

## Werk

**Titel:** Sur les nombres pseudopremiers de la forme  $nk + 1$ .

**Autor:** Rotkiewicz, A.

**Jahr:** 1966

**PURL:** [https://resolver.sub.uni-goettingen.de/purl?378850199\\_0021](https://resolver.sub.uni-goettingen.de/purl?378850199_0021) | log16

## Kontakt/Contact

[Digizeitschriften e.V.](#)  
SUB Göttingen  
Platz der Göttinger Sieben 1  
37073 Göttingen

✉ [info@digizeitschriften.de](mailto:info@digizeitschriften.de)

(3) ist nur möglich, wenn  $\gamma$  gerade ist. Also ist  $-a b c$  für fast alle  $p$  quadratischer Rest. Hieraus folgt nach einem früheren Satz<sup>2)</sup> (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<sup>3)</sup>

## 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]<sup>1)</sup> 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  $a x + b$ , où  $a$  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  $n m t + 1$ , où  $t$  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  $F_{m+k\varphi(b)} \equiv F_m \pmod{b}$  pour  $m \geq b$ ,  $k = 0, 1, 2, \dots$

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

$$\frac{\varphi(b)}{2^\alpha} \mid 2^{\varphi(b)} - 1. \quad (1)$$

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

$$\varphi(b) \mid 2^m (2^{k\varphi(b)} - 1) \quad \text{pour } k = 1, 2, 3, \dots \quad (2)$$

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

<sup>3)</sup> Herrn J. STEINIG (Zürich) danken wir für kritische Bemerkungen.

<sup>1)</sup> 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  $2^{2^m(2^k \varphi(b) - 1)} \equiv 1 \pmod{b}$ , d'où  $2^{2^m + k \varphi(b)} \equiv 2^{2^m} \pmod{b}$ , donc  $F_{m+k \varphi(b)} \equiv F_m \pmod{b}$  pour  $k = 1, 2, \dots$ , ce qui est évidemment vrai aussi pour  $k = 0$ . Le lemme 1 est ainsi démontré.

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

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

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

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

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

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  $3n = 2^\beta b$ , ou  $2 \nmid b > 1$ . Nous prouverons que le nombre

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

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

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

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

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

$$N \equiv 1 \pmod{b}. \quad (5)$$

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

$$N \equiv 1 \pmod{2^\beta}. \quad (6)$$

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

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

Nous avons ainsi démontré 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  $a^{P-1} \equiv 1 \pmod{P}$* , 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).