

TERQUEM

Théorèmes sur les puissances des nombres

Nouvelles annales de mathématiques 1^{re} série, tome 5
(1846), p. 70-78

http://www.numdam.org/item?id=NAM_1846_1_5__70_1

© Nouvelles annales de mathématiques, 1846, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

THÉORÈMES

sur les Puissances des Nombres.

—

1. *Théorème.* S'il est impossible de satisfaire à l'équation $X^n + Y^n = Z^n$, il est aussi impossible de satisfaire à l'équation $x^n + y^n = z^n$ (Lebesgue).

Démonstration. Il suffit évidemment de démontrer le théorème pour des nombres entiers.

a) Si deux des trois x, y, z ont un facteur commun, il divise aussi le troisième; on peut ainsi le faire disparaître; donc deux quelconques des trois nombres peuvent être

supposés premiers entre eux et il n'y a qu'un seul des trois nombres qui soit pair.

b) z ne peut être pair ; z^2 serait divisible par 4 ; et x et y étant alors impairs, la somme des deux carrés impairs $(x^n)^2 + (y^n)^2$ ne peut donner un nombre divisible par 4 ; donc l'un des deux nombres x, y est nécessairement pair et l'autre impair. Soit donc $x = 2^m p q$; m est au moins égal à l'unité ; p et q sont deux nombres impairs et premiers entre eux, et pouvant être l'unité, chacun ou ensemble. Ainsi les quatre nombres y, p, q, z sont impairs et premiers entre eux, pris deux à deux.

Premier cas. n pair.

L'équation peut alors évidemment prendre la forme

$$u^4 + v^4 = z^2 ; \text{ ou } 2^{4m} p^4 q^4 + v^4 = z^2 ; 2^{4m} p^4 q^4 = \\ = (z - v^2)(z + v^2).$$

a) $z + v^2$ et $z - v^2$ n'ont d'autre facteur commun que 2 ; car ce facteur commun appartient à la somme $2z$ et à la différence $2v^2$; z et v étant premiers, $2z$ et $2v^2$ n'ont que 2 pour facteur commun.

b) Il n'y a donc que ces deux décompositions possibles :

$$z + v^2 = 2p^4, \\ z - v^2 = 2^{4m-1} q^4 ;$$

ou bien :

$$z - v^2 = 2p^4, \\ z + v^2 = 2^{4m-1} q^4.$$

Le premier système donne $v^2 = p^4 - 2^{4m-2} q^4$; et le second, $v^2 = 2^{4m-2} q^4 - p^4$. Or, cette dernière équation est impossible ; car elle donne :

$$v^2 + p^4 = 2^{4m-2} q^4 ;$$

v^2 et p^4 étant deux carrés impairs, leur somme ne peut être

divisible par 4 ; on ne peut donc admettre que le premier système, dont on tire $2^{4m-3}q^4 = (p^2 + \nu)(p^2 - \nu)$. Faisons $q = rs$, r et s étant deux nombres impairs premiers entre eux ; et raisonnant comme dessus, on aura ces deux systèmes possibles :

$$\left. \begin{array}{l} p^2 + \nu = 2r^4 \\ p^2 - \nu = 2^{4m-3}s^4 \end{array} \right\} \left. \begin{array}{l} p^2 - \nu = 2r^4 \\ p^2 + \nu = 2^{4m-3}s^4 \end{array} \right\}$$

L'un et l'autre système donne $p^2 = r^4 + (2^{m-1}s)^4$ (1) ; donc si l'équation $(2^m pq)^4 + \nu^4 = r^4$ est possible, celle-ci, l'équation (1) le sera aussi, ou p, ν, s sont des nombres impairs premiers entre eux, et m est diminué d'une unité ; en continuant ainsi, on parviendra enfin à une équation $p'^2 = r'^4 + s'^4$, ou p', r', s' sont des nombres impairs, résultat absurde ; donc aussi la somme de deux bicarrés ne peut être un bicarré. Théorème de Fermat (*Théorème des Nombres*, t. II, p. 5, 3^e édit. 1830).

Deuxième cas. n est impair.

