# Sur l'équation $\varphi(x+k) = \varphi(x)$

par

A. Schinzel (Warszawa)

W. Sierpiński a démontré ([2], théorème 1) que pour tout nombre naturel $k$ il existe un nombre naturel $n_k$ tel que $\varphi(n_k+k) = \varphi(n_k)$ et j'ai démontré moi-même ([2], théorème 2) que pour tout nombre naturel $m$ il existe un nombre naturel $k$ tel que l'équation

$$\varphi(x+k) = \varphi(x) \tag{1}$$

a plus de $m$ solutions en nombres naturels $x$.

Nous avons déduit ces théorèmes de l'identité

$$\varphi(ql) = \varphi\big((q-1)l\big), \tag{2}$$

où $q$ est un nombre premier, $(q, l) = 1$, et tout diviseur premier du nombre $q-1$ est un diviseur du nombre $l$.

Dans le travail cité, W. Sierpiński a aussi posé la question si l'équation (1) a pour tout $k$ naturel plus d'une solution (ou bien si elle en a une infinité). Dans cet ordre d'idées je démontrerai ici les deux théorèmes suivants:

Théorème 1. *Pour tout nombre naturel $k$ il existe un nombre naturel $a$ tel que l'équation $\varphi(x+k^a) = \varphi(x)$ a au moins deux solutions.*

Théorème 2. *L'équation $\varphi(x+k) = \varphi(x)$ a au moins deux solutions pour tous les nombres naturels $k \leqslant 8 \cdot 10^{47}$.*

$m$ et $n$ étant deux entiers, nous écrivons $m|^*n$ pour exprimer que tout diviseur premier de $m$ est un diviseur de $n$. On démontre sans peine qu'on a $m|^*n$ si et seulement s'il existe un nombre naturel $a$ tel que $m|n^a$. Or, *si $m|^*n$ on a*

$$\varphi(mn) = m\varphi(n). \tag{3}$$

Démonstration du théorème 1. Soient $q_1$ et $q_2 > q_1$ les plus petits nombres premiers qui ne divisent pas $k$. Puisque $q_2-q_1 < q_2$ et $q_1 \nmid q_2-q_1$, on a $q_2-q_1 |^* k$. Il existe donc un nombre naturel $\beta$ tel que $q_2-q_1 | k^\beta$. Soit $a = \beta+1$, $k' = k^a/(q_2-q_1)$.

En posant successivement $l=k^a$, $q=q_1$, $l=k'$, $q=q_1$ et $l=q_1k'$, $q=q_2$ on a chaque fois $(q,l)=1$, $q-1|^*l$, donc en vertu de (2)

$$\varphi(q_1k^a)=\varphi[(q_1-1)k^a], \tag{4}$$

$$\varphi(q_1k')=\varphi[(q_1-1)k'], \tag{5}$$

$$\varphi(q_2q_1k')=\varphi[(q_2-1)q_1k']. \tag{6}$$

Or, d'après $(q_2,q_1k')=1$, la formule (5) et $(q_2,q_1-1)=1$ on a en vertu de la formule (6)

$$\varphi[(q_2-1)q_1k']=\varphi[q_2(q_1-1)k']. \tag{7}$$

Comme

$$(q_2-1)q_1k'-q_2(q_1-1)k'=(q_2-q_1)\frac{k^a}{q_2-q_1}=k^a$$

en vertu de (4) et (7) les nombres

$$x_1=(q_1-1)k^a \quad \text{et} \quad x_2=\frac{q_2(q_1-1)}{q_2-q_1}k^a>x_1$$

satisfont à l'équation $\varphi(x+k^a)=\varphi(x)$, ce qui achève la démonstration.

