AUTOUR DU PETIT THEOREME DE FERMAT

par Jean-René JOLY

Ce texte est une rédaction remaniée de l'exposé de Novembre 1982. Le § 1 montre, à travers la correspondance entre Fermat et l'"Académie Mersenne",

- d'une part, l'intérêt pris par Fermat, vers 1635-1640, aux nombres parfaits et aux nombres dits "de Mersenne" et "de Fermat" ;
- et d'autre part, la création progressive par Fermat de l'outil mathématique approprié à l'identification des nombres de Mersenne et de Fermat : le "petit" théorème de Fermat.

Le § 2 est consacré à l'histoire des démonstrations du petit théorème de Fermat (chez Fermat lui-même, Leibniz, Euler, Lagrange, Gauss, et enfin à l'époque contemporaine).

Le § 3, d'autre part, montre concrètement comment le petit théorème de Fermat permet de tester si un nombre 2^p-1 est premier (donc de Mersenne), ou si un nombre $2^{2^n}+1$ est premier (donc de Fermat) ; on traite explicitement les exemples classiques de $2^{37}-1$ (non premier, divisible par 223 : Fermat (1640)) ; et de $2^{32}+1$ (non premier, divisible par 641 : Euler (1732)).

Le texte est suivi de notes (références par numéros entre parenthèses) et d'une courte bibliographie (références par numéros entre crochets).

1. HISTOIRE DES NOMBRES PARFAITS ET GENESE DU PETIT THEOREME DE FERMAT.

Les Anciens, et notamment les Pythagoriciens, portaient un certain intérêt aux nombres parfaits ; rappelons qu'un nombre entier est dit parfait s'il est égal à la somme de tous ses diviseurs autres que lui-même ; ainsi,

$$6 = 1 + 2 + 3 \quad ; \quad 28 = 1 + 2 + 4 + 7 + 14 \ ,$$

sont des nombres parfaits. Les Anciens ne connaissaient d'ailleurs probablement que les quatre premiers nombres parfaits : 6 , 28 , 496 , 8 128 . (Voir note (1)).

On retrouve les nombres parfaits chez Euclide, vers 300 av. J.C. Au livre IX des Eléments, Euclide définit et étudie les nombres premiers, et prouve notamment le théorème suivant (de démonstration facile : exercice) :

THEOREME 1. - Si le nombre entier p est premier, et si le nombre $M_p = 2^p - 1$ est lui aussi premier, alors le nombre $P_p = 2^{p-1}(2^p-1) = 2^{p-1}M_p$ est parfait.

(Ainsi, les nombres parfaits 6, 28, 496, 8 128 correspondent respectivement à $p = 2, 3, 5, 7$).

Par ce théorème, Euclide caractérise une certaine famille de nombres parfaits pairs (disons : les nombres parfaits euclidiens), mais cette caractérisation soulève au moins trois problèmes :

a) Existe-t-il une infinité de nombres parfaits euclidiens ? Réponse : probablement non ; voir la suite.

b) Tout nombre parfait pair est-il euclidien ? Réponse : oui (Euler). Voir note (2).

c) Existe-t-il des nombres parfaits impairs ? Réponse : probablement non. Voir note (3).

*

Pendant les deux millénaires suivants (jusqu'au début du XVIIe siècle), l'intérêt porté aux nombres parfaits ne faiblit pas, mais on voit surtout fourmiller des assertions arbitraires ou approximatives, telles que : "le $k^{ième}$ nombre parfait possède k chiffres" - ce qui est complètement faux (voir la suite). De façon générale, l'étude des nombres parfaits est alors plus rhétorique que mathématique, et ne mérite pas d'être détaillée ici. (Le lecteur pourra consulter le livre de Dickson [1], pp. 3-12).

*

C'est vers 1635-1640 que l'étude mathématique des nombres parfaits va se trouver relancée (avec notamment Descartes, Mersenne, Frénicle et Fermat), et qu'on va voir apparaître une tehcnique arithmétique adaptée à cette étude : le "petit" théorème de Fermat.

Le scénario est à peu près le suivant :

• le 15 novembre 1638, Descartes écrit à Mersenne (voir note (4)) pour lui annoncer :

- qu'il sait prouver que tout nombre parfait pair est euclidien ;
- qu'il ne voit pas pourquoi il n'existerait pas de nombre parfait impair (voir cependant note (3)).

• Le 9 janvier 1639, Descartes "récidive" dans une lettre à Frénicle, où il décrit d'hypothétiques nombres parfaits impairs.

• En décembre 1638, Fermat annonce qu'il possède une méthode générale pour résoudre toutes les questions du type "somme des diviseurs", "nombres parfaits", etc.

