COLLOQUIUM MATHEMATICUM
VOL. X 1963 FASC. 1

SUR LES NOMBRES COMPOSÉS DE LA FORME $a^{2^n}+1$

PAR

W. SIERPIŃSKI (VARSOVIE)

Tous les nombres $a^{2^n}+1$, où $n = 1, 2, \ldots$, sont évidemment premiers pour $a = 1$, à savoir égaux à 2. Fermat supposait qu'il sont tous premiers aussi pour $a = 2$, mais Euler a trouvé que le nombre $2^{2^5}+1$ est composé, à savoir divisible par le nombre premier 641.

La question s'impose s'il existe pour tout entier $a > 1$ au moins un n naturel tel que le nombre $a^{2^n}+1$ est composé (**P 411**).

Je ne vais en établir ici qu'une réponse partielle.

THÉORÈME 1. *Il existe pour tout entier a tel que $1 < a \leqslant 100$ au moins un $n \leqslant 6$ naturel pour lequel le nombre $a^{2^n}+1$ est composé.*

C'est en effet évident pour $a > 1$ impairs, puisque les nombres $a^{2^n}+1$ (où $n = 1, 2, \ldots$) sont alors pairs et supérieurs à 2, donc composés. Soit donc $a \leqslant 100$ un nombre naturel pair.

On a, comme il vient d'être rappelé, $641 \mid 2^{2^5}+1$, donc aussi $641 \mid 4^{2^4}+1$ et $641 \mid 16^{2^3}+1$. Or on vérifie sans peine que $17 \mid 6^{2^3}+1$, $5 \mid 8^{2}+1$, $17 \mid 10^{2^3}+1$, $17 \mid 12^{2^3}+1$, $17 \mid 14^{2^3}+1$, $5 \mid 18^{2}+1$, $17 \mid 20^{2^3}+1$, $17 \mid 22^{2^3}+1$, $17 \mid 24^{2^3}+1$, $17 \mid 26^{2^2}+1$, $17 \mid 28^{2^3}+1$, $17 \mid 30^{2}+1$, $17 \mid 32^{2^2}+1$ et $13 \mid 34^{2}+1$.

Pour vérifier, par exemple, que $17 \mid 28^{2^3}+1$, on part de la congruence $28 \equiv 11 \pmod{17}$, d'où $28^2 \equiv 121 \equiv 2 \pmod{17}$, ce qui entraîne $28^{2^3} \equiv 2^{2^2} \equiv 16 \pmod{17}$, donc $28^{2^3}+1 \equiv 0 \pmod{17}$.

Vu les formules qui précèdent, on trouve sans peine pour $k = 1, 2, \ldots$ $17 \mid (34k+2)^{2^2}+1$, $17 \mid (34k+4)^2+1$, $17 \mid (34k+6)^{2^3}+1$, $17 \mid (34k+8)^{2^2}+1$, $17 \mid (34k+10)^{2^3}+1$, $17 \mid (34k+12)^{2^3}+1$, $17 \mid (34k+14)^{2^3}+1$, $17 \mid (34k+20)^{2^3}+1$, $17 \mid (34k+22)^{2^3}+1$, $17 \mid (34k+30)^2+1$ et $17 \mid (34k+32)^{2^2}+1$.

On en déduit qu'il existe pour tout $a \leqslant 100$ naturel pair un $n \leqslant 5$ naturel tel que le nombre $a^{2^n}+1$ est composé, sauf peut-être pour les nombres $a = 50$, 52, 68, 84 et 86. Or on a $50^2+1 = 2501 = 41 \cdot 61$, $5 \mid 52^2+1$, $5 \mid 68^2+1$, $257 \mid 84^{2^6}+1$ et $13 \mid 86^2+1$.

Le théorème 1 se trouve ainsi démontré.

