ATTI ACCADEMIA NAZIONALE DEI LINCEI
CLASSE SCIENZE FISICHE MATEMATICHE NATURALI

RENDICONTI

ANDRÉ ROTKIEWICZ

Sur les nombres naturels n et k tels que les nombres n et nk soni à la fois pseudopremiers

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche,
Matematiche e Naturali. Rendiconti, Serie 8, Vol. 36 (1964), n.6, p. 816–818.*
Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1964_8_36_6_816_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Matematica (Teoria dei numeri). — *Sur les nombres naturels n et k tels que les nombres n et nk sont à la fois pseudopremiers.* Nota di ANDRÉ ROTKIEWICZ, presentata (*) dal Socio straniero W. SIERPIŃSKI.

On appelle *pseudopremiers* les nombres composés n tels que $n \mid 2^n - 2$. Dans cette note je démontrerai les deux théorèmes suivants:

THÉORÈME 1. — *Le plus petit nombre entier $k > 1$ pour lequel il existe un nombre pseudopremier n tel que le nombre kn est aussi pseudopremier est le nombre $k = 23$.*

THÉORÈME 2. — *Si a et b sont des nombres naturels premiers entre eux et k un nombre naturel quelconque, il existe un nombre premier p et les nombres naturels $n_1, n_2, \dots, n_k$, tels que*

$$1^\circ p \equiv b \pmod{a};$$

$2^\circ n_1, n_2, \dots, n_k$ sont des nombres pseudopremiers et $n_i \equiv 1 \pmod{a}$ pour $i = 1, 2, \dots, k$,

$3^\circ pn_1, pn_2, \dots, pn_k$ sont des nombres pseudopremiers et $pn_i \equiv b \pmod{a}$ pour $i = 1, 2, \dots, k$.

LEMME 1. — *Si n et kn sont des nombres pseudopremiers, on a $n \mid 2^k - 2$.*

Démonstration du lemme 1. — Si n est un nombre pseudopremier impair, on a $n \mid 2^{n-1} - 1$, d'où:

$$(1) \quad n \mid 2^{(n-1)k} - 1.$$

Or, le nombre nk étant pseudopremier, on a $kn \mid 2^{kn} - 2$, d'où, vu que $2 \text{ non } \mid n$, on obtient:

$$(2) \quad n \mid 2^{nk-1} - 1.$$

Il résulte de (1) et (2) que $n \mid 2^{(nk-k, nk-1)} - 1 \mid 2^{k-1} - 1 \mid 2^k - 2$.

Si n est un nombre pseudopremier pair, on a $n = 2n_1$, où n_1 est un nombre impair et de $n \mid 2^n - 2$ on trouve $n_1 \mid 2^{n-1} - 1$ et de $kn \mid 2^{kn} - 2$ on trouve $n_1 \mid 2^{nk-1} - 1$ et, comme plus haut, on en déduit que $n_1 \mid 2^{k-1} - 1$, d'où $n \mid 2^k - 2$.

Démonstration du théorème 1. — Supposons que les nombres n et kn sont pseudopremiers. Vu que, pour $1 < k \leq 10$ et $k = 13, 14, 18$ le nombre $2^k - 2$ n'est pas divisible par aucun des nombres pseudopremiers, en vertu du lemme nous pouvons supposer que $k \geq 11$ et $k \neq 13, 14, 18$. Il ne peut pas être $k = 12, 16, 20$, on qu'il n'existe aucun nombre pseudopremier divisible par 4. Il nous reste donc à étudier les cas $k = 11, 15, 17, 19, 21, 22, 23$. On vérifie sans peine que tous les nombres pseudopremiers qui divisent respectivement les nombres $2^{11} - 2, 2^{15} - 2, 2^{17} - 2, 2^{19} - 2, 2^{21} - 2,$

(*) Nella seduta del 10 giugno 1964.

$2^{22} - 2$ sont respectivement $11 \cdot 31$, $43 \cdot 127$, $17 \cdot 257$, $19 \cdot 73$, $11 \cdot 31$, $127 \cdot 337$. Mais aucun des nombres $11^2 \cdot 31$, $15 \cdot 43 \cdot 127$, $17^2 \cdot 257$, $19^2 \cdot 73$, $21 \cdot 11 \cdot 31$, $22 \cdot 127 \cdot 337$ n'est pas pseudopremier. D'après le lemme 1 il ne peut pas donc être $k < 23$. Pour $k = 23$ les nombres pseudopremiers correspondants sont $n = 89 \cdot 683 = 60787$ et $kn = 23 \cdot 89 \cdot 683 = 1398101$.

Le théorème 1 se trouve ainsi démontré.

LEMME 2. — Si p et q sont des nombres premiers, $m_1, m_2, \dots, m_{k+2}$ sont des nombres naturels distincts, $m_i | m$, $f_n(2) = \prod_{i|n} (2^i - 1)^{\mu(n/i)}$, où μ est la fonction de Möbius,

$$(3) \quad m | p - 1 \quad , \quad \left(\frac{p-1}{m}, m \right) = 1,$$

$$(4) \quad q^2 | p - 1 \quad , \quad ma\varphi(ma) | q - 1$$

(où φ est la fonction de Euler),

$$(5) \quad \frac{p-1}{m} = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s} \quad , \quad q_1 < q_2 < \dots < q_s \quad ; \quad q_1^{\alpha_1} q_2^{\alpha_2} \dots q_{s-1}^{\alpha_{s-1}} \text{ non } | q_s - 1;$$

alors chacun des nombres

$$n_i = \frac{f_{p-1}(2)}{m_i} \frac{f_{p-1}(2)}{m_{i+1}} \quad \text{pour } i = 1, 2, \dots, k + 1$$

est pseudopremier et $n_i \equiv 1 \pmod{a}$.

