SUR LES SUITES D'ENTIERS DEUX A DEUX PREMIERS ENTRE EUX

Autor(en): **Sierpiski, W.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **10 (1964)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **03.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-39418

SUR LES SUITES D'ENTIERS DEUX A DEUX PREMIERS ENTRE EUX

par W. SIERPIŃSKI

Le but de cet article est de donner plusieurs théorèmes concernant les suites d'entiers deux à deux premiers entre eux. Ces théorèmes sont simples et leurs démonstrations sont élémentaires, mais je ne les ai pas trouvés dans la littérature mathématique qui m'était accessible.

THÉORÈME 1. *Tout entier* >6 *est une somme de deux entiers* >1 *premiers entre eux.*

Démonstration. Si n est un nombre impair >3, on a $n=2+(n-2)$ et, évidemment $n-2>1$ et $(2, n-2)=1$. Le théorème 1 est donc vrai pour les nombres impairs >3.

Voici maintenant la démonstration, due à M. A. MĄKOWSKI, pour les nombres n pairs >6.

Si n est un entier divisible par 4, $n=4k$, où, d'après $n>6$, k est un entier >1, on a $n=(2k-1)+(2k+1)$, où $2k+1>2k-1>1$ et les nombres $2k-1$ et $2k+1$, en tant que deux entiers impairs consécutifs, sont premiers entre eux.

Si, enfin, $n=4k+2$, où k est un entier >1 (puisque $n>6$), on a $n=(2k+3)+(2k-1)$ et les nombres $2k+3$ et $2k-1>1$ sont premiers entre eux, puisque si $0<d|2k-1$ et $d|2k+3$, on a $d|(2k+3)-(2k-1)$, donc $d|4$ et, comme d est un diviseur du nombre impair, on en conclut que $d=1$.

Le théorème 1 se trouve ainsi démontré. Or, M. A. MĄKOWSKI a remarqué aussi qu'il résulte sans peine d'une remarque de M. H. L. ADLER que le nombre $g(n)$ de toutes les décompositions d'un nombre naturel $n>6$ en une somme de deux entiers, $n=a+b$, où $1<a<b$ et $(a, b)=1$ est égal à $g(n)=\frac{1}{2}[\varphi(n)-2]$, où $\varphi(n)$ est la fonction bien connue d'Euler.

En effet, M. ADLER a remarqué que, pour n entier >1, $\varphi(n)$ est le nombre de tous les systèmes de deux nombres

naturels x, y, tels que $x+y = n$, $1 \leqslant x \leqslant n$ et $(x, n) = 1 = (y, n)$.[1]) Or, si $x+y = n$, on a $(x, y) = 1$ dans ce cas et seulement dans ce cas, où $(x, n) = (y, n) = 1$. Il en résulte que (pour $n > 1$) $\varphi(n)$ est le nombre de toutes les décompositions du nombre n en une somme de deux entiers positifs premiers entre eux. Si l'on exclut les décompositions $n = 1+(n-1)$ et $n = (n-1)+1$, alors, dans les $\varphi(n)-2$ décompositions qui resteront, les nombres x et y seront tous les deux >1, d'où la formule pour $g(n)$. Or, puisque, comme on le sait, $\varphi(n) > 2$ pour n entiers >6, il en résulte aussi tout de suite le théorème 1. M. A. Mąkowski a remarqué aussi que, vu que $\lim_{n=\infty} \varphi(n) = +\infty$, il en résulte aussi que $\lim_{n=\infty} g(n) = +\infty$.

Théorème 2. *Tout nombre naturel est, d'une infinité de manières, différence de deux nombres naturels premiers entre eux.*

Démonstration. Pour démontrer le théorème 2 il suffit de remarquer que si n est un nombre naturel donné, on a pour $k = 1, 2, 3, \ldots$ la décomposition

$$n = (nk+n+1)-(nk+1),$$

où

$$(nk+n+1,\ nk+1) = (n,\ nk+1) = 1.$$

Théorème 3. *Tout entier >17 est une somme de trois entiers >1, deux à deux premiers entre eux.*

Démonstration. Si n est un nombre pair >8, on a $n = 6k$, ou $n = 6k+2$, ou bien $n = 6k+4$ et, comme $n > 8$, nous pouvons admettre que dans les deux premiers cas k est un entier >1 et que dans le troisième cas k est un entier >0. Vu les formules

$$6k = 2+3+[6(k-1)+1], \quad 6k+2 = 3+4+[6(k-1)+1],$$
$$6k+4 = 2+3+(6k-1),$$

on conclut sans peine que n est une somme de trois entiers >1, deux à deux premiers entre eux.

