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

Autor(en): **Sierpiski, W.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **16 (1961)**

Heft 2

PDF erstellt am: **22.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-21285

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.

Pour démontrer ce théorème, je prouverai d'abord les trois lemmes suivants:

Lemme 1: *Si p est un nombre premier impair et k un nombre naturel, le nombre p^k ne peut pas donner deux décompositions en sommes de deux carrés de nombres naturels non décroissants premiers entre eux.*

Démonstration du lemme 1: Supposons que le nombre p^k admet deux décompositions en sommes de deux carrés de nombres naturels non décroissants premiers entre eux, $p^k = a^2 + b^2 = c^2 + d^2$, où $(a, b) = (c, d) = 1$, $a \geqq b$, $c \geqq d$, $a > c$. On en trouve

$$p^{2k} = (a\,c + b\,d)^2 + (a\,d - b\,c)^2 = (a\,d + b\,c)^2 + (a\,c - b\,d)^2 \tag{1}$$

et

$$(a\,c + b\,d)\,(a\,d + b\,c) = (a\,b + c\,d)\,p^k . \tag{2}$$

Il résulte de (2) qu'un au moins des nombres $a\,c + b\,d$ et $a\,d + b\,c$ est divisible par le nombre premier p. Si tous les deux nombres $a\,c + b\,d$ et $a\,d + b\,c$ étaient divisibles par p, on aurait, d'après (1), $a\,d \equiv b\,c \pmod p$ et $a\,c \equiv b\,d \pmod p$, d'où $p \mid c\,d(a^2 - b^2)$. Or, comme $p^k = c^2 + d^2$ et $(c, d) = 1$, les nombres c et d ne sont pas divisibles par p. On a donc $p \mid a^2 - b^2$ et, comme $p \mid a^2 + b^2$, on en trouve $p \mid 2\,a^2$, donc, p étant un nombre premier impair, $p \mid a$ et, comme $p \mid a^2 + b^2$, aussi $p \mid b$, contrairement à $(a, b) = 1$. Donc, des nombres $a\,c + b\,d$ et $a\,d + b\,c$ un et un seul est divisible par p. Or, leur produit étant, d'après (2), divisible par p^k, celui de nos deux nombres qui est divisible par p, est divisible par p^k. Si $p^k \mid a\,c + b\,d$, il résulte de (1) que $a\,d - b\,c = 0$, d'où $a/b = c/d$ et, comme $(a, b) = (c, d) = 1$, cela donne $a = c$, contrairement à l'hypothèse que $a > c$. Si $p^k \mid a\,d + b\,c$, (1) donne $a\,c - b\,d = 0$, d'où $a/b = d/c$, et, d'après $(a, b) = (c, d) = 1$ on en obtient $a = d$, contrairement à $a > c \geqq d$. Le lemme 1 se trouve ainsi démontré.

Lemme 2: *Si p est un nombre premier de la forme $4\,t + 1$ alors, pour $k = 1, 2, \ldots$, le nombre p^k est une somme de deux carrés de nombres naturels non décroissants premiers entre eux.*

Démonstration du lemme 2: Le lemme 2 est vrai pour $k = 1$. En effet, d'après un théorème bien connu de FERMAT, tout nombre premier de la forme $4\,t + 1$ est une somme de deux carrés de nombres naturels non décroissants[2]) et il est évident que ces nombres sont premiers entre eux.

Soit maintenant k un nombre naturel donné et supposons que le lemme (2) est vrai pour le nombre k. Il existe donc des nombres naturels c et d, tels que $(c, d) = 1$ et $p^k = c^2 + d^2$. Le lemme 2 étant vrai pour $k = 1$, il existe aussi deux nombres naturels a et b, tels que $(a, b) = 1$ et $p = a^2 + b^2$. On a donc

$$p^{k+1} = (a^2 + b^2)\,(c^2 + d^2) = (a\,c + b\,d)^2 + (a\,d - b\,c)^2 = (a\,d + b\,c)^2 + (a\,c - b\,d)^2 . \tag{3}$$

Si chacun des nombres $a\,d - b\,c$ et $a\,c - b\,d$ était divisible par p, on aurait $a\,d \equiv b\,c \pmod p$ et $a\,c \equiv b\,d \pmod p$, d'où $a^2\,c\,d \equiv b^2\,c\,d \pmod p$, donc $p \mid c\,d\,(a^2 - b^2)$ et comme $p^k = c^2 + d^2$ et $(c, d) = 1$, aucun des nombres c et d n'est pas divisible par p et on trouve $p \mid a^2 - b^2$, ce qui donne, d'après $p = a^2 + b^2$, $p \mid 2\,a^2$, donc, p étant impair, $p \mid a$ et, vu que $p = a^2 + b^2$, cela donne $p \mid b$, contrairement à $(a, b) = 1$. Donc un au moins des nombres $a\,d - b\,c$ et $a\,c - b\,d$ n'est pas divisible par p. Si le nombre

[2]) Voir, par exemple, M. KRAÏTCHIK, *Théorie des nombres*, Paris 1922, p. 99.

