2

ÉTUDE

Les nombres de Fermat

par Jean DE BIASI, Université Paul Sabatier, Toulouse.

Ce sont les nombres F_n de la forme $2^{(2^n)} + 1$ où n est un naturel quelconque. Fermat les croyait tous premiers, Euler lui a prouvé le contraire en montrant que F_5 est divisible par 641 ; actuellement, on sait que 46 de ces nombres sont composés (le plus grand d'entre eux étant F_{1945}) et on conjecture que pour tout $n \geqslant 5$, F_n est composé (problème toujours ouvert !).

Nous présentons ici une étude élémentaire non exhaustive de ces nombres. (Sauf mention contraire tous les nombres considérés sont des naturels).

1. Pourquoi étudier ces nombres ?

Théorème 1 : *Si $a^m + 1$ est premier, m est une puissance de 2.*

En effet, si m n'est pas une puissance de 2, m admet au moins un diviseur impair $d \geqslant 3$ et par suite :

$$a^m+1 = a^{dq}+1 = (a^q)^d+1 = (a^q+1)(a^{q(d-1)} - a^{q(d-2)}...+1)$$

(en vertu de l'identité
$x^d + 1 = (x+1)(x^{d-1}-x^{d-2}+x^{d-3}+...+1)$ valable par tout d impair) et $a^m + 1$ est composé.

Ainsi $a^m + 1$ ne peut être premier que si m est de la forme 2^n, $n \in \mathbf{N}$. Il paraît donc naturel d'étudier les plus simples de ces nombres c'est-à-dire ceux qui correspondent à $a = 2$ et en

particulier de se demander si réciproquement les nombres $2^{(2^n)} + 1$ ne seraient pas tous premiers.

Ce que fit *Fermat*.

2. Pourquoi Fermat croyait ses nombres premiers ?

Théorème 2 : *Quel que soit* $n \in \mathbb{N}$, F_n *divise* $2^{F_n} - 2$

Comme pour tout $n \in \mathbb{N}$, $n + 1 \leqslant 2^n$ alors $2^{n+1} \mid 2^{(2^n)}$ et comme par ailleurs pour tout $k \in \mathbb{N}$, $x - 1 \mid x^k - 1$ on a :

$$F_n \mid (2^{(2^n)} + 1)(2^{(2^n)} - 1) = 2^{(2^{n+1})} - 1 \mid 2(2^{2^{(2^n)}} - 1) = 2^{F_n} - 2$$

(Le symbole "a | b" est utilisé pour "a divise b").

Le "théorème" chinois : *Si* m *divise* $2^m - 2$ *alors* m *est premier.*

Ce résultat est *faux* comme le montre l'exemple $m = 341$.
(341 n'est pas premier puisque $341 = 11 \times 31$).

$$2^{341} - 2 = (2^5)^{68} \cdot 2 - 2 \equiv (-1)^{68} \cdot 2 - 2 = 0 \ [11]$$

d'où $2^{341} - 2 \equiv 0 \ [341]$

$$2^{341} - 2 = (2^5)^{68} \cdot 2 - 2 \equiv (-1)^{68} \cdot 2 - 2 = 0 \ [31]$$

mais comme il est vrai pour tous les naturels inférieurs à 341 on l'a longtemps cru vrai (*Fermat* en particulier d'où sa conjecture : "Tous mes nombres sont premiers").

Cela est vrai pour

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537$$

mais il est faux pour F_5 qui est divisible par 641 comme le montra *Euler*. Voici une démonstration relativement simple de ce résultat historique :

$$641 = 5^4 + 2^4 \mid 2^{28}(5^4 + 2^4) = 2^{32} + 5^4 \cdot 2^{28}$$

$$641 = 5 \cdot 2^7 + 1 \mid (5 \cdot 2^7 + 1)(5 \cdot 2^7 - 1) = 5^2 \cdot 2^{14} - 1 \mid (5^2 \cdot 2^{14} - 1)(5^2 \cdot 2^{14} + 1) = 5^4 \cdot 2^{28} - 1,$$

d'où $\quad 641 \mid 2^{32} + 5^4 \cdot 2^{28} - (5^4 \cdot 2^{28} - 1) = F_5$.

(*Remarques* : Le résultat : "si m est premier m divise $2^m - 2$" est vrai et découle du petit théorème de *Fermat* (voir plus loin). Les nombres m qui divisent $2^m - 2$ sont appelés nombres pseudo-premiers).

