L'HYPOTHÈSE DE FERMAT POUR LES EXPOSANTS NÉGATIFS

Autor(en): **Thérond, Jean-Daniel**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **13 (1967)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-41547

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'HYPOTHÈSE DE FERMAT POUR LES EXPOSANTS NÉGATIFS

par Jean-Daniel THÉROND

Rappelons tout d'abord l'hypothèse de Fermat et les derniers résultats connus.

Hypothèse de Fermat : L'équation diophantienne

$$F_n(x, y, z) \equiv x^n + y^n - z^n = 0$$

n'a pas de solution non triviale si l'entier n est strictement supérieur à 2.

Un calcul rapide ($F_n(ax, ay, az) \equiv a^n F_n(x, y, z)$) montre qu'il suffit de chercher x, y et z premiers entre eux; les racines seront alors appelées primitives. De plus, si $n = qp$, l'identité $F_n(x, y, z) \equiv F_p(x^q, y^q, z^q)$ nous conduit à ne démontrer la proposition uniquement lorsque n est 4 ou un nombre premier impair. Euler le fit pour 3 et 4, puis Legendre et Dirichlet pour $n = 5$ en 1825 seulement (l'hypothèse, publiée en 1670, date de 1637) et, en 1840, Lamé et Lebesgue pour $n = 7$.

Kummer crut trouver une démonstration générale en raisonnant dans l'extension $Z[\zeta]$ de Z, où ζ est une racine primitive n-ième de l'unité, et en écrivant $F_n(x, y, z) = 0$ sous la forme:

$$(x+y)(x+\zeta y)(x+\zeta^2 y) \cdot \ldots \cdot (x+\zeta^{n-1} y) = z^n .$$

Il avait en effet supposé implicitement, ce que les résultats de 1831 sur les entiers de Gauss pouvaient laisser espérer, que dans l'anneau $Z[\zeta]$ (anneau des entiers algébriques du corps cyclotomique $Q(\zeta)$) la décomposition en produit de facteurs premiers est unique (ce qui implique que si le produit de deux nombres premiers entre eux est une puissance n-ième d'un autre, chacun en est).

Or ce n'était pas le cas, comme il le démontra lui-même. Il réussit néanmoins, en créant la notion d'idéal et la théorie des corps de nombres algébriques, à démontrer l'hypothèse de Fermat pour les entiers n dits réguliers, c'est-à-dire tels que le nombre de classes de diviseurs du corps cyclotomique d'ordre n $Q(\zeta)$ soit divisible par n (on pourra en trouver la démonstration dans [5]). Ces nombres vérifient un certain critère où inter-

viennent les nombres de Bernouilli. L'hypothèse fut ainsi vérifiée pour tous les nombres premiers impairs inférieurs à 100 hormis 37, 59 et 67. Depuis, de très nombreux auteurs (cf. [4]) ont démontré d'autres résultats utilisant d'autres critères qui, vérifiés à l'aide de calculatrices, permettent d'affirmer:

L'hypothèse de Fermat est démontrée pour toutes les puissances n supérieures à 2 et telles que n comporte, dans sa décomposition en produit de facteurs premiers, soit 4 soit un nombre premier impair inférieur à 25 000 (cf. [3]).

Le problème n'a pas, semble-t-il, été examiné pour les exposants négatifs. C'est ce que, en admettant l'hypothèse de Fermat, on va faire maintenant en démontrant:

THÉORÈME 1: *L'équation diophantienne* $F_n(x, y, z) \equiv x^n + y^n - z^n = 0$ *où* $n \in \mathbf{Z}$

— *n'a pas de solution si* $n < -2$

— *possède des solutions si* $n = -1$ *ou* $n = -2$.

On calculera explicitement ces solutions.

DÉMONSTRATION: L'exposant de x, y et z étant dorénavant négatif, on l'écrira sous la forme $-n$ où $n > 0$.

$$F_{-n}(x, y, z) = 0 \Rightarrow z^n = \frac{x^n y^n}{x^n + y^n} \Rightarrow z = \frac{xy}{\sqrt[n]{x^n + y^n}}.$$

$$z \in \mathbf{N}^* \Rightarrow \sqrt[n]{x^n + y^n} \in \mathbf{Q}^* \Leftrightarrow \exists\, p \text{ et } q \in \mathbf{N}^* : \sqrt[n]{x^n + y^n} = \frac{p}{q}$$

qui implique

$$(qx)^n + (qy)^n - p^n = 0.$$

Or, d'après l'hypothèse de Fermat, l'équation diophantienne $F_n(qx, qy, p) = 0$ n'a pas de solution non triviale si $n > 2$, donc $F_{-n}(x, y, z) = 0$ n'a pas de solution en nombres entiers si $n > 2$. Ce qui démontre la première partie du Théorème 1.

