

Sur le problème de Catalan

Autor(en): **Rotkiewicz, A.**

Objektyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **15 (1960)**

Heft 6

PDF erstellt am: **13.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-20715>

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.

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 XV Nr. 6 Seiten 121–144 Basel, 10. November 1960

Sur le problème de Catalan

On ne sait pas si l'équation

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

a des solutions en entiers x, y, z, t plus grands que 1, sauf $x = 3, y = 2, z = 2, t = 3$. L'hypothèse qu'il n'existe pas de telles solutions a été exprimée en 1844 par CATALAN [1].

Récemment HAMPEL [2] a démontré que si les entiers x, y, z, t plus grands que 1 satisfont à l'équation (1), aucun des nombres x et y ne peut pas être de la forme 10^m , ni de la forme $2^n \cdot 3^m$. En utilisant les résultats obtenus par GERONO et OBLÁTH, HAMPEL en a déduit que, sauf la solution triviale citée, l'équation (1) n'a pas de solutions en entiers x, y, z, t plus grands que 1 si $x = a^m, y = b^n$ ($m, n = 1, 2, \dots$), où $14 \neq \min(a, b) \leq 19$.

Le but de cette Note est de démontrer ce théorème plus fort :

Théorème 1. *Si les entiers x, y, z, t sont > 1 et satisfont à l'équation (1) et si $(x, y, z, t) \neq (3, 2, 2, 3)$, chacun des nombres x et y a au moins deux diviseurs premiers distincts dont un est ≥ 11 .*

Démonstration. Soit x, y, z, t une solution de l'équation (1) en nombres naturels > 1 , autre que la solution 3, 2, 2, 3. D'après (1) on a $x^z = 1 + y^t$ et, comme LEBESGUE [3] a démontré que l'équation $x^n = 1 + y^2$, où n est un entier > 1 , n'a pas de solutions en nombres naturels x, y , le nombre t doit être impair ≥ 3 . Or, comme NAGELL [4] a démontré que l'équation $y^n = x^3 \pm 1$ n'a pas de solutions en nombres entiers, si $x \geq 2, n > 2$, et EULER [5] a démontré que l'équation $y^2 = x^3 + 1$ n'a pas de solutions en entiers $x > 2$ et y – le nombre t doit être impair ≥ 5 .

Soit p un diviseur premier du nombre $y + 1$. Comme $1 + y \mid 1 + y^t$ pour $2 \nmid t$, on trouve, d'après $x^z = 1 + y^t$, que $p \mid x$.

Nous utiliserons encore le théorème suivant de BIRKHOFF et VANDIVER [6]:

T. Si a et b et $m > 2$ sont des nombres naturels, $a > b$ et $(a, b) = 1$, alors, sauf le cas $a = 2, b = 1, m = 6$, le nombre $a^m - b^m$ a un diviseur premier p (dit primitif) de la forme $mk + 1$, tel que $p \nmid a^i - b^i$ pour $i = 1, 2, \dots, m - 1$.

Vu que $y > 1, t \geq 5$, d'après le théorème *T*, le nombre $y^{2t} - 1$ a un diviseur premier primitif $q \geq 2t + 1 \geq 2 \cdot 5 + 1 = 11$. Comme $y^{2t} - 1 = (y^t - 1)(y^t + 1)$ et $q \nmid y^i - 1$ pour $i = 1, 2, \dots, 2t - 1$, on a $q \mid y^t + 1$ et $p \neq q$. D'après $x^z = y^t + 1$ on a $p \mid x$ et le nombre x a deux diviseurs premiers distincts dont un est ≥ 11 .

De (1) il résulte que $y^t = x^z - 1$. Supposons que $z = 2$. D'après $(x - 1, x + 1) = 2$, on a ou bien

$$1) x - 1 = a^t, x + 1 = b^t, \text{ ou bien}$$

$$2) x - 1 = 2a^t, x + 1 = b^t/2, \text{ ou bien}$$

3) $x - 1 = a^t/2, x + 1 = 2b^t$, où a et b sont des nombres naturels. D'après $x \geq pq \geq 22$ on a $a > 1$ et $b > 1$. Dans le cas 1) on aurait