• En mars 1639, Frénicle, par l'intermédiaire de Mersenne, défie Fermat de trouver un nombre parfait de 20 ou 21 chiffres. (Dans ce contexte, parfait signifie visiblement parfait euclidien ; ceci sera sous-entendu dans toute la suite).

• Dès mai 1639, Fermat répond qu'il n'existe aucun nombre parfait de 20 ou 21 chiffres (et réfute ainsi l'assertion : "le $k^{ième}$ nombre parfait possède k chiffres").

C'est entre juin et octobre 1640, dans la correspondance entre Fermat et Mersenne-Frénicle, que l'on voit apparaître le petit théorème de Fermat, son application à l'étude des nombres parfaits, et aussi son application à l'étude des nombres de Fermat, c'est-à-dire des nombres premiers du type $F_n = 2^{2^n}+1$. Suite du scénario :

• en juin 1640, Fermat affirme essentiellement ceci : si n est premier, alors 2^n-2 est divisible par $2n$, et tout diviseur premier de 2^n-1 est de la forme $2kn+1$.

La première assertion est un cas particulier du (futur) petit théorème de Fermat. En ce qui concerne la seconde, Fermat donne les deux exemples suivants :

$2^{23}-1$ est divisible par $47 = 2.23+1$;
$2^{37}-1$ est divisible par $223 = 6.37+1$;

il en résulte évidemment que P_{23} et P_{37} ne sont pas parfaits.

• En août 1640, dans une lettre à Frénicle, Fermat déclare ceci :

> "Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme
>
> 3 5 17 257 65 537 4 294 967 297
>
> et le suivant de 20 lettres
>
> 18 446 744 073 709 551 617 ; etc.
>
> Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurais peine à me dédire."

En langage moderne, ceci veut dire :

THEOREME 2. - Pour tout entier $n \geq 0$, posons

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

Alors, tous les F_n sont des nombres premiers.

Les nombres écrits explicitement sont les F_n avec $0 \leq n \leq 6$. En fait, ce théorème 2 est faux dès F_5 ; Euler a en effet prouvé en 1732 que F_5 est divisible par 641 . Voir § 3.2 et note (5).

• Enfin, une lettre à Frénicle datée du 18 octobre 1640, Fermat déclare :

> "Il me semble après cela qu'il m'importe de vous dire le fondement sur lequel j'appuie les démonstrations de tout ce qui concerne les progressions géométriques, qui est tel :
>
> Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de ladite puissance est sous-multiple du nombre premier donné -1 ; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question".

En langage moderne, ceci devient, en notant p le nombre premier et a la base de la progression (géométrique) :

THEOREME 3. - Soient p un nombre premier, et a un entier positif non divisible par p . Alors :

1) il existe un plus petit entier $n \geq 1$ tel que p divise a^n-1 ;
2) cet entier n divise $p-1$;
3) tout entier m multiple de n est tel que p divise a^m-1 ;
4) en particulier, p divise $a^{p-1}-1$.

Il s'agit là exactement du petit théorème de Fermat ; Fermat le donne sans démonstration, mais non sans applications ; il traite notamment les exemples suivants, que nous reproduisons en notation moderne :

$\underline{p = 13}$, a = 3 ; p-1 = 12 ; n = 3 : $3^3 - 1 = 26$ est divisible par 13 , et 3 divise 12 .

$\underline{p = 23}$, a = 2 ; p-1 = 22 ; n = 11 : $2^{11} - 1$ est divisible par 23 , et 11 divise 22 .

$\underline{p = 47}$, a = 2 ; p-1 = 46 ; n = 23 : $2^{23} - 1$ est divisible par 47 , et 23 divise 46 .

$\underline{p = 223}$, a = 2 ; p-1 = 222 ; n = 37 : $2^{37} - 1$ est divisible par 223 , et 27 divise 222 .

(Les deux derniers exemples figurent dans la lettre de juin 1640, qui donne le petit théorème de Fermat pour a = 2).

*

La "grande période" de 1638-1640 s'achève pratiquement sur cette lettre de Fermat à Frénicle, qui, si l'on veut, permet de donner à la Théorie des Nombres "moderne" une date de naissance précise : le 18 octobre 1640. Par la suite, Fermat s'intéressera à d'autres questions, et se bornera (en ce qui concerne le sujet étudié dans ce § 1) à affirmer obstinément la primalité des nombres $F_n = 2^{2^n} + 1$, c'est-à-dire le théorème 2 (faux) ci-dessus : lettres à Carcavi, Huygens, Pascal,...