$a\,d - b\,c$ n'est pas divisible par p, alors, d'après (3), le nombre $a\,c + b\,d$ n'est pas divisible par p. Or, il résulte de (3) que tout diviseur commun des nombres $a\,c + b\,d$ et $a\,d - b\,c$ est un diviseur du nombre p^{k+1} et, ces nombres n'étant pas divisibles par p, ils sont premiers entre eux. Pareillement si le nombre $a\,c - b\,d$ n'est pas divisible par p, on conclut que les nombres $a\,d + b\,c$ et $a\,c - b\,d$ sont premiers entre eux. D'après (3) nous obtenons donc dans tout cas une décomposition du nombre p^{k+1} en une somme de deux carrés de nombres naturels premiers entre eux et il résulte toute de suite que le lemme 2 est vrai pour le nombre $k + 1$. Nous avons ainsi démontré le lemme 2 par l'induction.

Lemme 3: *Si m et n sont deux nombres impairs premiers entre eux et si chacun de ces nombres est une somme de deux carrés de nombres naturels premiers entre eux, alors le nombre $m\,n$ admet au moins deux décompositions en somme de deux carrés de nombres naturels premiers entre eux (qui se différent non seulement par l'ordre des termes).*

Démonstration du lemme 3: Supposons que m et n sont des nombres impairs, a, b, c et d des nombres naturels et que $(m, n) = (a, b) = (c, d) = 1$, $m = a^2 + b^2$, $n = c^2 + d^2$, et nous pouvons supposer que $a \geqq b$, $c \geqq d$. On a donc

$$m\,n = (a\,c + b\,d)^2 + (a\,d - b\,c)^2 = (a\,d + b\,c)^2 + (a\,c - b\,d)^2 \tag{4}$$

et

$$(a\,c + b\,d)\,(a\,d + b\,c) = c\,d\,m + a\,b\,n\,. \tag{5}$$

Les deux décompositions (4) en sommes de deux carrés différent et non seulement par l'ordre de leurs termes, puisque, s'il était $a\,c + b\,d = a\,d + b\,c$, on aurait $(a - b)\,(c - d) = 0$, donc $a = b$ ou bien $c = d$, ce qui est impossible, vu que les nombres m et n sont impairs, et s'il était $a\,c + b\,d = a\,c - b\,d$ (le nombre $a\,c - b\,d$ est $\geqq 0$, vu que $a \geqq b$ et $c \geqq d$), on aurait $b\,d = 0$, ce qui est impossible.

Pour démontrer le lemme 3 il suffira donc de prouver que $(a\,c + b\,d, a\,d - b\,c) = 1$ et $(a\,d + b\,c, a\,c - b\,d) = 1$.

S'il était $(a\,c + b\,d, a\,d - b\,c) > 1$, les nombres $a\,c + b\,d$ et $a\,d - b\,c$ auraient un diviseur premier commun p et, d'après (4), on aurait $p \mid m\,n$, donc $p \mid m$ ou bien $p \mid n$. S'il était $p \mid m$, on aurait, d'après (5), $p \mid a\,b\,n$ et, comme $p \mid m$ et $(m, n) = 1$, d'où $(p, n) = 1$, cela donne $p \mid a\,b$, et, vu que $p \mid m = a^2 + b^2$, on trouve $p \mid a$ et $p \mid b$, contrairement à $(a, b) = 1$. Or, s'il était $p \mid n$, on trouverait, d'après (5), $p \mid c\,d\,m$, et, vu que $(m, n) = 1$, cela donne $p \mid c\,d$ et, comme $p \mid c^2 + d^2$ et $(c, d) = 1$, on aboutit aussi à une contradiction. Le lemme 3 est ainsi démontré.