LEMME 1. *Si la suite des nombres premiers*

$$3=q_1<q_2<\ldots<q_n$$

*satisfait aux conditions*

$$q_i-2|q_1q_2\ldots q_{i-1} \quad (2\leqslant i\leqslant n), \tag{8}$$

$$q_i-1|^*2q_1q_2\ldots q_{i-1} \tag{9}$$

*l'équation* (1) *a au moins deux solutions pour tous les $k$ impairs qui ne sont pas divisibles par $q_1q_2\ldots q_n$.*

Démonstration. Soit $j$ le plus petit nombre tel que $k$ ne soit pas divisible par $q_j$. Donc

$$(k,q_j)=(k,2)=1 \tag{10}$$

et $q_j=3$ ou bien $q_1q_2\ldots q_{j-1}|k$ $(j\geqslant 2)$. D'après (8) et (9) on a $q_j-2|k$ et $q_j-1|^*2k$, d'où, en vertu de $(q_j-1,q_j-2)=1$ il résulte que $q_j-1|^*2k/(q_j-2)$.

Donc d'après (3) et (10).

$$\varphi\left(\frac{2k}{q_j-2}(q_j-1)\right)=(q_j-1)\varphi\left(\frac{2k}{q_j-2}\right)=\varphi(q_j)\varphi\left(\frac{k}{q_j-2}\right)=\varphi\left(q_j\frac{k}{q_j-2}\right).$$

Donc, puisque $\varphi(2k)=\varphi(k)$, l'équation (1) a au moins deux solutions $x_1=k$ et $x_2=\left(q_j/(q_j-2)\right)k>x_1$, ce qui achève la démonstration.



LEMME 2. *Si $k$ est un nombre pair, le nombre des solutions de l'équation* (1) *en nombres naturels $x\leqslant a$ est pour $a\geqslant k^2$ plus grand que le nombre des nombres premiers $p\leqslant a/2k+\frac{1}{2}$ tels que le nombre $q=2p-1$ soit premier et que $(k,p)=(k,q)=1$.*

Démonstration. Pour tout nombre premier $p\leqslant a/2k+\frac{1}{2}$ pour lequel $q=2p-1$ est un nombre premier et $(k,p)=(k,q)=1$ on a

$$\varphi(2pk)=\varphi(p)\varphi(2k)=2(p-1)\varphi(k)=(2p-2)\varphi(k)=\varphi(2p-1)\varphi(k)$$
$$=\varphi\big((2p-1)k\big)$$

$x(p)=(2p-1)k$ est donc une solution de l'équation (1) telle que

$$x(p)\leqslant(a/k)k=a.$$

Or, d'après (2), notre équation a encore la solution $x=(q_1-1)k$, où $q_1\leqslant k+1$ est le plus petit nombre premier qui ne divise pas $k$. Cette solution est distincte de chacun des nombres $x(p)$, puisque $2p-1>p-1\geqslant q_1-1$ ce qui achève la démonstration.

Démonstration du théorème 2. La suite des nombres premiers

$$3,5,7,17,19,37,97,113,257,401,487,631,971,1297,1801,19457,$$
$$22051,28817,65537$$

satisfait aux conditions (8) et (9) et on a $3\cdot5\cdot7\cdot\ldots\cdot65537>8\cdot10^{47}$.

Donc, en vertu du lemme 1, l'équation (1) a au moins deux solutions pour tous les $k$ impairs $\leqslant 8\cdot10^{47}$.

D'autre part, la suite des nombres premiers $p_i$ $(1\leqslant i\leqslant 22)$

$$3,7,31,37,97,139,157,199,211,229,271,307,331,337,367,379,$$
$$439,449,547,577,601,607$$

jouit de la propriété que pour tout indice $i\leqslant 22$ le nombre $2p_i-1$ est aussi premier. Donc, on a $2p_i-1\neq p_j$ pour $i,j\leqslant 22$.

Si pour un $k$ pair l'équation (1) avait une seule solution, alors, en vertu du lemme 2, pour tout $i\leqslant 22$ on aurait $p_i|k$ ou bien $2p_i-1|k$, d'où $2\prod_{i=1}^{22}r_i|k$ où $r_i=p_i$ ou bien $r_i=2p_i-1$.