Pour la seconde, on calculera effectivement les racines primitives.

* * *

Pour $n = 1$ on va montrer:

THÉORÈME 2: *Les racines primitives de l'équation diophantienne* $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$ *sont* $x = p+1$, $y = p(p+1)$, $z = p$ *où* $p \in \mathbf{N}^*$.

DÉMONSTRATION: Il existe p et q, premiers entre eux, tels que $px = qy$ (car $(x, y) = 1$), donc

$$F_{-1}(x, y, z) = 0 \Rightarrow \frac{1}{x} + \frac{q}{px} = \frac{p+q}{px} = \frac{1}{z} \Rightarrow z = \frac{px}{p+q}.$$

$(p, q) = 1 \Rightarrow (p, p+q) = 1$ or $z \in \mathbf{N}^*$ donc $p+q$ divise x, ainsi il existe un entier m vérifiant $x = m(p+q)$ d'où

$$z = pm \qquad y = \frac{p}{q}x = \frac{p}{q}m(p+q)$$

or l'on exige $(x, y, z) = 1$ d'où, en divisant x, y et z par m,

$$x = p+q \qquad y = \frac{p}{q}(p+q) \qquad z = p.$$

Or y n'est entier, puisque $(p, q) = 1$ et $(p+q, q) = 1$, que si $q = 1$, ce qui démontre le Théorème 2.

* * *

Pour $n = 2$ on utilisera le théorème suivant que l'on ne démontrera pas.

THÉORÈME 3: *Les racines primitives non triviales de l'équation diophantienne* $F_2(x, y, z) \equiv x^2 + y^2 - z^2 = 0$ *sont*

$$x = \frac{a^2 - b^2}{2} \qquad y = ab \qquad z = \frac{a^2 + b^2}{2}$$

où a *et* b *sont impairs et premiers entre eux.*

Démontrons, en utilisant ce résultat:

THÉORÈME 4: *Les racines primitives de l'équation diophantienne* $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$ *sont*

$$x = 4n(4n^2+1) \qquad y = (4n^2-1)(4n^2+1) \qquad z = 4n(4n^2-1) \qquad n \in \mathbf{N}^*$$

DÉMONSTRATION:

$$\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2} \Rightarrow z^2 = \frac{x^2 y^2}{x^2 + y^2}$$

où x, y et z sont premiers entre eux, donc x^2+y^2 est un carré que l'on notera t^2.

$x^2+y^2 = t^2 \Leftrightarrow F_2(x, y, t) = 0$ dont les solutions primitives sont (cf. th. 3)

$$x = \frac{a^2 - b^2}{2} \qquad y = ab \qquad t = \frac{a^2 + b^2}{2}$$

où $(a, b) = 1$, a et b impairs.
Donc

$$z = \frac{xy}{t} = \frac{a^2 - b^2}{a^2 + b^2}\, ab\,.$$

A quelles conditions z est-il entier ? Les entiers a et b étant impairs (et différents sinon $x = 0$ et x^{-2} n'est pas défini), posons

$a = 2p + 1 \qquad b = 2q + 1 \qquad$ avec $\qquad p > q \qquad$ (sinon $x < 0$)

où $p \in \mathrm{N}$ ainsi que q.

$$a + b = 2(p + q + 1) \qquad \text{et} \qquad a - b = 2(p - q)$$

donnent

$$z = \frac{2(p+q+1)\,2(p-q)(2p+1)(2q+1)}{(2p+1)^2 + (2q+1)^2}$$

dont le dénominateur égal à $4p^2 + 4p + (4q^2 + 4q + 2)$ égale aussi $4(p-q)(p+q+1) + 2(2q+1)^2$, donc

$$z = \frac{2(p+q+1)(p-q)(2p+1)(2q+1)}{2(p+q+1)(p-q) + (2q+1)^2}\,.$$

Le fait que z doive être entier exige que $2q+1$, premier avec $2p+1$, soit divisible par $p-q$ ou $p+q+1$ (qui sont premiers entre eux sinon $2p+1$ et $2q+1$ ne le seraient pas). Or $p+q+1 > 2q+1$ donc

$$2q + 1 = k(p - q) \Rightarrow p = \frac{(2+k)\,q + 1}{k}\,,$$

dans lequel l'entier k est impair, sinon p n'est pas entier.