Voici par exemple un extrait d'une lettre à Pascal (29 août 1654) :

"... les puissances carrées de 2 , augmentées de l'unité, sont toujours des nombres premiers :
$2^2 + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$, $2^{2^4} + 1 = 65\,537$,
sont premiers, et ainsi à l'infini. C'est une proposition de la vérité de laquelle je vous réponds. La démonstration en est très malaisée, et je vous avoue que je n'ai pu encore la trouver pleinement ; je ne vous la proposerais pas pour la chercher si j'en étais venu à bout...".

A propos des F_n , voir le § 3.2. Il faut signaler par ailleurs

qu'en 1644, Mersenne affirmera, sans démonstration, que $M_p = 2^p - 1$ est <u>premier</u> (et par conséquent que $P_p = 2^{p-1}(2^p-1)$ est <u>parfait</u>) pour les p (premiers) de la liste suivante :

$$2 \ , \ 3 \ , \ 5 \ , \ 7 \ , \ 13 \ , \ 17 \ , \ 19 \ , \ 31 \ , \ 67 \ , \ 127 \ , \ 257 \ ;$$

et que M_p est <u>composé</u> (et donc P_p <u>non parfait</u>) pour les 44 autres valeurs de p (premier) ≤ 257 . On sait maintenant que, pour les 55 valeurs de p envisagées, Mersenne avait commis 5 erreurs <u>seulement</u> (soit 9 %) : ceci est remarquable, vu la théorie et les moyens de calcul dont on disposait à l'époque. La notation M_p , et la qualification de <u>nombres de Mersenne</u> donnée aux M_p premiers, saluent cet exploit de Mersenne. Voir <u>note</u> (6).

2. DEMONSTRATIONS DU PETIT THEOREME DE FERMAT.

2.1. Fermat (vers 1640). -

Il est peu concevable que Fermat ait possédé une démonstration (au sens moderne) de son "petit" théorème. Il semble qu'au départ, il ait essayé expérimentalement de déterminer les diviseurs premiers p de nombres de la forme $2^m - 1$, puis $a^m - 1$, et qu'il se soit aperçu qu'il était beaucoup commode, pour a fixé, de fixer également p et de faire varier l'exposant m. La démarche devait être la suivante :

① se donner un a et un p fixés (p ne divisant pas a) ;

② calculer itérativement a^m pour $m = 0, 1, 2, \ldots$, en remplaçant chaque résultat plus grand que p par son reste de division par p (autrement dit, en travaillant modulo p avant la lettre : voir note (7)) ;

③ noter dans la "progression" ainsi obtenue les apparitions de 1 et les valeurs des exposants m correspondants ;

④ constater le caractère cyclique (de période $p-1$, ou diviseur de $p-1$) de ces apparitions de 1 .

Exemple (lettre à Frénicle d'Octobre 1640) :

$p = 13$, $a = 3$;

m : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

a^m : 1, 3, 9, 1, 3, 9, 1, 3, 9, 1, 3, 9, 1

(il s'agit évidemment de a^m réduit modulo p).

On laisse au lecteur le soin de traiter, sur calculatrice de poche, les exemples $a = 2$, $p = 23, 47, 223$.

Dans cette démarche, deux choses sont claires :

• l'intérêt de fixer p , et de travailler "modulo p", ce qui accélère les calculs et surtout montre mieux la structure du phénomène mathématique étudié ;

• le caractère cyclique de la suite $(a^m \bmod p)_{m\geq 0}$, et plus généralement du "groupe" des restes non nuls modulo p .

Il fallut attendre Gauss (vers 1800) pour voir apparaître systématiquement, aux premières pages de ses Disquisitiones Arithmeticae, l'arithmétique modulo p ; et Euler, Lagrange, etc. (1740-1800) pour voir poindre lentement les notions de groupe, groupe cyclique, etc... Voir la suite.

La "démonstration" de Fermat (d'ailleurs parfaitement convaincante en soi, et très conforme aux "canons" mathématiques contemporains) devait donc reposer sur deux axiomes (basés sur l'expérience ; voir note (8)) ;

- l'arithmétique modulo p "existe", et "marche bien" ;
- pout tout a non divisible par p , la suite des a^m réduits modulo p est cyclique, et passe par la valeur 1 pour $m = 0$ et $m = p-1$.

Tout le reste s'en déduit facilement par utilisation de la division euclidienne. Voir d'ailleurs en 2.5 la démonstration "moderne".

