NOMBRES PREMIERS

I. Définition et premières propriétés

DÉFINITION

Un ***nombre premier*** est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même.

REMARQUES : • 0 n'est pas premier, puisqu'il admet une infinité de diviseurs dans $\mathbb{N}$.
• 1 n'est pas premier : il n'admet qu'un seul diviseur, lui-même.
• le seul entier naturel premier qui est pair est 2.

Un entier non premier est appelé ***nombre composé***.

PROPRIÉTÉ

Soit n un entier naturel tel que $n \geqslant 2$.

Si n n'est pas premier, alors n admet au moins un diviseur premier p : son plus petit diviseur dans $\mathbb{N}$ autre que 1, tel que $2 \leqslant p \leqslant \sqrt{n}$.

Démonstration : soit $n \geqslant 2$ tel que n n'est pas premier.

On note E l'ensemble $\{k \in \mathbb{N},\ k \geqslant 2$ et $k \mid n\}$: n n'est pas premier donc $E \neq \emptyset$.
Donc E est une partie non vide de $\mathbb{N}$: elle admet donc un plus petit élément, noté p.
• Supposons par l'absurde que p n'est pas premier. Alors p admet un diviseur d tel que $1 < d < p$.
$d \mid p$ et $p \mid n$ donc $d \mid n$. Or p est le plus petit diviseur de n... Contradiction. Donc p est premier.
• $p \geqslant 2$ et $n = pq$ avec $1 < p \leqslant q$ donc $p^2 \leqslant pq$ donc $p^2 \leqslant n$ donc $p \leqslant \sqrt{n}$.

Par contraposée de cette propriété :

PROPRIÉTÉ TEST DE PRIMALITÉ (CRITÈRE D'ARRÊT)

Soit n un entier naturel tel que $n \geqslant 2$.

Si n n'est divisible par aucun nombre premier p tel que $2 \leqslant p \leqslant \sqrt{n}$, alors n est premier.

EXEMPLE C1

157 est-il premier ?

Rappelons le théorème de Gauss :

> Soient a, b et c trois entiers naturels non nuls.
> Si $c \mid ab$ et $\text{PGCD}(c;a)=1$, alors $c \mid b$.

On en déduit facilement :

> **PROPRIÉTÉ**
> Soient a et b deux entiers naturels non nuls, et p un nombre premier.
> Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration :

Si $\text{PGCD}(p;a)=1$ alors :

Si $\text{PGCD}(p;a)\neq 1$ alors :

Il en découle alors :

- si un nombre premier p divise a^n, alors p divise a.
- si un nombre premier p divise un produit de facteurs premiers, alors p est l'un d'entre eux.

EXEMPLE C2

Soit p un nombre premier supérieur ou égal à 7 qui divise 1985^{1211}.
Montrer que $p=397$.

> **THÉORÈME**
> Il existe une infinité de nombres premiers.

Démonstrations :

DÉMO. EX.
tome-a3-demo
< 7 min

ou

p. 138

2 démonstrations différentes

II. Décomposition en facteurs premiers et nombre de diviseurs

THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE

Soit n un entier naturel tel que $n \geqslant 2$.

n peut se décomposer en produit de facteurs premiers, et cette décomposition est unique à l'ordre des facteurs près : $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r}$.

Démonstration : théorème admis, mais démonstration possible en exercice.

Il découle de l'unicité de la décomposition en facteurs premiers que :

