LE PETIT THÉORÈME DE FERMAT

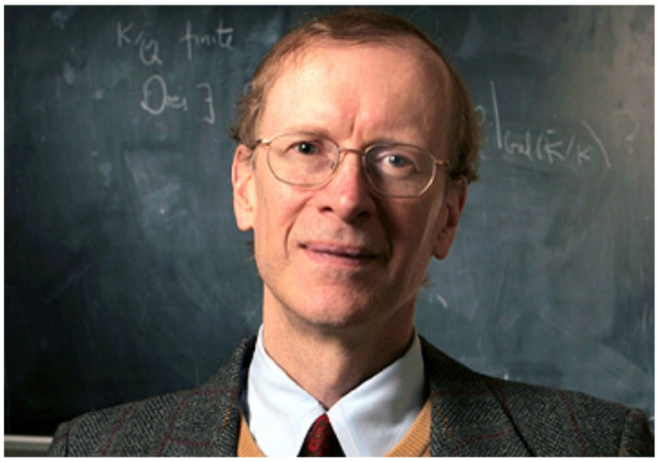
Notions réinvesties : congruences

En octobre 1640, dans une de ses lettres au mathématicien français Frénicle de Bessy, Pierre de Fermat énonçait une conjecture très importante. Démontrée par le mathématicien suisse Leonard Euler dès 1736, elle est désormais connue sous le nom de « petit » théorème de Fermat.

Fermat était un mathématicien atypique, il n'avait rien d'un génie : conseiller au parlement de Toulouse, c'était un réel amateur (au sens noble) en mathématiques.

Il ne faut pas croire que Fermat s'est toujours contenté dénoncer des résultats que d'autres se sont chargés de prouver. Il est l'inventeur de la descente infinie, a développé (avec Pascal) le calcul des probabilités et on lui doit, en optique, le célèbre « Principe de Fermat ».
Il fut sans aucun doute l'un des mathématiciens les plus féconds de son époque.

Il restera dans l'histoire des mathématiques pour son annotation placée en marge d'un de ses ouvrages de Diophante, indiquant que cette dernière était trop petite pour contenir une preuve de ce qu'on appelle aujourd'hui « le grand théorème de Fermat ». Cette conjecture, qui indique qu'il n'existe pas de quadruplet de nombres entiers x, y, z, n, avec x, y, z supérieurs à 1 et n supérieur à 2, tels que : $x^n+y^n=z^n$, ne fut démontrée qu'en 1994 par le mathématicien britannique Andrew Wiles. Autrement dit, il fallut plus de 400 ans et les efforts des plus grands génies des mathématiques pour démontrer ce résultat pourtant facile à énoncer.
La démonstration mise au point par Wiles est un travail énorme, qui utilise de nombreuses idées extrêmement ingénieuses et novatrices et qui a redynamisé une branche entière des mathématiques.



Andrew Wiles

Pierre de Fermat

- PETIT THÉORÈME DE FERMAT

Soit a un entier et p un nombre premier ne divisant pas a : $a^{p-1} \equiv 1\ [p]$.

Conséquence :

Soit p un nombre premier et a un entier premier avec p : $a^{p-1} \equiv 1\ [p]$.

- COROLLAIRE

Soit p un nombre premier et a un entier naturel : $a^p \equiv a\ [p]$.

Dans sa lettre, Fermat écrit :

« 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. »

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 $a^n - 1$.

À cette époque, il est d'usage de ne pas publier les preuves des théorèmes.
Ainsi Leibniz rédige une démonstration vers 1683 mais ne la publie pas.
En 1741, 1750 et 1761, Euler en publie deux qui procèdent par récurrence et utilisent le développement du binôme, et une qui étudie la répartition des restes modulo le nombre premier considéré.
On trouve cette dernière en 1801 dans les *Disquisitiones arithmeticae* de Gauss : il y résume également la première démonstration d'Euler, et en donne une version plus rapide utilisant le développement du multinôme.

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

A. DÉMONSTRATIONS

A.1 Démonstration arithmétique « classique »

Étape 1 : démontrer que $(p-1)!\,a^{p-1} \equiv (p-1)!$ [p].
Étape 2 : en déduire que $a^{p-1} \equiv 1$ [p].

Soit a un entier et p un nombre premier ne divisant pas a.
On note : $N = a \times 2a \times 3a \times \ldots \times (p-1)a$ *ie* $N = (p-1)!\,a^{p-1}$.

Alors $N \equiv r_1 r_2 r_3 \ldots r_{p-1}$ [p].

1. On note r_k le reste de la division euclidienne de ka par p (pour tout entier k de 1 à $p-1$).

a) Démontrer que ces $p-1$ restes sont tous différents.

b) En déduire que $N \equiv (p-1)!$ [p].

2. a) Démontrer que p divise $(p-1)!(a^{p-1}-1)$.

b) En déduire que p divise $a^{p-1}-1$ et conclure.

A.2 Démonstration du corollaire

Soit p un nombre premier et a un entier naturel.

Démontrer que : $a^p \equiv a$ [p].

A.3 Démonstration du corollaire par récurrence

Soit a un entier et p un nombre premier ne divisant pas a .

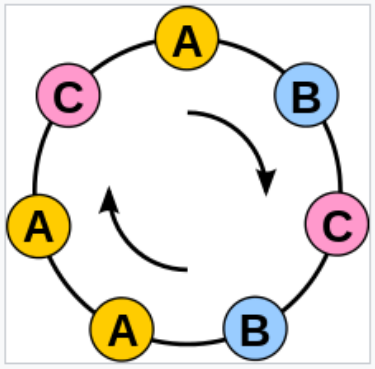
On rappelle que $(a+1)^p=\sum_{k=0}^{p}\binom{p}{k}a^k$.

