

JOURNAL  
DE  
MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

---

V.-A. LEBESGUE

**Démonstration de ce théorème : tout nombre impair est la  
somme de quatre carrés dont deux sont égaux**

*Journal de mathématiques pures et appliquées 2<sup>e</sup> série*, tome 2 (1857), p. 149-152.

[http://www.numdam.org/item?id=JMPA\\_1857\\_2\\_2\\_\\_149\\_0](http://www.numdam.org/item?id=JMPA_1857_2_2__149_0)



NUMDAM

Article numérisé dans le cadre du programme  
Gallica de la Bibliothèque nationale de France  
<http://gallica.bnf.fr/>

et catalogué par Mathdoc  
dans le cadre du pôle associé BnF/Mathdoc  
<http://www.numdam.org/journals/JMPA>

DÉMONSTRATION DE CE THÉORÈME :

TOUT NOMBRE IMPAIR EST LA SOMME DE QUATRE CARRÉS DONT DEUX SONT ÉGAUX;

PAR M. V.-A. LEBESGUE.

Le moyen de démonstration employé ici l'a déjà été par M. Lejeune-Dirichlet (*Journal de Crelle*, tome XL, page 228), pour prouver que tous les nombres de forme  $4k + 2$ ,  $8k + 1$ ,  $8k + 3$  et  $8k + 5$  sont la somme de trois carrés sans facteurs communs.

I. THÉORÈME. — *Tout nombre impair  $2n + 1 = x^2 + y^2 + 2z^2$ ,  $x$ ,  $y$ ,  $z$  étant des entiers sans diviseur commun.*

*Démonstration.* Soit

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

une forme ternaire de déterminant  $-2$ , ou telle que l'on ait

$$(2) \quad aa'^2 + bb'^2 + cc'^2 - abc - 2a'b'c' = -2.$$

D'après le théorème de Seeber [\*], on reconnaît sans peine que la réduite des formes (1) est unique, savoir

$$(3) \quad X^2 + Y^2 + 2Z^2;$$

on peut donc passer de (3) à (1) par la substitution

$X = \alpha x + \beta y + \gamma z$ ,  $Y = \alpha' x + \beta' y + \gamma' z$ ,  $Z = \alpha'' x + \beta'' y + \gamma'' z$ ,  
de déterminant 1. De sorte qu'on trouve

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

les nombres  $\alpha$ ,  $\alpha'$ ,  $\alpha''$  étant sans diviseurs communs.

---

[\*] Voir sur ce théorème le cahier de Novembre 1856.

Il suffit donc de montrer que l'équation (2) peut être résolue en nombres entiers,  $a$  étant un nombre impair quelconque  $2n + 1$ .

Considérons le cas particulier  $b' = 1$ ,  $c' = 0$  (comme le fait M. Lejeune-Dirichlet dans l'article cité plus haut), l'équation (2) devient

$$(4) \quad b = a(bc - a'^2) - 2 = a\Delta - 2.$$

Le nombre  $bc - a'^2$  étant essentiellement positif, soit

$$bc - a'^2 = \Delta = 2t + 1;$$

alors l'équation (4) donne

$$b = 2at + a - 2;$$

comme  $a$  est impair,  $2a$  et  $a - 2$  sont premiers entre eux; posant  $t = 0, 1, 2, 3, \dots$ , on aura une suite de nombres en progression arithmétique, et renfermant une infinité de nombres premiers. On rencontrerait même encore une infinité de pareils nombres, en se restreignant aux valeurs de  $t$  d'une forme particulière comme  $t = 4k + 2$ , ce qui donnerait  $\Delta = 8k + 5$ , ou  $t = 4k + 1$ , ce qui donnerait  $\Delta = 8k + 3$ .

