COLLOQUIUM MATHEMATICUM

VOL. XII 1964 FASC. 1

SUR LES FORMULES DONNANT DES NOMBRES PSEUDOPREMIERS

PAR

A. ROTKIEWICZ (VARSOVIE)

Sierpiński [2] a établi par l'induction l'existence d'une infinité de nombres pseudopremiers (c'est-à-dire des nombres composés n tels que $n \mid 2^n-2$). Les théorèmes qui suivent contiennent quelques formules donnant directement une infinité de tels nombres.

THÉORÈME 1. *Soit p un nombre premier. Les nombres $(2^{2p}-1)/3$ pour $p>3$ et les nombres $(2^{2p}+1)/5$ pour $p>5$ sont pseudopremiers.*

Démonstration. Erdős [1] a montré que les nombres $(2^{2p}-1)/3$, où $p>3$, sont pseudopremiers. Vu que $(2^{2p}+1)/5-1 = (4^p-4)/5$ et $p>5$, on a $4p \mid (2^{2p}+1)/5-1$, d'où

$$\frac{2^{2p}+1}{5}\,\Big|\, 2^{2p}+1 \mid 2^{4p}-1 \mid 2^{(2^{2p}+1)/5-1}-1, \qquad \frac{2^{2p}+1}{5}\,\Big|\, 2^{(2^{2p}+1)/5}-2.$$

Le nombre

$$\frac{2^{2p}+1}{5} = \frac{(2^p+1-2^{(p+1)/2})(2^p+1+2^{(p+1)/2})}{5}$$

est donc pseudopremier, puisque $2^p+1-2^{(p+1)/2}>5$ pour $p>5$, ce qui achève la démonstration.

Posons maintenant $F_n = 2^{2^n}+1$ pour $n = 1, 2, \ldots$

THÉORÈME 2. *Pour qu'un produit $F_{n_1}F_{n_2}\ldots F_{n_k}$ où $n_1, n_2, \ldots, n_k$ sont des nombres naturels et $k>1$ soit un nombre pseudopremier, il faut et il suffit que l'on ait*

$$n_i \neq n_j \ \textit{pour}\ i\neq j \quad \textit{et} \quad 2^{\min(n_1,n_2,\ldots,n_k)} > \max(n_1, n_2, \ldots, n_k).$$

Le théorème 2 a été démontré en 1904 par Cipolla [3]. Le problème se pose s'il existe pour tout entier $k>1$ un nombre pseudopremier qui soit un produit de k nombres de Mersenne distincts. Le théorème suivant en est la réponse affirmative:

THÉORÈME 3. *Quels que soient k nombres naturels $n_1 < n_2 < \ldots < n_k$ où $n_k < 2^{n_1}$, le nombre*

$$M = (2^{F_{n_1}}-1)\cdot(2^{F_{n_2}}-1)\cdot\ldots\cdot(2^{F_{n_k}}-1)$$

est pseudopremier.

Démonstration. L'hypothèse $n_k < 2^{n_1}$ entraîne $n_k+1 \leqslant 2^{n_1}$, d'où $2^{n_k+1} \mid F_{n_1}-1 = 2^{2^{n_1}}$ et à plus forte raison $2^{n_1+1} \mid F_{n_i}-1$ pour $i \geqslant 1$. On a donc pour $i = 1, 2, \ldots, k$ et $j = 1, 2, \ldots, k$ la relation $2^{n_i+1} \mid F_{n_j}-1$, d'où

$$F_{n_i} \mid 2^{2^{n_i+1}}-1 \mid 2^{F_{n_j}-1}-1 \mid 2^{F_{n_j}}-2.$$

Vu que $(F_{n_i}, F_{n_j}) = 1$ pour $i \neq j$, on a pour $j = 1, 2, \ldots, k$ la relation $F_{n_1}F_{n_2}\ldots F_{n_k} \mid 2^{F_{n_j}}-2$, d'où

$$2^{F_{n_j}}-1 \equiv 1 (\operatorname{mod} F_{n_1}F_{n_2}\ldots F_{n_k})$$

et $M = (2^{F_{n_1}}-1)(2^{F_{n_2}}-1)\ldots(2^{F_{n_k}}-1) \equiv 1 (\operatorname{mod} F_{n_1}F_{n_2}\ldots F_{n_k})$. Par conséquent,

$$2^{F_{n_i}}-1 \mid 2^{F_{n_1}F_{n_2}\ldots F_{n_k}}-1 \mid 2^{M-1}-1 \mid 2^M-2,$$

et comme $(2^{F_{n_i}}-1, 2^{F_{n_j}}-1) = 2^{(F_{n_i}, F_{n_j})}-1 = 2^1-1 = 1$ pour $i \neq j$, on a $M \mid 2^M-2$, ce qui achève la démonstration.

COROLLAIRE. *Les nombres de la forme $(2^{F_n}-1)(2^{F_{n+1}}-1)$ sont pseudopremiers pour $n = 2, 3, \ldots$*

Remarque 1. *Il n'existe pas de nombres pseudopremiers divisibles par un carré d'un nombre de Mersenne.*

En effet, en supposant que $M_n^2 x \mid 2^{M_n^2 x}-2$ pour un x naturel et un $M_n = 2^n-1$, on aurait $M_n^2 \mid 2^{M_n^2 x-1}-1$ et le nombre 2, qui appartenant modulo 2^n-1 à l'exposant n, appartiendrait modulo $(2^n-1)^2$ à l'exposant $n(2^n-1)$ (voir mon travail [5], p. 6-7, et celui de LeVeque [6], p. 52). On aurait donc $n(2^n-1) \mid M_n^2 x-1$, ce qui est évidemment impossible.