Faisant toujours $x = 2^m pq$, il vient $(2^m pq)^{2n} + y^{2n} = z^2$; $2^m pq)^{2n} = (z - y^n)(z + y^n)$, d'où deux systèmes possibles :

$$\left. \begin{array}{l} z - y^n = 2p^{2n}, \quad \text{ou bien } z + y^n = 2p^{2n} \\ z + y^n = 2^{2mn-1}q^{2n}, \quad \quad z - y^n = 2^{2mn-1}q^{2n}. \end{array} \right\}$$

Le second système donne

$$y^{2n} = p^{2n} - 2^{2mn-1}q^{2n} = [p^n - (2^{mn-1}q)^n][p^n + (2^{mn-1}q)^n] ;$$

faisant $y = rs$ en supposant r et s impairs et premiers entre eux, on aura :

$$\begin{aligned} r^{2n} &= p^n + 2^{mn-1}q^n ; \quad s^{2n} = p^n - 2^{mn-1}q^n ; \quad \text{d'où } r^{2n} - s^{2n} = 2^{mn}q^n = \\ &= (2^m q)^n ; \quad \text{et } r^n = s^n + (2^m q)^n. \end{aligned}$$

Or, cette équation est supposée impossible ; donc... etc.

Pour le premier système, il suffit de supposer que y , ou que l'un des diviseurs r ou s est négatif et l'on parvient à la même conclusion.

Si $n = 1$, en obtient la solution connue :

$$\begin{aligned} \pm y &= p^2 - (2^{m-1}q)^2 \\ z &= p^2 + (2^{m-1}q)^2 \\ x &= 2^m pq. \text{ (Voir } \textit{Annales}, \text{ t. I, p. 184.)} \end{aligned}$$

Observation. La première partie du théorème, savoir que la somme de deux quatrièmes puissances ne peut être un carré, est indépendante du théorème de Fermat sur l'impossibilité de trouver une puissance de nom quelconque, la seconde exceptée, égale à la somme de deux puissances de même nom.

II. *Théorème.* $y^{2n} - x^{2n} = 2z^n$ est une équation impossible, en nombres rationnels pour $n > 1$.

Démonstration. Faisons $x^{2n} + z^n = u$; $u + z^n = y^{2n}$;

$$u - z^n = x^{2n} ; u^2 - z^{2n} = (xy)^{2n} ; \text{ d'où } (xy)^{2n} + z^{2n} = u^2,$$

équation impossible d'après le théorème précédent ; donc...

Corollaire. Ainsi la différence de deux bicarrés ne peut être égale au double d'un carré.

Observation. Ce théorème est de M. Liouville (*Journ. des Math.*, t. V, p. 360. 1840).

III. *Théorème.* La différence de deux bicarrés ne peut être un carré.

Démonstration. Soit l'équation $x^4 - y^4 = z^2$; il suffit de prouver l'impossibilité de cette équation en nombres entiers et premiers entre eux, pris deux à deux ; il y a donc deux nombres impairs et un nombre pair ; x ne peut être pair, car la somme $y^4 + z^2$ de deux carrés impairs ne peut être égale à un carré. Il y a donc deux cas possibles :

Premier cas. x impair ; y pair ; z impair.

Faisons $y=2^m pq$; m au moins = 1 ; p et q nombres impairs premiers entre eux et premiers avec x et z , l'équation devient $(x^2 + z)(x^2 - z) = 2^{4m} p^4 q^4$; $x^2 + z$ et $x^2 - z$ n'ont que 2 pour facteur commun ; donc $x^2 \pm z = 2p^4$

$$x^2 \mp z = 2^{4m-1} q^4$$

$$x^2 = p^4 + 2^{4m-2} q^4 ; (x - p^2)(x + p^2) = 2^{4m-2} q^4 ;$$

$x - p^2$ et $x + p^2$ n'ont que 2 en facteur commun ; d'où :

$$x - p^2 = 2 ; \quad p^2 = 2^{4m-4} q^4 - 1 ; \quad 1 + p^2 = 2^{4m-4} q^4 ,$$

$$x + p^2 = 2^{4m-2} q^4$$

équation impossible, car la somme de deux carrés impairs ne peut être égale à un carré ; donc...

Deuxième cas. x impair ; y impair ; z pair.

$$z = 2^m pq ; (x^2 - y^2)(x^2 + y^2) = 2^{2m} p^2 q^2 ; x^2 + y^2 = 2p^2 ;$$

$$x^2 - y^2 = 2^{2m-1} q^2 ; x^2 = p^2 + 2^{2m-2} q^2 ; y^2 = p^2 - 2^{2m-2} q^2 ;$$

$$x^2 y^2 = p^4 - (2^{2m-1} q)^2 ;$$

si $m = 1$, l'équation est impossible, puisque p, q, x, y sont des nombres impairs ; si $m > 1$, l'équation rentrant dans le cas précédent, est encore impossible.

