Sur le problème de Catalan. Part II

ELEMENTE DER MATHEMATIK
Revue de mathématiques élémentaires – Rivista di matematica elementare

Zeitschrift zur Pflege der Mathematik
und zur Förderung des mathematisch-physikalischen Unterrichts
Organ für den Verein Schweizerischer Mathematik- und Physiklehrer

Publiziert mit Unterstützung des Schweizerischen Nationalfonds
zur Förderung der wissenschaftlichen Forschung

El. Math. Band XVI Nr. 2 Seiten 25–48 Basel, 10. März 1961

Sur le problème de Catalan, II

Dans le travail [1][1]) j'ai démontré que l'équation

$$x^z - y^t = 1 \tag{1}$$

n'a pas de solutions en entiers x, y, z, t plus grand que 1, où min $(x, y) < 22$, sauf la solution $x = 3$, $y = 2$, $z = 2$, $t = 3$. Ici je démontrerai le théorème suivant.

Théorème 1. *Si les entiers x, y, z, t plus grands que* 1 *satisfont à l'équation* (1) *et ne sont pas le système $x = 3$, $y = 2$, $z = 2$, $t = 3$, on a $x > 1000$ et $y > 1000$.*

Démonstration. Vu les résultats de LEBESGUE, EULER, NAGELL et SELBERG (voir [2]) il suffira de démontrer notre théorème dans les deux cas suivants:

1) $z = 2$. 2) Tout diviseur premier des nombres z et t est $\geqq 5$.

Si $z = 2$, et si $(x, y, t) \neq (3, 2, 3)$, on a $t > 50000$ [1]. D'autre part, d'après le théorème 2 du travail [1], si $z = 2$ et $(x, y, t) \neq (3, 2, 3)$, chacun des nombres x et y a un diviseur premier de la forme $k\,t + 1$. Donc, pour $z = 2$, $(x, y, t) \neq (3, 2, 3)$, les nombres x et y sont > 50000.

Dans le cas 2) soient p et q respectivement des diviseurs premiers des nombres z et t. D'après (1) on a alors

$$(x^{z/p})^p - (y^{t/q})^q = 1\,, \quad \text{où} \quad p \mid z,\, q \mid t\,. \tag{2}$$

D'après le théorème 4 du travail [1], on a $q\,r \mid x^{z/p}$ et $p\,s \mid y^{z/q}$, où r et s sont respectivement des nombres premiers de la forme $q\,k + 1$ et $p\,k + 1$, $q \geqq 5$, $p \geqq 5$. On a donc $q\,r \mid x$, $p\,s \mid y$. Donc, si le nombre x ou y avait seulement deux diviseurs premiers, on aurait soit $x = q^\alpha r^\beta$, soit $y = p^{\alpha_1} s^{\beta_1}$. Soit $x = q^\alpha r^\beta$. De (1) nous obtenons $(q^\alpha r^\beta)^z - 1 = y^t$. Le nombre z étant impair, le nombre $(q^\alpha r^\beta)^z - 1$ est divisible par la même puissance du nombre 2 que le nombre $q^\alpha r^\beta - 1$. Or, le nombre $q^\alpha r^\beta$ étant impair, on a $2 \mid q^\alpha r^\beta - 1$ et, comme $q \mid t$, on trouve

$$2^q \mid q^\alpha r^\beta - 1. \tag{3}$$

Pareillement, s'il était $y = p^{\alpha_1} s^{\beta_1}$, on aurait

$$2^p \mid p^{\alpha_1} s^{\beta_1} + 1\,. \tag{4}$$

[1]) Les chiffres en crochets renvoient aux travaux cités à la page 27.