*

2.2. Leibniz (vers 1680), Euler (1732-1765). -

Leibniz découvrit les travaux de Fermat (mort en 1665) lors de son séjour à Paris (1672-1676). On lui doit une démonstration du petit théorème de Fermat qui, en notation moderne, peut se décrire ainsi :

- si p est premier, tous les coefficients binomiaux sont divisibles par p , sauf C_p^0 et C_p^p , qui valent 1 ;
- si a et b sont deux entiers, on a donc : $(a+b)^p = a^p + b^p +$ mult. de p ;
- en particulier, avec $b = 1$, et en raisonnant par récurrence sur $a \geq 1$, on trouve successivement $2^p = 2 +$ mult. de p ; $3^p = 3 +$ mult. de p ; ...

et de façon générale, pour $1 \leq a \leq p-1$,
$a^p = a +$ mult. de p , donc $a^{p-1} = 1 +$ mult. de p .

(Ceci prouve en fait les points 1) et 4) du théorème 3, mais on sait que 2) et 3) s'en déduisent immédiatement).

Euler eut lui-même connaissance des travaux arithmétiques de Fermat à Saint-Pétersbourg, vers 1730, par l'intermédiaire de Goldbach. Le premier résultat arithmétique obtenu par Euler est la divisibilité par 641 du nombre de Fermat $F_5 = 2^{32} + 1$, donc la preuve de la fausseté du théorème 2, si cher à Fermat (voir note (5)). On doit à Euler trois démonstrations du petit théorème de Fermat ; les deux premières sont pratiquement équivalentes à celle de Leibniz ; la troisième est plus intéressante, c'est-à-dire plus proche des préoccupations du § 1. En la modernisant un peu, elle se réduit à ceci :

- si p est premier, et si $0 < a < p$, au plus $p-1$ des restes de division par p des termes 1 , a , a^2 , a^3 ,..., sont distincts ; d'où l'existence de ℓ et m , avec $0 \leq \ell < m$, tels que $a^m - a^\ell$ soit divisible par p ; puis l'existence, avec $n = m - \ell > 0$, d'un $n > 0$ tel que $a^n - 1$ soit divisible par p ;
- supposons de plus n minimum ; alors 1 , a , a^2 ,..., a^{n-1} ont des restes de division par p distincts, d'où $n \leq p-1$;
- si $n = p-1$, le petit théorème de Fermat est prouvé ; sinon, il existe b , $0 < b < p$, qui n'est reste de division par p d'aucune puissance de a ; alors les termes b , ba , ba^2 ,..., ba^{n-1} ont des restes de division par p distincts, et aucun de ces restes n'est reste d'une puissance de a . D'où $2n \leq p-1$, et $n \leq \frac{p-1}{2}$;
- si $n = \frac{p-1}{2}$, le petit théorème de Fermat est prouvé ; sinon, il existe c , $0 < c < p$, etc.

*

2.3. Lagrange (vers 1770). -

C'est lors de son séjour à Berlin (1766-1787) que Lagrange eut connaissance (notamment grâce aux travaux d'Euler) du petit théorème de Fermat, et également (grâce aux Meditationes Algebraicae de Waring, publiées en 1770) du théorème de Wilson. Il s'agit de l'énoncé suivant (non démontré avant Lagrange) :

THEOREME 4. - Soit p un nombre premier. Alors, le nombre $(p-1)! + 1$ est divisible par p .

A des détails près, la démonstration par Lagrange des théorèmes de Fermat et de Wilson est la suivante ([4] ; pour condenser l'exposition, nous employons ici la notation congruentielle) : posons

$$f(x) = x(x+1)\dots(x+p-1) \quad ;$$

on a évidemment

$$f(x+1) = (x+1)(x+2)\dots(x+p) = f(x) + pg(x) \quad ,$$

avec $g(x) = (x+1)(x+2)\dots(x+p-1)$. Si $a_0, a_1, \dots, a_p$ sont les coefficients de $f(x)$, on a donc :

$$a_0(x+1)^p + a_1(x+1)^{p-1} + \dots + a_{p-1}(x+1) + a_p$$
$$\equiv a_0x^p + a_1x^{p-1} + \dots + a_{p-1}x + a_p \pmod p \quad ,$$

ce qui signifie que les coefficients des puissances correspondantes de x dans les deux membres sont congrus modulo p . (Noter que $a_0 = 1$, $a_p = 0$, et surtout $a_{p-1} = (p-1)!$, ce qui justifie l'introduction de $f(x)$). On a donc successivement, pour les degrés p , $p-1$, $p-2$,..., 0 :

$$C_p^0 a_0 \equiv a_0 \pmod p$$

$$C_p^1 a_0 + C_{p-1}^0 a_1 \equiv a_1 \pmod p$$

$$C_p^2 a_0 + C_{p-1}^1 a_1 + C_{p-2}^0 a_2 \equiv a_2 \pmod p$$

$$\vdots$$

$$C_p^p a_0 + C_{p-1}^{p-1} a_1 + \dots + C_i^1 a_{p-i} + C_0^0 a_p \equiv a_p \pmod p \quad .$$

