Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 21 (1966)
Heft: 2

Artikel: Sur les nombres pseudopremiers de la forme nk + 1
Autor: Rotkiewicz, A.
DOI: https://doi.org/10.5169/seals-24649

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 23.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

(3) ist nur möglich, wenn γ gerade ist. Also ist $-a\,b\,c$ für fast alle p quadratischer Rest. Hieraus folgt nach einem früheren Satz[2]) (E. TROST [4]) $-a\,b\,c = v^2$, also $b = b_1^2$ (wegen $(a\,c, b) = 1$) im Widerspruch zur Voraussetzung.

G. JAESCHKE, Sindelfingen und E. TROST, Zürich[3])

LITERATURVERZEICHNIS

[1] PÓLYA-SZEGÖ, *Aufgaben und Lehrsätze aus der Analysis II*, Nr. 107, S. 134.
[2] A. SCHINZEL, *On the Congruence* $a^x \equiv b \pmod p$, Bull. Acad. pol. Sci. (Ser. Sci. math. astr. phys.) *8*, 307–309 (1960).
[3] W. J. LEVEQUE, *Topics in Number Theory* I, S. 34.
[4] E. TROST: *Zur Theorie der Potenzreste*, Nieuw Archief Wisk. *18*, 58–61 (1934).

Sur les nombres pseudopremiers de la forme $n\,k + 1$.

On appelle pseudopremiers les nombres composés n tels que $n \mid 2^n - 2$. Dans le travail [2][1]) j'ai démontré qu'*il existe une infinité de nombres pseudopremiers de la forme* $n\,k + 1$ en utilisant le théorème de ZSIGMONDY (voir [4]). Dans le travail [3], en utilisant le théorème de LEJEUNE-DIRICHLET sur la progression arithmétique j'ai démontré que *toute progression arithmétique* $a\,x + b$, *ou* a *et* b *sont des nombres naturels premiers entre eux, contient une infinité de nombres pseudopremiers*. Le but de cette note est de démontrer d'une façon élémentaire et directe (sans faire appel au théorème de ZSIGMONDY ni au théorème de LEJEUNE-DIRICHLET) le théorème suivant:

T. *Pour tout nombre naturel* n *il existe une infinité de nombres pseudopremiers de la forme* $n\,k + 1$, *où* k *est un nombre naturel.*

Il est d'abord à remarquer que pour démontrer le théorème ***T*** il suffit de démontrer que pour tout nombre naturel n il existe au moins un nombre pseudopremier de la forme $n\,k + 1$, où k est un nombre naturel, puisque alors pour tous deux nombres naturels m et n il existe au moins un nombre pseudopremier de la forme $n\,m\,t + 1$, ou t est un nombre naturel, et ce nombre pseudopremier est évidemment $> m$ et de la forme $n\,k + 1$ (où k est un nombre naturel).

Lemme 1. *Si* b *est un nombre impair* > 1 *et si* $F_m = 2^{2^m} + 1$, *alors* $F_{m + k\varphi[\varphi(b)]} \equiv F_m \pmod b$ *pour* $m \geqslant b$, $k = 0, 1, 2, \ldots$

Démonstration du lemme 1. Supposons que $2^\alpha \mid \varphi(b)$ et $2^{\alpha+1} \nmid \varphi(b)$. On aura $\varphi(b)/2^\alpha \mid 2^{\varphi[\varphi(b)/2\alpha]} - 1 \mid 2^{\varphi[\varphi(b)]} - 1$, donc

$$\frac{\varphi(b)}{2^\alpha} \,\Big|\, 2^{\varphi[\varphi(b)]} - 1\,. \tag{1}$$

Comme $2^m > m \geqslant b > \varphi(b) \geqslant 2^\alpha$, on a $2^\alpha \mid 2^m$ et il résulte de (1) que $\varphi(b) \mid 2^m (2^{\varphi[\varphi(b)]} - 1) \mid 2^m (2^{k\varphi[\varphi(b)]} - 1)$, donc

$$\varphi(b) \mid 2^m (2^{k\varphi[\varphi(b)]} - 1) \quad \text{pour } k = 1, 2, 3, \ldots\,. \tag{2}$$

---

[2]) Ist b für fast alle p n-ter Potenzrest und $n \not\equiv 0 \pmod 8$, so ist $b = b_1^n$. Für $n \equiv 0 \pmod 8$ ist ausserdem noch $b = 2^{n/2} b_2^n$ möglich. «Fast alle» bedeutet hier, dass die Menge der Ausnahmeprimzahlen verschwindende (Kroneckersche) Dichte hat.

[3]) Herrn J. STEINIG (Zürich) danken wir für kritische Bemerkungen.

[1]) Les chiffres en crochets renvoient aux travaux cités, page 33.

