JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

G. LEJEUNE-DIRICHLET

Sur la possibilité de la décomposition des nombres en trois carrés

Journal de mathématiques pures et appliquées 2^e série, tome 4 (1859), p. 233-240.
<http://www.numdam.org/item?id=JMPA_1859_2_4__233_0>

SUR

LA POSSIBILITÉ DE LA DÉCOMPOSITION DES NOMBRES EN TROIS CARRÉS;

PAR M. G. LEJEUNE-DIRICHLET.

Journal de Crelle, t. XL, p. 228.

TRADUIT DE L'ALLEMAND PAR M. J. HOUEL.

La théorie de la décomposition des nombres entiers n qui ne sont pas de l'une des formes $4k$, $8k + 7$ en trois carrés sans diviseur commun, est l'une des plus compliquées de l'arithmétique transcendante, lorsqu'on veut développer cette théorie complétement, c'est-à-dire, non-seulement démontrer la possibilité de la décomposition, mais encore déterminer en même temps le nombre de toutes les décompositions possibles, nombre qui peut être exprimé, soit, comme Gauss l'a fait voir le premier [*], au moyen du nombre des formes binaires de déterminant $-n$, soit encore indépendamment de ce nombre [**]. Il y a cependant des cas où il suffit de supposer la possibilité de la décomposition, comme cela a lieu, par exemple, dans la démonstration donnée par Cauchy [***] et simplifiée depuis par Legendre, pour le théorème de Fermat relatif aux nombres polygonaux, démonstration qui s'appuie seulement sur ce que tout nombre, à l'exception de ceux qui ont été précédemment exclus, est la somme de trois carrés. Il semble donc qu'une démonstration simple de la possibilité de la décomposition n'est pas tout à fait dépourvue d'intérêt. Nous allons en exposer une dans la présente Note.

[*] *Disq. Arith.*, art. 229.

[**] *Journal de Crelle*, t. XXI, p. 155.

[***] *Exercices mathématiques*, par Cauchy, 2e année, p. 265.

On a besoin d'abord, pour cela, de cette proposition connue, que toute forme ternaire positive de déterminant -1, c'est-à-dire toute expression telle que

$$(1) \qquad ax^2 + by^2 + cz^2 + 2a'yz + 2b'xz + 2c'xy,$$

dont les coefficients sont des nombres entiers satisfaisant à l'équation

$$(2) \qquad aa'^2 + bb'^2 + cc'^2 - abc - 2a'b'c' = -1,$$

et soumis en outre aux conditions que

$$a, \quad b, \quad c, \quad bc - a'^2, \quad ac - b'^2, \quad ab - c'^2$$

soient positifs (conditions dont la première et la quatrième entraînent d'ailleurs les quatre autres), est équivalente à la forme

$$(3) \qquad x^2 + y^2 + z^2.$$

Il suffit, pour démontrer cette proposition, de se convaincre que, pour le déterminant -1, l'expression (3) est la seule forme réduite positive. Si la forme (1) est une forme réduite, alors, en vertu de la proposition démontrée à la fin du précédent Mémoire, abc ne doit pas être plus grand que 2; d'où, si l'on suppose

$$a \leq b \leq c,$$

il résulte immédiatement

$$a = b = 1.$$

Mais comme d'ailleurs, par la définition des formes réduites, $2c'$ et $2b'$, abstraction faite du signe, ne doivent pas être plus grands que a, ni $2a'$ plus grand que b, il vient

$$a' = b' = c' = 0$$

et, par suite, en vertu de l'équation (2),

$$c = 1.$$

Cela posé, la possibilité de la décomposition du nombre positif a sera établie, dès qu'on aura trouvé une forme ternaire positive (1) de déterminant -1 dont le premier coefficient soit a. En effet, une telle

forme étant équivalente à la forme (3), celle-ci peut être transformée dans la première, et il vient

$$a = \alpha^2 + \alpha'^2 + \alpha''^2,$$

α, α', α'' étant trois des neuf coefficients de la substitution et ne pouvant avoir aucun diviseur commun, parce que chaque terme du déterminant formé avec ces neuf coefficients contient en facteur soit α, soit α', soit α'', et que ce déterminant est égal à l'unité.

