whence

$$\Delta x_n = \sum_{\nu=0}^{p-1} \frac{(-1)^\nu}{2^{\nu+1}} \Delta^{\nu+1} b_n + \frac{(-1)^p}{2^p} \Big\{ \sum_{\nu=1}^{\infty} [(-1)^{\nu-1} - (-1)^\nu] \Delta^p b_{n+\nu} \Big\} - \frac{(-1)^p}{2^p} \Delta^p b_n$$

$$= \sum_{\nu=0}^{p-1} \frac{(-1)^\nu}{2^{\nu+1}} \Delta^{\nu+1} b_n + \frac{(-1)^{p-1}}{2^{p-1}} \sum_{\nu=0}^{\infty} (-1)^\nu \Delta^p b_{n+\nu} - \frac{(-1)^{p-1}}{2^p} \Delta^p b_n$$

$$= \sum_{\nu=0}^{p-2} \frac{(-1)^\nu}{2^{\nu+1}} \Delta^{\nu+1} b_n + \frac{(-1)^{p-1}}{2^{p-1}} \sum_{\nu=0}^{\infty} (-1)^\nu \Delta^p b_{n+\nu}.$$

Repeating this procedure applied successively for Δx_n, $\Delta^2 x_n$, etc. p-times, we obtain finally

$$\Delta^p x_n = \sum_{\nu=0}^{\infty} (-1)^\nu \Delta^p b_{n+\nu}.$$

Applying the operation Δ^{r-p} to both sides of the above equality we get

$$\Delta^r x_n = \sum_{\nu=0}^{\infty} (-1)^\nu \Delta^r b_{n+\nu}.$$

The series occurring on the right-hand side of the above relation may be also written in the form

$$-\sum_{\nu=0}^{\infty} \{\Delta^r b_{n+2\nu+1} - \Delta^r b_{n+2\nu}\} = -\sum_{\nu=0}^{\infty} \Delta^{r+1} b_{n+2\nu}.$$

Since the terms $\Delta^{r+1} b_{n+2\nu}$ have a constant sign, the terms $\Delta^r x_n$ also have a constant sign. Moreover, we have by (3) and (9)

$$x_{n+1} + x_n = \sum_{\nu=0}^{p-1} \frac{(-1)^\nu}{2^{\nu+1}} \{\Delta^\nu b_{n+1} + \Delta^\nu b_n\} + \frac{(-1)^p}{2^p} \Delta^p b_n,$$

whence, according to lemma I,

$$x_{n+1} + x_n = b_n.$$

Consequently, the sequence x_n defined by formula (3) actually has all the desired properties. The uniqueness of such a sequence follows from lemma III in view of the fact that condition (2) and the inequality $r \geqslant p$ imply the relation

$$\lim_{n\to\infty} \Delta^r b_n = 0.$$

This completes the proof.

Reçu par la Rédaction le 24. 9. 1960 ; en version modifiée le 21. 2. 1961

COLLOQUIUM MATHEMATICUM

VOL. IX 1962 FASC. 1

SUR QUELQUES GÉNÉRALISATIONS DES NOMBRES PSEUDOPREMIERS

PAR

A. ROTKIEWICZ (VARSOVIE)

Soient $a > 0$ et $b > 0$ des entiers tels que $a > b$ et $(a, b) = 1$. Considérons une fonction $f(n)$ à valeurs entières positives, définie pour tout entier $n > 0$ et assujettie à la condition

$$(p-1, f(n)) \mid f(np) \tag{1}$$

pour tout p premier tel que $p \nmid n$. On a alors les théorèmes suivants:

THÉORÈME 1. *S'il existe un n_0 premier tel que $2 < f(n_0) \geqslant n_0$, $n_0 \mid a^{f(n_0)} - b^{f(n_0)}$ et $f(n) \geqslant n-1$ pour $n > n_0$, il existe aussi, pour tout entier $s > 1$, un n composé, produit de s nombres premiers distincts, et tel que*

$$n \mid a^{f(n)} - b^{f(n)}. \tag{2}$$

THÉORÈME 2. *S'il existe un n_0 pair tel que $f(n_0) > 2$ et $f(n) \geqslant n-1$ pour $n \geqslant n_0$, et qui satisfait à l'une des conditions*

$$n_0 \mid a^{f(n_0)+1} b - a b^{f(n_0)+1}, \tag{3}$$

$$n_0 \mid a^{f(n_0)} - b^{f(n_0)}, \tag{4}$$

il existe aussi une infinité de nombres pairs satisfaisant à (3) ou à (4) respectivement.

