\left(a+\frac{1}{2}\right)^2+\left(b+\frac{1}{2}\right)^2+\left(c+\frac{1}{2}\right)^2+\left(d+\frac{1}{2}\right)^2 ;$$

une tentative quelque peu aventureuse de donner une dimension visuelle à un

problème qui, *a priori*, n'avait rien de géométrique !

COURRIER DES LECTEURS

L'énoncé 218 rebondit !

Un peu tard, mais mieux vaut tard que jamais, deux contre-exemples me sont parvenus pour l'énoncé 218, prouvant que deux groupes ayant le même nombre d'éléments de chaque ordre ne sont pas obligatoirement isomorphes. Le premier m'est envoyé par Marie-Nicole GRAS (Brésilley), et les deux par Gérard LAVAU (Dijon), l'auteur de l'énoncé, qui les tient de M.QUERCIA (Dijon).

Le premier est le groupe engendré par deux éléments s et r tels que : $s^2 = r^8 = 1$ et $sr = r^5 s$. Ce groupe G_1 a 16 éléments : $(1, r, r^2, \ldots, r^7, s, sr, \ldots sr^7)$ et la relation $sr = r^5 s$ se généralise en $\forall k,\ sr^k = r^{5k}s$, donc $(sr^k)^2 = r^{-2k}$ de sorte que, si $k \neq 0$, sr^k a le même ordre que r^k. Il y a donc un élément d'ordre 1, trois d'ordre 2, quatre d'ordre 4 et huit d'ordre 8, tout comme dans $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/8\mathbf{Z})$, engendré lui par s et r tels que $s^2 = r^8 = 1$ et $sr = rs$, et qui n'est pas isomorphe à G_1, car il est commutatif alors que G_1 ne l'est pas.

G_1 peut être représenté comme un sous-groupe du groupe des permutations de 8 éléments $\{1, 2, 3, 4, 5, 6, 7, 8\}$, r étant la permutation circulaire notée (1, 2, 3, 4, 5, 6, 7, 8) qui à 1 associe 2, à 2 associe 3, ... à 8 associe 1, et s la permutation qui échange 2 et 6 et échange 4 et 8, notée (2, 6) (4, 8). Mais on peut aussi géométriquement, considérer les deux faces d'un prisme octogonal, s étant la symétrie plane qui transforme une face dans l'autre, et r la "rotation" qui fait tourner une face de $\pi/4$ et l'autre de $5\pi/4$.

Le second exemple est le groupe multiplicatif G_2 des matrices de la forme

$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, où a, b et c appartiennent à $\mathbf{Z}/3\mathbf{Z}$. Il est clair que, pour toutes ces matrices M, $(M - I)^3 = 0$; mais comme le corps des coefficients est de caractéristique 3, $(M - I)^3 = M^3 - I^3$, si bien que parmi les 27 matrices de G_2, l'identité est d'ordre 1 et les 26 autres d'ordre 3, tout comme dans le groupe additif $(\mathbf{Z}/3\mathbf{Z})^3$ qui n'est pas isomorphe à G_2, car il est commutatif alors que G_2 ne l'est pas. On notera que l'on aurait pu remplacer $\mathbf{Z}/3\mathbf{Z}$ par tout corps fini de caractéristique ≥ 3, et l'on aurait même pu généraliser à beaucoup d'autres groupes multiplicatifs de matrices triangulaires.

Ces deux exemples permettent de répondre négativement à deux des questions posées à propos de cet énoncé 218 :

Si deux groupes G et G' admettent des sous-groupes distingués H et H' isomorphes, avec G/H isomorphe à G'/H', et si en outre les ordres des éléments de G sont les mêmes que les ordres des éléments de G', G et G' ne sont pas nécessairement isomorphes, même dans le cas très particulier où G/H est isomorphe à $\mathbf{Z}/2\mathbf{Z}$. En effet, G_1 possède trois sous-groupes distingués d'ordre 8, un isomorphe à $\mathbf{Z}/8\mathbf{Z}$ et deux iso-

morphes à $(\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$, et il n'est pas isomorphe à $(\mathbf{Z}/8\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ qui possède lui aussi quatre sous-groupes distingués isomorphes à $(\mathbf{Z}/8\mathbf{Z})$ ou à $(\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$; de même, G_2 possède quatre sous-groupes distingués isomorphes à $(\mathbf{Z}/3\mathbf{Z})^2$. Notons au passage qu'un sous-groupe H d'ordre k d'un groupe G d'ordre $2k$ est nécessairement distingué, car l'application qui, à tout élément de H associe 0 et à tout autre élément de G associe 1 est un morphisme de G dans $\mathbf{Z}/2\mathbf{Z}$, admettant H pour noyau, alors qu'il n'en va pas de même d'un sous-groupe H d'ordre k d'un groupe G d'ordre $3k$: le groupe symétrique S_3 possède des sous-groupes non distingués d'ordre 2.

Par ailleurs, la connaissance de l'ordre des éléments d'un groupe ne suffit pas à savoir si ce groupe est commutatif. Dans certains cas, il permet de prouver que le groupe est non-commutatif (exemple: un gronpe ayant des éléments d'ordre 2 et des éléments d'ordre 3 sans avoir des éléments d'ordre 6 est non-commutatif), dans d'autres cas, il permet de prouver que le groupe est commutatif (par exemple: un groupe ayant un nombre premier d'éléments est cyclique, donc commutatif), mais il arrive, comme l'attestent les groupes G_1 et G_2, qu'un groupe commutatif et un groupe non-commutatif aient le même nombre d'éléments de tous ordres.