Il reste donc à prouver que parmi ces nombres premiers il en est qui permettent de déterminer  $c$  et  $a'$  par l'équation

$$(5) \quad bc - a'^2 = \Delta.$$

Pour que cette équation soit possible, il faut et il suffit qu'on ait

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

or l'équation

$$b = a\Delta - 2$$

donne

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

ces signes ayant le sens que leur donne Jacobi (voir *Journal de Mathématiques*, 1<sup>re</sup> série, tome XII, page 497).

Or

$$\left(\frac{\Delta}{b}\right) = \left(\frac{b}{\Delta}\right) (-1)^{\frac{b-1}{2} \cdot \frac{\Delta-1}{2}};$$

par suite,

$$\left(\frac{-\Delta}{b}\right) = \left(\frac{\Delta}{b}\right) (-1)^{\frac{b-1}{2}} = \left(\frac{b}{\Delta}\right) (-1)^{\frac{b-1}{2} + \frac{b-1}{2} \cdot \frac{\Delta-1}{2}};$$

d'ailleurs

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

et par conséquent

$$\left(\frac{-\Delta}{b}\right) = (-1)^{\frac{b-1}{2} + \frac{\Delta-1}{2} + \frac{\Delta^2-1}{8} + \frac{b-1}{2} \cdot \frac{\Delta-1}{2}} = (-1)^E.$$

Cela posé,

pour  $a=4n+1$ ,  $\Delta=8k+5$ , on trouve  $b=4h+3$ ,  $E \equiv 0 \pmod{2}$ ,

pour  $a=4n+3$ ,  $\Delta=8k+3$ , on trouve  $b=4h+3$ ,  $E \equiv 0 \pmod{2}$ ;

ainsi l'équation

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

est toujours satisfaite, et l'on a

$$(6) \quad 2n+1 = \alpha^2 + \alpha'^2 + 2\alpha''^2,$$

ce qu'il fallait démontrer.

II. Si l'on double l'équation (6), il vient

$$4n+2 = (\alpha + \alpha')^2 + (\alpha - \alpha')^2 + (2\alpha'')^2,$$

ou

$$2p = X^2 + Y^2 + Z^2.$$

J'ai montré qu'en général,  $p$  étant un nombre premier de forme  $\mu\pi + 1$ , on avait toujours (*Journal de Mathématiques*, 1<sup>re</sup> série, tome XIX, page 298)

$$2p = (a_0 - a_1)^2 + (a_1 - a_2)^2 + \dots + (a_{\mu-1} - a_0)^2,$$

les nombres  $a_0, a_1, \dots, a_{\mu-1}$  étant faciles à trouver par le moyen du *Canon Arithmeticus* de Jacobi.

Pour  $\mu = 3$ ,

$$2p = (a_0 - a_1)^2 + (a_1 - a_2)^2 + (a_2 - a_0)^2 = f^2 + g^2 + h^2.$$

Si aucun des nombres  $f, g, h$  n'était divisible par 3, chaque carré ayant la forme  $(3n \pm 1)^2 = 3N + 1$ ,  $2p$  serait divisible par 3, ce qui est impossible.

Soit donc  $a_0 - a_1$  divisible par 3, il vient

$$4p = 2(a_0 - a_1)^2 + (a_1 - a_0)^2 + (a_1 - 2a_2 + a_0)^2,$$

ou

$$4p = (a_1 - 2a_2 + a_0)^2 + 27 \left( \frac{a_1 - a_0}{3} \right)^2 = L^2 + 27M^2,$$

formule de Jacobi.

*N. B.* Quelques mots qui manquent à la page 298 citée plus haut (1<sup>re</sup> série du Journal, tome XIX) rendent une démonstration incomplète; il faut lire, ligne 8 en remontant,

« Comme  $(a_0 - a_1) + (a_1 - a_2) + (a_2 - a_0) = 0$ , l'une des trois » différences est divisible par 3, *car autrement on aurait p divisible par 3, ce qui est impossible.*

Sans les mots en caractères italiques, il n'y a plus démonstration.