Comme $2 \nmid b$, on a $2^{\varphi(b)} \equiv 1 \pmod{b}$ et, d'après (2) aussi $2^{2^m(2^{k\varphi[\varphi(b)]}-1)} \equiv 1 \pmod{b}$, d'ou $2^{2^m+k\varphi[\varphi(b)]} \equiv 2^{2^m} \pmod{b}$, donc $F_{m+k\varphi[\varphi(b)]} \equiv F_m \pmod{b}$ pour $k = 1, 2, \ldots$, ce qui est évidemment vrai aussi pour $k = 0$. Le lemme 1 est ainsi démontré.

Lemme 2 (théorème de CIPOLLA, cf. [1]): *Si $k > 1$, $n_1, n_2, \ldots, n_k$ sont des nombres naturels, $n_1 < n_2 < \ldots < n_k < 2^{n_1}$, alors le nombre $N = F_{n_1} F_{n_2} \ldots F_{n_k}$ est pseudopremier.*

Démonstration du lemme 2. Vu que $n_1 < n_2 < \ldots < n_k$, on a $N \equiv 1 \pmod{2^{2^{n_1}}}$, d'ou, vu que $2^{n_1} > n_k$ (donc $2^{n_1} \geqslant n_k + 1$), $N \equiv 1 \pmod{2^{n_k+1}}$. On a donc, pour $i = 1, 2, \ldots, k$:

$$F_{n_i} = 2^{2^{n_i}} + 1 \mid 2^{2^{n_i+1}} - 1 \mid 2^{2^{n_k+1}} - 1 \mid 2^{N-1} - 1 ,$$

et, les nombres de Fermat distincts étant premiers entre eux, on en déduit que

$$N = F_{n_1} F_{n_2} \ldots F_{n_k} \mid 2^{N-1} - 1 \mid 2^N - 2 ,$$

ce qui prouve que N est un nombre pseudopremier. Le lemme 2 est ainsi démontré.

Démonstration du théorème ***T***. Soit n un nombre naturel donné quelconque et soit $3 n = 2^\beta b$, ou $2 \nmid b > 1$. Nous prouverons que le nombre

$$N = F_{3n} F_{3n+\varphi[\varphi(b)]} F_{3n+2\varphi[\varphi(b)]} \cdots F_{3n+[\varphi(b)-1]\varphi[\varphi(b)]} \tag{3}$$

est un nombre pseudopremier de la forme $3 n t + 1$.

Vu que $3 n \geqslant b$ et en vertu du lemme 1, nous avons $F_{3n} \equiv F_{3n+k\varphi[\varphi(b)]} \pmod{b}$ pour $k = 0, 1, 2, \ldots$ On a donc

$$N \equiv F_{3n}^{\varphi(b)} \pmod{b} . \tag{4}$$

Tout diviseur > 1 du nombre F_{3n} étant, comme on le sait, de la forme $2^{3n} l + 1 \geqslant 2^{3n} + 1 > 3 n \geqslant b$, on trouve $(F_{3n}, b) = 1$ et, d'après le théorème d'EULER, (4) donne

$$N \equiv 1 \pmod{b} . \tag{5}$$

Or, on a $2^{3n} > 3 n = 2^\beta b > \beta$, donc $2^\beta \mid 2^{2^{3n+k\varphi[\varphi(b)]}}$, $k = 0, 1, 2, \ldots$, d'ou $F_{3n+k\varphi[\varphi(b)]} \equiv 1 \pmod{2^\beta}$ pour $k = 0, 1, 2, \ldots$ ce qui donne, d'après (3):

$$N \equiv 1 \pmod{2^\beta} . \tag{6}$$

Les formules (5) et (6) donnent $N \equiv 1 \pmod{3 n}$. En vertu du lemme 2 il nous reste à démontrer que $2^{3n} > 3 n + [\varphi(b) - 1] \varphi[\varphi(b)]$. Pour $n = 1$ (ou $b = 3$) nous vérifions cette inégalité directement, et pour $n \geqslant 2$ elle est valable aussi, puisqu'alors on a

$$2^{3n} > 3 n + (3 n)^2 > 3 n + [\varphi(3 n) - 1] \varphi [\varphi(3 n)] \geqslant 3 n + [\varphi(b) - 1] \varphi [\varphi(b)] .$$

Nous avons ainsi démontrè que, pour tout nombre naturel $n > 1$ il existe au moins un nombre pseudopremier de la forme $n k + 1$ ou k est un nombre naturel, et, comme nous le savons, il en résulte notre théorème ***T***. A. ROTKIEWICZ, Varsovie

TRAVAUX CITÉS

[1] M. CIPOLLA, *Sui numeri composti P che verificano la congruenza di Fermat $a^{P-1} \equiv 1$ (mod P)*, Annali di Matematica *9*, 139–160 (1904).

[2] A. ROTKIEWICZ, *Sur les diviseurs composés des nombres $a^n - b^n$*, Bulletin de la Société Royale des Sciences de Liège *32*, 191–195 (1963).

[3] A. ROTKIEWICZ, *Sur les nombres pseudopremiers de la forme $a x + b$*, Comptes rendus, Acad. Sciences, Paris *257*, 2601–2604 (1963).

[4] K. ZSIGMONDY, *Zur Theorie der Potenzreste*, Monatshefte für Math. *3*, 265–284 (1892).