donc

$$K(n) = \frac{1}{2}\sum_{s=1}^{[\log_2 n]}([\sqrt[s]{n}]^2 + [\sqrt[s]{n}]) - [\log_2 n].$$

De la même manière, en sommant les nombres (19) et ensuite les sommes ainsi obtenues pour tous les k satisfaisant à (18), il vient

$$S(n) = \frac{1}{2}\sum_{k=2}^{n}([\log_k n]^2 + [\log_k n]).$$

SUR LA SOLUTION D'UNE CONGRUENCE EN NOMBRES COMPOSÉS

PAR

K. MATULEWICZ (GÓRA ŚLĄSKA)

Les recherches sur la congruence $2^n \equiv 2 \pmod{n}$, poursuivies depuis plusieurs siècles, se rattachent au problème de trouver un théorème réciproque de celui de Fermat d'après lequel, a étant un entier quelconque et n étant un nombre premier, on a

(1) $$a^n \equiv a \pmod{n}.$$

D'après Lehmer[1]), les Chinois, qui ont trouvé ce théorème pour $a=2$, ont aussi formulé, il y a 25 siècles, le théorème réciproque que voici:

(*) *Si $2^n - 2$ est divisible par n, le nombre n est premier.*

Dickson[2]) cite les travaux de plus de 25 auteurs, écrits entre 1675 et 1913, sur la congruence (1). En 1830, un auteur anonyme a trouvé l'exemple $2^{341} \equiv 2 \pmod{341}$, où $341 = 11\cdot 31$, qui contredit le théorème (*).

Sierpiński a démontré que la congruence $2^n \equiv 2 \pmod{n}$ est satisfaite pour tout n qui est d'une des deux formes suivantes:

(a) $n = 2^{2^k} + 1$, où k est un nombre naturel quelconque[3]),

(b) $n = 2^k - 1$, si $2^k \equiv 2 \pmod{k}$, où k est un nombre impair[4]).

Toutes les solutions de la congruence

$$2^n \equiv 2 \pmod{n}$$

---

[1]) D. H. Lehmer, *On the converse of Fermat's theorem*, The American Mathematical Monthly 43 (1936), p. 347-354.

[2]) L. E. Dickson, *History of the theory of numbers*, I, Washington 1934, p. 91-96.

[3]) W. Sierpiński, *Teoria liczb*, Monografie Matematyczne, Warszawa-Wrocław 1950, p. 61.

[4]) Ibidem, p. 66, exercice 15; voir aussi W. Sierpiński, *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n-2)/n$, Colloquium Mathematicum 1 (1947), p. 9.

en nombres composés pour $n \leqslant 2000$ ont été données par T. Banachiewicz [5]): $341=11\cdot31$, $561=3\cdot11\cdot17$, $645=3\cdot5\cdot43$, $1105=5\cdot13\cdot17$, $1387=19\cdot73$, $1729=7\cdot13\cdot19$, $1905=3\cdot5\cdot127$. J'ai trouvé toutes les solutions analogues pour $2000<n\leqslant4033$, à savoir: $2047=23\cdot89$, $2465=5\cdot17\cdot29$, $2821=7\cdot13\cdot31$, $3277=29\cdot113$, $4033=37\cdot109$. De plus, je donne à l'aide du théorème I une méthode pour obtenir des solutions de (1) en nombres composés; cette méthode fournit en outre des solutions qui sont différentes de celles contenues dans (a) et (b).

Théorème I. S'il existe, pour les nombres naturels a, r_1 et r_2, un nombre naturel s tel que

$$r_1r_2 \mid a^{s-1}-1, \qquad s-1 \mid r_1-1, \qquad s-1 \mid r_2-1,$$

on a

$$a^{r_1r_2} \equiv a \pmod{r_1r_2}.$$

J'ai démontré ce théorème pour $a=2$ [6]). La démonstration est la même pour a quelconque.

Théorème II. Si p et $q>p$ sont des nombres premiers et $(a,p)=1$, $(a,q)=1$, $p-1 \mid q-1$ et $a^{pq}\equiv a \pmod{pq}$, alors $q \mid a^{p-1}-1$.

Démonstration. Compte tenu de ce que $a^{p-1}\equiv1\pmod{p}$, $a^{q-1}\equiv1\pmod{q}$ et $p-1\mid q-1$, on trouve

$$a^{q-1}\equiv1 \pmod{pq}. \tag{2}$$

En vertu du théorème connu d'Euler

$$a^{\varphi(pq)}=a^{(p-1)(q-1)}=a^{pq-1-(p-1)-(q-1)}\equiv1 \pmod{pq}. \tag{3}$$

Les congruences (2) et (3) donnent

$$a^{pq-1-(p-1)}\equiv1 \pmod{pq},$$

et, ensuite,

$$a^{pq-1}-1\equiv a^{p-1}-1 \pmod{pq},$$

d'où l'on déduit, en vertu de la relation $a^{pq}\equiv a\pmod{pq}$, que

$$a^{p-1}-1\equiv0 \pmod{pq},$$

donc

$$q\mid a^{p-1}-1.$$

[5]) Voir la note citée de W. Sierpiński, p. 9.

[6]) K. Matulewicz, *Sur les nombres composés satisfaisant à la congruence* $2^n\equiv2\pmod{n}$, Annales de la Société Polonaise de Mathématique 22 (1949), p. 291.

Exemples. Soit $s=23$; alors $2^{s-1}-1=2^{22}-1=3\cdot\mathbf{23}\cdot\mathbf{89}\cdot\mathbf{683}$. Un couple quelconque des facteurs imprimés en gros caractère satisfait aux hypothèses du théorème I pour $a=2$; nous avons donc $2^n\equiv2\pmod{n}$ pour $n=23\cdot89$, $n=23\cdot683$ et $n=89\cdot683$. Voici pour $a=2,3,\ldots,10$ des valeurs de s pour lesquels la décomposition en facteurs du nombre $a^{s-1}-1$ permet de trouver, à l'aide du théorème I, des solutions composées de la congruence $a^n\equiv a\pmod{n}$:

a	2	3	4	5	6	7	8	9	10
s	11	7	3	7	3	7	3	5	3
n	341	91	15	217	35	817	21	205	33

Ainsi, par exemple, pour $a=8$ et $s=3$, on a $a^{s-1}-1=63=3^2\cdot7$. En posant $r_1=s=3$ et $r_2=7$, on trouve $r_2-1=3(s-1)$, d'où $8^{21}\equiv8\pmod{21}$, ce que l'on peut d'ailleurs vérifier directement.

Remarquons encore que les théorèmes précités de Sierpiński se laissent modifier, pour a quelconque, de la manière suivante:

(i) *On a pour tout k naturel*

$$a^{a^{a^k}+1}\equiv\pm a \pmod{a^{a^k}+1},$$

où le signe $+$ est pris pour a pair et le signe $-$ pour a impair.

(ii) *Si p est un nombre naturel, $(a,p)=1$ et $a^p\equiv a\pmod{p}$, on a*

$$a^{a^p-1}\equiv a^{a-1} \pmod{a^p-1}.$$