Tout revient donc, en considérant a comme donné, à satisfaire à l'équation (2) au moyen de cinq nombres entiers b, c, a', b', c', qui doivent en outre être assujettis à la condition que $bc - a'^2$ soit positif. En prenant

$$b' = 1, \quad c' = 0,$$

l'équation devient

$$b = a\Delta - 1,$$

où l'on a posé

$$\Delta = bc - a'^2,$$

et il ne reste plus qu'à faire voir que l'on peut choisir le nombre positif Δ de telle sorte que $-\Delta$ soit un résidu quadratique de $b = a\Delta - 1$, puisque, dans cette hypothèse, on peut toujours déterminer c et a' de telle façon, que l'on ait

$$a'^2 - bc = -\Delta.$$

Nous allons maintenant faire voir que la condition dont nous parlons peut toujours être satisfaite au moyen d'une valeur impaire de Δ, et que pour cette valeur, si a est de la forme $4k + 2$, $b = a\Delta - 1$ devient égal à un nombre premier impair p, tandis que si a est impair sans être de la forme $8k + 7$, b est égal au double d'un pareil nombre premier p. En commençant par le second cas, nous avons l'équation

$$2p = a\Delta - 1,$$

où nous ne supposerons pas encore tout d'abord que p soit un nombre premier, mais seulement un nombre impair. En posant

$$\Delta = 8t + \varepsilon,$$

ε étant égal à l'un des nombres 1, 3, 5, 7, on voit immédiatement que, dans chacun des quatre cas que peut présenter a relativement au diviseur 8, Δ admet deux formes relativement au même diviseur, ou bien ε admet deux valeurs, lorsque p doit être impair, comme nous le supposons. Pour chacun des huit cas qui se présentent ainsi, appliquons la loi de réciprocité au premier membre de l'équation

$$\left(\frac{p}{\Delta}\right) = \left(\frac{-2}{\Delta}\right),$$

laquelle résulte de $2p = a\Delta - 1$, et où la notation de Legendre est employée avec la signification plus étendue introduite par Jacobi; remplaçons $\left(\frac{-2}{\Delta}\right)$ par sa valeur connue et multiplions ensuite par

$$\left(\frac{-1}{p}\right) = \pm 1,$$

où l'on connaîtra aussi le signe de ± 1, d'après la forme linéaire que p aura dans chaque cas particulier. On obtient ainsi les résultats suivants :

$$a = 8k+1, \quad \begin{cases} \Delta = 8t+3, & p = 4s+1, & \left(\frac{-\Delta}{p}\right) = +1, \\ \Delta = 8t+7, & p = 4s+3, & \left(\frac{-\Delta}{p}\right) = -1, \end{cases}$$

$$a = 8k+3, \quad \begin{cases} \Delta = 8t+1, & p = 4s+1, & \left(\frac{-\Delta}{p}\right) = +1, \\ \Delta = 8t+5, & p = 4s+3, & \left(\frac{-\Delta}{p}\right) = +1, \end{cases}$$

$$a = 8k+5, \quad \begin{cases} \Delta = 8t+3, & p = 4s+3, & \left(\frac{-\Delta}{p}\right) = +1, \\ \Delta = 8t+7, & p = 4s+1, & \left(\frac{-\Delta}{p}\right) = -1, \end{cases}$$

$$a = 8k+7, \quad \begin{cases} \Delta = 8t+1, & p = 4s+3, & \left(\frac{-\Delta}{p}\right) = -1, \\ \Delta = 8t+5, & p = 4s+1, & \left(\frac{-\Delta}{p}\right) = -1. \end{cases}$$

On voit que si l'on n'a pas $a = 8k+7$, la condition $\left(\frac{-\Delta}{p}\right) = 1$ peut

toujours être satisfaite. Mais aussi dans chacun des huit cas p peut être un nombre premier, comme cela ressort de l'expression

$$p = \tfrac{1}{2}(a\Delta - 1) = 4at + \tfrac{1}{2}(a\varepsilon - 1),$$

dans laquelle $\frac{1}{2}(a\varepsilon - 1)$, d'après le choix de ε, est impair et, de plus, sans diviseur commun avec a. Cette expression est donc le terme général d'une progression arithmétique qui contient nécessairement des nombres premiers. Si l'on a maintenant un nombre premier p pour lequel $\left(\frac{-\Delta}{p}\right)$ soit $= 1$, alors $-\Delta$ est résidu quadratique de p et par suite aussi de $2p$. C. Q. F. D.

Dans le cas de a pair, nous poserons de suite

$$a = 4k + 2,$$

parce que l'on sait d'avance que, pour $a = 4k$, la condition ne peut être remplie. Puisque, dans l'équation

$$p = a\Delta - 1,$$

nous supposons Δ impair, p est donc de la forme $4s + 1$, et l'on a

$$\left(\frac{-1}{\Delta}\right) = \left(\frac{p}{\Delta}\right) = \left(\frac{\Delta}{p}\right) = \left(\frac{-\Delta}{p}\right).$$

Il faut donc donner à Δ la forme $4t + 1$ pour que $\left(\frac{-\Delta}{p}\right)$ devienne $= 1$. On obtient ainsi

$$p = 4at + a - 1,$$

expression qui peut encore être un nombre premier, auquel cas $-\Delta$ est résidu quadratique de p.

L'application du procédé que l'on vient de développer n'est pas restreinte au cas du déterminant -1, et nous allons encore en donner un second exemple pour le déterminant -3.