Mais on sait que $C_m^0 = 1$ pour $m \geq 0$, que $C_1^1 = 1$, et surtout que les C_p^i sont congrus à $0 \pmod p$, à l'exception de C_p^0 et de C_p^p , qui valent 1 . Ce système de congruences, pris à partir de la deuxième ligne, donne donc successivement

$$a_1 \equiv 0 , \quad a_2 \equiv 0 , \ldots , a_{p-2} \equiv 0 \pmod p$$

et surtout (puisque $a_0 = 1$)

$$1 + a_{p-1} \equiv 0 \pmod p ,$$

c'est-à-dire $(p-1)! + 1 \equiv 0 \pmod p$, ce qui établit le théorème 4 (Wilson). Ce calcul montre également (puisque $a_0 = 1$ et $a_p = 0$) que

$$f(x) \equiv x^p - x \pmod p ,$$

d'où, en simplifiant par x ,

$$(x+1)(x+2)\ldots(x+p-1) \equiv x^{p-1} - 1 \pmod p ,$$

ou encore, en changeant x en $-x$, et en notant que (sauf pour le cas trivial $p = 2$, qui se règle directement) $p-1$ est pair,

$$(x-1)(x-2)\ldots(x-(p-1)) \equiv x^{p-1} - 1 \pmod p .$$

Le premier membre est nul $(\text{mod } p)$ pour $a = 1, 2, \ldots, p-1$: d'où $a^{p-1} \equiv 1 \pmod p$, ce qui établit en définitive le théorème 3 (Fermat). ■

L'intérêt de cette démonstration est évidemment qu'elle donne la factorisation de $x^{p-1} - 1 \pmod p$, c'est-à-dire dans $\mathbb{F}_p[x]$ (avec $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) : les théorèmes de Fermat et de Wilson ne sont que des corollaires de ce "théorème de Lagrange". Cette démonstration montre également que Lagrange était parfaitement à l'aise (en 1771) avec le calcul algébrique dans l'anneau $\mathbb{F}_p[x]$: on a le sentiment, en lisant le "mémoire" de Lagrange [4], de voir naître ce qu'on appelait naguère l'"Algèbre moderne".

*

2.4. Gauss (vers 1800). -

On doit à Gauss [5] l'introduction de la notation congruentielle (voir note (7)). Comme on l'a vu, cette notation permet d'écrire le petit théorème de Fermat sous la forme suivante : si $a \not\equiv 0 \pmod p$, alors $a^{p-1} \equiv 1 \pmod p$. Voici la démonstration annoncée :

• tout d'abord, l'application $x \mapsto xa$ (où $x, a, xa, \ldots$ sont conçus comme restes modulo p) est bijective : car $xa \equiv ya \pmod p$ implique que p divise $xa - ya = (x-y)a$, mais p est premier avec a , donc (lemme de Gauss !) p divise $x-y$, et donc $x \equiv y \pmod p$: d'où l'injectivité. La bijectivité résulte alors du fait que l'ensemble des restes modulo p est fini (à p éléments).

• Il résulte de cette bijectivité que les deux suites :

$1, 2, \ldots, p-1$, et $a, 2a, \ldots, (p-1)a$,

(dont les termes sont conçus comme restes modulo p), sont identiques, à l'ordre des termes près ; on a donc par multiplication

$$1.2.\cdots.(p-1) \equiv (a)(2a)\ldots((p-1)a) \pmod p$$

d'où $(p-1)! \equiv a^{p-1}(p-1)! \pmod p$, et finalement, après simplification

$$a^{p-1} \equiv 1 \pmod p \ . \blacksquare$$

(Assez malicieusement, cette démonstration fait apparaître $(p-1)! \pmod p$, mais ne permet pas d'obtenir le théorème de Wilson ; voir d'autre part note (7a)).

*

2.5. Démonstration des théorèmes 3 et 4 dans le style "moderne". -

Cette démonstration utilise essentiellement le langage "groupes, anneaux, corps" (mais n'ajoute en fait rien à la démonstration de Lagrange).

