Arithmétique : le petit théorème de Fermat

Énoncé du petit théorème de Fermat :

Fermat énonce son théorème dans sa lettre à Frénicle du 18 octobre 1640 :

Il me semble après cela qu'il 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 moins 1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous multiple du nombre premier –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.

Exemple : soit la progression donnée

1 2 3 4 5 6

3 9 27 81 243 729 etc.

avec ses exposants en dessus. Prenez, par exemple, le nombre premier 13. Il mesure la troisième puissance moins 1, de laquelle 3, exposant, est sous-multiple de 12, qui est moindre de l'unité que le nombre 13, et parce que l'exposant de 729, qui est 6, est multiple du premier exposant, qui est 3, il s'ensuit que 13 mesure aussi la dite puissance 729- 1. Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers ; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

Autrement dit :

$3^3 \equiv 1[13]$ et $3|12$ avec $12 = 13 - 1$; $3^6 = (3^3)^2 = 729$ alors $729 \equiv 1[13]$:

$3^{12} \equiv 1[13]$ et d'une manière générale $(3^3)^n \equiv 1[13]$.
Il s'agit alors de chercher la plus petite puissance λ pour laquelle $3^\lambda \equiv 1[13]$, ici 3 et dans le cas général, il s'agit de chercher la plus petite puissance λ pour laquelle $a^\lambda \equiv 1[p]$ avec p nombre entier premier et a un entier non divisible par p pour vérifier $a^{p-1} \equiv 1[p]$.

Deux énoncés équivalents :

(1) Si p est un nombre premier et si a est un entier non divisible p, alors $a^{p-1} - 1$ est un multiple de p

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

(2) Si p est un nombre premier et si a est un entier *quelconque*, alors $a^p - a$ est un multiple de p

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

Exemple : $3^{12} - 1$est divisible par 13 ou $3^{13} - 3$ est divisible par 13

Pierre de Fermat (XVIIe) l'énonce pour la première fois en 1640 dans un lettre adressée à son ami Bernard Frenicle de Bessy, il ne donnera pas de preuve de ce théorème :

« *Tout nombre premier mesure infailliblement une des puissances – 1 de quelque progression que ce soit, et l'exposant de la dite 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. »

Soit en termes modernes, pour tout nombre premier p et tout nombre a (premier avec p),
il existe un entier t tel que p divise $a^t - 1$, et, t étant le plus petit entier vérifiant ceci, t divise $p - 1$
et tous les multiples n de t vérifient que p divise $a^p - 1$.

On trouve la dénomination *petit théorème de Fermat* dans un ouvrage de Kurt Hensel de 1913.

Deux résultats :
Lemme d'Euclide (Proposition32 d'Euclide)
si un nombre premier divise un produit, alors il divise l'un des facteurs du produit.
On le rencontre aussi sous sa forme contraposée : si un nombre premier p ne divise ni a ni b, alors il ne divise pas le produit ab.

Lemme de Gauss :
Soient a, b et c trois entiers. Si a divise le produit bc et si a est premier avec b, alors a divise c.

Remarque : une fois le lemme de Gauss démontré, le Lemme d'Euclide devient un corollaire,
or ces résultats sont apparus dans un ordre contraire. La démonstration du Lemme d'Euclide se fait par l'absurde, celle de Gauss utilise l'identité de Bézout, le lemme de Gauss est une généralisation du lemme d'Euclide.

Équivalence des deux propositions :

Deux énoncés équivalents :

(1) Si p est un nombre premier et si a est un entier non divisible p, alors $a^{p-1} - 1$ est un multiple de p

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

(2) Si p est un nombre premier et si a est un entier *quelconque*, alors $a^{p} - a$ est un multiple de p

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

Supposons (1) Si p est un nombre premier et si a est un entier non divisible p, alors $a^{p-1} - 1$ est un multiple de p :

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

$a^{p} - a$ est égal au produit $a\ (a^{p-1} - 1)$ donc est toujours divisible par p, car si le premier facteur, a, n'est pas divisible par p, alors le second, $a^{p-1} - 1$, est divisible par p.

Supposons (2) Si p est un nombre premier et si a est un entier *quelconque*, alors $a^{p} - a$ est un multiple de p :

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

$a\ (a^{p-1} - 1)$ est divisible par p et a et p sont premiers entre eux, d'après le lemme d'Euclide $a^{p-1} - 1$ est divisible par p.

Image wikipédia

Démonstration du petit théorème de Fermat :
La première preuve publiée de ce théorème est une preuve d'Euler (XVIIIe) en 1741.