Le second système, $x^2 - y^2 = 2p^2$; $x^2 + y^2 = 2^{2m-2} q^2$ mène à l'équation impossible $y^2 + p^2 = 2^{2m-2} q^2$; donc, etc.

Corollaire. Donc ni la somme de deux bicarrés, ni leur différence ne peut être un bicarré.

IV. Théorème. Lorsque la somme des deux carrés est un carré, le produit des racines ne peut être le double d'un carré.

Démonstration. Soit $x^2 + y^2 = u^2$; $xy = 2v^2$; on en tire $(x^2 - y^2)^2 = u^4 - (2v)^4$; mais la différence de deux bicarrés ne peut être un carré ; donc...

observation. Lorsque les côtés d'un triangle rectangle sont des nombres rationnels, l'aire ne peut être un nombre carré.

V. *Théorème.* L'équation $x^4 + 4y^4 = z^2$ est impossible, excepté pour $y = 0$.

Démonstration. x et z sont impairs et premiers entre eux ; $x^4 = (z + 2y^2)(z - 2y^2)$; ces deux derniers facteurs sont impairs et premiers entre eux ; donc :

$$z + 2y^2 = r^4 ; z - 2y^2 = s^4 ; 4y^2 = r^4 - s^4 ;$$

équation impossible (théorème III) ; donc...

Observation. Une démonstration analogue fait voir que la formule $x^4 - 4y^4$ ne peut devenir un carré.

VI. *Théorème.* L'équation $x^4 + 2y^4 = z^2$ est impossible en nombres rationnels, excepté pour $y = 0$.

Démonstration. Raisonnant toujours comme ci-dessus, il est évident que x et z sont impairs et premiers entre eux ;

$$2y^4 = z^2 - x^4 = (z + x^2)(z - x^2) ;$$

le second nombre est parement pair ; donc y doit être pair.

D'après la théorie des carrés, on a :

$$z = p^2 + 2q^2 ; x^2 = p^2 - 2q^2 ; y^2 = 2pq ;$$

par la même théorie, l'équation $p^2 - x^2 = 2q^2$ donne :

$$x = m^2 - 2n^2 ; p = m^2 + 2n^2 ; q = 2mn ;$$

d'où $y^2 = 4mn(m^2 + 2n^2)$; m et n sont premiers entre eux ; il faut donc que $m, n, m^2 - 2n^2$ soient des carrés. Faisons $m = f^2$; $n = g^2$; ni f ni g ne peut devenir nul, à moins qu'on ait $y = 0$; nous devons donc avoir $f^4 + 2g^4 = v^2 = p$, équation semblable à celle qui est donnée ; mais $p^2 < z$; $v < \sqrt[4]{z}$; le second membre de l'équation donnée peut donc aller en diminuant sans pouvoir devenir nul, ce qui est impossible ; donc..., etc.

VII. *Théorème.* L'équation $x^4 - 8y^4 = z^2$ est impossible en nombres rationnels, excepté pour $y = 0$.

Démonstration. On déduit de cette équation

$$z^2 + 2(2xy)^4 = (x^4 + 8y^4)^2,$$

équation impossible, etc.

VIII. *Théorème.* L'équation $x^4 - 4y^4 = z^2$ est impossible en nombres rationnels, excepté pour $y = 0$.

Démonstration. On a

$$x^2 = p^2 + q^2; 2y^2 = p^2 - q^2; z = 2pq; \text{ d'où } 2x^2y^2 = p^4 - q^4,$$

équation impossible (théor. II).

IX. *Récapitulation.*

$$\begin{aligned} x^4 \pm y^4 = z^2; \quad x^4 - y^4 = 2z^2; \quad x^4 + 2y^4 = z^2; \\ x^4 \pm 4y^4 = z^2; \quad x^4 - 8y^4 = z^2 \end{aligned}$$

sont des équations impossibles en nombres rationnels (Voir Legendre, *Théorie des nombres*).

X. *Théorème.* Aucun nombre triangulaire, excepté l'unité, n'est égal à un bicarré.

Démonstration. Soit $x(x-1) = 2z^4$; faisons $z = mn$; il n'y a que deux décompositions possibles.