$$2 = b^t - a^t = (b - a)(b^{t-1} + \dots + a^{t-1}) > b^{t-1},$$

ce qui est impossible, vu que $b > 1$ et $t \geq 5$. Dans le cas 2) on aurait

$$x + 1 = 2a^t + 2 = 2(a^t + 1).$$

Soit p un diviseur premier quelconque du nombre $a + 1$ et soit q un diviseur premier primitif du nombre $a^{2t} - 1$ (un tel diviseur q existe, d'après le théorème T , vu que $a > 1, t \geq 5$). On aura

$$p \mid a^{2t} - 1 = (a^t - 1)(a^t + 1)$$

et, comme $q \nmid a^i - 1$ pour $i = 1, 2, \dots, 2t - 1$, on a $q \mid a^t + 1$. D'après $a + 1 \mid a^t + 1$ (puisque t est un nombre impair ≥ 5), on trouve $p q \mid a^t + 1 \mid x^2 - 1 = y^t$, d'où $p q \mid y$ et $q \geq 2t + 1 \geq 11$, $(p, q) = 1$. Enfin, dans le cas 3) on a $x - 1 = 2(b^t - 1)$ et, en désignant par q un diviseur premier primitif du nombre $b^t - 1$, nous aurons $2q \mid 2(b^t - 1) \mid x^2 - 1 = y^t$, d'où $2q \mid y$, où, vu que $2 \nmid t \geq 5$, on a $q \geq 2 \cdot 5 + 1 = 11$.

Si $z = 3$, on a $y^t = x^3 - 1$ et $x = 2, y = 3, t = 2$, puisque NAGELL [4] a démontré que l'équation $y^n = x^3 \pm 1$, où n est un nombre naturel > 2 n'a pas de solutions en nombres naturels x et y .

On a donc $z \geq 5, 3 \nmid z$. Soit p un diviseur premier du nombre $x - 1$ et q un diviseur premier primitif du nombre $x^z - 1$ (d'après $z \geq 5, x > 1$ et le théorème T , un tel q existe). D'après T , q est de la forme $zk + 1$. Comme $z \geq 5$, on a $q \geq 6$. S'il était $q = 7$, on aurait $z = 6$, contrairement à $3 \nmid z$. On a donc $q \geq 11$. Or, on a $p \neq q$, puisque $q \nmid x^i - 1$ pour $i = 1, 2, \dots, z - 1$. Donc $p q \mid x^z - 1 = y^t$ et $p q \mid y$, où $q \geq 11$ et $(p, q) = 1$.

Notre théorème est ainsi démontré. Il résulte tout de suite de notre théorème que si les nombres x, y, z, t sont des entiers > 1 , autres que $x = 3, y = 2, z = 2, t = 3$, et satisfont à l'équation (1), alors aucun des nombres x et y n'est pas de la forme $2^n, 3^m, 5^k, 7^l, 2^n \cdot 3^m, 2^n \cdot 5^k, 2^n \cdot 7^l, 3^m \cdot 5^k, 3^m \cdot 7^l, 5^k \cdot 7^l, 2^n \cdot 3^m \cdot 5^k, 2^n \cdot 3^m \cdot 7^l, 2^n \cdot 5^k \cdot 7^l, 3^m \cdot 5^k \cdot 7^l, 2^n \cdot 3^m \cdot 5^k \cdot 7^l$.

Vu que le nombre a^m , où $m = 1, 2, \dots, a < 22$ n'a pas deux diviseurs premiers distincts dont un soit ≥ 11 , il résulte de notre théorème ce

Corollaire: Sauf le cas $x = 3, y = 2, z = 2, t = 3$, l'équation (1) n'a pas de solutions en nombres naturels > 1 , où $x = a^m, y = b^n$ ($m, n = 1, 2, \dots$), $c = \min(a, b) < 22$.

OBLÁTH [7,8] a démontré que si a, b et y sont des nombres naturels > 1 , tels que $a^2 - by = 1$, où $(a, b, y) \neq (3, 2, 3)$, on a $2^{p-1} \equiv 1 \pmod{p^2}$ et $3^{p-1} \equiv 1 \pmod{p^2}$ pour tous les nombres premiers p tels que $p \mid y$. On en peut déduire (voir [9, 11]) que l'équation $a^2 - by = 1$, où $(a, b, y) \neq (3, 2, 3)$, n'a pas de solutions en nombres naturels a, b et y plus grands que 1 pour $y < 50000$.

