Les Nombres de Fermat

Résumé

Ce document traite des principales propriétés des nombres de la forme $F_n = 2^{2^n} + 1$, appelés Nombre de Fermat. Des conseils, des suggestions? N'hésitez pas à laisser un message : <*lhooq4me@yahoo.fr*>

Table des matières

1 Introduction

1.1 Un peu d'histoire ...

Pierre de Fermat, homme de loi et conseiller au Parlement de Toulouse[1], postula en 1640 dans un courrier à son ami Bernard Frenicle de Bessy[2], et

1. Les mathématiques, et en particulier l'arithmétique, constituaient en effet plus un loisir qu'un métier, et la frontière entre «amateur» et «professionnel», notions pour le moins relatives, n'était pas encore tracée.

2. Mathématicien français, membre de la première Académie des Sciences.

cela au regard de certains résultats, que tout nombre de la forme $F_n = 2^{2^n}+1$, avec n entier naturel, était premier.

Ne réussissant pas à démontrer ce résultat, il proposa ce problème difficile à Blaise Pascal, accompagné du commentaire du suivant :

> « Je ne vous demanderais pas de travailler à cette question si j'avais pu la résoudre moi-même »

Ce dernier ne s'y intéressant guère, il soumit également cette question à Lord William Brouncker et John Wallis[3], en vain... Et pour cause : la conjecture de Fermat était fausse.

Ce fut le mathématicien Leonhard Euler qui, en proposant une factorisation de F_5, démontra que Fermat s'était trompé[4]. Et pourtant l'espoir était là d'avoir enfin trouvé une suite d'entier dont les termes décrivent une partie de la suite infinie des nombres premiers.

1.2 Pourquoi $2^{2^n}+1$?

Avant tout, posons-nous la question : pourquoi ces nombres-ci et pas d'autres ?

L'intérêt porté à ces nombres résulte avant tout de l'attention accordée aux critères de primalité des nombres de la forme $a^m + 1$ résumés dans le théorème suivant :

Théorème 1.2.1 *Tout nombre premier de la forme $a^m + 1$ vérifiant $a > 1$ et $m > 1$ est de la forme $a^{2^n} + 1$ et l'entier a est pair.*

Démonstration : Supposons en effet que m ne soit pas une une puissance de deux, alors m admet un diviseur impair $q \geq 3$, et donc :

$$a^m + 1 = a^{qk} + 1 = (a^k)^q - (-1)^q, k \in \mathbb{N}$$

Or, d'après la formule du binôme[5], cette expression se factorise de la façon suivante :

$$(a^k)^q - (-1)^q = (a^k + 1)((a^k)^{q-1} - (a^k)^{q-2} + \cdots + 1) \qquad (1)$$

3. Mathématiciens anglais. Wallis contribua énormément au développement du calcul différenciel, et est considéré à ce titre comme un des mathématiciens les plus influents avant Newton.

4. Il est à noter qu'à ce jour, il s'agit de la seule conjecture de Fermat qui se soit avérée fausse.

5. $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}), n \in \mathbb{N}$.

On déduit du résultat (1) que $a^m + 1$ admet $a^k + 1$ comme diviseur. Celui-ci n'étant ni égal à 1 ($a > 1$, donc $a^k + 1 > 2$), ni égal à $a^m + 1$ (dans ce cas là, nous aurions alors $q = 1$, contraire à l'hypothèse sur q), l'entier $a^m + 1$ n'est donc pas premier. *m est donc une puissance de deux.*
Et compte-tenu des hypothèses sur a et m, il est clair que $a^m + 1$ est un nombre premier impair, et que donc a^m est un nombre pair, ce qui revient à dire que *a est pair.*

Cqfd

Les éventuels nombres premiers de la forme $a^m + 1$ sont donc à chercher dans les listes de type $a^{2^n} + 1$ avec a pair et n entier naturel. Or, il s'avère que pour $a = 2$, les 5 premiers termes de la suite $F_n = 2^{2^n} + 1$ sont premiers :

n	F_n
0	3
1	5
2	17
3	257
4	65537

TAB. 1 – *Les 5 premiers Nombres de Fermat*

Seulement voilà : à l'image de $F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$, les termes de cette suite deviennent rapidement énorme ce qui rend quasiment impossible la vérification par le calcul commun du fait qu'il soit premier. Aussi l'hypothèse de Fermat reposa-t-elle uniquement sur les 5 premiers termes, et probablement aussi sur la difficulté à trouver un diviseur à des termes plus grand.

2 Des diviseurs premiers particuliers

Après avoir évoqué les relations existant entre les Nombres de Fermat, nous aborderons dans cette section le résultat qui permit à Euler de montrer que F_5 n'était pas premier.

2.1 Sur la relation entre deux Nombres de Fermat consécutifs

Lemme *Etant donné $n \in \mathbb{N}$, $F_{n+1} = (F_n - 1)^2 + 1$.*

Ph.B.