THÉORÈME 4. *Chacune des progressions arithmétiques $8k+1$, $8k+3$, $8k+5$ et $8k+7$ contient une infinité de nombres pseudopremiers.*

Démonstration. Les nombres F_nF_{n+1} où $n = 2, 3, \ldots$, qui sont pseudopremiers d'après le théorème 2, sont évidemment de la forme $8k+1$.

Il est facile de voir que les nombres $2^{F_nF_{n+1}}-1$ où $n = 2, 3, \ldots$ sont aussi pseudopremiers; or ils sont évidemment de la forme $8k+7$.

D'après le théorème 1, les nombres $(2^{2p}-1)/3$ où p est premier et $p > 3$ sont pseudopremiers; or on constate facilement qu'ils sont de la forme $8k+5$.

Enfin, les nombres

$$N_p = \frac{2^p+1}{3}\cdot\frac{2^{3p}-1}{7(2^p-1)}\cdot\frac{2^{5p}-1}{31(2^p-1)}$$

où $p \equiv 1 \pmod{12}$ sont des nombres pseudopremiers de la forme $8k+3$. En effet, soit $N_p \equiv r \pmod 8$, donc

$$(2^p+1)(2^{3p}-1)(2^{5p}-1) \equiv 3\cdot 7\cdot 31(2^p-1)^2 r \pmod 8.$$

Vu que $p \geqslant 13$ par hypothèse, il en résulte que $1 \equiv 3r \pmod 8$, d'où $r \equiv 3 \pmod 8$ et $N_p \equiv 3 \pmod 8$. Reste donc à montrer que le nombre N_p est pseudopremier. Or on a $9\cdot 5 \mid 2^{12}-1 \mid 2^{p-1}-1$ en vertu de l'hypothèse admise sur p et l'identité $(2^p+1)/3-1 = 2(2^{p-1}-1)/3$ entraîne

(4) $$30p \,\Big|\, \frac{2^p+1}{3}-1.$$

Pareillement, l'identité

$$\frac{2^{3p}-1}{7(2^p-1)}-1 = \frac{(2^{p-1}-1)(2^{2p+1}+2^{p+2}-6)}{7(2^p-1)}$$

entraîne

(5) $$30p \,\Big|\, \frac{2^{3p}-1}{7(2^p-1)}-1$$

et l'identité

$$\frac{2^{5p}-1}{31(2^p-1)}-1 = \frac{(2^{p-1}-1)(2^{4p+1}+2^{3p+2}+2^{2p+3}+2^{p+4}-30)}{31(2^p-1)}$$

entraîne

(6) $$30p \,\Big|\, \frac{2^{5p}-1}{31(2^p-1)}-1.$$

Il résulte de (4)-(6) que

(7) $$30p \mid N_p-1.$$

Les nombres $(2^p+1)/3$, $(2^{3p}-1)/7(2^p-1)$ et $(2^{5p}-1)/31(2^p-1)$ sont deux à deux premiers entre eux, car $2^p+1 \mid 2^{3p}+1$, $2^p+1 \mid 2^{5p}+1$ et $(2^{3p}+1, 2^{3p}-1) = (2^{5p}+1, 2^{5p}-1) = 1$, d'où

$$\left(\frac{2^p+1}{3}, \frac{2^{3p}-1}{7(2^p-1)}\right) = \left(\frac{2^p+1}{3}, \frac{2^{5p}-1}{31(2^p-1)}\right) = 1$$

et comme $(2^{3p}-1, 2^{5p}-1) = 2^{(3p,5p)}-1 = 2^p-1$, on a aussi

$$\left(\frac{2^{3p}-1}{7(2^p-1)}, \frac{2^{5p}-1}{31(2^p-1)}\right) = 1.$$

En écrivant les relations (4)-(6) sous la forme

$$\frac{2^p+1}{3} \Big| 2^{30p}-1, \qquad \frac{2^{3p}-1}{7(2^p-1)} \Big| 2^{30p}-1 \quad \text{et} \quad \frac{2^{5p}-1}{31(2^p-1)} \Big| 2^{30p}-1,$$

on conclut donc de (7) que $N_p \mid 2^{30p}-1 \mid 2^{N_p-1}-1 \mid 2^{N_p}-2$, ce qui prouve que le nombre N_p est pseudopremier.

Remarque 2. On peut démontrer que le plus petit nombre pseudopremier de la forme $8k+3$ est le nombre $1387 = 19\cdot 73$.

J'ai démontré (voir [4]) que toute progression infinie de la forme $ax+b$ où a et b sont des nombres naturels premiers entre eux contient une infinité de nombres pseudopremiers.

TRAVAUX CITÉS

[1] P. Erdős, *Problem 4319*, American Mathematical Monthly 57 (1950), p. 346.

[2] W. Sierpiński, *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n-2)/n$, Colloquium Mathematicum 1 (1947), p. 9.

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

[4] A. Rotkiewicz, *Sur les nombres pseudopremiers de la forme* $ax+b$, Comptes Rendus de l'Académie des Sciences, Paris, 257 (1963), p. 2601-2604.

[5] — *O własnościach wyrażenia* a^n-b^n, Prace Matematyczne 6 (1961), p. 1-20.

[6] W. J. LeVeque, *Topics in number theory*, vol. I, Reading 1956.

Reçu par la Rédaction le 6. 5. 1963