SUR LES SOMMES DE TROIS ET QUATRE CARRÉS

Autor(en): **Weil, André**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-46904

SUR LES SOMMES DE TROIS ET QUATRE CARRÉS

par André WEIL

A Carl Ludwig Siegel
en toute amitié

Comme chacun sait, c'est Lagrange qui a publié, en 1770, la première démonstration du célèbre théorème de Fermat sur la décomposition des entiers en quatre carrés [1]. Cette démonstration, qui prenait comme point de départ un travail antérieur d'Euler, fut bientôt améliorée par Euler lui-même [2]; traduite dans le langage des quaternions, elle a été exposée à nouveau par Hurwitz. C'est une démonstration par « descente infinie », et il est permis de supposer qu'elle ne diffère pas substantiellement de celle que Fermat disait avoir obtenue (« perfectam demonstrationem a me inventam moneo », *Œuvres* II, p. 403); on ne voit pas en effet pourquoi on mettrait en doute l'affirmation maintes fois réitérée de Fermat à cet égard.

Ni Lagrange ni Euler n'ont fait mention du nombre de représentations d'un entier par quatre carrés. Il est bien connu que la première détermination de ce nombre fut obtenue par Jacobi, par le moyen des fonctions thêta, au cours de ses recherches sur les fonctions elliptiques. Peu après, en 1834, Jacobi donna une démonstration élémentaire du même résultat [3], tout en ajoutant que celle-ci ne diffère que par la forme de la précédente. En 1856, Dirichlet se donna la peine d'en présenter une version améliorée dans une lettre à Liouville [4].

En ce qui concerne les sommes de trois carrés, ce qu'on pourrait appeler la préhistoire du sujet est plus obscure. A son affirmation sur les sommes de quatre carrés, Fermat en a plusieurs fois joint une autre sur les sommes de « nombres polygonaux »: tout nombre, dit-il, est somme de trois nombres triangulaires (au plus), de quatre carrés, de cinq nombres pentagonaux, etc. Des nuances de style, il est vrai, pourraient suggérer que parfois il ne s'est pas senti tout à fait sûr de lui sur ce terrain. En ce qui concerne les nombres triangulaires, son énoncé revient à dire que tout entier de la forme $8n + 3$ est somme de trois carrés. Or il spécifie qu'il ne sait pas démontrer que $2p$ est somme de trois carrés chaque fois que p est un nombre premier de la forme $8n - 1$ (*Œuvres* II, p. 405). Il est donc certain que ses méthodes,

quelles qu'elles fussent, ne lui permettaient pas de traiter des sommes de trois carrés en toute généralité.

Ce problème a été traité pour la première fois avec succès par Gauss dans les *Disquisitiones*, et a fait l'objet par la suite d'assez nombreux travaux qu'il serait superflu d'énumérer ici. L'énoncé de Fermat sur les nombres triangulaires figure comme cas particulier parmi les résultats de Gauss; mais ceux-ci sont présentés comme conséquences de la théorie des formes quadratiques binaires et ternaires; et, même à présent, on ne connaît aucune démonstration de l'énoncé de Fermat qu'on puisse attribuer à celui-ci avec la moindre vraisemblance.

Il y a cependant un travail de Kronecker [5], composé tout à fait dans l'esprit de la démonstration élémentaire de Jacobi-Dirichlet citée plus haut, et qui donne, non seulement le résultat annoncé par Fermat, mais la détermination complète du nombre de décompositions d'un entier en trois carrés. Comme ce travail est resté peu connu, il ne sera peut-être pas inutile d'en donner ici un exposé un peu simplifié (v. cependant [6]).

Pour $i = 2, 3, 4$, nous noterons $N_i(m)$ le nombre de solutions $(x_1, \ldots, x_i)$ de

$$m = x_1^2 + x_2^2 + \ldots + x_i^2;\ x_h > 0, x_h \equiv 1 \,(\mathrm{mod.}\ 2), 1 \leqslant h \geqslant i\,.$$

Bien entendu, ce nombre est 0 sauf si $m > 0$, $m \equiv i$ (mod. 8). En vertu d'un raisonnement facile et élémentaire, basé sur l'identité

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

le nombre de décompositions de tout entier en deux resp. quatre carrés doit être considéré comme connu dès qu'on connaît $N_2(m)$ resp. $N_4(m)$ pour tout m. Il n'en est pas de même pour les décompositions en trois carrés. Néanmoins, comme notre objet ici est de présenter le principe de la démonstration de Kronecker plutôt que d'obtenir des résultats complets qui sont bien connus par ailleurs, nous nous bornerons par la suite à la détermination de $N_3(m)$, ou, ce qui revient au même, du nombre de décompositions de m en trois carrés pour $m \equiv 3$ (mod. 8); il suffira au lecteur de savoir que la méthode de Kronecker s'applique aussi aux autres cas, au prix de quelques complications supplémentaires.