Mais pourquoi penser à 641 comme diviseur possible de F_5 ? En étudiant la question suivante :

3. Quels sont les diviseurs possibles des nombres de Fermat ?

La réponse ne peut être apportée qu'après avoir rappelé quelques résultats.

Théorème 3 : *Si $\varphi(n)$ représente le nombre des entiers naturels inférieurs à n et premiers avec n et si a est un naturel premier avec n alors $a^{\varphi(n)} - 1 \equiv 0\ [n]$.*

(Ce théorème est dû à *Euler* et $\varphi(n)$ est appelé indicateur (ou indicatrice) d'Euler de n — voir (V)).

En effet, dans $\mathbb{Z}/_{n\mathbb{Z}}$ la classe de a appartient au groupe des éléments inversibles, groupe d'ordre $\varphi(n)$.

(*Remarque* : un cas particulier du résultat précédent est le *petit théorème de Fermat* obtenu pour n premier ; dans ce cas $\varphi(n) = n-1$ et par suite : *si n est premier et ne divise pas a, alors $a^{n-1} - 1 \equiv 0\ [n]$*).

Théorème 4 : *Si $(a \wedge n) = 1$ la congruence $a^x - 1 \equiv 0\ [n]$ a une infinité de solutions : ce sont tous les nombres $k\delta$ où $k \in \mathbb{N}$ et δ est la plus petite solution.*

($a \wedge n$ est le PGCD de a et n).

δ est l'ordre de la classe de a dans le groupe des éléments inversibles de $\mathbb{Z}/_{n\mathbb{Z}}$.

Comme $\varphi(n)$ est une solution de cette congruence, il vient le

Corollaire : *La plus petite des solutions naturelles de la congruence $a^x - 1 \equiv 0\ [n]$ est un diviseur de l'indicateur d'Euler $\varphi(n)$ de n.*

Théorème 5 : *Soit a un nombre pair et n un naturel quelconque. Si p est un nombre premier divisant $a^{(2^n)} + 1$ alors p est de la forme $2^{n+1} . k+1$.*

Comme $p \mid a^{(2^n)} + 1$, p divise $a^{(2^{n+1})} - 1 = (a^{(2^n)}+1)(a^{(2^n)}-1)$ mais p ne peut pas diviser $a^{(2^n)}-1$ car sinon il diviserait $a^{(2^n)}+1-(a^{(2^n)}-1) = 2$, par suite p serait égal à 2 ce qui est impossible puisque pour a pair $a^{(2^n)} + 1$ est impair. Si δ est alors la plus petite solution de $a^x - 1 \equiv 0\ [p]$ dont une solution est $x = 2^{n+1}$, on a $\delta \mid 2^{n+1}$.

Mais comme $\delta = 2^n$ ou $\delta < 2^n$ est impossible, on a donc $\delta = 2^{n+1}$. Le théorème de Fermat implique alors $a^{p-1} - 1 \equiv 0 \,[p]$ d'où $\delta \mid p-1$, soit $2^{n+1} \mid p-1$, et enfin $p = 2^{n+1} k + 1$.

Ainsi, pour F_5 les diviseurs premiers éventuels sont de la forme $64k + 1$ et $641 = 64.10 + 1$. Mais il est possible de limiter encore les recherches en améliorant le résultat précédent grâce au

Théorème 6 : *Pour $n > 1$ tout diviseur du nombre F_n est de la forme $2^{n+2} k+1$, $k \in \mathbb{N}$.*

Il suffit de démontrer ce résultat pour les diviseurs premiers de F_n car un diviseur quelconque de F_n est un produit de diviseurs premiers et

$$(2^{n+2}k+1)(2^{n+2}k'+1) = 2^{n+2}(2^{n+2}k+2^{n+2}k'+k+k')+1 = 2^{n+2}k''+1$$

Soit alors p un diviseur premier de F_n.

La démonstration du théorème 5 dans le cas $a = 2$ montre que 2^{n+1} est la plus petite solution dans N de la congruence $2^x - 1 \equiv 0 \,[p]$ et le théorème 5 lui-même montre que p est de la forme $2^{n+1} k + 1$. Si l'on suppose alors $n > 1$, p est donc de la forme $8q + 1$.

Considérons alors la suite de nombres $(1, 2, \ldots p-1) = S$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps (avec les opérations addition et multiplication), pour chaque $x \in S$ il existe $y \in S$ tel que $x \cdot y \equiv 2 \,[p]$ et il est immédiat que $x_1 \neq x_2$ implique $y_1 \neq y_2$.

