ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

LÉON POMEY

Sur les nombres de Fermat et de Mersenne

Annales de la faculté des sciences de Toulouse 3^e série, tome 16 (1924), p. 135-138

<http://www.numdam.org/item?id=AFST_1924_3_16__135_0>

SUR LES NOMBRES DE FERMAT ET DE MERSENNE

Par M. Léon POMEY.

1. On appelle souvent *Nombres de Fermat* les nombres premiers de la forme $2^m \pm 1$, ou plus particulièrement ceux de la forme $2^m + 1$, qui interviennent dans la théorie de la division du cercle (1), réservant alors le nom de *Nombres de Mersenne* à ceux de la forme $2^m - 1$, en raison de ce que cet auteur a donné (sans démonstration) leurs valeurs jusqu'à $m = 257$ dans ses « Cogitata physico-mathematica », valeurs qu'il tenait, supposent certains, de Fermat lui-même.

Les propositions, que nous indiquons ci-après et dont plusieurs ont été publiées dans une Note des *Comptes Rendus de l'Académie des Sciences* (T. 170, 1920, p. 100 et T. 171, 1920, p. 940), ont trait à ces deux sortes de nombres; elles découlent du théorème suivant d'Ed. Lucas (*Atti. d. R. Acad. d. Sc. di Torino*, 1878, p. 284 et *Récréations mathématiques*, T. II, p. 233) :

Pour que le nombre $M = 2^m - 1$ (*où* $m = 1 + 2n + 4nq$) *soit premier, il faut et il suffit que l'on ait*

$$(1) \qquad (2^n + \sqrt{2^{2n} + 1})^{\frac{M+1}{2}} + (2^n - \sqrt{2^{2n} + 1})^{\frac{M+1}{2}} \equiv 0 \pmod{M}.$$

Il y a lieu de chercher les valeurs de n les plus simples et indépendantes, si possible, de M.

(1) On sait qu'un nombre $2^m + 1$, pour être premier doit avoir comme exposant m une puissance de 2; mais cette condition n'est pas suffisante comme Euler l'a montré le premier pour $\eta = 2^5$, contrairement à une présomption de Fermat, dont celui-ci reconnaissait lui-même ne pas avoir de preuve (Lettre de Fermat à Mersenne, du 25 déc. 1640). Ed. Lucas, substituant une autre intuition à celle de Fermat, suppose que les *Nombres de Fermat* auraient exclusivement pour exposants les nombres $2, 2^2, 2^{2^2}, \ldots$.

Parallèlement, il est permis, semble-t-il, de penser que les nombres de Mersenne auraient exclusivement pour exposant m (forcément premier) un nombre de Fermat ou de Mersenne...

2. Remarquons tout d'abord que n est un diviseur quelconque de $\frac{m-1}{2}$ assujetti à la seule condition de contenir la même puissance de 2 que $\frac{m-1}{2}$, et que ses valeurs les plus simples sont :

1° $n=1$ quand m est de la forme $4h+3$ (c'est-à-dire de la forme $8h'+3$ ou $8h'+7$), d'où la congruence

$$(2+\sqrt{5})^{\frac{M+1}{2}}+(2-\sqrt{5})^{\frac{M+1}{2}}\equiv 0 \pmod{M}.$$

2° $n=2^{\alpha-1}$ quand $m=8h'+1$ avec $4h'=2^{\alpha-1}(2K+1)$ ou $m=1+2^{\alpha}(2K+1)$ d'où

$$(2^{2^{\alpha-1}}+\sqrt{2^{2^{\alpha}}+1})^{\frac{M+1}{2}}+(2^{2^{\alpha}}-\sqrt{2^{2^{\alpha}}+1})^{\frac{M+1}{2}}\equiv 0 \pmod{M}.$$

3° $n=2$ quand $m=8h'+5$, d'où

$$(4+\sqrt{17})^{\frac{M+1}{2}}+(4-\sqrt{17})^{\frac{M+1}{2}}\equiv 0 \pmod{M}.$$

Particularisons encore plus le nombre premier m en le supposant lui aussi de la forme 2^p-1 (p premier impair). On pourra prendre pour n le nombre p (en vertu du théorème de Fermat) et par suite pour $2^n\pm\sqrt{2^{2n}+1}$ l'expression $m+1\pm\sqrt{(m+1)^2+1}$.

3. Théorèmes corrélatifs des précédents. — Nous allons indiquer pour les nombres premiers M une autre congruence caractéristique, de nature analogue à (1), mais susceptible de revêtir une forme particulière *plus simple* que toutes les précédentes et pourtant applicable à *toutes* les valeurs de m.