1. Rappelons d'abord le résultat bien connu (et qui en substance était déjà connu de Fermat; cf. *Œuvres* II, p. 214) au sujet de $N_2(m)$. Soit $\chi(n)$ égal à $+1$ ou à -1, pour n impair > 0, suivant que n est $\equiv 1$ ou $\equiv -1$ (mod. 4), et égal à 0 pour toute autre valeur de n. On a alors:

$$N_2(m) = \sum_{d/m} \chi(d) \qquad (m \equiv 2 \,(\mathrm{mod.}\ 4),\ m > 0)\,,$$

comme on le voit par exemple en écrivant la fonction zêta du corps $\mathbf{Q}(i)$ comme produit de $\zeta(s)$ et de la fonction L formée au moyen du caractère χ. Cela peut s'écrire aussi:

$$(1) \qquad N_2(m) = \sum_{m=2ab} \chi(a) \qquad (m \equiv 2 \pmod 4,\ m>0).$$

On notera d'autre part qu'on a:

$$(2) \qquad \chi(n)\,\chi(n') = (-1)^{(n-n')/2}$$

chaque fois que $n \equiv n' \equiv 1 \pmod 2$, $n>0$, $n'>0$.

Passons au calcul de $N_4(m)$. Soit $m \equiv 4 \pmod 8$, $m>0$. On a évidemment:

$$N_4(m) = \sum N_2(r)\,N_2(s) \quad (m=r+s,\ r \equiv s \equiv 2 \pmod 4,\ r>0,\ s>0).$$

D'après (1) et (2), cela donne:

$$N_4(m) = \sum (-1)^{(a-c)/2}$$
$$(m=2ab+2cd,\ a \equiv b \equiv c \equiv d \equiv 1 \pmod 2,\ a,b,c,d>0).$$

Sur les indices de sommation, faisons le changement de variables:

$$a = x+y,\ c = x-y,\ b = z-t,\ d = z+t.$$

Les conditions imposées à a, b, c, d donnent alors:

$$(3) \qquad m = 4(xz-yt),\ |y|<x,\ |t|<z,\ y \not\equiv x,\ t \not\equiv z \pmod 2,$$

ce qui, d'après la condition imposée à m, implique

$$xz - yt \equiv 1,\ y \equiv t \equiv \frac{a-c}{2} \pmod 2.$$

On a donc $N_4(m) = \sum(-1)^y$, les conditions de sommation étant données par (3). Soient N_0, N_+, N_- les sommes $\sum(-1)^y$ étendues respectivement aux solutions de (3) pour lesquelles $y=0$, $y>0$, $y<0$. Le calcul de N_0 est immédiat; pour $y=0$, (3) donne $xz = m/4$, donc $x \equiv z \equiv 1 \pmod 2$, puis $|t|<z$, $t \equiv 0 \pmod 2$. Si donc d est un diviseur impair >0 de m, il y aura d solutions de (3) pour lesquelles $y=0$, $z=d$, $x=m/4d$. Cela donne $N_0 = \sum d$.

Dans (3), on peut changer (x,y,z,t) en $(x,-y,z,-t)$; on a donc $N_+ = N_-$. Soit d'autre part (x,y,z,t) une solution de (3) avec $y>0$. Alors x/y est >1 et ne peut être un entier impair, puisque $y \not\equiv x \pmod 2$; il y a donc un entier u et un seul tel que $2u-1 < x/y < 2u+1$. Posons:

$$(4) \qquad x' = 2uz - t,\ y' = z,\ z' = y,\ t' = 2uy - x.$$

On vérifie immédiatement que (x', y', z', t') est aussi une solution de (3) avec $y' > 0$, $y' \not\equiv y \pmod 2$. Réciproquement, si une telle solution (x', y', z', t') est donnée, u est aussi l'entier unique tel que $2u - 1 < x'/y' < 2u + 1$; autrement dit, (4) définit une permutation de l'ensemble de ces solutions. Donc $N_+ = -N_+$; par suite $N_+ = N_- = 0$, $N_4(m) = N_0 = \sum d$, et le théorème de Jacobi est démontré.

