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 !