On a le théorème (T) suivant [1]:

(T) *Si $a > 0$, $b > 0$ et $m > 2$ sont des entiers tels que $a > b$ et $(a, b) = 1$, alors, sauf le cas où $a = 2$, $b = 1$ et $m = 6$, le nombre $a^m - b^m$ a un diviseur p premier (dit $primitif$) tel que $m \mid p-1$ et que p ne divise le nombre $a^k - b^k$ pour aucun $k = 1, 2, \ldots, m-1$.*

LEMME. *Sous les mêmes hypothèses, il existe un p premier tel que*

$$p \mid a^m - b^m \quad \text{et} \quad m \mid p-1.$$

[1] Cf. [2], p. 386. Ce théorème a été démontré par Birkhoff et Vandiver [1].

En effet, si $a = 2$, $b = 1$ et $m = 6$, il suffit de poser $p = 7$. Dans les autres cas, le lemme est une conséquence immédiate du théorème (T).

Démonstration du théorème 1 (2). D'après le lemme, il existe un p premier tel que

$$p|a^{f(n_0)} - b^{f(n_0)} \tag{5}$$

et $f(n_0)|p-1 < p$. Vu que $f(n_0) \geqslant n_0$, on a $n_0 < p$ et $(n_0, p) = 1$. Il en résulte donc en vertu de (1) que $f(n_0) = (p-1, f(n_0))|f(n_0 p)$, d'où $f(n_0)|f(n_0 p)$. Puisque $n_0|a^{f(n_0)} - b^{f(n_0)}$ par hypothèse, on a en vertu de (5) $n_0|a^{f(n_0 p)} - b^{f(n_0 p)}$ et $p|a^{f(n_0 p)} - b^{f(n_0 p)}$. Comme $(p, n_0) = 1$, il vient $pn_0|a^{f(n_0 p)} - b^{f(n_0 p)}$.

Le théorème 1 est ainsi démontré pour $s = 2$. Or admettons que n est le produit de $s \geqslant 2$ nombres premiers distincts et satisfait à (2). On a dans ce cas $f(n) \geqslant n-1 > 2$ par hypothèse et il existe, d'après le lemme, un q premier tel que $q|a^{f(n)} - b^{f(n)}$ et $f(n)|q-1 < q$. Vu que $f(n) \geqslant n-1$, on a $n-1 < q$ et $n \leqslant q$. De plus, n étant un nombre composé, on a $(n, q) = 1$. En répétant ce raisonnement, nous concluons par récurrence que $nq|a^{f(nq)} - b^{f(nq)}$ pour $q > n$. Le théorème 1 se trouve ainsi établi.

Remarque 1. Si $f(1) > 2$, on peut prendre pour n_0 un diviseur premier quelconque du nombre $a^{f(1)} - b^{f(1)}$. On voit donc que s'il existe un nombre premier $n_0 > 2$ tel que $n_0|a^{f(n_0)} - b^{f(n_0)}$ et que $f(n) \geqslant n$ pour $n \geqslant n_0$, il existe aussi, pour tout entier $s > 0$, un nombre composé n, produit de s nombres premiers distincts et tel que $n|a^{f(n)} - b^{f(n)}$.

Démonstration du théorème 2. D'après le lemme, il existe un diviseur premier p du nombre $a^{f(n_0)} - b^{f(n_0)}$, tel que $2|p-1$ et $2 < f(n_0)|p-1$. L'hypothèse que $f(n) \geqslant n-1$ pour $n \geqslant n_0$ entraîne $p \geqslant f(n_0)+1 \geqslant n_0-1+1 = n_0$ et $p \geqslant n_0$. Le nombre p étant impair, il ne divise pas n_0, puisque $2|n_0$. D'après (1) on a donc $f(n_0) = (p-1, f(n_0))|f(n_0 p)$ et le même raisonnement que celui employé dans la démonstration du théorème 1 montre que le nombre pn_0 satisfait à (3) ou à (4) respectivement. Le théorème 2 en résulte, vu que $pn_0 > n_0$.

Remarque 2. On voit facilement que, dans le théorème 2, l'hypothèse $f(n_0) > 2$ peut être remplacée par $n_0 > 2$. On voit aussi sans peine que la condition (1) est la plus faible pour laquelle la méthode précédente soit encore applicable (3).

Le théorème 1 entraîne deux corollaires suivants:

Corollaire 1. *Quels que soient les entiers a, b et $s > 1$, il existe un nombre composé n, produit de s entiers distincts, et tel que $n|a^{\sigma(n)} - b^{\sigma(n)}$, où $\sigma(n)$ est la somme de tous les diviseurs du nombre n.*

(2) Quelques simplifications de cette démonstration sont dues à W. Narkiewicz.

(3) Je dois à A. Schinzel l'idée d'introduire cette condition.

