NOUVELLES ANNALES DE MATHÉMATIQUES

LEBESGUE

Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + I$

Nouvelles annales de mathématiques 1re série, tome 9 (1850), p. 178-181

<http://www.numdam.org/item?id=NAM_1850_1_9__178_0>

SUR L'IMPOSSIBILITÉ, EN NOMBRES ENTIERS, DE L'ÉQUATION $x^m = y^2 + 1$;

PAR M. LEBESGUE.

Selon M. Catalan, deux nombres consécutifs, autres que 8 et 9, ne peuvent être des puissances (*Ann.*, t. I, p. 520); en d'autres termes, l'équation $x^m = y^n + 1$ est impossible.

L'impossibilité est manifeste pour $m = n$, et plus généralement pour le cas dans lequel m et n ont un diviseur commun. On peut donc ramener tous les cas à ceux de m et n premiers en changeant les inconnues. Voici la démonstration pour le cas de $n = 2$ et m impair.

Elle repose sur les propriétés élémentaires des nombres entiers complexes $a + b\sqrt{-1}$ (a, b entiers, positifs ou négatifs), introduits par M. Gauss dans la *Théorie des Nombres*. Il suffira de dire ici qu'en représentant par a_1, a_2, a_3, etc., une suite d'entiers $\alpha_1 + \beta_1\sqrt{-1}$, $\alpha_2 + \beta_2\sqrt{-1}$, etc., liés par des équations telles que

$$a_i = q_i\, a_{i-1} + a_{i+1};$$

mettant le quotient $\frac{a_i}{a_{i+1}}$ sous la forme $b_i + c_i\sqrt{-1}$, et faisant $q_i = \mathrm{B}_i + \mathrm{C}_i\sqrt{-1}$, en supposant que B_i, C_i soient les entiers les plus près (par excès ou défaut) de b_i, c_i, c'est-à-dire tels, que les valeurs absolues des différences $b_i - \mathrm{B}_i$, $c_i - \mathrm{C}_i$ ne surpassent jamais $\frac{1}{2}$, alors le carré du module de a_{i+2}, ou $(\alpha_{i+2})^2 + (\beta_{i+2})^2$, en faisant $a_{i+2} = \alpha_{i+2} + \beta_{i+2}\sqrt{-1}$, sera moindre que la moitié du carré du module de a_{i+1}.

(*Nota*. On donne le nom de *norme* au carré du module.) On voit donc que la série a_1, a_2, a_3, etc., se terminera par un nombre dont la norme sera 0 ou 1. (Voir *Nouvelles Annales*, tome III, page 340.)

Au moyen de ce théorème de M. Gauss, on peut étendre aux entiers $a + b\sqrt{-1}$ toutes les propositions correspondantes à celles qui existent pour les entiers ordinaires, relativement à la décomposition en facteurs simples ou premiers. De là, au moyen du théorème de Waring, on établirait sans difficulté que tout nombre premier p de forme $4k+1$ est la somme de deux carrés :

$$p = a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1}).$$

Il suffira d'avoir indiqué en passant cette application déjà faite par M. Dirichlet.

Au moyen du même théorème, on peut prouver aussi l'impossibilité de l'équation

$$x^m = y^2 + 1 = (y + \sqrt{-1})(y - \sqrt{-1}).$$

Si les facteurs $y + \sqrt{-1}$, $y - \sqrt{-1}$ avaient un facteur commun, il diviserait la différence $2\sqrt{-1}$; or, y impair donnerait $y^2+1 = 4k+2$ qui n'est pas une puissance; donc y est divisible par 2; $\sqrt{-1}$ ne l'est pas; les facteurs communs ne peuvent donc être que $+1$, -1, $\sqrt{-1}$, $-\sqrt{-1}$, qui sont diviseurs de tous les nombres. Ainsi $y + \sqrt{-1}$ et $y - \sqrt{-1}$ sont premiers entre eux; et puisque $y^2 + 1$ est une puissance $m^{ième}$, il faudra poser

$$y + \sqrt{-1} = (u + v\sqrt{-1})^m (\sqrt{-1})^\alpha,$$
$$y - \sqrt{-1} = (u - v\sqrt{-1})^m (-\sqrt{-1})^\alpha,$$
$$y^2 + 1 = (u^2 + v^2)^m = x^m, \quad x = u^2 + v^2.$$