On en déduit

$$k\geqslant 2\prod_{i=1}^{22}r_i\geqslant 2\prod_{i=1}^{22}p_i>8\cdot10^{47},$$

ce qui achève la démonstration.

Il résulte du lemme 2 que s'il existe une infinité de nombres premiers $p$ pour lesquels le nombre $2p-1$ est premier, l'hypothèse H suivante est vraie:

H. *Pour tout nombre $k$ pair l'équation* (1) *a une infinité de solutions.*

L'hypothèse analogue pour $k$ impair ne serait pas justifiée. Il est vrai que l'équation $\varphi(x+1) = \varphi(x)$ a pour $x \leqslant 10000$, 18 solutions 1, 3, 15, 104, 164, 194, 255, 495, 584, 975, 2204, 2625, 2834, 3255, 3705, 5186, 5187 (cf. [1]), mais l'équation $\varphi(x+3) = \varphi(x)$ a pour $x \leqslant 10000$ les seules solutions $x = 3$ et $x = 5$, alors que l'équation $\varphi(x+2) = \varphi(x)$ a 80 solutions pour $x \leqslant 10000$.

### Travaux cités

[1] L. Moser, *Some equations involving Euler's totient function*, The American Math. Monthly 56 (1949), p. 21-22.

[2] W. Sierpiński, *Sur une propriété de la fonction* $\varphi(n)$, Publ. Math., Debrecen, 4 (1956), p. 184-185.

*Reçu par la Rédaction le 17. 5. 1957*

---

# Sur certaines hypothèses concernant les nombres premiers

par

A. Schinzel et W. Sierpiński (Warszawa)

La répartition des nombres premiers parmi les nombres naturels n'est pas encore suffisamment étudiée: c'est pourquoi depuis les temps les plus anciens on a énoncé diverses hypothèses concernant les nombres premiers. Plusieurs de ces hypothèses se sont montrées fausses; quelques unes d'elles ne sont pas encore mises en défaut, et il y en a qui sont vérifiées pour tous les nombres ne dépassant pas un nombre très grand.

Une de plus anciennes hypothèses sur les nombres premiers, ayant au moins 25 siècles, était celle des Chinois: un nombre naturel $n > 1$ est premier si et seulement si le nombre $2^n - 2$ est divisible par $n$. La nécessité de cette condition a été démontrée il y a quelques centaines d'années. En 1681 Leibniz a essayé de démontrer qu'elle est suffisante, mais sa démonstration était basée sur un raisonnement faux, et en 1819 on a trouvé que l'hypothèse des Chinois était fausse, puisque le nombre $2^{341} - 2$ (qui a 103 chiffres) est divisible par 341, bien que le nombre $341 = 11 \cdot 31$ ne soit pas premier. Ensuite on a démontré (de nos temps) qu'il existe une infinité de nombres composés $n$ pour lesquels le nombre $2^n - 2$ est divisible par $n$, impairs aussi bien que pairs. (Le plus petit de ces nombres pairs est le nombre $n = 161038 = 2 \cdot 73 \cdot 1103$ trouvé en 1950 par D. H. Lehmer).

P. Fermat supposait premiers tous les nombres $F_n = 2^{2^n} + 1$, où $n = 0, 1, 2, \ldots$ Cela est vrai pour $n = 0, 1, 2, 3$ et 4, mais, comme l'a trouvé L. Euler en 1772, le nombre $F_5$ (qui a 10 chiffres) est composé, car il est divisible par 641. Maintenant nous connaissons 29 nombres $F_n$ composés, pour $n = 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 39, 55, 63, 73, 117, 125, 144, 150, 207, 226, 228, 268, 284, 316, 452$.

On peut donc énoncer l'hypothèse qu'il existe une infinité de nombres $F_n$ composés. On a même énoncé l'hypothèse plus forte: les nombres $F_n$ premiers sont en nombre fini. Ce sont peut-être seulement ceux que connaissait Fermat, à savoir les nombres $F_n$ pour $n \leqslant 4$.