En effet, sans restreindre la généralité, on peut admettre que $(a, b) = 1$ et $a > b$. Puisque $\sigma(n) > n$ pour $n > 1$, et que la fonction $f(n) = \sigma(n)$ satisfait (comme on le prouve sans peine) à la condition (1), il suffit, d'après le théorème 1, de trouver un nombre premier n_0 tel que $\sigma(n_0) > 2$ et que $n_0|a^{\sigma(n_0)} - b^{\sigma(n_0)}$. Or il est aisé à vérifier que l'on peut prendre pour n_0 un diviseur premier quelconque du nombre $a^2 - b^2$.

Corollaire 2. *Soient a, b et $s > 1$ des entiers, $a_1, a_2, \ldots, a_k$ des entiers non négatifs dont l'un au moins n'est pas nul, et a_0 un entier tel que $0 \leqslant a_0 \neq 1$. Alors en posant $N = a_k(n-1)^k + \ldots + a_1(n-1) + a_0$, il existe un n composé, produit de s nombres premiers distincts, et tel que*

$$n|a^N - b^N.$$

En effet, sans restreindre la généralité, on peut admettre que $(a, b) = 1$ et $a > b$. Si $a_0 = a_2 = \ldots = a_k = 0$ et $a_1 = 1$, le corollaire 2 résulte du théorème établi dans mon travail [3]. Dans le cas contraire, soit $f(n) = a_k(n-1)^k + \ldots + a_1(n-1) + a_0$.

On a alors $(p-1, f(n))|(np-1)-(n-1)|f(np)-f(n)$, $(p-1, f(n))|f(np)$ et $f(n) \geqslant n-1$ pour $n \geqslant 1$.

Reste donc à trouver un n_0 premier tel que $n_0|a^{f(n_0)} - b^{f(n_0)}$ et $n_0 \leqslant f(n_0) > 2$. Lorsque $a_0 = 0$ et $a_i > 0$ pour un $i > 1$, ou bien que $a_1 > 1$, on peut prendre pour n_0 un $p > 2$ premier tel que $(p, ab) = 1$, et lorsque $a_0 \geqslant 2$, on peut prendre pour n_0 un diviseur premier quelconque du nombre $a^{a_0} - b^{a_0}$.

Le théorème 2 entraîne à son tour deux corollaires suivants:

Corollaire 3. *Si les nombres $a, b, a_1, \ldots, a_k$ satisfont aux hypothèses du corollaire 2 et si $a_0 \geqslant 0$, il existe une infinité de nombres n pairs et tels que $n|a^M b - ab^M$, où*

$$M = a_k n^k + \ldots + a_1 n + a_0. \tag{6}$$

En effet, sans restreindre la généralité, on peut admettre encore que $(a, b) = 1$ et $a > b$. Soit $f(n) = a_k n^k + a_{k-1} n^{k-1} + \ldots + a_1 n + a_0 - 1$ (4).

Il vient $f(n) \geqslant n-1$ pour $n \geqslant 1$ et $(p-1, f(n))|f(np)$, puisque $np - n|f(np) - f(n)$. Reste à trouver le nombre n_0. Soit (a, b) un couple différent de $(2, 1)$. Si $2|ab \geqslant 4$, on peut poser $n_0 = ab$; si ab est impair, on peut prendre $n_0 = 2ab$. Soit maintenant $a = 2$ et $b = 1$. Pour $f(2) > 2$, on peut prendre $n_0 = 2$; pour $f(2) = 1$, on a $f(n) = n-1$ et $n|2^n - 2$ pour $n = 2 \cdot 73 \cdot 1103$ (comme l'a trouvé D. H. Lehmer; cf. Sierpiński [6], p. 181) et il suffit de poser $n_0 = 2 \cdot 73 \cdot 1103$. Enfin, pour $f(2) = 2$, on a $f(n) = n$, on peut donc prendre $n_0 = 6$. Ainsi, *quel que soit l'entier $a > 0$,*

(4) Pour $f(n) = n-1$ c'est le théorème 1 de mon travail [4].

il existe une infinité de nombres pairs n tels que $n|a^M-a$ pour M défini par (6).

COROLLAIRE 4. *Si $(a,b)=1$, $2|a-b\geqslant 4$, $a_0\geqslant 0$ et les nombres $a_1,\ldots,a_k$ satisfont aux hypothèses du corollaire 2, il existe une infinité de n pairs tels que $n|a^{M-1}-b^{M-1}$ pour M défini par* (6).

En effet, pour $f(n)=M-1$, on n'a qu'à poser $n_0=a-b$ [5].