Gauss mentionne en 1801 que « Ce théorème remarquable, tant par son élégance que par sa grande utilité, s'appelle ordinairement *théorème de Fermat*, du nom de l'inventeur ».

Nous allons voir ***trois démonstrations*** du petit théorème de Fermat, ces trois démonstrations ont un intérêt historique et pédagogique. En effet, les différentes approches de cette démonstration fournissent un recueil de différenciation pédagogique, ***une différenciation par le contenu*** des outils mathématiques utilisés et aussi une différenciation par les raisonnements utilisés.

<u>Voici un extrait de la Théorie des nombres de Legendre [1], démonstration d'Euler (Mémoire de Pétersbourg)</u>

§ I. *Théorèmes sur les nombres premiers.*

(129) THÉORÈME. « Si c est un nombre premier, et N un nombre « quelconque non divisible par c, je dis que la quantité $N^{c-1}-1$ « sera divisible par c, de sorte qu'on aura $\frac{N^{c-1}-1}{c}=$entier$=\mathfrak{Q}$ » (1).

Soit x un nombre entier quelconque, si on considère la formule connue

$$(1+x)^c = 1 + cx + \frac{c.c-1}{1.2}x^2 + \frac{c.c-1.c-2}{1.2.3}x^3 + \ldots + cx^{c-1} + x^c,$$

il est aisé de voir que tous les termes de cette suite, à l'exception du premier et du dernier, sont divisibles par c. En effet, soit M le coefficient de x^m, on aura $M=\frac{c.c-1.c-2\ldots.c-m+1}{1.2.3.\ldots\ldots m}$, ou $M.1.2.3\ldots m = c.c-1.c-2\ldots c-m+1$; et puisque le second membre est divisible par c, il faut que le premier le soit aussi. Mais l'exposant m, dans les termes dont il s'agit, ne surpasse pas $c-1$; donc c, qui est supposé un nombre premier, ne peut diviser le produit $1.2.3\ldots m$; donc il divise nécessairement M pour toute valeur de m depuis 1 jusqu'à $c-1$. Donc la quantité $(1+x)^c-1-x^c$ est divisible par c, quel que soit l'entier x.

Soit maintenant $1+x=N$, la quantité précédente deviendra $N^c-(N-1)^c-1$; et puisqu'elle est divisible par c, si on omet les multiples de c, on aura $N^c-1=(N-1)^c$, ou $N^c-N=(N-1)^c-(N-1)$. Mais en mettant $N-1$ à la place de N, et négligeant toujours les multiples de c, on aura semblablement $(N-1)^c-(N-1)=(N-2)^c-(N-2)$. Continuant ainsi de restes égaux en restes égaux, on parviendra nécessairement au reste $(N-N)^c-(N-N)$, lequel est évidemment zéro. Donc tous les restes précédents le sont ; donc N^c-N est divisible par c.

Mais N^c-N est le produit de N par $N^{c-1}-1$, donc puisque N est supposé non divisible par c, il faudra que $N^{c-1}-1$ soit divisible par c ; *ce qu'il fallait démontrer*.

(1) Ce théorème, l'un des principaux de la théorie des nombres, est dû à Fermat ; il a été démontré par Euler dans divers endroits des Mémoires de Pétersbourg, et notamment dans le tome I des *Novi commentarii*.

« Traduire » cette démonstration pour l'adapter à la classe, Identifier le(s) raisonnement(s).

Note : les congruences ont été introduites plus tard par Gauss.

Exemple de questions pour la classe, les réponses aux questions sont dans le texte de Legendre :

Soit un nombre réel x, on admet que $(1+x)^n = 1 + nx + \cdots + \binom{n}{i} x^{n-1} + \cdots + nx^{n-1} + x^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i}$.

En particulier, on choisira x entier, n est un entier.

1. Montrer que pour i entier compris entre 1 et $n-1$, $\binom{n}{i}$ est divisible par n.
2. En déduire que le nombre entier $(1+x)^n - 1 - x^n$ est divisible par n.
3. On pose $1 + x = a$,
   a. Montrer que pour tout entier naturel a,
   $$a^n - 1 \equiv (a-1)^n [n]$$
   Et
   $$a^n - a \equiv (a-1)^n - (a-1)[n]$$
   b. En déduire que pour tout entier naturel a,
   $$(a-1)^n - (a-1) \equiv (a-2)^n - (a-2)[n]$$
   c. Justifier que pour tout entier naturel a, pour tout i entier compris entre 1 et a,
   $$(a-i)^n - (a-i) \equiv 0[n]$$
   Puis
   $$a^n \equiv a[n]$$

Démonstration par Euler et Leibniz (raisonnement par récurrence) :

a est un entier positif et p nombre premier et la proposition $a^p \equiv a[p]$.

