Nombres de Fermat, nombres de Mersenne et nombres parfaits

I Rappel sur les nombres premiers

Un nombre entier naturel premier est un nombre qui admet exactement deux diviseurs distincts, un et lui-même.

Exemples : 2, 3, 5, 7, 11, 13, 17, 19, 23,…

Il existe une infinité de nombres premiers.

Si un nombre est premier et strictement supérieur à 2, alors son chiffre des unités est soit 1,3,7 ou 9 car il n'est divisible ni par 2, ni par 5.

Petit théorème de Fermat :

Si p est un nombre premier qui ne divise pas un entier naturel a, alors :

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

Autre propriété :

Si il existe un plus petite entier naturel non nul m tel que

$$\boldsymbol{a^m \equiv 1\ [p]}$$

alors, pour tout entier naturel k :

$$\boldsymbol{a^k \equiv 1\ [p] \Leftrightarrow \exists\, q \in \mathbb{N} : k = m\,q}$$

Preuve :

Supposons :

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

Effectuons une division euclidienne de k par m :

$$k = m\,q + r, \qquad 0 \leq r < m$$

Alors :

$$(a^m)^q\ a^r \equiv 1\ [p]$$

Donc :

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

Donc :

$$r = 0$$

Ainsi k est multiple de m.

Réciproquement, supposons :

$$\exists\, q \in \mathbb{N} : k = m\, q$$

Alors :

$$a^k = (a^m)^q \equiv 1\ [p]$$

II Nombres de forme particulière

Soit a et m deux nombres entiers naturels non nuls alors a divise a^m tout en étant distinct de 1 et de a^m. Donc a^m n'est pas premier. Afin de déterminer des nombres premiers particuliers, on est donc amené à s'intéresser à des nombres de la forme $a^m + 1$ et $a^m - 1$. Les premiers ont été étudiés par Fermat et les seconds par Mersenne pour $a = 2$.

Voyons d'abord des conditions nécessaires pour que de tels nombres soient premiers :

Si $\boldsymbol{a^m + 1}$ est premier alors $\boldsymbol{m}$ est de la forme $\boldsymbol{2^n}$ où $\boldsymbol{n} \in \mathbb{N}$

Si $\boldsymbol{a^m - 1}$ est premier alors $\boldsymbol{m}$ est premier et $\boldsymbol{a = 2}$.

Preuves :

Supposons $a^m + 1$ premier avec $m = p\, q$, q impair. Alors :

$$a^m + 1 = (a^p)^q - (-1)^q = (a^p + 1) \sum_{k=0}^{q-1} (a^p)^{q-1-k}\, (-1)^k$$

Donc $a^p + 1$ divise $a^m + 1$ tout en étant distinct de 1 et de ce nombre. Cela contredit l'hypothèse.

Ainsi m n'a pas de diviseur impair donc est de la forme 2^n.

Supposons $a^m - 1$ premier. Alors, d'une part :

$$a^m - 1 = (a - 1) \sum_{k=0}^{m-1} a^k$$

Donc, si $a \neq 2$ alors $a - 1$ divise $a^m - 1$ tout en étant distinct de 1 et de ce nombre, ce qui contredit l'hypothèse. Ainsi $a = 2$.

D'autre part , supposons $m = p\, q$, q distinct de 1 et de m. Alors :

$$2^m - 1 = (2^p)^q - 1 = (2^p - 1) \sum_{k=0}^{q-1} (2^p)^k$$

Donc $2^p - 1$ divise $2^m - 1$ tout en étant différent de 1 et de ce nombre, ce qui contredit le caractère premier de $2^m - 1$. Ainsi m est premier.

III Nombres de Fermat

Définition :

Les nombres de Fermat sont, pour $n \in \mathbb{N}$, les nombres de la forme :

$$F_n = 2^{2^n} + 1$$

Les cinq premiers nombres de Fermat sont premiers, à savoir :

$$F_0 = 2^{2^0} + 1 = 3$$

$$F_1 = 2^{2^1} + 1 = 5$$

$$F_2 = 2^{2^2} + 1 = 17$$

$$F_3 = 2^{2^3} + 1 = 257$$

$$F_4 = 2^{2^4} + 1 = 65\,537$$

Mais pas le sixième, comme nous le verrons un peu plus loin.