Première décomposition :

$$x = 2m^4; \quad x+1 = n^4; \text{ d'où } 1 = n^4 - 2m^4; \text{ ou } 2m^4 + 1 = n^4,$$

équation impossible (th. VI).

Deuxième décomposition :

$$x = n^4; \quad x+1 = 2m^4; \quad 1 = 2m^4 - n^4;$$

on en tire :

$$-n^4 = 1 - 2m^4; \quad m^8 - n^4 = (m^4 - 1)^2;$$

équation impossible (th. III), à moins de supposer $m=n=1$.

XI. Théorème. Ni la somme d'un nombre et de son réciproque, ni leur différence ne peut être un carré.

Démonstration. Soit l'équation $z \pm \frac{1}{z} = v^2$; z étant un nombre quelconque entier ou fractionnaire, on en tire :

$z = \frac{1}{2} v^2 \pm \frac{1}{2} \sqrt{v^4 \pm 4}$; et, faisant $v = \frac{p}{q}$, $p^4 \pm 4q^4$ ne peut être un carré; donc..., etc.

Autrement. Soit $z = \frac{p}{q}$; p et q nombres premiers entre eux; alors $\frac{z^2 \pm 1}{z} = \frac{p^2 \pm q^2}{pq}$; $p^2 \pm q^2$ et pq sont aussi premiers entre eux; donc, pour que cette expression soit un carré, il faut que pq et $p^2 \pm q^2$ soient des carrés; or, p et q étant premiers entre eux, il faut que p et q soient chacun un carré, et alors $p^2 \pm q^2$ étant la somme ou la différence de deux bicarrés, ne peut être un carré; donc..., etc.

Observation. $\frac{x}{y} \pm \frac{y}{x}$ ne peut donc être un carré; donc on ne peut avoir $\frac{x}{y} \pm \frac{y}{x} = 1$, ou $x^2 \pm y^2 = xy$ (Théorème de M. Vachette, voir p. 111).

XII. Trouver à quelle condition on peut satisfaire en nombres rationnels à l'équation $y^2 + myx^2 + a = 0$; m et a sont des nombres donnés.

Solution. $y = -\frac{1}{2} ax^2 \pm \frac{1}{2} \sqrt{m^2 x^4 - 4a}$; ainsi il faut que la formule $m^2 p^4 - 4aq^4$, ou ce qui revient au même, que la somme $p^4 - 4am^2 q^4$ puisse devenir un carré.

XIII. Remarque. Quelqu'un répétait devant d'Alembert l'assertion banale que la géométrie servait à rectifier l'esprit. Oui, reprit d'Alembert, à rectifier les esprits droits. Cette réponse spirituelle est d'une grande justesse. Il est vrai pour-

tant de dire que l'étude des sciences exactes rend en général l'esprit difficile sur le mérite des *preuves*. Euler croit que la théorie des nombres en particulier est plus propre encore que la géométrie à donner de la rectitude au jugement et de l'intensité à la faculté méditative. Si l'on introduisait les principales propositions de cette théorie dans l'enseignement classique, les examinateurs acquerraient un excellent criterium pour classer les intelligences. Ce moyen est infiniment préférable à celui qui est en usage, et qui consiste à rendre difficiles des lieux communs, à accumuler des minuties puritaines, plus propres à cambrer les esprits qu'à les rendre droits. Admettons donc dans nos collèges le calcul différentiel pour faciliter, abrégé, étendre les études, et la théorie des nombres pour en augmenter la force. La véritable logique s'apprendra alors dans nos classes. Surtout depuis que nos philosophes désertent les sciences, ne veulent plus être que des écrivains et des littérateurs et croient pouvoir se passer des sciences exactes. Platon, Aristote, Descartes, Leibnitz, Mallebranche, Gassendi, Spinoza, Clarke, Kant, n'étaient pas de cet avis. On ne voit pas ce que la philosophie a gagné à cette ignorance-là.

Comment d'ailleurs nos prétendus disciples de Platon feraient-ils pour entrer dans l'école du maître, laquelle portait l'inscription connue : Οὐδείς ἀγεωμέτρητος εἰσέλτω, qu'aucun non-géomètre n'entre ici ?

Dans un article spécial, nous signalerons les nombreuses lacunes, l'état honteusement arriéré de l'enseignement mathématique universitaire et nous indiquerons les moyens faciles d'y remédier, par les programmes d'examen.

Tm.