De nos considérations résulte la proposition suivante:

Théorème 2. Si les nombres naturels > 1 , a , b et y , satisfont à l'équation $a^2 - b^y = 1$, alors, sauf le cas $a = 3$, $b = 2$, $y = 3$, chacun des nombres a et b a un diviseur premier de la forme $yk + 1$.

Des raisonnements utilisés dans la démonstration du théorème 1 il résulte aussi le

Théorème 3. Si les entiers x, y, z, t plus grands que 1 satisfont à l'équation $x^z - y^t = 1$ et ne sont pas le système $x = 3, y = z = 2, t = 3$, alors x a au moins un diviseur premier de la forme $tk + 1$ et le nombre y a au moins un diviseur premier de la forme $zk + 1$.

Récemment CASSELS [10] a démontré que si les nombres premiers p et q , tels que $p > q \geq 2$ satisfont à l'équation

$$a^p - b^q = \pm 1, \quad (2)$$

où a et b sont des entiers > 1 , on a

$$q \mid a \text{ et } p \mid b. \quad (3)$$

Comme, d'après les résultats de LEBESGUE et NAGELL, dans l'équation $x^z - y^t = 1$, où $(x, y, z, t) \neq (3, 2, 2, 3)$, $x > 1$, $y > 1$, $z > 1$, $t > 1$, ne peut pas être $t = 2$ ni $t = 3$, il résulte du théorème de CASSELS que si l'on a l'équation (1), alors, sauf les solutions triviales citées, le nombre x a au moins un diviseur premier ≥ 5 .

Or, du théorème de CASSELS et des théorèmes 1 et 3 résulte le

Théorème 4. Si les nombres premiers p et q tels que $p > q \geq 2$ satisfont à l'équation (2), où a et b sont des nombres naturels > 1 , $(a, b, p, q) \neq (3, 2, 2, 3)$, $(a, b, p, q) \neq (2, 3, 3, 2)$, alors on a

$$qr \mid a \text{ et } ps \mid b, \quad (4)$$

où r est un nombre premier de la forme $qk + 1$ et s est un nombre premier de la forme $pk + 1$.

Il est encore à remarquer que du théorème T (de BIRKHOFF et VANDIVER) résulte tout de suite le théorème de MORET-BLANC d'après lequel l'équation

$$x^y - y^x = 1 \quad (5)$$

a, en nombres naturels x, y seulement les solutions $x = 2, y = 1$ et $x = 3, y = 2$.

En effet, si $y = 1$, on a $x - 1 = 1$ et $x = 2$. Si $y = 2$, on a $x^2 - 2^x = 1$, donc $(x - 1)(x + 1) = 2^x$, ce qui, vu que $(x - 1, x + 1) \mid 2$, donne $x - 1 = 2$, donc $x = 3$. Or, s'il était $y > 2$, alors, d'après le théorème T le nombre $x^y - 1$ (sauf le cas $y = 6, x = 2$) aurait un diviseur premier p de la forme $ky + 1 \geq y + 1$ et, d'après $x^y - 1 = y^x$, le nombre premier $p \geq y + 1$ serait un diviseur du nombre y , ce qui est évidemment impossible. Comme $6^2 - 2^6 \neq 1$, le théorème de MORET-BLANC se trouve démontré.

A. ROTKIEWICZ (Varsovie)

BIBLIOGRAPHIE

- [1] E. CATALAN, J. reine angew. Math. 27, 192 (1844).
- [2] R. HAMPEL, Sur le problème de Catalan (en polonais), Prace Matematyczne IV, 11-19 (1960).
- [3] V. A. LEBESGUE, Nouv. Ann. Math. I, 9, 178-181 (1850).
- [4] T. NAGELL, Norsk mat. Foren. Skr., I, 2, 8 (1921-22).
- [5] L. EULER, Theorematum quorundam arithmeticonum demonstrationes, Comm. Acad. Sci. Petropolitanae, 10 (1738).
- [6] G. D. BIRKHOFF and H. S. VANDIVER, On the integral divisors of $a^n - b^n$, Ann. Math. (2), 5, 173-180 (1904).
- [7] R. OBLÁTH, Math. Phys. Lapok 47, 58-77 (1940).