---

1) H. L. Adler, *A generalization of the Euler φ-function*, Amer. Math. Monthly 65 (1958), p. 690-692.

Voici maintenant la démonstration de M. A. Mąkowski pour n impairs >17. Vu que $19 = 3+5+11$, nous pouvons même supposer que n est un nombre impair >19. Si n est un tel nombre, on a $n = 12k+\gamma$, où $\gamma = 1, 3, 5, 7, 9$ ou 11, et où k est un entier positif et même, pour $\gamma \leqslant 7$, $k>1$. Vu les identités

$$\begin{aligned}
12k+1 &= 9+(6k-7)+(6k-1),\\
12k+3 &= 3+(6k-1)+(6k+1),\\
12k+5 &= 3+(6k-5)+(6k+7),\\
12k+7 &= 9+(6k+5)+(6k-7),\\
12k+9 &= 9+(6k-1)+(6k+1),\\
12k+11 &= 3+(6k+7)+(6k+1)
\end{aligned}$$

on conclut que n est toujours une somme de trois entiers >1. Les nombres dans les parenthèses sont, dans chacune de ces six égalités, premiers par rapport aux nombres 3 et 9 et premiers entre eux, puisque ils sont tous impairs, non divisibles par 3, et leur différence est respectivement 6, 2, 12, 12, 2 et 6. On a donc dans chacun de ces six cas la décomposition du nombre impair $n>19$ en une somme de trois entiers >1, deux à deux premiers entre eux.

Le théorème 3 est ainsi démontré.

Or, on démontre sans peine que le nombre 17 n'est pas une somme de trois entiers >1, deux à deux premiers entre eux.

Or, on peut démontrer que le nombre 30 n'est pas une somme de quatre entiers >1, deux à deux premiers entre eux, mais que tout entier >30 est une telle somme. Il se pose le problème si, pour tout entier $s>4$, tout entier suffisamment grand est une somme de s entiers >1, deux à deux premiers entre eux.

Théorème 4. *Il existe des progressions arithmétiques aussi longues que l'on veut, formées de nombres naturels* >1, *deux à deux premiers entre eux.*

Démonstration. Soit n un entier donné quelconque >1 et soit $a = n!$ Les n nombres

$$a+1,\ 2a+1,\ 3a+1,\ \ldots,\ na+1,$$

sont deux à deux premiers entre eux. En effet, si, pour les entiers k et l, tels que $0<k<l\leqslant n$, les nombres $ka+1$ et $la+1$ n'étaient pas premiers entre eux, ils auraient un diviseur premier commun p et on aurait $p|(l-k)a$, donc soit $p|l-k$, soit $p|a$. Mais, comme $l-k<l\leqslant n$, on a $(l-k)|n! = a$. On a donc toujours $p|a$, ce qui est impossible, vu que $p|ka+1$.

Le théorème 4 est ainsi démontré.

Il est à remarquer qu'il n'existe aucune progression arithmétique $ak+b$ ($k = 1, 2, \ldots$), où a et b sont des entiers positifs, dont tous les termes seraient deux à deux premiers entre eux. Nous démontrerons ici le théorème plus général suivant:

THÉORÈME 5. *Si* f (x) *est un polynôme en* x *aux coefficients entiers, où le coefficient de la plus grande puissance de* x *est positif, les termes de la suite infinie*

$$f(1), f(2), f(3), \ldots,$$

ne peuvent pas être deux à deux premiers entre eux.

Démonstration. Le coefficient de la plus haute puissance de x dans le polynôme $f(x)$ étant >0, il existe un entier $n>0$, tel que $m = f(n)>1$. Mais alors, comme on voit sans peine, le nombre $f(m+n)$ est divisible par m et les nombres $f(n)$ et $f(m+n)$ ont un diviseur commun $m>1$ et par suite ne sont pas premiers entre eux. Le théorème 5 est ainsi démontré.

THÉORÈME 6. *Si* f (x) *est un polynôme en* x *aux coefficients entiers, où le coefficient de la plus grande puissance de* x *est positif, la condition nécessaire et suffisante pour qu'il existe une infinité des entiers positifs* $x_1, x_2, x_3, \ldots$, *tels que tous deux des nombres* $f(x_1), f(x_2), f(x_3), \ldots$ *soient premiers entre eux, est la condition C suivante:*

C. Il n'existe aucun nombre entier $d>1$ *tel qu'on ait* $d|f(x)$ *quel que soit l'entier positif* x.

La nécessité de la condition C étant évidente, nous démontrerons seulement leur suffisance. Dans ce but nous démontrerons le lemme suivant:

LEMME. s *étant un entier positif et* $q_1, q_2, \ldots, q_s$ *des nombres premiers distincts pour lesquels il existe des entiers positifs* $t_1, t_2, \ldots,$

t_s, *tels que* $q_i \nmid f(t_i)$ *pour* $i = 1, 2, \ldots, s$, *il existe un entier positif* t *tel que* $q_i \nmid f(t)$ *pour* $i = 1, 2, \ldots, s$.