• Comme p est premier, l'anneau $F = \mathbb{Z}/p\mathbb{Z}$ des classes d'entiers modulo p est un corps (ceci résulte du lemme de Gauss) et l'ensemble G (représenté par $1, 2, \ldots, p-1$) des classes d'entiers non nulles modulo p est un groupe commutatif d'ordre $p-1$;

• si $\bar{a}$ est la classe de $a \pmod p$, $\bar{a}$ est dans G ; et si n est l'ordre de $\bar{a}$, on a :

$$\bar{a}^n = 1 \ , \quad \text{donc} \quad a^n \equiv 1 \pmod p \ ;$$

ceci prouve 1) (la minimalité de n résulte de la définition de l'ordre d'un élément dans un groupe) ;

• de plus, l'ordre n de $\bar{a} \in G$ divise l'ordre $p-1$ du groupe G tout entier ("théorème de Lagrange"!) : donc n divise $p-1$, ce qui prouve 2) ;

• les assertions 3) et 4) du théorème 3 sont alors évidentes ;

• le théorème 3 étant démontré, passons au théorème 4 ; le théorème 3 prouve que dans l'anneau de polynômes $F(X)$, le polynôme $X^{p-1} - 1$ a pour racines $\bar{1}, \bar{2}, \ldots, \overline{p-1}$; d'où immédiatement

$$X^{p-1} - \bar{1} = (X-\bar{1})(X-\bar{2})\ldots(X-\overline{p-1}) \ ;$$

en égalant les termes constants, on arrive en particulier à :

$$-1 \equiv (-1)^{p-1}(p-1)! \pmod p \ ;$$

mais (en écartant encore le cas trivial $p=2$), on voit que $p-1$ est pair, que $(-1)^{p-1} \equiv 1 \pmod p$, et donc finalement que :

$$(p-1)! \equiv -1 \pmod p \ ;$$

le théorème 4 est également démontré. ■

3. APPLICATIONS DU PETIT THEOREME DE FERMAT AUX NOMBRES PARFAITS, AUX NOMBRES DE MERSENNE ET AUX NOMBRES DE FERMAT.

3.1. Nombres parfaits et nombres de Mersenne. -

Compte tenu du théorème d'Euclide (th. 1), la recherche des nombres parfaits euclidiens P_p se ramène à celle des nombres de Mersenne M_p, c'est-à-dire à celle des p premiers tels que $M_p = 2^p - 1$ soit lui-même premier. L'application à cette recherche du petit théorème de Fermat tient dans les deux lemmes suivants, implicites chez Fermat (voir § 1) :

LEMME 1. - Soit q le plus petit diviseur premier de M_p. Alors, pour que M_p soit un nombre de Mersenne, et que P_p soit donc un nombre parfait, il faut et il suffit que $q = M_p = 2^p - 1$.

(Evident !)■

LEMME 2. - Tout diviseur premier q de $M_p = 2^p - 1$ est de la forme $1 + 2kp$, k entier $\equiv 1$. (On suppose $p \neq 2$).

Démonstration. - (Attention ! Dans cette démonstration, comme dans celle du lemme 3, on va travailler modulo p : le nombre premier fixé n'est pas p, mais q ; et p joue le rôle d'un exposant). Le petit théorème de Fermat (th. 3), démontré "rigoureusement" en fin de § 2, montre qu'il existe un plus petit n positif tel que $2^n \equiv 1 \pmod q$; et que n est un diviseur de $q-1$; il montre également, puisque $2^p \equiv 1 \pmod q$, que n est un diviseur de p, et donc (comme évidemment $n > 1$ et que p est premier) que $n = p$. Finalement, p divise $q-1$. Par ailleurs, $2^p - 1$ est impair, donc $q-1$ est impair, donc 2 divise $q-1$. Comme, pour $p \neq 2$, 2 est premier avec p, on voit au total que $q-1$ est divisible par $2p$; finalement, $q - 1 = 2kp$, et $q = 1 + 2kp$. ■

(Pour $p = 2$, on a $M_p = 2^2 - 1 = 3$ et $1 + 2p = 5$; le lemme 2 ne s'applique pas, mais c'est évidemment sans importance !).

Application à P_{37} et M_{37} . - (On laisse au lecteur le plaisir d'allumer sa calculatrice de poche et d'examiner par exemple les valeurs $p = 11, 13, 17, \ldots$). D'après le lemme 2, les diviseurs premiers de M_{37} sont tous de la forme $1 + 74k$, et appartiennent donc à la liste

$$149 \ , \ 223 \ , \ 593 \ , \ldots$$

Pour chaque terme (disons ℓ) de cette liste, il faut alors examiner $2^{37} \pmod{\ell}$. Si ce reste est différent de 1 , ℓ ne divise pas M_{37} ; si ce reste égale 1 , ℓ divise M_{37} ; etc. Pratiquement :

$\ell = 149$: les congruences étant mod 149 , on a

$2^7 \equiv 128$, et $2^{10} \equiv 130$, donc

$2^{37} \equiv 2^7 . 2^{30} \equiv 128 . (130)^3 \equiv 105 \not\equiv 1$;

$\ell = 149$ ne divise donc pas M_{37} .