Démonstration : Etant donné $n \in \mathbb{N}$, on a :

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

Cqfd

2.2 Sur la relation entre deux nombres de Fermat distincts

Démontrons avant tout le lemme suivant :

Lemme *Etant donné $n \geq 1, n \in \mathbb{N}$, on a $F_n - 2 = \prod_{k=0}^{n-1} F_k$*

Démonstration : Démontrons ce résultat par récurrence. Pour $n = 1$, nous avons $F_1 - 2 = 3 = F_0$, donc vrai pour $n = 1$
Etant donné un entier naturel $m \geq 1$, supposons la proposition vraie au rang m, et montrons que celle-ci est vraie au rang $m + 1$. D'après le lemme précédent, nous avons :

$$F_{m+1} - 2 = [(F_m - 1)^2 + 1] - 2 = (F_m - 1)^2 - 1 = F_m(F_m - 2)$$

Ce qui d'après l'hypothèse de récurence nous donne :

$$F_{m+1} - 2 = F_m \prod_{k=0}^{m-1} F_k = \prod_{k=0}^{k=m} F_k$$

Cqfd

Ce lemme nous permet alors d'introduire un résultat intéressanrt :

Théorème 2.2.1 *Soient $m, n > 0$ deux entier naturels distincts . Alors F_m et F_n sont premiers entre eux.*

Démonstration : Nous supposons ici $n > m$ (la démonstration est identique dans le cas $m > n$).
D'après le corollaire précédent, nous avons :

$$F_n - 2 = F_m(\prod_{k=0}^{m-1} F_k)(\prod_{k=m+1}^{n-1} F_k)$$

Soit :

$$F_n = qF_m + 2, q \in \mathbb{Z}$$

Ph.B.

Soit $d = PGCD(F_m, F_n)$. 2 étant le reste dans la division euclidienne de F_n par F_m, on a[6]:

$$d = PGCD(F_m, 2)$$

Les seuls diviseurs positifs de 2 étant 1 et 2, on a donc $PGCD(F_m, 2) = 1$, puisque F_m ne peut être pair. Soit :

$$PGCD(F_m, F_n) = 1.$$

Cqfd

2.3 Sur la forme d'un diviseur premier de F_n

Nous désignons pour le résultat suivant a comme étant un entier et p un nombre premier ne divisant pas a. On suppose alors qu'il existe au moins un entier naturel k non nul tel que $a^k \equiv 1[p]$, et définissons k_0 comme étant le plus petit d'entre eux.

Lemme *Tout entier naturel k est un multiple de k_0.*

Démonstration : Supposons que k ne soit pas un multiple de k_0. Il existe alors $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $k = qk_0 + r, 0 < r < k_0$

$$a^{qk_0+r} \equiv 1[p] \tag{2}$$

De plus :

$$a^{k_0} \equiv 1[p] \Rightarrow a^{qk_0} \equiv 1[p] \Rightarrow a^{qk_0+r} \equiv a^r[p] \tag{3}$$

Nous avons donc d'après (2) et (3) :

$$a^r \equiv 1[p]$$

Or ce dernier résultat contredit l'hypothèse selon laquelle k_0 est le plus petit entier à vérifier cette propriété.
On a donc bien $r = 0$

Cqfd

Ce résultat nous permet alors d'introduire ce théorème fondamental :

Théorème 2.3.1 *Soit p un diviseur premier de F_n tel que $p \neq F_n$. Alors il existe un entier k tel que $p = 2^{n+1}k + 1$, k admettant un diviseur impair supérieur ou égal à 3.*

6. On montre en effet facilement que dans une division euclidienne, le PGCD du dividende et du diviseur est identique au PGCD du diviseur et du reste.

Démonstration : Sachant que p divise F_n, nous avons donc :

$$2^{2^n} + 1 \equiv 0[p] \Rightarrow 2^{2^n} \equiv -1[p] \Rightarrow 2^{2^{n+1}} \equiv 1[p]$$

Montrons alors que 2^{n+1} est le plus petit entier à vérifier cette relation. Soit m le plus petit entier à vérifier cette relation. Nous savons d'après le lemme précédent que m divise 2^{n+1}. Il existe donc un entier $q \leq n+1$ tel que $m = 2^q$.
Supposons alors $q < n+1$, ce qui équivaut à dire que $q \leq n$. Il existe alors un entier $h \geq 0$ tel que $n = q + h$.

$$2^{2^q} \equiv 1[p] \Rightarrow 2^{2^{q+h}} \equiv 1[p] \Rightarrow 2^{2^n} \equiv 1[p]$$

Or cela contredit le fait que nous avons $2^{2^n} \equiv -1[p]$. L'hypothèse $q < n+1$ est donc fausse, ce qui implique $q = n+1$. 2^{n+1} *est bien le plus petit entier à vérifier la relation précédente.*