Démonstration du lemme. Le lemme est évident pour $s = 1$. Soit maintenant s un nombre naturel donné et supposons que le lemme est vrai pour s nombres. Soient $q_1, q_2, \ldots, q_s, q_{s+1}$ des nombres premiers distincts, pour lesquels il existe des entiers positifs $t_1, t_2, \ldots, t_{s+1}$, tels que $q_i \nmid f(t_i)$ pour $i = 1, 2, \ldots, s+1$. Le lemme étant par hypothèse, vrai pour s nombres, il existe un entier positif t_0, tel que $q_i \nmid f(t_0)$ pour $i = 1, 2, \ldots, s$. Or, on a $q_{s+1} \nmid f(t_{s+1})$. Les nombres premiers $q_1, q_2, \ldots, q_{s+1}$ étant tous distincts, on a $(q_1 q_2 \ldots q_s, q_{s+1}) = 1$, d'où il résulte, comme on sait, qu'il existe des nombres naturels k et l tels que $t_0 + k q_1 q_2 \ldots q_s = t_{s+1} + l q_{s+1}$. Soit $t = t_0 + k q_1 q_2 \ldots q_s = t_{s+1} + l q_{s+1}$ On aura

$$f(t) \equiv f(t_0) \bmod q_i \text{ pour } i = 1, 2, \ldots, s \text{ et } f(t) \equiv f(t_{sH}) \bmod q_{s+1}$$

d'où, vu que $q_i \nmid f(t_0)$ pour $i = 1, 2, \ldots, s$ et $q_{s+1} \nmid f(t_{s+1})$, il résulte que $q_i \nmid f(t)$ pour $i = 1, 2, \ldots, s, s+1$. Le lemme est donc vrai pour $s+1$ nombres. Il se trouve ainsi démontré par l'induction.

Démonstration du théorème 6. Supposons que le polynôme $f(x)$ satisfait à la condition C. Le coefficient de la plus grande puissance de x étant dans le polynôme $f(x)$ positif, il existe un nombre naturel x_1 tel que $f(x_1) > 1$. Soit maintenant n un entier donné $\geqslant 1$ et supposons que nous avons déjà déterminé les n nombres naturels $x_1, x_2, \ldots, x_n$ tels que (dans le cas où $n > 1$) les nombres $f(x_1), f(x_2), \ldots, f(x_n)$ sont deux à deux premiers entre eux. Soient q_i $(i = 1, 2, \ldots, s)$ tous les diviseurs premiers du nombre $f(x_1)\, f(x_2) \ldots f(x_n)$. Le polynôme $f(x)$ satisfaisant à la condition C, il existe des entiers positifs $t_1, t_2, \ldots, t_s$, tels que $q_i \nmid f(t_i)$ pour $i = 1, 2, \ldots, s$, d'où, d'après notre lemme, nous concluons qu'il existe un nombre naturel x_{n+1}, tel que $q_i \nmid f(x_{n+1})$ pour $i = 1, 2, \ldots, s$. Vu la définition des nombres q_i $(i = 1, 2, \ldots, s)$, il en résulte tout de suite que $(f(x_{n+1}), f(x_1)\, f(x_2) \ldots f(x_n)) = 1$. Les nombres

$$f(x_1), f(x_2), \ldots, f(x_n), f(x_{n+1}),$$

sont donc premiers deux à deux.

Les nombres x_n $(n = 1, 2, ...)$ sont ainsi définis par l'induction et la suitei nfinie

$$f(x_1), f(x_2), f(x_3), \ldots,$$

est telle que leurs termes sont deux à deux premiers entre eux. Nous avons ainsi démontré que la condition C est suffisante. Le théorème 6 se trouve ainsi démontré.

THÉORÈME 7. *Si* $u_1, u_1, \ldots$ *est la suite infinie de Fibonacci* (c'est-à-dire la suite définie par les conditions: $u_1 = u_2 = 1$ et $u_{n+2} = u_n + u_{n+1}$ pour $n = 1, 2, ...$), *il existe une suite infinie des entiers positifs croissants* $n_1, n_2, \ldots$, *telle que les nombres de la suite infinie*

$$u_{n_1}, u_{n_2}, \ldots, \tag{1}$$

sont deux à deux premiers entre eux.