- $a^p \equiv a[p]$ est vraie pour $a = 1$.
- Tout entier k vérifie : $(k+1)^p \equiv k^p + 1[p]$.
  Il suffit, pour cela, de développer l'expression $(k+1)^p$ et de remarquer que tous les coefficients binomiaux à l'exception du premier et du dernier sont des multiples de p car p est premier.
- Si la proposition est vraie pour $a = k$ alors elle l'est aussi pour $a = k+1$. En effet, grâce au point précédent, il est prouvé que $(k+1)^p \equiv k^p + 1[p]$.
  Si de plus $k^p \equiv k[p]$, alors $(k+1)^p \equiv k + 1[p]$.

Cette démonstration nécessite d'avoir au préalable démontré la question 2. de l'exemple d'activité de la démonstration d'Euler par Legendre.

Démonstration de Jules Tannery à l'Ecole Normale Supérieure en 1894 :

p est un nombre premier, chaque nombre non divisible par p est premier à ce nombre : si donc dans l'expression ax où a n'est pas divisible par p on substitue $p - 1$ nombres x non congrus entre eux deux à deux et non congrus à 0 (mod.p), on obtiendra $p - 1$ nombres congrus à ces mêmes nombres x_1 , x_2 ,…x_{p-1} rangés dans un autre ordre ; le produit des nombres ax_1 , ax_2 ,…ax_{p-1} est donc congru (mod.p) au produit $x_1\, x_2 \ldots x_{p-1}$, et comme le dernier produit est premier à p, on en conclut $a^{p-1} - 1 - 1 \equiv 0$ (mod.p). C'est le célèbre théorème de Fermat, qui joue, dans la théorie des nombres, un rôle essentiel et dont nous rencontrerons incidemment d'autres démonstrations ; observons qu'on en déduit immédiatement la proposition suivante : quel que soit le nombre entier a et le nombre premier p, on a $a^p - a \equiv 0$ (mod.p).

Exemple d'exercice pour la classe :

p est un nombre premier et a un nombre entier.

1. Soient $p-1$ nombres $x_1, x_2, \ldots, x_{p-1}$ non congrus entre eux deux à deux et non congrus à 0 modulo p, on note respectivement $r_1, r_2, \ldots, r_{p-1}$ leurs restes de leur division par p. Montrer que ces $p-1$ restes sont tous différents modulo p et qu'ils sont les entiers de 1 à $p-1$.
2. Soit le nombre $ax_i - ax_j$ pour $i \neq j$. Montrer que $ax_i - ax_j$ n'est pas divisible par p.
3. En déduire que les nombres $ax_1, ax_2, \ldots, ax_{p-1}$ sont congrus aux $p-1$ restes non nuls r_1, $r_2 \ldots, r_n$ modulo p puis $ax_1 ax_2 \ldots ax_{p-1} \equiv x_1 x_2 \ldots x_{p-1}[p]$.
4. En déduire $a^{p-1} - 1$ est divisible par p.

Cette démonstration utilise une bijection de l'ensemble des x_i dans l'ensemble des r_i, le raisonnement par l'absurde, et par deux fois le théorème de Gauss.

Exemple d'exercice pour la classe :

p est un nombre premier et a est un entier.

1. On pose $N = a.2a.3a \ldots .(p-1)a$ et r_k le reste de la division euclidienne de ka par p, pour tout entier k de 1 à $p-1$.
2. Montrer que les restes r_i sont deux à deux distincts et non nuls et qu'ils sont les nombres entiers compris entre 1 et $p-1$.
3. Justifier que $N = (p-1)!\, a^{p-1}$.
4. Montrer que $N \equiv r_1 r_2 \ldots r_{p-1}[p]$ soit $N = (p-1)![p]$.
5. En déduire que $a^{p-1} - 1$ est divisible par p.

Bibliographie :

[1] A.M LEGENDRE, Théorie des Nombres, Paris, 1830. Réédition Blanchard 1955

Sitographie :

https://irem.u-paris.fr/utilisation-de-lhistoire-dans-lenseignement-de-larithmetique

https://www.apmep.fr/POUR-UN-SUIVI-EN-ARITHMETIQUE-DE

https://fr.wikipedia.org/wiki/Petit_th%C3%A9or%C3%A8me_de_Fermat