$\ell = 223$: les congruences étant maintenant modulo 223 , on a

$2^7 \equiv 128$, et $2^{10} \equiv 132$, donc

$2^{37} \equiv 128 . (132)^3 \equiv 1$;

$\ell = 223$ divise donc M_{37} , et comme 223 est visiblement plus petit que M_{37} , on voit (lemme 1) que M_{37} n'est pas premier. Ainsi, M_{37} n'est pas un nombre de Mersenne, et P_{37} n'est pas un nombre parfait.

(Il est bien entendu inutile désormais de tester $\ell = 593, \ldots$, même si l'on cherche à décomposer M_{37} en facteurs premiers ; en effet, dans ce genre de situation, l'expérience, et de vagues considérations statistiques, montrent que le deuxième facteur premier de M_p est très grand).

*

3.2. Nombres de Fermat. -

On s'intéresse ici à la recherche des nombres de Fermat, c'est-à-dire à la recherche des entiers $n \geq 0$ tel que $F_n = 2^{2^n}+1$ soit un nombre premier. L'application à cette recherche du petit théorème de Fermat tient dans le lemme 1 (3.1) et dans le lemme 3 ci-dessous, réplique du lemme 2 (3.1).

LEMME 3. - Tout diviseur premier q de F_n est de la forme $1 + 2^{2^{n+1}} k$, k entier ≥ 1 .

Démonstration. - Tout d'abord, $q \neq 2$, puisque F_n est impair. De plus, le petit théorème de Fermat prouve qu'il existe un plus petit entier positif (notons-le ici N) tel que $2^N \equiv 1 \pmod q$; et que N divise $q-1$. Il montre également (puisque $2^{2^n} \equiv -1 \pmod q$ et que par suite $2^{2^{n+1}} \equiv 1 \pmod q$) que N divise $2^{2^{n+1}}$; N est donc de la forme 2^{2^i} , $0 \leq i \leq n+1$; mais la possibilité que $i \leq n$ est exclue, car on aurait alors $2^{2^n} \equiv 1 \pmod q$, donc $F_n - 1 \equiv 1 \pmod q$, ou $F_n \equiv 2 \pmod q$: absurde, puisque q est impair et divise F_n . On a donc en fait $N = 2^{2^{n+1}}$; $2^{2^{n+1}}$ divise $q-1$, $q-1$ est donc de la forme $2^{2^{n+1}} k$, $k \geq 1$, et finalement

$$q = 1 + 2^{2^{n+1}} k \ . \blacksquare$$

Application à $F_5 = 2^{2^5}+1 = 2^{32}+1$. - D'après le lemme 3, les diviseurs premiers de F_5 sont tous de la forme $1 + 64k$, et appartiennent donc à la liste

193 , 257 , 449 , 577 , 641 ,...

Notons tout de suite que $257 = F_3$ ne divise pas F_5 : en fait (exercice facile), quels que soient m et n , $0 \leq m < n$, F_m et F_n sont premiers entre eux. Pour chaque terme (disons ℓ) de la nouvelle liste (privée de 257)

193 , 449 , 577 , 641 ,...

il faut alors examiner $2^{32} \pmod{\ell}$; si ce reste est différent de -1 , ℓ ne divise pas F_5 ; sinon, ℓ divise F_5 , etc. En fait :

$\ell = 193, \ldots$: on laisse au lecteur le soin de faire le calcul comme au § 3.1. On constate que les $\ell < 641$ ne divisent pas F_5 .

$\ell = 641$: les congruences étant prises modulo 641 , on a (par exemple)

$$2^2 \equiv 4 \text{ , et } 2^{10} \equiv 1024 \equiv 383 \text{ , donc}$$
$$2^{32} \equiv 4.(383)^3 \equiv 640 \equiv -1 \text{ ;}$$

$\ell = 641$ divise donc F_5 , et comme 641 est visiblement plus petit que F_5 , on voit (lemme 1) que F_5 n'est pas premier (et n'est pas un nombre de Fermat).

*

3.3. En guise de conclusion. -

On a vu au § 1 que Fermat avait découvert le facteur premier 223 de $M_{37} = 2^{37} - 1$; le § 3.1 montre quelle était sa méthode. Le § 3.2 montre par ailleurs que les calculs nécessaires pour trouver le facteur premier 641 de $F_5 = 2^{32} + 1$ ne sont pas beaucoup plus longs. Il est donc surprenant que Fermat n'ait jamais découvert ce facteur premier, et ait persisté toute sa vie durant (voir § 1) à croire à la primalité de tous les F_n .