Démonstration de M. A. ROTKIEWICZ. Comme on sait, si m et n sont des entiers positifs, on a $(u_m, u_n) = u_{(m, n)}$ [1]. Comme $u_1 = 1$, il en résulte tout de suite que si $n_1, n_2, \ldots$ est une suite infinie croissante des entiers positifs deux à deux premiers entre eux, les termes de la suite infinie (1) sont deux à deux premiers entre eux. On peut prendre ici, par exemple $n_k = p_k$ $(k = 1, 2, ...)$, où p_k est le k - ième nombre premier, ou bien prendre $n_k = F_k = 2^{2^k} + 1$, où $k = 1, 2, \ldots$

M. A. ROTKIEWICZ a remarqué aussi qu'il résulte de la formule pour (u_m, u_n), que si $n_1, n_2, \ldots$ est une suite infinie croissante d'entiers positifs, les nombres de la suite infinie (1) sont dans ce cas et seulement dans ce cas deux à deux premiers entre eux, si, quels que soient les entiers k et l, tels que $1 \leqslant k < l$, on a $(n_k, n_l) \leqslant 2$.

Remarque. Dans la suite infinie de tous les nombres consécutifs de Fermat, $F_n = 2^{2^n} + 1$ $(n = 1, 2, ...)$, les termes de cette suite sont, comme on le démontre sans peine, deux à deux premiers entre eux. Dans la suite de nombres de Mersenne, $M_n = 2^n - 1$ $(n = 1, 2, ...)$ les nombres de la suite M_{p_k} $(k = 1, 2, ...)$ où p_k est le k - ième nombre premier, sont deux à deux premiers entre eux. On peut aussi démontrer que les termes de la suite

[1]) Voir, par exemple, mon livre *Teoria Liczb* II, Warszawa 1959. p. 280, exercice 5 L'édition anglaise de ce livre est sous presse.

infinie $M_{F_n} = M_{2^{2^n}+1} = 2^{2^{2^n}+1} - 1$ (n = 1, 2, ...) sont deux à deux premiers entre eux.

THÉORÈME 8. *a, b et c* étant des entiers positifs, *si l'équation* ax+by = c *a une solution en nombres entiers x, y, elle a une infinité de solutions en nombres entiers x, y premiers entre eux.*

Démonstration. Nous pouvons admettre que $(a, b) = 1$, puisque, si $d = (a, b)$, $a = da_1$, $b = db_1$, alors, d'après $ax+by = c$ on trouve $d|c$, donc $c = dc_1$, et notre équation est équivalente à l'équation $a_1x+b_1y = c_1$, où $(a_1, b_1) = 1$.

Supposons donc que a, b et c sont des entiers positifs, $(a,b) = 1$ et qu'il existe des entiers x_0 et y_0 tels que $ax_0+by_0 = c$. On aura donc aussi $a(x_0+bt)+b(y_0-at) = c$, quel que soit l'entier t.

Comme $(a,b) = 1$, il existe, comme on sait, des entiers u et v tels que $au+bv = 1$.

Posons

$$t = kc-(x_0 v - y_0 u)+1\,, \tag{2}$$

en choisissant l'entier positif k de sorte que l'entier (2) soit positif, ce qui subsiste pour tous les k suffisamment grands. Il résulte de (2) que

$$(t+(x_0 v - y_0 u)\,,\ c) = 1\,. \tag{3}$$

Soit d un entier positif tel que $d \mid x_0+bt$ *et* $d \mid y_0-at$. Il en résulte que $d|ax_0+by_0 = c$ et, comme $au+bv = 1$, on a

$$d \mid (x_0+bt)v-(y_0-at)u = x_0v-y_0u+(au+bv)\,t = x_0v-y_0u+t\,.$$

On a donc $d|c$ et $d|x_0v-y_0u+t$, d'où il résulte, d'après (3), que $d = 1$. Les entiers $x = x_0+bt$ et $y = y_0-at$ sont donc premiers entre eux et on a $ax+by = c$. Le théorème 8 se trouve ainsi démontré.

D'après une remarque de M. A. SCHINZEL le théorème 8 peut être déduit sans peine d'un théorème de M. T. SKOLEM, publié dans *Norsk Mat. Tidsskrift* 15, p. 25-27 (cf. aussi *Jahrbuch über die Fortschritte der Math.* 59_I (1933), Sonderheft II, p. 129).

W. Sierpiński
Konopczyńskiego 5/7 m. 38
Warszawa 1.

(Reçu le 8 novembre 1962.)