En cherchant encore, comme précédemment, les formes réduites appartenant à ce déterminant, la condition

$$abc \leqq 6,$$

dans l'hypothèse de $a \leqq b \leqq c$, donne pour a la valeur 1, tandis que b peut être $= 1$ ou $= 2$. Maintenant $2c'$ et $2b'$ ne pouvant être numériquement plus grands que $a = 1$, il s'ensuit que

$$b' = c' = 0,$$

et l'équation d'où l'on doit tirer le déterminant se réduit à

$$a'^2 - bc = -3.$$

Or $2a'$ ne pouvant être non plus $> b$ numériquement, on a donc, pour $b = 1$, $a' = 0$, et par suite $c = 3$. Si au contraire $b = 2$, on a alors

$$2a' = 0 \quad \text{ou} \quad 2a' = \pm 2.$$

La première de ces valeurs ne satisfait pas à l'équation précédente dans laquelle $bc \geqq 4$. Il ne reste donc qu'à supposer

$$a' = \pm 1,$$

d'où résulte $c = 2$. En négligeant le signe inférieur, ce qui revient à un simple changement de signe de z, on obtient les deux formes réduites

$$(4) \qquad \begin{cases} x^2 + y^2 + 3z^2, \\ x^2 + 2y^2 + 2z^2 + 2yz, \end{cases}$$

de sorte que toute forme ternaire positive (1) de déterminant -3, c'est-à-dire dont les coefficients satisfont à l'équation

$$(5) \qquad aa'^2 + bb'^2 + cc'^2 - abc - 2a'b'c' = -3,$$

sera équivalente à l'une des formes (4). En cherchant maintenant les résidus que donnent les expressions (4) par rapport au diviseur 8, lorsque dans ces expressions on donne aux éléments x, y, z toutes les combinaisons de valeurs paires et impaires, à l'exclusion du seul cas de trois valeurs paires simultanées (puisque nous supposons toujours les éléments sans diviseur commun), on trouve que la première des formes (4) donne tous les résidus possibles relativement au module 8, tandis que la seconde expression n'admet pour aucune combinaison ni l'une ni l'autre des formes $8k + 5$, $4k$. Si l'on consi-

dère en outre que deux formes équivalentes représentent toujours les mêmes nombres, on en pourra conclure immédiatement que si une forme de déterminant -3 représente un nombre $8k+5$ ou $4k$ (ce qui arrive toujours lorsque l'un de ses trois premiers coefficients, b par exemple, est un nombre de cette espèce), cette forme n'est pas équivalente à la seconde des formes (4), et qu'elle l'est par conséquent à la première.

Pour démontrer maintenant que le nombre donné a peut être représenté par la première des formes (4), en procédant alors comme ci-dessus et posant derechef dans l'équation (5)

$$b' = 1, \quad c' = 0, \quad \Delta = bc - a'^2,$$

il ne reste plus qu'à établir que le nombre positif Δ peut être déterminé de telle sorte, que $b = a\Delta - 3$ prenne la forme $8k+5$ ou $4k$, et que $-\Delta$ soit en même temps résidu quadratique de b. Nous nous restreindrons ici aux nombres a qui n'ont avec le déterminant aucun facteur commun, c'est-à-dire qui ne sont pas divisibles par 3. Si l'on pose

$$\Delta = 8\Delta',$$

Δ' devant être impair et non divisible par 3, alors b sera premier avec Δ' et de la forme $8k+5$, et nous n'aurons plus qu'à remplir l'autre condition. De l'équation

$$b = 8a\Delta' - 3,$$

résulte immédiatement

$$\left(\frac{b}{\Delta'}\right) = \left(\frac{-3}{\Delta'}\right),$$

ou, en remarquant que

$$b \equiv 1 \pmod{\Delta},$$

et appliquant les propositions connues,

$$\left(\frac{b}{\Delta'}\right) = \left(\frac{\Delta'}{b}\right) = \left(\frac{-\Delta'}{b}\right) = \left(\frac{-3}{\Delta'}\right).$$

En multipliant par

$$\left(\frac{8}{b}\right) = \left(\frac{2}{b}\right) = -1,$$

on en tire

$$\left(\frac{-\Delta}{b}\right) = -\left(\frac{-3}{\Delta'}\right),$$

et l'on voit que la condition

$$\left(\frac{-\Delta}{b}\right) = 1$$

est satisfaite lorsque l'on fait

$$\Delta' = 6t - 1$$

et, par suite,

$$b = 48at - 8a - 3.$$

Or comme évidemment cette dernière expression peut devenir égale à un nombre premier, il est donc démontré que tout nombre non divisible par 3 peut être représenté par la forme

$$x^2 + y^2 + 3z^2,$$

de telle sorte que x, y, z n'aient aucun diviseur commun. Des considérations analogues peuvent s'appliquer aux nombres divisibles par 3, la possibilité de leur représentation étant soumise à une condition facile à apercevoir; elles peuvent également s'appliquer aux nombres qui peuvent être représentés par la seconde des formes (4).