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

J. LIOUVILLE

Démonstration d'un théorème sur les nombres premiers de la forme $8\mu + 3$

Journal de mathématiques pures et appliquées 2^e série, tome 3 (1858), p. 84-88.
<http://www.numdam.org/item?id=JMPA_1858_2_3__84_0>

DÉMONSTRATION D'UN THÉORÈME

SUR

LES NOMBRES PREMIERS DE LA FORME $8\mu + 3$;

PAR M. J. LIOUVILLE

Il s'agit d'un théorème dont j'ai déjà donné l'énoncé dans ce journal, à savoir que *le double d'un nombre premier de la forme* $8\mu + 3$ *s'exprime toujours par la somme d'un carré et du produit d'un autre carré, par un nombre premier de la forme* $8\nu + 5$. Ainsi, pour prendre les exemples les plus simples, on a

$$2.3 = 1^2 + 5.1^2, \quad 2.11 = 3^2 + 13.1^2.$$

La méthode qui m'a conduit à ce théorème (méthode que j'ai empruntée à un Mémoire de M. Bouniakowsky) repose sur un lemme, concernant la somme des diviseurs d'un nombre, dont il faut d'abord dire un mot.

Soit

$$m = 2^s.a^\alpha\, b^\beta \ldots c^\gamma$$

un nombre entier décomposé en ses facteurs premiers, et qui peut d'ailleurs être pair ou impair, s se réduisant à zéro dans ce dernier cas. La somme $\int m$, ou $\zeta_1(m)$, des diviseurs de ce nombre est égale au produit

$$(1 + 2 + 2^2 + \ldots + 2^s)(1 + a + a^2 + \ldots + a^\alpha)(1 + b + b^2 + \ldots + b^\beta)\ldots,$$

dont le premier facteur est évidemment toujours impair. Quant aux autres facteurs, il est clair que comme a, b, ..., c sont impairs, ils seront tous impairs si les exposants α, β, ... γ sont tous pairs, mais que si un de ces exposants est pair, le facteur correspondant sera lui-même pair. On voit donc que la valeur de $\zeta_1(m)$ ne peut être impaire que quand m est de la forme $2^s.k^2$, c'est-à-dire que quand m est un carré

ou le double d'un carré. Cette condition est à la fois nécessaire et suffisante.

Cherchons maintenant dans quel cas la valeur de $\zeta_1(m)$ est simplement paire, c'est-à-dire est de la forme $2(2\rho+1)$. Il faut évidemment pour cela que l'un des exposants $\alpha, \beta, \ldots, \gamma$, par exemple α, soit impair, que tous les autres soient pairs, et que de plus le facteur $1+a+\ldots+a^{\alpha}$, correspondant à l'exposant impair α, soit lui-même simplement pair. Or cela ne peut jamais avoir lieu si a est de la forme $4\lambda+3$, car alors $1+a$, $1+a+a^2+a^3$, etc., sont évidemment des multiples de 4; ainsi a doit être de la forme $4\lambda+1$; ajoutons que l'exposant α doit être aussi de la forme $4l+1$, et concluons enfin que $\zeta_1(m)$ est un nombre simplement pair, sous la condition nécessaire et suffisante que m soit le produit d'un nombre premier $4\lambda+1$, élevé à la puissance 1 ou $4l+1$, par un carré ou par le double d'un carré que le nombre premier $4\lambda+1$ d'abord employé ne divise pas.

On exprimerait une condition nécessaire, mais non plus suffisante, en disant que $\zeta_1(m)$ ne peut avoir une valeur simplement paire que quand m est le produit d'un carré ou du double d'un carré par un nombre premier de la forme $4\lambda+1$.

L'alternative à propos du facteur 2 n'existe plus quand le nombre m est impair. Alors, pour que $\zeta_1(m)$ soit un nombre simplement pair, il faut et il suffit que m soit le produit d'un carré par la puissance 1 ou $4l+1$ d'un nombre premier $4\lambda+1$ qui ne divise pas ce carré; il faut, par conséquent, mais il ne suffit pas que m soit le produit d'un carré par un nombre premier $4\lambda+1$.

Cela posé, je me sers de la formule suivante, qui est connue ou facile à déduire de théorèmes connus, et où $\zeta_1(m)$ continue à désigner la somme des diviseurs de m, tandis que $\zeta_3(m)$ représente la somme de leurs cubes:

$$\zeta_3(m)=\zeta_1(1)\zeta_1(2m-1)+\zeta_1(3)\zeta_1(2m-3)+\zeta_1(5)\zeta_1(2m-5)+\ldots+\zeta_1(2m-1)\zeta_1(1).$$

Le nombre m est impair; le premier membre $\zeta_3(m)$ est, je le répète, la somme des cubes des diviseurs de m, et dans le terme général du second membre,

$$\zeta_1(n)\zeta_1(2m-n),$$

n est aussi impair et varie de 1 à $2m-1$. Comme on a

$$2m = n + (2m - n),$$

et comme on sait que $\zeta_4(n)$ est le nombre des décompositions de $4n$ en une somme de quatre carrés impairs, il est visible que notre formule exprime cette vérité connue, que $\zeta_3(m)$ est le nombre des décompositions de $8m$ en une somme de huit carrés impairs.