2. Telle est en substance la démonstration de Jacobi-Dirichlet. On peut aussi la présenter un peu autrement, au moyen d'un lemme qui jouera un rôle essentiel dans la démonstration de Kronecker. Pour plus de clarté nous ferons précéder ce lemme d'un autre plus simple, qui ne nous servira pas mais fera mieux comprendre de quoi il s'agit.

LEMME 1. — *Soient a, b, n des entiers > 0. Soit $f(a, b, n)$ le nombre de solutions entières de*

$$(5) \qquad aX + bY = n,\ 0 < X < b,\ Y > a,\ Y \not\equiv 0 \pmod a.$$

Alors $f(a, b, n) = f(b, a, n)$.

Il est clair que $f(a, b, n) = 0$ sauf si n est $\geqslant ab + a + b$ et est multiple du p.g.c.d. de a et b. Soit (X, Y) une solution de (5); soit u l'entier tel que $u < Y/a < u + 1$. Posons $X' = Y - ua$, $Y' = X + ub$. C'est une solution du problème obtenu en échangeant a et b dans (5). Comme u est aussi déterminé par $u < Y'/b < u + 1$, on a ainsi établi une bijection entre les solutions des deux problèmes.

LEMME 2. — *Soient a, b des entiers > 0; soit m un entier, et soient α, β des entiers modulo 2. Soit $\varphi(a, b, \alpha, \beta, m)$ le nombre de solutions de*

$$(6)\ aX + bY = m,\ |X| < b,\ Y > a,\ X \equiv \alpha \pmod 2,\ Y \equiv \beta \pmod 2,\ Y \not\equiv a \pmod{2a}.$$

Alors $\varphi(a, b, \alpha, \beta, m) = \varphi(b, a, \beta, \alpha, m)$.

Soit (X, Y) une solution de (6). Alors il y a un entier unique u tel que $|Y - 2ua| < a$, et, si on pose $X' = Y - 2ua$, $Y' = X + 2ub$, (X', Y') est une solution du problème obtenu en échangeant (a, α) et (b, β) dans (6). De plus, u est l'entier unique tel que $|Y' - 2ub| < b$. La conclusion s'ensuit comme pour le lemme 1. On notera que $\varphi(a, b, \alpha, \beta, m) = 0$ sauf si m est multiple du p.g.c.d. de a et b, $m \geqslant a + b$, et $m \equiv a\alpha + b\beta \pmod 2$. On notera aussi que la condition $Y \not\equiv a \pmod{2a}$, dans (6), est conséquence de $Y \equiv \beta \pmod 2$ chaque fois que $a \not\equiv \beta \pmod 2$.

Cela posé, reprenons les notations du n° 1, et considérons les solutions de (3) pour lesquelles y, z ont des valeurs données > 0; (3) implique d'ailleurs qu'on doit prendre $y \not\equiv z \pmod 2$. Ecrivant $(y, z, -t, x)$ au lieu de (a, b, X, Y) dans (6), on voit immédiatement que le nombre de ces solutions n'est autre que $\varphi(y, z, y, z, m/4)$. On a donc:

$$N_+ = \sum (-1)^y \varphi(y, z, y, z, m/4),$$

la sommation étant étendue à tous les (y, z) tels que $y > 0$, $z > 0$ et $y \not\equiv z \pmod 2$; c'est une somme finie, puisque les termes pour lesquels $y + z > m/4$ sont nuls. Echangeant y et z, et appliquant le lemme 2, on voit de nouveau que $N_+ = -N_+$.