Ne connaissant jusqu'à présent aucun nombre de Fermat composé dépassant $F_{1945} = 2^{2^{1945}}+1$, nous ignorons s'il existe pour $a = 2^{2^{1945}}$ un n naturel tel que le nombre $a^{2^n}+1$ est composé; en effet, ce serait un nombre de Fermat composé dépassant F_{1945}. Nous savons cependant démontrer qu'il existe une infinité de nombres pairs a pour lesquels tous les nombres $a^{2^n}+1$ (où $n = 1, 2, \ldots$) sont composés. Tels sont, par exemple, les nombres $a = 2^k$, où $k > 1$ est un entier impair, car le nombre $a^{2^n}+1 = (2^{2^n})^k+1$ (où $n = 1, 2, \ldots$) est alors divisible par $2^{2^n}+1$.

Il est à remarquer que s'il existait pour tout entier $a > 1$ un n naturel tel que le nombre $a^{2^n}+1$ est composé, il existerait pour tout entier $a > 1$ une infinité de tels n naturels, car il existerait alors pour tout entier $a > 1$ et pour tout k naturel un m naturel tel que le nombre $(a^{2^k})^{2^m}+1 = a^{2^{k+m}}+1$ serait composé, et il en résulterait en particulier l'existence d'une infinité de nombres de Fermat composés.

Nous ne savons pas plus s'il existe un entier $a > 1$ pour lequel tout nombre $a^{2^n}+1$, où $n = 1, 2, \ldots$, est premier. Or il résulte d'une hypothèse de Schinzel [1] l'existence, pour tout nombre naturel s, d'un entier $a > 1$ pour lequel tous les nombres $a^{2^n}+1$, où $n = 1, 2, \ldots, s$, sont premiers. Il serait cependant difficile de trouver un tel nombre a déjà pour $s = 5$.

THÉORÈME 2. *Il y a dans la suite infinie*

$$2^2+1,\ 6^2+1,\ 2^{2^2}+1,\ 6^{2^2}+1,\ 2^{2^3}+1,\ 6^{2^3}+1, \ldots,\ 2^{2^n}+1,\ 6^{2^n}+1, \ldots$$

une infinité de termes qui sont des nombres composés.

C'est en effet évident, s'il n'existe qu'un nombre fini de nombres de Fermat premiers. Admettons donc qu'il en existe une infinité.

Soit $n > 1$. D'après un théorème bien connu, on a $3^{2^{2^n-1}} \equiv -1 \pmod{F_n}$, d'où $6^{2^{2^n-1}} = 2^{2^{2^n-1}} \cdot 3^{2^{2^n-1}} \equiv -2^{2^{2^n-1}} \pmod{F_n}$, donc $6^{2^{2^n-1}}+1 \equiv -(2^{2^{2^n-1}}-1) \pmod{F_n}$. Or on a $n+1 \leqslant 2^n-1$ pour $n = 2, 3, \ldots$, d'où $2^{n+1} \mid 2^{2^n-1}$, donc $2^{2^n}+1 \mid 2^{2^{n+1}}-1 \mid 2^{2^{2^n-1}}-1$ et par conséquent $2^{2^{2^n-1}}-1 \equiv 0 \pmod{F_n}$ et $6^{2^{2^n-1}}+1 \equiv 0 \pmod{F_n}$. On a aussi $2^n-1 > n$ pour $n = 2, 3, \ldots$, d'où $6^{2^{2^n-1}} > 6^{2^n} > 2^{2^n}$ et par conséquent $6^{2^{2^n-1}}+1 > F_n$. Le nombre $6^{2^{2^n-1}}+1$ est donc composé, divisible par le nombre premier F_n.

[1] A. Schinzel et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arithmetica 4 (1958), p. 188.

Il est ainsi démontré que si le nombre F_n, où $n > 1$, est premier, le nombre $6^{2^{2^n-1}}+1$ est composé, ce qui achève la démonstration du théorème 2.

En particulier, les nombres F_n étant, comme on sait, premiers pour $n = 2$, 3 et 4, on trouve que les nombres $6^{2^3}+1$, $6^{2^7}+1$ et $6^{2^{15}}+1$ sont composés et divisibles respectivement par F_2, F_3 et F_4.

On peut montrer également que si, pour un n naturel, le nombre F_n est premier, le nombre $12^{2^{2^n-1}}+1$ est composé et divisible par F_n.

Reçu par la Rédaction le 29. 1. 1962