En revanche, il n'est pas surprenant qu'il ait fallu près d'un siècle (disons : de 1645 à 1732) pour que ce facteur premier soit découvert : les travaux arithmétiques de Fermat étaient tombés (avant même sa mort en 1665) dans le manque d'intérêt puis l'oubli les plus profonds, et Euler est en fait le premier grand mathématicien à s'y être passionnément et efficacement intéressé.

NOTES

(1) L'intérêt porté par les Anciens aux nombres parfaits était purement purement mystique. Voir à ce sujet le livre de Dickson [1], pp. 2-5.

(2) La démonstration figure dans les papiers posthumes d'Euler ; elle est courte et élémentaire ; on en trouvera un résumé dans [1], p. 19.

(3) En fait, on sait essentiellement à l'heure actuelle qu'il n'existe pas de nombre parfait impair $\leq 10^{50}$: d'où la vague conjecture qu'il n'en existe pas du tout !

(4) La place nous manque totalement ici pour décrire l'importance du Père Marin Mersenne (1588-1648) dans le développement scientifique en France au XVIIe siècle. Mersenne réunissait autour de lui une sorte d' "Académie", et correspondait de façon permanente avec de nombreux savants français (Descartes, Fermat (à partir de 1636),...) et européens ; ainsi se trouvait réalisée une communication rapide des idées, des découvertes, et aussi des défis (du genre : trouver un nombre parfait de 20 ou 21 chiffres : défi de Frénicle à Fermat...). A propos de Fermat lui-même (1601-1665), voir par exemple [7].

(5) Euler (1707-1783) est le premier mathématicien a avoir tiré de l'oubli les travaux de Fermat, et à avoir (en donnant des démonstrations de la plupart des résultats de Théorie des Nombres simplement énoncés par Fermat) créé effectivement cette branche des Mathématiques, aussitôt suivi par Lagrange (1736-1813), Gauss (1777-1855), etc. La divisibilité de $F_5 = 2^{32}+1$ par 641 date de 1732, et est le premier "résultat" arithmétique d'Euler. Voir [3].

(6) Les nombres premiers $p \leq 5\,000$ tels que M_p soit premier (donc de Mersenne) sont en fait :

2 , 3 , 5 , 7 , 13 , 17 , 19 , 31 , 61 , 89 ,
107 , 127 , 521 , 607 , 1279 , 2203 , 2281 ,
3217 , 4253 , 4423 ;

on sait en outre qu'entre 5 000 et 50 000 , les nombres premiers p suivants ont la même propriété :

9689 , 9941 , 11213 , 19937 , 21701 , 23209 , 44497 ;

mais cette deuxième liste n'est probablement pas complète. On conjecture que l'ensemble des nombres de Mersenne est fini.

(7) La notation congruentielle est due à Gauss ([5], 1799) ; rappelons que $a \equiv b \pmod{m}$ signifie que $a-b$ est divisible par le "module" m (≥ 1) .

(7a) Cette démonstration se lit entre les lignes dans [5], mais j'en ignore la référence exacte. Disons donc prudemment qu'elle est "à la manière de Gauss". A propos de Gauss et de Fermat-Wilson, voir [1], p. 75.

(8) A vrai dire, Fermat savait certainement en un certain sens "démontrer" le premier "axiome" ; en fait, la question n'est pas là ; il faut simplement se rappeler que le symbolisme algébrique utilisé par Fermat (l'algèbre de Viète) était insuffisant pour <u>écrire</u> telle ou telle démonstration (et à vrai dire Fermat a toujours montré une certaine maladresse à "rédiger") ; mais ceci n'empêchait nullement Fermat d'avoir une conception parfaitement claire de ce que serait cette démonstration. Feuilleter [2].

BIBLIOGRAPHIE

[1] DICKSON, Theory of Numbers, Vol. I (Chelsea).

[2] FERMAT, Oeuvres complètes, Vol. II (Gauthier-Villars), spécialement pp. 205-213.

[3] EULER, Oeuvres complètes, spécialement les premiers volumes.

[4] LAGRANGE, "Démonstration d'un théorème nouveau concernant les nombres premiers", Oeuvres complètes, Vol. III.

[5] GAUSS, Recherches Arithmétiques, traduction française par A.C.M. Poullet-Delisle (Blanchard).

[6] HARDY and WRIGHT, The Theory of Numbers (Oxford).

[7] ITARD, Pierre Fermat (Birkhaüser).

(novembre 83)