3. Passons maintenant à la détermination de $N_3(m)$. La méthode de Kronecker exige (et c'est là son point faible) la connaissance préalable du résultat à démontrer. Pour énoncer celui-ci, nous noterons $H(m)$, pour tout m, le nombre de solutions (a, b, c) de

$$(7) \quad m = 4ac - b^2, \quad b > 0, \quad b < 2a, \quad b < 2c, \quad b \equiv 1 \pmod 2$$

en entiers a, b, c. Naturellement $H(m)$ est nul sauf si $m > 0$, $m \equiv -1 \pmod 4$. De plus, si par exemple $a \leqslant c$, (7) entraîne $0 < b \leqslant 2a - 1$, $m + 1 \geqslant 4a(c - a + 1)$, donc $H(m)$ est fini.

THÉORÈME. — *On a* $N_3(m) = H(m)$ *chaque fois que* $m \equiv 3 \pmod 8$.

Il est clair d'abord qu'on a, pour $m \equiv 4 \pmod 8$:

$$N_4(m) = \sum N_3(m - x^2),$$

la sommation étant étendue aux entiers impairs $x > 0$. La valeur de $N_4(m)$ a été obtenue au n° 1. Si nous faisons voir que, pour tout $m \equiv 4 \pmod 8$, on a aussi

$$(8) \qquad N_4(m) = \sum H(m - x^2),$$

le théorème s'ensuivra aussitôt par récurrence sur m. Il suffira donc de démontrer cette dernière relation. Pour la commodité des notations, nous écrirons $m = 4n$ avec n impair, et nous désignerons par X_n le second membre de (8), qu'on peut écrire aussi:

$$X_n = \frac{1}{2} \sum H(4n - x^2)$$

si on étend cette fois la sommation à tous les entiers x impairs, positifs ou négatifs. De plus, si R désigne un système de relations (égalités, inégalités,

congruences) où figurent, outre n, des lettres a, b, c, x, y, etc., nous conviendrons d'écrire $\{ R \}$ pour le nombre de solutions $(a, b, c, x, y, \ldots)$ du système R en nombres entiers, étant entendu que le nombre impair $n > 0$ est fixé une fois pour toutes. Nous pouvons écrire alors:

$$X_n = \frac{1}{2}\left\{ n = ac + \frac{x^2 - b^2}{4}, b > 0, b < 2a, b < 2c, b \equiv x \equiv 1 \,(\text{mod. } 2)\right\}.$$

Puisque $b \equiv x \,(\text{mod. } 2)$, on peut poser $b + x = 2y$, $b - x = 2z$ et écrire:

$$X_n = \frac{1}{2}\left\{ n = ac - yz, y + z > 0, y + z < 2a, y + z < 2c, y \not\equiv z \,(\text{mod. } 2)\right\},$$

où nous notons que les conditions imposées entraînent que yz est pair, donc ac impair, donc $c - z \neq a - y$. Ces conditions étant symétriques en a et c, et en y et z, on diminue de moitié le nombre de solutions qui figure au second membre en ajoutant la condition $c - z > a - y$; mais alors, comme ces conditions entraînent aussi $y + z < a + c$, on a même $c - z > |a - y|$. Cela donne:

$$X_n = \{ n = ac - yz, y + z > 0, y + z < 2a, y + z < 2c, \\ c - z > |a - y|, y \not\equiv z \ (\text{mod. } 2) \}.$$

Soit A l'ensemble des (a, c, y, z) défini par ces dernières conditions; il est contenu dans l'ensemble B défini par

$$(B) \qquad n = ac - yz, 0 < y + z < 2a, c - z > |a - y|, y \not\equiv z \ (\text{mod. } 2),$$

et la différence $C = B - A$ est l'ensemble défini par

$$(C) \qquad n = ac - yz, 0 < y + z < 2a, y + z > 2c, \\ c - z > |a - y|, y \not\equiv z \ (\text{mod. } 2).$$

Parmi ces dernières conditions, $y + z < 2a$ est conséquence des autres, à savoir de $0 < y + z$, $y + z > 2c$, $c - z > y - a$, qui entraînent aussi $a > |c|$. Notons aussi que les conditions qui définissent B entraînent que yz est pair, donc a et c impairs.