Démonstration du lemme 2. — En vertu du théorème de Zsigmondy (voir [3]) et d'après la formule (5), tout diviseur premier du nombre $\frac{f_{p-1}(2)}{m_i}$ est $\equiv 1 \pmod{\frac{p-1}{m_i}}$, d'où, d'après $m_i | m$ on trouve

$$(6) \quad \frac{f_{p-1}(2)}{m_i} \equiv 1 \pmod{\frac{p-1}{m}}.$$

D'autre part, comme $m_i | m$, il résulte de (4) que $q^2 | \frac{p-1}{m_i}$ et $ma\varphi(ma) | q - 1$ et, en vertu du lemme 1 du travail [2] (voir aussi [1]) on a

$$(7) \quad \frac{f_{p-1}(2)}{m_i} \equiv 1 \pmod{am}.$$

D'après (3) les formules (6) et (7) donnent

$$(8) \quad \frac{f_{p-1}(2)}{m_i} \equiv 1 \pmod{p-1}.$$

Il résulte de (8) que

$$(9) \quad \frac{f_{p-1}(2)}{m_i} \frac{f_{p-1}(2)}{m_{i+1}} \equiv 1 \pmod{p-1} \quad \text{pour } i = 1, 2, \dots, k + 1.$$

Comme $m_i \neq m_{i+1}$, le nombre $n_i = \frac{f_{p-1}(2)}{m_i} \frac{f_{p-1}(2)}{m_{i+1}}$ divise le nombre $2^{p-1} - 1$ et, d'après la formule (9), on a $n_i | 2^{p-1} - 1 | 2^{n_i-1} - 1 | 2^{n_i} - 2$ et, comme $\frac{f_{p-1}(2)}{m_i} > 1$, $\frac{f_{p-1}(2)}{m_{i+1}} > 1$, n_i est un nombre pseudopremier.

D'après (7) on a $n_i \equiv 1 \pmod{a}$ et le lemme 2 se trouve démontré.

Démonstration du théorème 2. - Soient a et b deux nombres naturels quelconques premiers entre eux. Soit m un nombre naturel quelconque, tel que $(a, m) = 1$, et vient m_i ($i = 1, 2, \dots, k+2$) des nombres naturels distincts, tels que $m_i | m$ pour $i = 1, 2, \dots, k+2$, et soit q un nombre premier tel que $am\varphi(am) | q-1$. Comme $(a, mq^2) = 1$, il existe un nombre naturel r tel que

$$(10) \quad r \equiv b \pmod{a} \quad \text{et} \quad r \equiv 1 \pmod{mq^2}.$$

Vu que $(a, b) = 1$, il résulte de (10) que $(amq^2, r) = 1$ et, de même façon qu'on a démontré le lemme 2 du travail [1], on démontre qu'il existe une infinité de nombres premiers p de la forme $amq^2x + r$ (où x est un entier non négatif) pour lesquels on a la formule (5).

Soit p un nombre premier de la forme $amq^2x + r$, pour lequel on a la formule (5). Alors d'après (10) on a $p \equiv b \pmod{a}$. En vertu du lemme 2 tout nombre $n_i = \frac{f_{p-1}}{m_i}(2) \frac{f_{p-1}}{m_{i+1}}(2)$ ($i = 1, 2, \dots, k+1$) est pseudopremier.

Le nombre premier p divise un au plus des nombres $\frac{f_{p-1}}{m_i}(2)$ ($i = 1, 2, \dots, k+2$) ou bien ne divise aucun de ces nombres. Dans le premier cas, sans diminuer la généralité de la démonstration, nous pouvons supposer que $p | \frac{f_{p-1}}{m_{k+2}}(2)$. Dans tous les deux cas on a

$$(11) \quad p \frac{f_{p-1}}{m_i}(2) \frac{f_{p-1}}{m_{i+1}}(2) | 2^{p-1} - 1 \quad \text{pour} \quad i = 1, 2, \dots, k$$

et, comme, d'après (8), $n_i \equiv 1 \pmod{p-1}$, on a

$$(12) \quad pn_i | 2^{n_i-1} - 1 | 2^{pn_i-1} - 1 | 2^{pn_i} - 2$$

et pn_i est un nombre pseudopremier. Vu que $n_i \equiv 1 \pmod{a}$ et $p \equiv b \pmod{a}$, on a $pn_i \equiv b \pmod{a}$ et le théorème 2 se trouve démontré.

TRAVAUX CITÉS.

- [1] A. ROTKIEWICZ, *Sur les nombres pseudopremiers de la forme $ax + b$* , « Comptes rendus, Acad. Sciences Paris », 257, 2601-2604 (1963).
- [2] A. ROTKIEWICZ et A. SCHINZEL, *Sur les nombres pseudopremiers de la forme $ax^2 + bxy + cy^2$* , ibidem, 258, 3617-3620 (1964).
- [3] K. ZSIGMONDY, *Zur Theorie der Potenzreste*, « Monatshefte für Math. », 3, 265-284 (1892).