Peut-on avoir $x = y$, c'est-à-dire existe-t-il $x \in S$ tel que $x^2 \equiv 2 \,[p]$?

Si la réponse est affirmative, on dira que 2 est un *résidu quadratique* modulo p.

Remarquons d'abord que si un tel x existe, $p - x$ est aussi de ce type puisque $(p-x)^2 \equiv x^2 \,[p]$ et ensuite qu'il n'y en a pas d'autres puisque pour tout z de ce type, on aurait $x^2 \equiv z^2 \,[p]$ d'où $p \mid (x-z)(x+z)$ et comme $x, z \in S$ les seules possibilités sont $z = x$ et $z = p - x$.

Donnons alors le résultat suivant, dont la démonstration, un peu savante, est seulement esquissée :

Proposition 1 : *Pour tout p premier de la forme $8q \pm 1$, 2 est un résidu quadratique modulo p.*

[Soient F_p le corps(commutatif) $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ et F_p^* le groupe multiplicatif de F_p, F_p^* est un groupe d'ordre p−1 et par suite, pour tout $x \in F_p^*$, $x^{p-1} = 1$; par ailleurs, dans F_p, $(a+b)^p = a^p + b^p$.

Admettons de plus que pour tout corps commutatif K, il existe un *corps algébriquement clos* Ω_K *appelé clôture algébrique de* K, tel que K soit isomorphe à un sous-corps de Ω_K (Ω_K joue pour K un rôle analogue à celui de C pour R). En particulier, dans $\Omega_K{}^*$ tout élément de $\Omega_K{}^*$ a n racines n-èmes si n n'est pas un multiple de p. Ces racines constituent un groupe cyclique G ; si α engendre G, on dit que α est une racine n-ème primitive.

Soit $x \in F_p^*$ et soit $y \in \Omega^*{}_{F_p} = \Omega^*$ tel que $s = y^2$. Puisque x^{p-1} on a $x^{\frac{p-1}{2}} = \pm 1$ d'où $y^{p-1} = \pm 1$. La condition "x est un carré dans F_p^*" équivaut alors à $y \in F_p^*$, c'est-à-dire à $y^{p-1} = 1$, car F_p est dans Ω l'ensemble des racines du polynome $X^p - X$.

Prenons le cas $p \equiv \pm 1\ [8]$ et soit α une racine 8ème *primitive* de 1. On a donc $\alpha^4 = -1$ d'où $\alpha^2 + \alpha^{-2} = 0$, soit $(\alpha + \alpha^{-1})^2 = 2$. Si l'on pose alors $y = \alpha + \alpha^{-1}$, l'élément $y \in \Omega^*$ vérifie $y^2 = 2$. Mais comme $y^p = \alpha^p + \alpha^{-p}$, si $p = 8q \pm 1$, $\alpha^p = \alpha^{\pm 1}$, d'où $y^p = \alpha + \alpha^{-1} = y$ et comme $y \neq 0$, $y^{p-1} = 1$.

Ainsi pour $p = 8q \pm 1$, 2 est bien résidu quadratique modulo p.

Remarque 1 : On pourrait établir le résultat plus fort suivant

p premier	2 est un résidu
$p \equiv \pm 1\ [8]$	quadratique modulo p

en vérifiant que pour $p \equiv \pm 3\ [8]$ l'élément $y = \alpha + \alpha^{-1}$ est tel que $y^2 = 2$ et $y^p = -y$.

Remarque 2 : Cette démonstration est inspirée de (IV) ; celle de (V) est plus élémentaire mais bien plus longue.]

Dans le cas présent, 2 est donc résidu quadratique modulo p. Par suite, dans δ tous les éléments sauf deux de la forme x, p − x avec $x^2 \equiv 2\ [p]$ peuvent être groupés par paires du type $[x_i, y_i]$ avec $x_i . y_i \equiv 2\ [p]$. Comme il y a $\frac{p-1}{2} - 1$ paires de cette

forme, on en conclut que :

$$(p-1)\,! \equiv 2^{\frac{p-1}{2}-1} \cdot x\,(p-x) \equiv -2^{\frac{p-1}{2}} \;[p]$$

or, d'après le théorème de *Wilson*, on sait que pour tout nombre premier p, (p—1) ! est congru à — 1 modulo p d'où :

$$(p-1)\,! \equiv -1\;[p] \text{ qui, avec } (p-1)\,! \equiv -2^{\frac{p-1}{2}}\;[p],$$

$$\text{donne } \quad 2^{\frac{p-1}{2}} - 1 \equiv 0\;[p].$$

$\frac{p-1}{2}$ est donc une solution de la congruence $2^x - 1 \equiv 0\;[p]$, mais comme 2^{n+1} est la plus petite de ces solutions dans N, le théorème 4 permet d'écrire :

$$2^{n+1} \mid \frac{p-1}{2} \text{ d'où } 2^{n+2} \mid p-1 \text{ soit enfin } p = 2^{n+2}k + 1.$$