Pour cela appelons ν le quotient de $\sqrt{\frac{M+1}{2}}$ (ou $2^{\frac{m-1}{2}}$) par 2^n et multiplions la congruence (1) par la quantité $2^{\frac{M+1}{4}}\nu^{\frac{M+1}{2}}$. On obtient ainsi une nouvelle congruence qui, après suppression des multiples de M, nous donne le théorème suivant, corrélatif en quelque sorte de celui de Lucas :

THÉORÈME I. — *Pour que le nombre* $M = 2^m - 1$ *(où* $m = 1 + 2n + 4nq$*) soit premier, il faut et il suffit que l'on ait*

$$(2) \qquad (1 + \sqrt{1 + 2\nu^2})^{\frac{M+1}{2}} + (1 - \sqrt{1 + 2\nu^2})^{\frac{M+1}{2}} \equiv 0 \pmod{M},$$

avec $\nu = 2^{\frac{m-1}{2} - n}$.

D'où l'on déduit immédiatement (en prenant $n = \frac{m-1}{2}$) ce corollaire.

THÉORÈME II. — *Pour que le nombre* $M = 2^m - 1$ *soit premier, il faut et il suffit que l'on ait*

$$(3) \qquad (1 + \sqrt{3})^{\frac{M+1}{2}} + (1 - \sqrt{3})^{\frac{M+1}{2}} \equiv 0 \pmod{M}.$$

On voit que cette congruence est bien générale, que sa forme ne dépend plus expressément de n et qu'elle est la plus simple possible.

Les autres cas envisagés précédemment (§ 2) fournissent autant de théorèmes corrélatifs, que nous n'énoncerons pas pour abréger.

4. Si on élève au carré les congruences (1) et (2) et si l'on supprime les termes où est en facteur le nombre M supposé premier, on obtient (en tenant compte pour la congruence (2) de ce que la congruence $2^{\frac{M-1}{2}} \equiv 1 \pmod{M}$ est vérifiée du moment que $\frac{M-1}{2}$ est de la forme $4h + 3$) les conditions nécessaires suivantes :

$$(1') \qquad (1 + 2^n)^{\frac{M-1}{2}} + 1 \equiv 0 \pmod{M}.$$

$$(2') \qquad (1 + 2\nu^2)^{\frac{M-1}{2}} + 1 \equiv 0 \pmod{M}.$$

Autrement dit :

THÉORÈME III. — *Si* $M = 2^m - 1$ *est premier, les nombres* $(1 + 2^n)$ *et* $(1 + 2\nu^2)$ *sont des non-restes quadratiques de* M.

Ou, sous une autre forme :

Si M est premier, il divise les nombres

$$\frac{(1 + 2^n)^{\frac{M-1}{2}} + 1}{2(1 + 2^{n-1})} \quad \text{et} \quad \frac{(1 + 2\nu^2)^{\frac{M-1}{2}} + 1}{2(1 + \nu^2)}.$$

On obtiendra divers énoncés particuliers en particularisant n ou ν comme on l'a indiqué précédemment (n^{os} 2 et 3).

5. Nous allons maintenant déduire de la congruence (1') un critérium de primalité pour le nombre $F = 1 + 2^n$.

Si ce nombre F *est premier*, on a en effet, en vertu de la loi de réciprocité

$$M^{\frac{F-1}{2}} + 1 \equiv 0 \pmod{F}. \tag{6}$$

Autrement dit :

THÉORÈME IV. — *Si* $F = 1 + 2^n$ *est premier, tout nombre premier* $M = 2^m - 1$ (*avec* $m = 1 + 2n + 4nq$) *est un non-reste quadratique de* F, *et par suite, comme l'on sait, une racine primitive de* F.

D'ailleurs inversement s'il existe un nombre M (même non premier) tel que F divise $M^{\frac{F-1}{2}} + 1$, il en résulte évidemment que le nombre F divise $M^{F-1} - 1$, mais qu'il ne divise aucun nombre de la forme $M^{\lambda} - 1$, où λ est un diviseur de $F - 1$. Or, d'après la Réciproque du Théorème de Fermat due à Ed. Lucas, si un nombre jouit d'une telle propriété, il est premier. D'où cette proposition.

THÉORÈME V. — *Pour que le nombre* $F = 1 + 2^n$ *soit premier, il faut que,* $M = 2^{1+2n+4nq} - 1$ *étant premier, on ait*

$$M^{\frac{F-1}{2}} + 1 \equiv 0 \pmod{F}$$

et cela suffit (même si M n'est pas premier).