Dans (B), nous ferons le changement de variables

$$y = a - u, z = u + w, c = u + v + w.$$

Il transforme B en l'ensemble des (a, u, v, w) qui satisfont à

$$(D) \qquad n = u^2 + av + uw, \ |w| < a, \ v > |u|, \ w \not\equiv a \ (\text{mod. } 2).$$

Comme ces conditions sont équivalentes à (B), elles entraînent aussi $a \equiv 1 \pmod 2$, donc $w \equiv 0 \pmod 2$. Considérons d'abord les solutions de (D) pour lesquelles $u = 0$; celles qui correspondent à une valeur donnée de a sont au nombre de a, et, comme on peut prendre pour a n'importe quel diviseur > 0 de n, le nombre total de ces solutions n'est pas autre chose que le nombre $\sum d$ déjà obtenu au n° 1 comme valeur de $N_4(4n)$. Comme de plus (D) ne change pas si on y change (u, w) en $(-u, -w)$, on voit que le nombre d'éléments de B est $N_4(4n) + 2Y$, où Y est le nombre d'éléments de l'ensemble défini par

$$(D')\quad n - u^2 = av + uw,\ |w| < a,\ v > u > 0,\ a \equiv 1,\ w \equiv 0 \pmod 2.$$

D'ailleurs ces conditions impliquent $v \not\equiv u \pmod 2$. Dans ces conditions, ceux des éléments de cet ensemble qui correspondent à des valeurs données de a et de u sont au nombre de $\varphi(u, a, 0, u+1, n-u^2)$, de sorte qu'on a:

$$Y = \sum \varphi(u, a, 0, u+1, n-u^2),$$

où la sommation est étendue à tous les couples (u, a) pour lesquels $u > 0$, $a > 0$, $a \equiv 1 \pmod 2$. D'après ce qu'on a vu à la suite du lemme 2, tous les termes de cette somme sont nuls à l'exception de ceux pour lesquels $n - u^2 \geqslant u + a$, ce qui montre que l'ensemble B est fini.

Passons à (C), où, comme on l'a vu, on peut omettre la condition $y + z < 2a$. Cette fois nous ferons le changement de variables

$$a = u + v + w,\ y = u + w,\ z = c - u,$$

qui transforme C en l'ensemble des (u, v, w, c) défini par

$$n = u^2 + cv + uw,\ w > |c|,\ u > |v|,\ w \not\equiv c \pmod 2,$$

conditions qui entraînent de nouveau $c \equiv 1$, $w \equiv 0 \pmod 2$. Comme par conséquent $c \neq 0$, et qu'on peut changer (c, v) en $(-c, -v)$, le nombre d'éléments de C est $2Y'$, où Y' est le nombre d'éléments de l'ensemble défini par

$$n - u^2 = cv + uw,\ w > c > 0,\ u > |v|,\ c \equiv 1,\ w \equiv 0 \pmod 2.$$

Tout comme plus haut, les éléments de cet ensemble qui correspondent à des valeurs données de c et de u sont au nombre de $\varphi(c, u, u+1, 0, n-u^2)$, et l'on a

$$Y' = \sum \varphi(c, u, u+1, 0, n-u^2),$$

où la somme est étendue aux couples (c, u) tels que $c > 0$, $u > 0$ et $c \equiv 1 \pmod 2$. Le lemme 2 donne $Y' = Y$, ce qui achève la démonstration.

BIBLIOGRAPHIE

[1] LAGRANGE. Démonstration d'un théorème d'arithmétique. *Nouveaux Mémoires de l'Acad. royale des Sc. et Belles-L. de Berlin*, 1770 = *Œuvres III*, 189-201.

[2] EULER. Novae demonstrationes circa resolutionem numerorum in quadrata. *Nova Acta Erud.* 1773, 193-211 = *Opera Omnia, (I) 3*, 218-239.

[3] JACOBI. De compositione numerorum e quatuor quadratis. *J. de Crelle 12* (1834), 167-172 = *Ges. Werke VI*, 245-251.

[4] DIRICHLET. Sur l'équation $t^2 + u^2 + v^2 + w^2 = 4m$, *J. de Liouville (II)* 1 (1856), 210-214 = *Werke II*, 201-208.

[5] KRONECKER. Über bilineare Formen mit vier Variabeln. *Abh. d. K. Pr. Akad. d. Wiss* 1883_2, 1-60 = *Werke II*, 425-495.

[6] VENKOV, B.A. *Elementary number-theory* (transl. from the Russian), Wolters-Noordhoff, Groningen, 1970

André Weil

The Institute for Advanced Study
Princeton, N.J., 08540

(Reçu le 23 avril 1974)