De cette formule, on tire, en groupant les termes à égale distance des extrêmes :

$$\frac{1}{2}[\zeta_3(m) - \zeta_1(m)^2] = \zeta_1(1)\zeta_1(2m-1) + \zeta_1(3)\zeta_1(2m-3) + \ldots + \zeta_1(m+1)\zeta_1(m-1).$$

Admettons que $2m$ ne puisse pas être la somme de deux carrés, ce qui sera certainement vrai si m est un nombre premier p de la forme $8\mu + 3$; alors dans le terme général

$$\zeta_1(n)\,\zeta_1(2m-n),$$

n et $2m-n$ ne pourront pas être à la fois des carrés, ni, par suite, les deux facteurs $\zeta_1(n)$ et $\zeta_1(2m-n)$ être à la fois impairs.

Ce terme général sera donc un nombre pair. Mais il faudra que pour certaines valeurs de n on le trouve simplement pair, si le premier membre

$$\frac{1}{2}[\zeta_3(m) - \zeta_1(m)^2]$$

de notre équation est lui-même simplement pair. On voit même qu'il faudra que le nombre des termes simplement pairs de la suite

$$\zeta_1(1)\zeta_1(2m-1) + \zeta_1(3)\zeta_1(2m-3) + \ldots + \zeta_1(m+1)\zeta_1(m-1)$$

soit lui-même impair. Or pour que le produit

$$\zeta_1(n)\,\zeta_1(2m-n)$$

soit simplement pair, il faut que l'un des facteurs $\zeta_1(n)$, $\zeta_1(2m-n)$ soit simplement pair et que l'autre soit impair. Il faut donc que des deux nombres impairs, n et $2m-n$, l'un soit un carré et l'autre le

produit d'un carré par la puissance 1 ou $4l+1$ d'un facteur premier de la forme $4\lambda+1$ qui ne divise pas ce carré.

Les deux conditions que nous exigeons, à savoir que $2m$ ne puisse pas être la somme de deux carrés, et que

$$\tfrac{1}{2}[\zeta_3(m)-\zeta_1(m)^2]$$

soit un nombre simplement pair, sont remplies en prenant pour m un nombre premier p de la forme $8\mu+3$. Cela est évident pour la première condition et le devient pour la seconde, en observant qu'on a alors

$$\zeta_3(m)=1+(8\mu+3)^3, \quad \zeta_1(m)=1+(8\mu+3),$$

d'où

$$\tfrac{1}{2}[\zeta_3(m)-\zeta_1(m)^2]=2(8\mu+3)(16\mu^2+10\mu+1).$$

Il est donc prouvé que le double $2p$ de tout nombre premier $8\mu+3$ s'exprime par la formule

$$2p=x^2+qy^2,$$

q désignant un nombre premier $4\lambda+1$ qui, s'il divise y, doit y entrer comme facteur avec un exposant pair. Puisque p est impair, x et y sont impairs, et λ aussi doit l'être, sans quoi l'on aurait $x^2+qy^2\equiv 2 \pmod 8$, tandis que $2p$ est $\equiv 6 \pmod 8$. Donc q est de la forme $8\nu+5$, et notre théorème est démontré. Il est établi en outre que le nombre des décompositions de $2p$, sous la forme citée, est nécessairement impair.

C'est ainsi que l'on a pour 2.19, c'est-à-dire pour le nombre 38, les trois décompositions que voici :

$$1^2+37.1^2, \quad 3^2+29.1^2, \quad 5^2+13.1^2.$$

Le lemme concernant la fonction $\zeta_1(m)$, qui fournit les conditions sous lesquelles $\zeta_1(m)$ est un nombre impair ou un nombre simplement pair, a ses analogues pour d'autres fonctions numériques. Ainsi la fonction $\varphi(m)$, qui marque le nombre des entiers premiers à m contenus dans la suite 1, 2, 3,..., m, ne peut avoir une valeur impaire que quand $m=1$ ou 2, et une valeur simplement paire que quand

m est égal à 4 ou est de l'une des deux formes a^{α}, $2a^{\alpha}$, a désignant un nombre premier de la forme $4\mu + 3$. On peut encore citer les fonctions $\zeta_2(m)$, $\zeta_3(m)$, etc., qui expriment la somme des carrés, la somme des cubes, etc., des diviseurs de m, la fonction $\zeta(m)$ qui exprime leur nombre, et une foule d'autres fonctions que l'on peut même créer à volonté pour le besoin des problèmes dont on s'occupe. Cette remarque si simple (que je pourrai développer une autre fois par de nombreux exemples) agrandit singulièrement le champ des questions auxquelles la méthode de M. Bouniakowsky s'applique.