$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

Propriétés des nombres de Fermat :

Pour tout $n \in \mathbb{N}$:

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

$$F_n - 2 = \prod_{k=0}^{n-1} F_k$$

Preuves :

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = \left(2^{2^n}\right)^2 - 1 = \left(2^{2^n} + 1\right)\left(2^{2^n} - 1\right) = F_n\,(F_n - 2)$$

Par récurrence triviale :

$$F_n - 2 = F_{n-1}\,(F_{n-1} - 2) = F_{n-1}\,F_{n-2}\,(F_{n-2} - 2) = F_{n-1}\,F_{n-2} \ldots F_0\,(F_0 - 2)$$

$$= F_{n-1}\,F_{n-2} \ldots F_0$$

Pour tout $(n, m) \in \mathbb{N}^2$:

Si $n > m$ **alors F_n et F_m sont premiers entre eux.**

Preuve :

$$F_n - 2 = F_0\,F_1 \ldots F_{m-1}\,F_m \ldots F_{n-1}$$

Donc, il existe un entier naturel q tel que :

$$F_n = q\,F_m + 2$$

Soit alors d un diviseur commun de F_n et F_m alors d divise 2 et $d \neq 2$ car 2 ne divise pas F_n donc $d = 1$ et F_n et F_m sont premiers entre eux.

Pour tout $\boldsymbol{n} \in \mathbb{N}$:

Si $\boldsymbol{p}$ est un diviseur premier de $\boldsymbol{F_n}$ distinct de $\boldsymbol{F_n}$ alors il existe un entier naturel $\boldsymbol{k}$ possédant un diviseur impair distinct de 1 tel que :

$$\boldsymbol{p = 2^{n+1}\, k + 1}$$

Cette propriété est utile pour déterminer si un nombre de Fermat est premier ou non comme nous le verrons plus loin.

Preuve :

Soit p un diviseur premier de F_n distinct de F_n. Alors :

$$F_n \equiv 0\ [p]$$

Donc :

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

D'où :

$$\left(2^{2^n}\right)^2 \equiv 1\ [p]$$

Soit :

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

soit alors m le plus petit entier naturel non nul tel que :

$$2^m \equiv 1\ [p]$$

Alors m est un diviseur de 2^{n+1} donc :

$$m = 2^q, \qquad q \leq n + 1$$

Supposons $q \leq n$ et posons :

$$r = n - q$$

Alors :

$$2^{2^n} = 2^{2^{q+r}} = \left(2^{2^q}\right)^{2^r} \equiv 1\ [p]$$

Ce qui contredit le fait :

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

Donc :

$$q = n + 1$$

Ainsi :

$$m = 2^{n+1}$$

Appliquons alors le petit théorème de Fermat :

p est premier et ne divise pas 2 donc :

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

Ainsi $p-1$ est multiple de 2^{n+1} donc il existe un entier naturel k tel que :

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

Supposons alors que k n'ait aucun diviseur impair distinct de 1, alors il est de la forme :

$$k = 2^s, \qquad s \in \mathbb{N}^*$$

Et :

$$p = 1 + 2^{n+s+1} = F_{n+s+1}$$

Or F_{n+s+1} est premier avec F_n. Donc p est premier avec F_n donc ne divise pas F_n, ce qui est absurde.

Donc k admet un diviseur impair.

Application :

Considérons le sixième nombre de Fermat :

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1$$

Soit p diviseur premier de F_5 alors il existe un entier naturel k ayant au moins un diviseur impair distinct de 1 tel que :

$$p = 2^6\ k + 1 = 64\ k + 1$$

Déterminons alors le premier nombre premier rencontré pour les valeurs de k ayant au moins un diviseur impair distinct de 1, qui sont :

$$k = 3, 5, 6, 7, 9, 10, \ldots.$$

Le premier nombre est :

$$64\ \times 3 + 1 = 193$$

Et il est premier. Or :

$$2^8 = 256 \equiv 63\ [193]$$

$$2^{16} \equiv 63^2 = 3969 \equiv 109\ [193]$$

$$2^{32} \equiv 109^2 \equiv 108\ [193]$$

$$2^{32} + 1 \equiv 109\ [193]$$

Donc 193 ne divise pas F_5

On recommence avec le nombre suivant et on constate que jusqu'à $k = 9$, les nombres p premiers obtenus ne divisent pas F_5.