Aucun des nombres $q^\alpha r^\beta$ ou $p^{\alpha_1} s^{\beta_1}$ qui sont $\leqq 1000$ (c'est-à-dire aucun des nombres $5 \cdot 11$, $5 \cdot 31$, $7 \cdot 29$, $5 \cdot 41$, $11 \cdot 23$, $5^2 \cdot 11$, $7 \cdot 43$, $5 \cdot 61$, $5 \cdot 71$, $7 \cdot 71$, $5 \cdot 101$, $5 \cdot 11^2$, $5 \cdot 131$, $13 \cdot 53$, $11 \cdot 67$, $5 \cdot 151$, $5^2 \cdot 31$, $7 \cdot 113$, $7 \cdot 127$, $5 \cdot 181$, $5 \cdot 191$, $11 \cdot 89$), comme on le vérifie sans peine, ne satisfait pas aux conditions (3) et (4); il en résulte que chacun des nombres x et y qui sont $\leqq 1000$ et satisfont à l'équation (1) a plus que deux diviseurs premiers. Vu que $5 \cdot 11 \cdot 31 > 1000$, $7 \cdot 29 \cdot 43 > 1000$ et comme $q\,(q\,k_1 + 1)\,(q\,k_2 + 1) > 1000$ pour $q \geqq 11$, le nombre x dans (1) ne peut pas avoir deux diviseurs premiers distincts de la forme $q\,k + 1$. Pareillement le nombre y dans (1) ne peut pas avoir deux diviseurs premiers distincts de la forme $p\,k+1$. Supposons qu'on a dans (1) $x = x_1\,q\,(q\,k + 1)^\varepsilon \leqq 1000$ ou bien $y = y_1\,p\,(p\,k_1 + 1)^{\varepsilon_1} \leqq 1000$, où x_1 et y_1 sont des entiers >1 et $p, q, p\,k_1 + 1, q\,k + 1$ sont des nombres premiers. Vu que $2 \cdot 5 \cdot 11^2 > 1000$, on a ici $\varepsilon = \varepsilon_1 = 1$. Il résulte des inégalités $x_1\,q \geqq 2 \cdot 5$, $y_1\,p \geqq 2 \cdot 5 = 10$, $x \leqq 1000, y \leqq 1000$ que $q\,k + 1 < 100$ et $p\,k_1 + 1 < 100$. Comme $q\,(q\,k + 1) \geqq 5 \cdot 11 = 55$ et $x \leqq 1000$, on a $x_1 < 1000/55$ et $1 < x_1 \leqq 18$. D'après (1) on a

$$[x_1\,q\,(q\,k + 1)]^z = y^t + 1, \quad \text{où } q \mid t,\ q\,k + 1 < 100\,. \tag{5}$$

D'après le théorème 3 du travail [1], si x, y, z, t sont des entiers >1 satisfaisant à l'équation (1) et ne sont pas le système $x = 3, y = 2, z = 2, t = 3$, alors x a un diviseur premier de la forme $t\,k + 1$ et le nombre y a un diviseur premier de la forme $z\,k + 1$. Donc, si $t = q^\alpha$, où $\alpha \geqq 3$, d'après (5), le nombre $x = x_1\,q\,(q\,k + 1)$ a un diviseur premier de la forme $2\,q^\alpha\,k + 1 > 2 \cdot 5^3 = 250$, ce qui, d'après $1 < x_1 \leqq 18$, $q\,k + 1 < 100$ est impossible. D'après le théorème 3 du travail [1] pour $t = q^2$ le nombre $x = x_1\,q\,(q\,k + 1)$, a un diviseur premier de la forme $2\,q^2\,k + 1$ et, comme $3 \mid 2\,q^2 + 1$ pour $q > 3$, on a $k > 1$ et $2\,q^2\,k + 1 \geqq 2 \cdot 5^2 \cdot 2 + 1 = 101$, ce qui, d'après $1 < x_1 \leqq 18$, $q\,k + 1 < 100$ est impossible. Si le nombre t a un diviseur premier q_1, où $5 \leqq q_1 \neq q$, alors, d'après le théorème 3 du travail [1], le nombre x a un diviseur premier de la forme $2\,t\,k + 1 \geqq 2 \cdot 5 \cdot 7 + 1 = 71$. Vu le théorème de Cassels [2], si $x^p - y^q = 1$, où p et q sont des nombres premiers distincts, on a $q \mid x$ et $p \mid y$. Donc, d'après $q \mid t$, $q_1 \mid t$, dans le cas où t a deux diviseurs premiers distincts, on a $q \mid x$, $q_1 \mid x$ et $x \geqq q\,q_1 \cdot 71 \geqq 5 \cdot 7 \cdot 71 > 1000$. Donc, si $x \leqq 1000$ et si l'on a la formule (5), on a $t = q$. On a donc

$$[x_1\,q\,(q\,k + 1)]^z = y^q + 1\,. \tag{6}$$

On a $(y^q + 1)/(y + 1) > y^{q-1} \geqq 2^{q-1} > q$ pour $q \geqq 5$. Vue que tout diviseur premier du nombre $(y^q + 1)/(y + 1) > q$ est de la forme $q\,k + 1$ ou bien est $= q$ et pour $q \mid y^q + 1$ on a $q \mid (y^q + 1)/(y + 1)$ et $q^2 \nmid (y^q + 1)/(y + 1)$ [3], th. 1042, 1043, p. 320–322, et le nombre $x = x_1\,q\,(q\,k + 1)$ n'a qu'un seul diviseur premier de la forme $q\,k + 1$, il résulte de (6) que $y + 1 = x_1^z\,q^{z-1}$ et on obtient:

$$[x_1\,q\,(q\,k + 1)]^z = (x_1^z\,q^{z-1} - 1)^q + 1\,. \tag{7}$$

Comme, pour $x > 1$ on a $x^p - (x - 1)^p = x^{p-1} + x^{p-2}\,(x - 1) + \cdots + (x - 1)^{p-1} < p\,x^{p-1}$, donc, pour $x > 1$, $(x - 1)^p > x^p - p\,x^{p-1} = x^{p-1}\,(x - p)$, d'où il résulte que

$$(x - 1)^p > x^{p-1} \quad \text{pour} \quad x > p\,, \tag{8}$$

et, d'après $q\,k+1<100$, on a

$$(x_1^z q^{z-1}-1)^q > (x_1^z q^{z-1})^{q-1} = x_1^z q^z x_1^{z(q-2)} q^{(z-1)(q-2)-1} \geqq$$
$$\geqq x_1^z q^z \cdot 2^{5\cdot 3} \cdot 5^{(z-1)\cdot 3-1} = x_1^z q^z \frac{2^{15}}{5^4} \cdot 125^z > x_1^z q^z \cdot 125^z > [x_1 q\,(q\,k+1)]^z,$$

contrairement à (7).

Il doit donc être $x>1000$. Pareillement, s'il était $y=y_1 p\,(p\,k+1)<1000$, alors, par la même méthode comme dans la démonstration que $x>1000$, on obtiendrait $z=p$, $x^p-1=[y\,p\,(p\,k+1)]^t$, $x-1=y_1^t p^{t-1}$ et

$$(y^t p^{t-1}+1)^p-1=[y_1 p\,(p\,k_1+1)]^t, \tag{9}$$

ce qui est impossible, puisque

$$(y_1^t p^{t-1}+1)^p-1 > (y_1^t p^{t-1})^p \geqq y_1^t p^t p^{(t-1)\cdot 4-1} =$$
$$= y_1^t p^t p^{4t-5} \geqq y_1^t p^t p^{3t} \geqq y_1^t p^t \cdot 125^t > [y_1 p\,(p\,k+1)]^t,$$

et $p\,k+1<100$. On a donc $y>1000$.

Corollaire. *Sauf le cas* $x=3$, $y=2$, $z=2$, $t=3$, *l'équation* (1) *n'a pas de solutions en nombres entiers* >1 *pour* $x=a^m$, $y=b^n$ *où* min $(a, b) \leqq 1000$ *et* a, b, m *et* n *sont des nombres naturels.*

Une méthode pareille permet de démontrer ce

Théorème 2. Si les nombres entiers x *et* y *plus grands que* 1 *et les nombres premiers* z *et* t *satisfont à l'équation* (1), *et ne sont pas le système* $x=3$, $y=2$, $z=2$, $t=3$, *on a* $x>10^6$ *et* $y>10^6$.

A. ROTKIEWICZ (Varsovie)

[1] A. ROTKIEWICZ, *Sur le problème de Catalan*, El. Math., *15*, 121–124 (1960).
[2] J. W. S. CASSELS, *On the equation* $a^x - b^y = 1$, II. Proc. Cambridge Phil. Soc. [2], *56*, (1960), p. 97–103.
[3] E. LANDAU, *Vorlesungen über Zahlentheorie*, Bd. III (New York 1945).

Sur les nombres impairs admettant une seule décomposition en une somme de deux carrés de nombres naturels premiers entre eux

Le but de cet article est de démontrer le théorème suivant que je suppose être nouveau, puisque je ne l'ai pas trouvé dans la littérature qui m'était accessible. C'est le théorème suivant:

Théorème: *Pour qu'un nombre impair* n *soit et d'une seule façon somme de deux carrés de nombres naturels non décroissants premiers entre eux, il faut et il suffit qu'il soit une puissance à l'exposant naturel d'un nombre premier de la forme* $4\,k+1$[1]).

[1]) A. FERRIER dans son livre *Les nombres premiers*, Paris 1947 à la p. 11 écrit: *Pour qu'un nombre* $4\,n+1$, *non carré, soit premier, il faut et il suffit qu'il soit, et d'une seule façon, somme de deux carrés premiers entre eux.* Il ajoute que EULER a utilisé cette propriété pour reconnaître si un nombre est premier.

Or, cette proposition est évidemment fausse, vu que, par exemple, le nombre non carré 125 est, comme on le vérifie sans peine, d'une seule façon somme de deux carrés premiers entre eux: $125 = 11^2 + 2^2$.

L. HOLZER dans son livre *Zahlentheorie, I*, Leipzig 1958, à la p. 53 écrit: *Satz 20: Eine Zahl der Form* $4\,n+1$ *ist dann und nur dann eine Primzahl, wenn sie sich im wesentlichen eindeutig als Summe zweier teilerfremder Quadrate darstellen lässt.*

Im wesentlichen eindeutig heisst: Zwei Darstellungen durch dieselben Summanden in verschiedener Reihenfolge werden als gleich betrachtet.