- [8] R. OBLATH, *Über die Zahl $x^2 - 1$* , *Mathematica B*, Zutphen, 8, 161–172 (1940).
 [9] – *Über die Gleichung $x^m + 1 = y^n$* . *Annales Polonici Mathematici* 1, 73–76 (1954).
 [10] J. W. S. CASSELS, *On the equation $a^x - b^y = 1$* . *Proc. Camb. Phil. Soc.* 56, 2, 73–103 (1960).
 [11] C. E. FRÖBERG, *Some computations of Wilson and Fermat remainders*, *Math. Tables and other Tids to Computation* 12, 281 (1958).

Die Kegelschnittsfunktionen

1. Schon JAMES GREGORY (1638–75) hat in seiner *Vera circuli et hyperbolae quadratura*, Padua 1667, gezeigt, wie man mit Hilfe einbeschriebener und umbeschriebener Vielecke die Flächeninhalte von Ellipse und Hyperbel nach demselben elementaren Verfahren wie beim Kreis bestimmen kann. Nicht allgemeiner bekannt zu sein scheint, dass man auch die Theorie der Kreis- und Hyperbelfunktionen als eine Theorie der Kegelschnittsfunktionen völlig einheitlich und elementar *ohne jeden rechnerischen Grenzübergang* aufbauen kann. Zwar weiss jeder, dass Hyperbelsinus und -cosinus Funktionen nicht des Hyperbelbogens, sondern des doppelten Hyperbelsektors sind und dass man auch beim Kreis den Bogen als doppelten Sektor auffassen kann. Weniger bekannt ist, dass diese Dinge der affinen Geometrie angehören und damit eine ganz elementare Theorie ermöglichen, bei denen Kreis- und Hyperbelfunktionen in gleicher Bezeichnung erscheinen. Besonders für die gemeinsame Behandlung der beiden in der nichteuklidischen Geometrie scheint sie mir nützlich zu sein¹⁾.

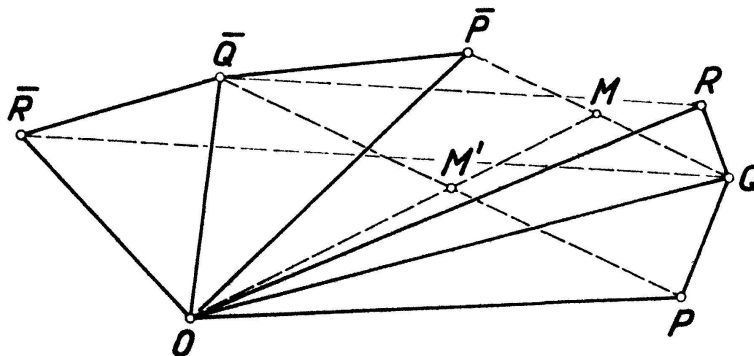
2. Wir nehmen die Gleichung des Mittelpunktskegelschnitts, bezogen auf ein affines $x_1 | x_2$ -Koordinatensystem in der Gestalt

$$x_1^2 + \varepsilon x_2^2 = 1 \quad (1)$$

an. Die Koordinatenachsen sind konjugierte Durchmesser. Ist $P(p_1 | p_2)$ ein Punkt von (1), so hat der Endpunkt P' des zu \overline{OP} konjugierten Halbmessers $\overline{OP'}$ ($\Delta OPP'$ habe positiven Umlaufsinn) die Koordinaten $(-\varepsilon p_2 | p_1)$. Dabei ist im Fall der Hyperbel ($\varepsilon = -1$) P' allerdings der reelle Ersatzpunkt auf der konjugierten Hyperbel $\varepsilon x_1^2 + x_2^2 = 1$.

Ist ferner $Q(q_1 | q_2)$ ein beliebiger von P verschiedener Punkt von (1), so ist

$$2 \Delta OPQ = p_1 q_2 - p_2 q_1, \quad 2 \Delta OQP' = p_1 q_1 + \varepsilon p_2 q_2. \quad (2)$$



Figur 1

¹⁾ Vergleiche dazu L. HEFFTER, *Grundlagen und analytischer Aufbau der Geometrie* 3, S. 153ff., Stuttgart 1958.