En revanche, pour $k = 10$, le nombre $p = 641$ est bien premier et :

$$2^{16} = 65\ 536 \equiv 154\ [641]$$

$$2^{32} \equiv 154^2 = 23\,716 \equiv -1\ [641]$$

$$2^{32} + 1 \equiv 109\ [641]$$

Donc 641 divise F_5 qui n'est donc pas premier.

Remarque :

Pour $n \geq 2$ le chiffre des unités de F_n est 7.

Preuve : Par récurrence sur n.

Initialisation :

$$F_2 = 2^{2^2} + 1 = 17$$

Hérédité : supposons que le chiffre des unités soit 7 pour F_n pour une valeur de $n \geq 2$.

Alors :

$$F_n \equiv 7\ [10]$$

Donc :

$$F_n - 2 \equiv 5\ [10]$$

$$F_n\ (F_n - 2) \equiv 35 \equiv 5\ [10]$$

Soit :

$$F_{n+1} - 2 \equiv 5\ [10]$$

D'où :

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

le chiffre des unités de F_{n+1} est donc 7.

IV Nombres de Mersenne

Définition :

Les nombres de Mersenne sont, pour p entier naturel premier, les nombres de la forme :

$$M_p = 2^p - 1$$

On peut vérifier à l'aide d'un ordinateur que M_p est premier pour les valeurs de p suivantes : 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127. On en connait à ce jour 46.

Nombres parfaits :

Un nombre entier naturel est parfait s'il est la somme de tous ses diviseurs autres que lui-même.

Exemple : Le premier entier naturel parfait est 6 car ses diviseurs autres que lui-même sont 1,2,3 et :

$$1 + 2 + 3 = 6$$

Somme des diviseurs d'un nombre entier naturel

Définition de la fonction $s(n)$

Soit n un entier naturel non nul. Notons $s(n)$ la somme de ses diviseurs y compris lui-même.

Propriétés de la fonction $s(n)$

1) Si n est premier alors :

$$\boldsymbol{s(n) = n + 1}$$

2) Un nombre n est parfait si et seulement si $s(n) = 2\,n$

3) si p est premier et $r \in \mathbb{N}^*$:

$$\boldsymbol{s(p^r) = \frac{p^{r+1} - 1}{p - 1}}$$

4) Si n a pour décomposition en facteurs premiers :

$$\boldsymbol{n = \prod_{i=1}^{k} {p_i}^{r_i}}$$

Alors :

$$\boldsymbol{s(n) = \prod_{i=1}^{k} s({p_i}^{r_i})}$$

5) Si n et m sont deux nombres entiers naturels premiers entre eux, alors :

$$\boldsymbol{s(n\,m) = s(n)\,s(m)}$$

Preuves :

1) et 2) évident

3)

$$s(p^r) = 1 + p + \cdots + p^r = \frac{p^{r+1} - 1}{p - 1}$$

4)

$$s(n) = \sum_{\substack{1 \le s_1 \le r_1 \\ 1 \le s_2 \le r_2 \\ \vdots \\ 1 \le s_k \le r_k}} {p_1}^{s_1}\,{p_2}^{s_2} \dots {p_k}^{s_k} = \left(\sum_{s_1=1}^{r_1} {p_1}^{s_1}\right)\left(\sum_{s_2=1}^{r_2} {p_2}^{s_2}\right) \dots \left(\sum_{s_k=1}^{r_k} {p_k}^{s_k}\right)$$

Donc :

$$s(n) = s({p_1}^{r_1})\,s({p_2}^{r_2}) \dots s({p_k}^{r_k})$$

5) Décomposons n et m en produit de facteurs premiers.

$$n = {p_1}^{r_1}\ {p_2}^{r_2} \dots\ {p_s}^{r_s},\ \ m = {p_{s+1}}^{r_{s+1}}\ {p_{s+2}}^{r_{s+2}} \dots\ {p_k}^{r_k}$$