Comme y est pair et x impair, l'un des nombres u, v

est pair. De là

$$2\sqrt{-1} = \left[(u+v\sqrt{-1})^m - (u-v\sqrt{-1})^m\right](-1)^{\alpha}(\sqrt{-1})^{\alpha};$$

savoir, pour α pair $= 2\beta$,

$$(-1)^{\beta} = m.u^{m-1}v - \frac{m.m-1.m-2}{1.2.3}u^{m-3}v^3 + \ldots \pm v^m;$$

et pour α impair $= 2\beta + 1$.

$$(-1)^{\beta} = u^m - \frac{m.m-1}{1.2}u^{m-2}v^2 + \ldots \pm muv^{m-1};$$

la première équation donne $v = \pm 1$, la deuxième $u = \pm 1$, puisque u et v divisent $(-1)^{\beta} = \pm 1$.

On aura donc, dans les deux cas,

$$1 - \frac{m.m-1}{1.2}p^2 + \frac{m.m-1.m-2.m-3}{1.2.3.4}p^4 - \ldots = \pm 1;$$

p étant égal à u ou à v, et toujours pair. Avec le signe inférieur, l'équation est impossible, car elle donnerait 2 divisible par 4. Avec le signe supérieur on a, en divisant par p^2,

$$(A) \quad \frac{m.m-1}{1.2} - \frac{m.m-1.m-2.m-3}{1.2.3.4}p^2 + \ldots = 0.$$

Or cette équation est impossible. Cela est évident pour $\frac{m.m-1}{1.2}$ impair; pour $\frac{m.m-1}{1.2}$ pair, l'impossibilité s'établit ainsi qu'il suit :

Soit $A\theta^{\alpha} + B\theta^{\beta} + C\theta^{\gamma} + \ldots$ une fonction entière où les entiers A, B, C, etc., sont premiers à θ; si les exposants entiers positifs α, β, γ, etc., ne vont pas en décroissant, et que α soit moindre que tous les autres, on ne saurait avoir $A\theta^{\alpha} + B\theta^{\beta} + \ldots = 0$; car il en résulterait

$A + B\theta^{\beta-\alpha} + C\theta^{\gamma-\alpha} + \ldots = 0$, d'où A divisible par θ contre l'hypothèse.

Or l'équation (A) rentre dans ce cas. Si l'on prend le terme général de l'équation A, et qu'on l'écrive ainsi

$$\frac{m.m-1}{1.2} \times \frac{m-2.m-3\ldots m-2k+1}{1.2\ldots 2k-2} \times \frac{1.2.p^{2k-2}}{2k-1.2k};$$

les deux premiers facteurs étant entiers, et le premier pair par hypothèse, le dernier facteur n'est pas nécessairement entier; mais la puissance de 2 qui divise le numérateur surpasse la puissance de 2 qui divise le dénominateur, si la puissance de 2, qui divise p^{2k-2}, surpasse la puissance de 2 qui divise k. Or, c'est ce qui a lieu; p est pair, donc p^{2k-2} est divisible au moins par

$$2^{2k-2} = (1+1)^{2k-2} = 1 + 2k - 2 + \alpha = k + k - 1 + \ldots > k.$$

Ainsi le troisième facteur a la forme $\frac{2^{\alpha}.i}{i'}$, i et i' étant des entiers impairs; on voit donc que dans le terme général, qui est nécessairement entier, l'exposant de 2 est plus grand que dans le premier terme $\frac{m.m-1}{1.2}$; l'équation (A) est donc impossible.

Les autres cas de l'équation $x^m = y^n + 1$ paraissent présenter plus de difficulté. Je n'ai pu savoir jusqu'ici ce que M. Catalan a trouvé à ce sujet.