Soit maintenant k un entier $\geqq 2$ et $n_1, n_2, \ldots, n_k$ des nombres naturels deux à deux premiers entre eux. Vu que pour $i = 2, 3, \ldots, k$ on a $(n_1\,n_2 \ldots n_{i-1}, n_i) = 1$, on déduit sans peine par l'induction du lemme 3 le corollaire suivant:

Corollaire: *Si k est un entier $\geqq 2$ et $n_1, n_2, \ldots, n_k$ sont des nombres impairs deux à deux premiers entre eux, dont chacun est une somme de deux carrés de nombres naturels premiers entre eux, alors le nombre $n_1\,n_2, \ldots n_k$ admet au moins deux décompositions en somme de deux carrés de nombres naturels premiers entre eux* (qui différent non seulement par l'ordre des termes).

Passons maintenant à la démonstration de notre théorème. Soit k un nombre naturel et p un nombre premier de la forme $4\,t + 1$. D'après le lemme 2 le nombre p^k

est une somme de deux carrés de nombres naturels non décroissants premiers entre eux et, d'après le lemme 1, il n'y a qu'une telle décomposition. La condition de notre théorème est donc suffisante.

Soit maintenant n un nombre impair et supposons que n admet et une seule décomposition en somme de deux carrés de nombres naturels non décroissants premiers entre eux, soit $n = a^2 + b^2$. Soit p un diviseur premier du nombre n: ce sera donc un nombre impair. S'il était $p = 4t + 3$, alors, vu que $a^2 \equiv -b^2 \pmod{p}$, en élévant les deux côtés de cette congruence à la puissance à l'exposant

$$\frac{p-1}{2} = 2t + 1,$$

on aurait $a^{p-1} \equiv -b^{p-1} \pmod{p}$; or, d'après le théorème de FERMAT, vu que, d'après $(a, b) = 1$ et $p \mid a^2 + b^2$, on a $(a, p) = (b, p) = 1$, on trouve $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$. On aurait donc $1 \equiv -1 \pmod{p}$, donc $p \mid 2$, ce qui est impossible. Tout diviseur premier du nombre n est donc de la forme $4t + 1$, et le nombre n a le développement en facteurs premiers $n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$, où k et $\alpha_1, \alpha_2, \dots, \alpha_k$ sont des nombres naturels et q_i $(i = 1, 2, \dots, k)$ sont des nombres premiers distincts, chacun de la forme $4t + 1$. S'il était $k = 1$, notre théorème serait évidemment démontré. Supposons donc que $k > 1$. Tous deux des nombres $q_1^{\alpha_1}, q_2^{\alpha_2}, \dots, q_k^{\alpha_k}$ sont évidemment premiers entre eux et, d'après le lemme 2, chacun d'eux est une somme de deux carrés de nombres naturels premiers entre eux. D'après le corollaire du lemme 3 il en résulte que le nombre n admet au moins deux décompositions en somme de deux carrés de nombres naturels premiers entre eux qui diffèrent non seulement par l'ordre des termes – contrairement à l'hypothèse sur le nombre n. Nous avons ainsi démontré qu'il ne peut pas être $k > 1$. On a donc $k = 1$ et notre théorème se trouve démontré.

W. SIERPIŃSKI (Varsovie)

Ungelöste Probleme

Nr. 39. Unter einer räumlichen vollständigen und richtungsstetigen Geradenschar verstehen wir eine Gesamtheit von Geraden des gewöhnlichen Raumes mit den folgenden beiden Eigenschaften:

a) Zu jeder Geraden des Raumes enthält die Gesamtheit genau eine parallele Gerade;
b) die Geraden der Gesamtheit ändern sich stetig mit ihrer Richtung.

Ein Geradenbüschel, also die Gesamtheit aller durch einen festen Raumpunkt hindurchlaufenden Geraden, bilden ein besonders einfaches Beispiel einer vollständigen richtungsstetigen Geradenschar. Man überlegt sich aber leicht, dass es andere nichttriviale Scharen der verlangten Art gibt. Unsere Bilder deuten zwei ebene Scharen an, die durch Rotation um die vertikale Symmetrieachse zwei räumliche vollständige richtungsstetige Geradenscharen erzeugen. Figur 1 stellt die triviale ebene Schar (Geradenbüschel) dar, die bezogen auf ein cartesisches Koordinatensystem und den Parameter a durch

$$(\sin a)x - (\cos a)y = 0 \qquad [0 \leqslant a < \pi]$$