Applications

- *$F_4 = 2^{(2^4)} + 1$ est-il premier ?*

Les diviseurs premiers éventuels sont du type 64k + 1 et il suffit d'essayer ceux qui sont inférieurs à $\sqrt{F_4}$, c'est-à-dire inférieurs à 2^8. Le seul vérifiant ces conditions est 193 et comme $F_4^4 = 65537$ n'est pas divisible par 193, *F_4 est premier.*

- *$F_5 = 2^{(2^5)} + 1$ est-il premier ?*

Les diviseurs premiers éventuels sont du type 128k + 1 et les deux premiers s'obtiennent pour k = 2 (257) et k = 5 (641). On démontre alors que 641 | F_5 et par suite *F_5 est composé.* En fait, $F_5 = 641.6700417$, ces deux facteurs étant premiers.

- *$F_6 = 2^{(2^6)} + 1$ est-il premier ?*

Les diviseurs premiers éventuels sont de la forme 256k + 1 et le premier à convenir est obtenu pour k = 1071 et vaut 274177. Ainsi, *F_6 est composé* (Résultat dû à Landry en 1880) et est, comme F_5, produit de 2 nombres premiers.

Remarque : Le théorème 6 ne permet à lui tout seul de répondre à la question :

"F_n est-il premier ou non ?" que si le diviseur à étudier, de la forme 2^{n+2} k + 1 ne correspond pas à k trop grand. Par exemple, pour F_7 et F_8, malgré de nombreuses tentatives, on n'a pas encore réussi à trouver des facteurs premiers de ce nombre, cependant,

Morehead et Western ont démontré en 1909 qu'il était composé. Leur preuve utilise, pour la démonstration, le résultat suivant (voir (V)) :

Proposition 2 : *(F_n premier)* $3^{\frac{F_n-1}{2}} + 1 \equiv 0\ [F_n]$

qui permet, grâce à l'introduction des nombres r_i suivants :

$$r_1 = 3\ ,\quad r_{i+1} = \overline{r_i^2} \qquad i = 1, 2, \ldots$$

(où d'une façon générale, $\overline{r}$ désigne le reste de la division de F_n par r) pour lesquels une récurrence immédiate montre que F_n divise :

$$3^{(2^{i-1})} - r_i$$

quel que soit i ce qui pour $i = 2^n$ montre que $F_n \mid 3^{\frac{F_n-1}{2}} - r_{2^n}$ soit $3^{\frac{F_n-1}{2}} + 1 \equiv r_{2^n+1}\ [F_n]$ de se ramener à l'étude des congruences $r_i + 1 \equiv 0\ [F_n]$ pour i variant de 1 à 2^n. Pour F_7 cela exige le calcul de 128 carrés de nombres d'au plus 39 chiffres puis la division de ces carrés par F_7 lequel a 39 chiffres. Certaines calculatrices actuelles effectuent ces opérations sans difficulté mais ayons une pensée admirative pour ceux qui, au début du siècle, les effectuèrent "à la main".

4. Comment a-t-on pu établir que F_{1945} est composé ?

(Ce nombre s'écrit en base dix avec plus de 10^{582} chiffres !)

Ses diviseurs premiers possibles sont de la forme $2^{1947}\,k + 1$ mais pour $k = 1$, $2^{1947} + 1$ est divisible par 3 et donc composé, pour $k = 2$, $2^{1948} + 1 = (2^4)^{487} + 1$ est divisible par $2^4 + 1$, donc composé, pour $k = 3$, $2^{1947}.3 + 1$ est $\equiv 0\ [5]$ (car $2^4 \equiv 1\ [5]$ d'où

$$2^{1947} \cdot 3 + 1 \equiv (2^4)^{486} \cdot 2^3 \cdot 3 + 1 \equiv 2^3 \cdot 3 + 1 \equiv 0\ [5]$$

donc composé, pour $k = 4$, $2^{1947}.4 + 1 = 2^{1949} + 1$ est divisible par 3 donc composé.