Alors , la décomposition en produit de facteurs premiers de $n\ m$ est :

$$n\ m = {p_1}^{r_1}\ {p_2}^{r_2} \dots\ {p_s}^{r_s}\ {p_{s+1}}^{r_{s+1}}\ {p_{s+2}}^{r_{s+2}} \dots\ {p_k}^{r_k}$$

Donc :

$$s(n\ m) = s({p_1}^{r_1})\ s({p_2}^{r_2}) \dots\ s({p_s}^{r_s})\ s({p_{s+1}}^{r_{s+1}})\ s({p_{s+2}}^{r_{s+2}}) \dots\ s({p_k}^{r_k})$$

$$= s(n)\ s(m)$$

Théorème d'Euclide :

Si M_p est premier pour p premier alors $2^{p-1}\ M_p = 2^{p-1}\ (2^p - 1)$ est pair et parfait

Réciproque d'Euler :

Si un nombre entier naturel pair est parfait alors il est de la forme $2^{p-1}\ (2^p - 1)$ avec p premier

Preuve :

Théorème d'Euclide :

Les diviseurs de $2^{p-1}\ (2^p - 1) = 2^{p-1}\ M_p$ sont :

$$1, 2, \dots., 2^{p-1}, M_p, 2\ M_p, \dots, 2^{p-2}\ M_p$$

La somme de ces diviseurs est alors :

$$1 + \ 2 + \ \dots. + 2^{p-1} + \ M_p + \ 2\ M_p + \ \dots + \ 2^{p-2}\ M_p = \frac{2^p - 1}{2 - 1} + \frac{2^{p-1} - 1}{2 - 1} M_p =$$

$$2^p - 1 + (2^{p-1} - 1)\ (2^p - 1) = 2^{p-1}\ (2^p - 1)$$

Réciproque d'Euler :

Soit n un nombre entier naturel pair et parfait. Alors n peut se mettre sous la forme :

$$n = 2^q\ (2\ m + 1), \qquad q \in \mathbb{N}^*$$

2^q et $2\ m + 1$ étant premiers entre eux, on a :

$$s(n) = s(2^q)\ s(2\ m + 1) = (2^{q+1} - 1)\ s(2\ m + 1)$$

D'autre part, comme n est parfait :

$$s(n) = 2\ n$$

Donc :

$$(2^{q+1} - 1)\ s(2\ m + 1) = 2^{q+1}\ (2\ m + 1)$$

Or $2^{q+1} - 1$ est premier avec 2^{q+1} donc il divise $2\ m + 1$. Donc il existe un entier naturel k tel que :

$$2\ m + 1 = (2^{q+1} - 1)\ k$$

Donc, en reportant dans la précédente égalité :

$$s(2\,m+1) = 2^{q+1}\,k$$

Donc k est un diviseur de $2\,m+1$ et :

$$s(2\,m+1) = 2\,m+1+k$$

Supposons par l'absurde : $k > 1$. Alors, puisque $1 < k < s(2\,m+1)$:

$$s(2\,m+1) \geq 1 + k + (2\,m+1) > 2\,m+1+k$$

Ceci est contradictoire, donc :

$$k = 1$$

Ainsi :

$$s(2\,m+1) = (2\,m+1)+1$$

Donc n'admet que deux diviseurs distincts, 1 et $2\,m+1$. Il est donc premier et de la forme $2^{q+1}-1$.

Il en résulte :

$$n = 2^q\,(2^{q+1}-1) = 2^q\,M_{q+1}$$

Soit en posant : $q = p-1$:

$$n = 2^{p-1}\,M_p$$

où $p = q+1$ est premier car $M_p = 2^p - 1$ l'est.

<u>Exemple</u> :

Le caractère premier de M_2, M_3, M_5, M_7 permet de mettre en évidence les nombres parfaits suivant :

$$6 = 2 \times 3 = 2\,M_2$$

$$28 = 4 \times 7 = 2^2\,M_3$$

$$496 = 16 \times 31 = 2^4\,M_5$$

$$8128 = 64 \times 127 = 2^6\,M_7$$

Et pour M_7 on obtient le nombre parfait :

$$8\,589\,869\,056 = 65\,536 \times 131\,071 = 2^6\,M_7$$