Remarque 3. A propos du corollaire 2, on peut poser la question suivante: existe-t-il, pour des entiers positifs a et b quelconques, une infinité de n composés et tels que $n|a^n-b^n$. Il en est ainsi, lorsque $a-b>1$, car, comme on le démontre sans peine, on a $n|a^n-b^n$ pour tout n de la forme $(a-b)^m$ (a,b et m étant des entiers positifs quelconques, et $a-b>0$, on a $(a-b)^{m+1}|a^{(a-b)^m}-b^{(a-b)^m}$). Or il n'existe aucun entier $n>1$ tel que $n|(a+1)^n-a^n$, puisque si $n=q_1^{a_1}q_2^{a_2}\ldots q_k^{a_k}$, où $q_1<q_2<\ldots<q_k$ sont des nombres premiers, on a $(q_1,a(a+1))=1$ et $q_1|(a+1)^{q_1^{a_1}\ldots q_k^{a_k}}-a^{q_1^{a_1}\ldots q_k^{a_k}}$, vu que $n|(a+1)^n-a^n$. Il en résulte que le plus petit entier $m>0$ tel que $q_1|(a+1)^m-a^m$ est au moins égal à q_1, contrairement à la relation $q_1|(a+1)^{q_1-1}-a^{q_1-1}$.

Remarque 4. Si a est de la forme $4k+1$, le nombre composé $n=(a^a-1)/(a-1)$ satisfait à la relation $n|a^{n-1}-1$.

En effet, j'ai démontré dans [5] que l'entier $\left((4k+1)^{4k+1}-1\right)/4k$ est composé pour tout $k=1,2,\ldots$ Il reste donc à démontrer que $n|a^{n-1}-1$. Or $a\left|\dfrac{a^a-1}{a-1}-1\right.$, d'où $a^a-1\left|a^{\frac{a^a-1}{a-1}}-1\right.$, donc $\dfrac{a^a-1}{a-1}\left|a^{\frac{a^a-1}{a-1}}-1\right.$.

THÉORÈME 3. *Quels que soient les entiers a, b et $s>1$, il existe un n composé, produit de s nombres premiers distincts, et tel que $n|a^{\theta(n)}-b^{\theta(n)}$, où $\theta(n)$ est le nombre des diviseurs entiers positifs du nombre n.*

Démonstration. On peut évidemment admettre que $(a,b)=1$ et $a>b$. Soit q_2 un diviseur premier quelconque du nombre a^2-b^2 et, pour $k>1$, q_{2k} un diviseur premier primitif du nombre $a^{2^k}-b^{2^k}$ (qui existe d'après le théorème (T)). On a $n=q_2q_{2^2}\ldots q_{2^s}|a^{2^s}-b^{2^s}=a^{\theta(n)}-b^{\theta(n)}$ et le théorème 3 se trouve démontré.

Le corollaire 1 et le théorème 3 donnent lieu aux problèmes ouverts suivants:

P 352. Existe-t-il une infinité de nombres n composés et tels que $n|a^{\sigma(n)}-b^{\sigma(n)}$ pour tous les entiers positifs a et b tels que $(ab,n)=1$?

On montre sans peine que les seuls nombres n en question de la forme $n=pq$, où p et q sont des nombres premiers distincts, sont les suivants: $2\cdot3$, $2\cdot7$, $3\cdot5$, $5\cdot7$, $5\cdot13$, $7\cdot17$ et $13\cdot29$.

[5] Dans le cas $f(n)=n-1$, le corollaire 4 résulte du théorème 2 de mon travail [4].

P 353. Existe-t-il une infinité de n composés qui divisent les nombres $2^{\sigma(n)}-1$ et $3^{\sigma(n)}-1$?

L'un de tels nombres est par exemple $n=5\cdot7$.

P 354. Existe-t-il une infinité de n composés qui divisent les nombres $2^{\theta(n)}-1$ et $3^{\theta(n)}-1$?

TRAVAUX CITÉS

[1] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of a^n-b^n*, Annals of Mathematics 5 (1904), p. 173-180.

[2] L. E. Dickson, *History of the Theory of Numbers*, New York 1952.

[3] A. Rotkiewicz, *Sur les nombres composés n qui divisent $a^{n-1}-b^{n-1}$*, Rendiconti del Circolo Matematico di Palermo, Serie II, 8 (1959), p. 115.

[4] — *Sur les nombres pairs n pour lesquels les nombres a^nb-ab^n, respectivement $a^{n-1}-b^{n-1}$, sont divisibles par n*, ibidem, p. 341.

[5] — *O liczbach postaci $\dfrac{(4k+1)^{4k+1}-1}{4k}$, $\dfrac{(4k+3)^{4k+3}+1}{4k+4}$*, Prace Matematyczne 5 (1961), p. 95-99.

[6] W. Sierpiński, *Teoria liczb, II*, Warszawa 1959.

Reçu par la Rédaction le 10. 12. 1960