Le premier diviseur premier possible est donc $2^{1947}.5 + 1$ (qui s'écrit avec 587 chiffres !). Mais diviser F_{1945} par $2^{1947}.5 + 1$ ne paraît pas réalisable.

Introduisons alors les nombres r_i, $i = 1, 2, 3 \ldots$ définis par $r_1 = 2^2$, $r_2 = \overline{r_1^2}$, ..., $r_{i+1} = \overline{r_i^2}$, ... où r_i^2 désigne le reste de la

division de r_i^2 par $m = 2^{1947}.5 + 1$. Un raisonnement par récurrence, élémentaire, montre alors que m divise $2^{(2^i)} - r_i$ pour tout $i = 1, 2, \ldots$ D'où :

$$m = 2^{1947}.5+1 \mid F_{1945} - r_{1945} - 1$$

et $F_{1945} \equiv r_{1945} + 1 \ [2^{1947}.5 + 1]$

Pour voir si m divise F_{1945}, il "suffit" donc de former la suite des nombres r_i, $1 \leqslant i \leqslant 1945$, chacun d'eux ayant moins de 587 chiffres (ce qui au passage nécessite le calcul de leurs carrés lesquels ont moins de 1175 chiffres). Certaines machines actuelles sont capables d'effectuer ces calculs et elles ont conclu par l'affirmative :

$2^{1947}.5 + 1$ divise F_{1945} donc F_{1945} est composé !

Pour les amateurs, signalons que F_{17} (lequel s'écrit avec environ 39000 chiffres) est le plus petit nombre de Fermat dont on ignore encore s'il est premier ou non.

Bibliographie

L'essentiel de cet article est tiré de (V) dont nous recommandons la lecture.

(I) ITARD (J), *Arithmétique et théorie des nombres* (Que sais-je ? , n° 1093)

(II) ITARD (J), *Les nombres premiers* (Que sais-je ? , n° 571)

(III) HALLYBURTON and BRILLHART, *Mathematics of computation*, n° 129, janvier 1975.

(IV) SERRE (J.P.), *Cours d'arithmétique* (PUF)

(V) SIERPINSKI (W), *Elementary theory of Numbers* (Varsovie, 1964).

Tables extraites de Mathematics of computation par Hallyburton and Brillhart
Volume 29, n° 129, janvier 1975, pages 109 et 112

Facteurs de F_m, $5 \leqslant m \leqslant 22$

m	Facteurs premiers	Date	Découverts par :
5	641	1732	Euler
5	6700417	1732	Euler
6	274177	1880	Landry
6	67280421310721	1880	Landry, LeLasseur, Gérardin
7	59649589127417217	1970	Morrison, Brillhart
7	5704689200635129054721	1970	Morrison, Brillhart
8	c	1909	Morehead, Wertern
9	2424833	1903	Western
9	c*	1967	Brillhart
10	45592577	1953	Selfridge
10	6487031809	1962	Brillhart
10	c*	1967	Brillhart
11	319489	1899	Cunningham
11	974849	1899	Cunningham
12	114689	1877	Lucas, Pervouchine
12	26017793	1903	Western
12	63766529	1903	Western
12	190274191361	1974	Hallyburton, Brillhart
13	2710954639361	1974	Hallyburton, Brillhart
14	c	1961	Selfridge, Hurwitz
15	1214251009	1925	Kraitchik
16	825753601	1953	Selfridge
17	?		
18	13631489	1903	Western
19	70525124609	1962	Riesel
19	646730219521	1963	Wrathall
20	?		
21	448529642913	1963	Wrathall
22	?		

? Nature de F_m inconnue
c Nombre composé

Connaissances actuelles

m	Nature de F_m
0, 1, 2, 3, 4	Premier
5, 6, 7	Composé et complètement factorisé
16+, 11, 12*, 19, 30, 38	Deux ou quatre* facteurs connus (+ cofacteur est composé)
9+, 13, 15, 16, 18, 21, 23, 25, 26, 27, 32, 36, 39, 42, 52, 56, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 250, 267, 268, 284, 316, 452, 1945	seulement un facteur premier connu
8, 14	Composé mais pas de facteur connu
17, 20, 22, 24, 28, 29, 31, etc.	Nature inconnue