Ainsi

$$z = \frac{2(p+q+1)(2p+1)(2q+1)}{2(p+q+1) + (2q+1)\,k}$$

Or

$$2p + 1 = (2q+1)\frac{k+2}{k} \qquad \text{et} \qquad p + q + 1 = \frac{k+1}{k}\,(2q+1)$$

d'où

$$z = \frac{2\left[(2q+1)\dfrac{k+1}{k}\right]\left[(2q+1)\dfrac{k+2}{k}\right](2q+1)}{2(2q+1)\dfrac{k+1}{k} + (2q+1)\,k}$$

d'où

$$z = \frac{2(k+1)(k+2)}{k\left[(k+1)^2+1\right]}(2q+1)^2 .$$

Or $(k, 2) = 1$ (sinon $p \notin \mathbf{N}$); $(k, k+1) = 1$ et $(k, k+2) = 1$ car k est impair, ce qui implique, en outre, $((k+1)^2 + 1, 2) = 1$. Il existe $p = 1$ et $q = -(k+1)$ tels que $p((k+1)^2 + 1) + q(k+1) = 1$, donc $k+1$ et $K = (k+1)^2 + 1$ sont premiers entre eux. En divisant $(k+1)^2 + 1$ par $k+2$ suivant l'algorithme d'Euclide, on obtient comme dernier reste non nul 1 car k est impair; ainsi ces deux nombres sont premiers entre eux.

Donc kK est premier avec $2(k+1)(k+2)$ il faut donc que $(2q+1)^2$, donc $2q+1$, soit divisible par kK; ainsi $2q+1 = ckK$ pour un certain entier c donc $2q+1 = b = ckK$ et

$$a = 2p+1 = (2q+1)\frac{k+2}{k} = (2+k)cK.$$

Ainsi

$$x = \frac{a^2-b^2}{2} = 2(k+1)c^2K^2 \qquad t = \frac{a^2+b^2}{2} = c^2K^3$$

$$y = ab = k(k+2)c^2K^2 \qquad z = \frac{xy}{t} = 2k(k+1)(k+2)c^2K .$$

Or l'on désire $(x, y, z) = 1$ d'où, en divisant x, y et z par c^2K et en remplaçant K par sa valeur

$$x = 2(k+1)\left[(k+1)^2+1\right]$$

$$y = k(k+2)\left[(k+1)^2+1\right] = \left[(k+1)-1\right]\left[(k+1)+1\right]\left[(k+1)^2+1\right]$$

$$z = 2k(k+1)(k+2) = 2\left[(k+1)-1\right](k+1)\left[(k+1)+1\right]$$

où k est impair donc $k+1 = 2n$ où $n \in \mathbf{N}^*$, ce qui termine la démonstration en donnant les valeurs annoncées.

Les premières valeurs des triplets (x, y, z), pour $n = 1$ à 10, sont: (20, 15, 12); (136, 255, 120); (444, 1 295, 420); (1 040, 4 095, 1 008); (2 020, 9 999, 1 980); (3 480, 20 735, 3 432); (5 516, 38 415, 5 460); (8 224, 65 535, 8 160); (10 900, 97 775, 10 828); (16 040, 159 999, 15 960).

BIBLIOGRAPHIE

[1] MORDELL, L. J. *Le dernier théorème de Fermat.* Presses universitaires de France, Paris, 1929 (41 p. traduit de l'anglais).

[2] NOGUES, R. *Théorème de Fermat, son histoire.* Vuibert, Paris, 1932.

[3] SELFRIDGE, J. L. and B. W. POLLACK. Fermat's last theorem is true for any exponent up to 25 000. *Am. Math. Soc. Not.*, 1964, t. 11, n° 1, part I, p. 97.

[4] VANDIVER, H. S. Fermat's last theorem, its history and the nature of the known results concerning it. *The Am. Math. Monthly*, Vol. 53, Feb. 1946, pp. 555-578.

[5] BOREVITCH, Z. I. et I. R. CHAFAREVITCH. *Théorie des Nombres.* 489 p. Gauthier-Villars, Paris, 1967 (traduit du russe, existe aussi en anglais et en allemand).

(Reçu le 15 avril 1968)

Institut de Mathématiques
Université de Montpellier.