On admettra que : $\binom{p}{k}=\frac{p!}{k!(p-k)!}$ *ie* $\binom{p}{k}=\frac{p(p-1)(p-2)...(p-k+1)}{k!}$

Démontrer par récurrence sur a que $a^p \equiv a\ [p]$.

A.4 Démonstration du corollaire par double dénombrement

On peut démontrer le petit théorème de Fermat en comptant de deux manières différentes le nombre de mots de p symboles dans un alphabet à a symboles comportant au moins deux symboles différents.



Collier représentant 7 mots différents.

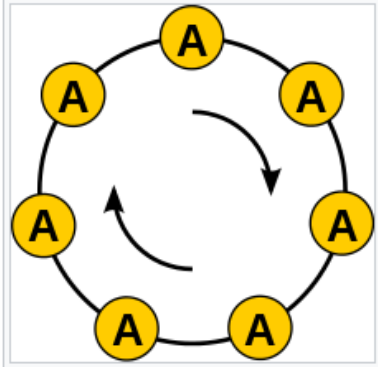
Soit p un nombre premier et a un nombre entier. Considérons un alphabet constitué de a symboles. Comptons les n mots de longueur p dans lesquels il y a au moins deux symboles distincts.

Première méthode : il y a en tout a^p mots de longueur p dans l'alphabet, desquels il faut retirer les a mots constitués d'un seul et même symbole : $n = a^p - a$

Deuxième méthode : ces mots peuvent être groupés en ensembles de mots qui peuvent être déduits l'un de l'autre par permutation circulaire.

On appelle ces ensembles des colliers *(illustration)*.

Par exemple, si l'alphabet est $\{A, B, C, D\}$ et si l'on considère des mots de trois lettres, les trois mots ABD, BDA et DAB sont dans le même collier.



Collier ne représentant qu'un seul mot.

Il y a p mots de p symboles dans chaque collier. En effet, chacune des p permutations donne un mot différent, car p est premier. Ce ne serait pas le cas si p n'était pas premier, il n'y a par exemple que 2 mots différents de 4 symboles dans le collier $ABAB$. On a donc :

$n = p \times$ (nombre de colliers)

En écrivant l'égalité entre ces deux expressions pour n, on trouve que $a^p - a$ est divisible par p.

B. COMPLÉMENTS

Fils d'un riche marchand, Fermat suit des études de droit à Toulouse, Bordeaux et Orléans. Il obtient un confortable poste de conseiller au Parlement de Toulouse. Toutefois, peu passionné par ses fonctions administratives, il réfléchit aux questions mathématiques, qu'il découvre notamment en lisant les œuvres de Diophante traduites par Bachet. Cette activité le conduit à échanger des lettres avec Mersenne et Pascal. Il reçoit le premier à Toulouse, mais n'aura jamais d'échange direct avec le second.

Fermat attrape la peste en 1652, mais en réchappe miraculeusement. Il meurt à Castres 13 ans plus tard.

Le travail mathématique de Fermat porte sur la théorie des probabilités et - ce qui nous intéresse ici - sur l'arithmétique, à laquelle il contribue à redonner vie après une nuit presque totale de plus d'un millénaire.

Il ne publie aucun ouvrage, préférant écrire des lettres et annoter soigneusement les ouvrages qu'il étudie.

Après sa mort, certaines de ses notes sont publiées par son fils dans un ouvrage intitulé *Arithmetica*, qui n'est que la réédition des œuvres de Diophante accompagnée des annotations de Fermat.

L'une des méthodes de démonstration préférées de Fermat, qu'il nomme la descente infinie, est la combinaison d'un raisonnement par l'absurde et d'un raisonnement par récurrence :
pour une propriété donnée $\mathrm{P}(n)$ qui n'est pas vraie pour 0, on démontre que, si $\mathrm{P}(n)$ est vraie, alors $\mathrm{P}(m)$ est vraie pour un entier *m* inférieur à *n*.
Si l'on suppose à présent que $\mathrm{P}(n)$ est vraie pour un entier *n* supérieur à 1, alors on est confronté à une absurdité puisque, de proche en proche, on arrive à $\mathrm{P}(0)$.
On conclut donc que, pour tout n, $\mathrm{P}(n)$ est fausse.

Malgré son caractère parcellaire, la contribution de Fermat à l'arithmétique est importante.
Il a ainsi montré que tout nombre premier impair est différence de deux carrés d'une seule façon.

Fermat remarque que les nombres de la forme $\mathrm{F}_n = 2^{2^n} + 1$ (nommés ***nombres de Fermat***) sont premiers pour $n = 1$, 2, 3 et 4, et conjecture - un peu hâtivement - que cela est vrai pour tout *n*.
Euler lui donnera tort en prouvant que le nombre de Fermat de rang 5 est composé, puisque :

$$\mathrm{F}_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417 .$$

En 1880, F. Landry montrera que : $\mathrm{F}_6 = 274\,177 \times 67\,280\,421\,310\,721$.

On sait même, aujourd'hui, que tous les nombres de Fermat de F_5 à F_{30} sont composés.

On ignore si, parmi les nombres de Fermat, une infinité sont premiers.
De même, on ignore si une infinité de ces nombres sont composés, bien que l'une des deux affirmations soit forcément vraie (et peut-être les deux).