Montrons ensuite que $p-1$ vérifie la relation $2^{p-1} \equiv 1[p]$. Nous savons d'après le petit théorème de Fermat [7] que $2^p \equiv 2[p]$. Il existe donc un entier q tel que $2^p - 2 = pq$, soit $2(2^{p-1} - 1) = pq$. On en déduit d'après le théorème de Gauss que p divise $2^{p-1} - 1$, soit :

$$2^{p-1} \equiv 1[p]$$

Compte-tenu de ces deux résultats, nous déduisons du lemme précédent que $p-1$ est un multiple de 2^{n+1}. Il existe donc un entier k tel que :

$$p = 2^{n+1}k + 1$$

Reste à montrer que k admet un diviseur impair supérieur ou égal à 3. Raisonnons par l'absurde et supposons que k soit une puissance de 2. Dans ce cas-là, nous avons $p = 1 + 2^m$ avec m entier naturel non nul. Sachant que p est premier, nous déduisons du théorème (1.2.1) que m est nécessairement une puissance de deux, ce qui fait tout simplement de p un Nombre de Fermat. Sachant de plus que p est distinct de F_n on en déduit d'après le 2.2.1 que p est premier avec F_n, ce qui contredit le fait que p est un diviseur de F_n. k *admet bien un diviseur impair superieur ou égal à 3.*

Cqfd

7. Etant donnés un entier a et un nombre premier p tel que p ne divise pas a, alors $a^p \equiv a[p]$.

Ph.B.

3 Euler, F_5, et les autres ...

3.1 Sur les diviseurs de F_5

Nous connaissons désormais la forme d'un diviseur premier de F_n. Intéressons nous alors au cas de $F_5 = 2^{32} + 1$. Supposons que F_5 admette un diviseur premier p. Nous savons alors d'après le théorème (2.3.1) qu'il existe un entier k tel que $p = 2^6k + 1 = 64k + 1$. Les diviseurs premiers potentiels de F_5 sont donc de la forme $64k+1$, où k admet un diviseur impair ≥ 3. Les valeurs possibles de k sont donc $3, 5, 6, 7, 9 \ldots$.

Pour $k = 10$ il s'avère que nous avons $p = 641$ qui est un nombre premier. Maintenant que nous avons un candidat, voyons si celui-ci correspond à nos attentes :

$$2^{16} = 65536 = 641 \times 102 + 154 \equiv 154[641]$$

Soit

$$2^{32} \equiv 154^2 = 23716 = (641 \times 36 + 640) \equiv -1[641]$$

Donc :

$$2^{32} + 1 \equiv 0[641]$$

F_5 admet donc bien un diviseur premier différent de lui-même, ce qui dans le même temps infirme la conjecture de Fermat.

3.2 ... $F_{723}, F_{724}\, F_{725}$...

Il faut attendre plus d' un siècle pour qu'un mathématicien du nom de Landry, qui factorise alors beaucoup de nombre de la forme $2^n + 1$ et $2^n - 1$, démontre que F_6 est le produit de deux nombres premiers, à savoir 277 177 et 67 280 421 310 721, alors que l'on avait déjà découvert que F_{12} était divisible par $7\times2^{14}+1$. Les Nombres de Fermat, tout comme les Nombres de Mersenne, constituent dès lors un terrain d'entraînement idéal pour les tests de primalité et les méthodes de factorisation[8], ce qui dans le même temps tend à montrer que Fermat s'est probablement entièrement trompé, étant donné qu'il ne semble plus y avoir de nombre premier au delà de F_4.

8. Aujourd'hui encore, ces nombres continuent à faire l'objet de recherche. C'est ainsi que F_7 a été factorisé en 1970, alors que l'on trouva un diviseur premier de F_8 en 1981 seulement.

Ph.B.

3.3 Le chiffre des unités

A tout cela s'ajoute une propriété singulière :

Lemme *Pour $n \geq 2$, le chiffre des unité de F_n vaut 7.*

Démonstration : Pour $n = 2$, le résultat est évident.
Soit un entier naturel k. Supposons la propriété vraie au rang k, et montrons celle-ci au rang $k + 1$.
D'après l'hypothèse de récurrence, nous avons :

$$F_k \equiv 7[10] \Rightarrow F_k - 1 \equiv 6[10] \Rightarrow (F_k - 1)^2 + 1 \equiv 37 \equiv 7[10]$$

On en déduit d'après le lemme précédent que :

$$F_{k+1} \equiv 7[10]$$

Sachant qu'un nombre est congru au chiffre des ses unités modulo dix[9], on en déduit que 7 est le chiffre des unités de F_n pour $n \geq 2$.

Cqfd

9. Un entier ≥ 10 auquel on ôte le chiffre des unités est en effet un multiple de 10.