PROPRIÉTÉS

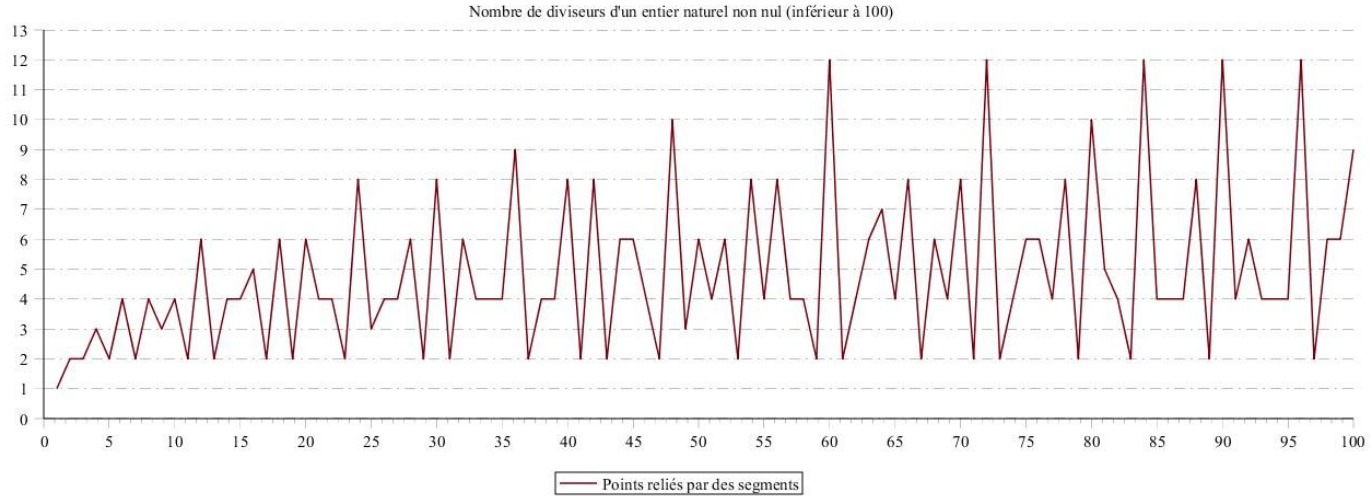
Soit n un entier naturel tel que $n \geqslant 2$: $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r}$.

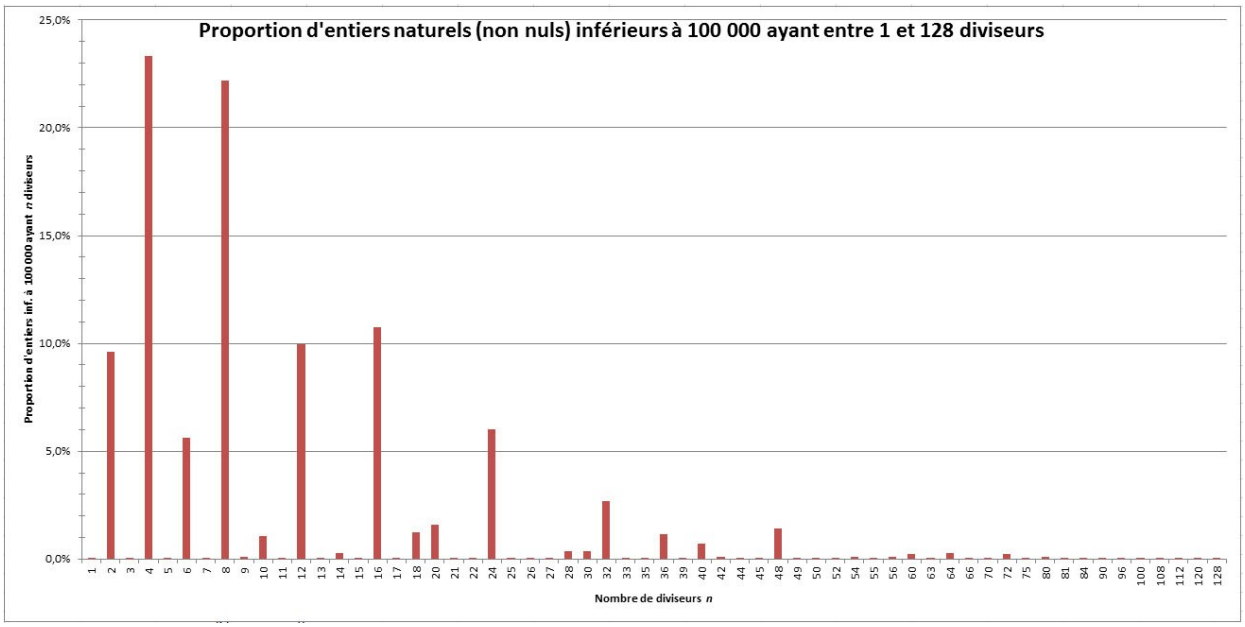
• Tout diviseur de n a pour décomposition $p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_r^{\beta_r}$ où $0 \leqslant \beta_i \leqslant \alpha_i$.

• Le nombre de diviseurs de n est : $\prod_{i=1}^{r} (\alpha_i + i)$.

Voici quelques extraits d'un article que j'ai écrit en 2017 :

lien : https://www.mathemathieu.fr/33-theorie-probabiliste-nombres-thm-fondateurs





REMARQUE : les entiers naturels non nuls inférieurs à n ont, en moyenne, environ $\ln n$ diviseurs (cette approximation étant d'autant plus précise que n est grand). On dit qu'en ***ordre moyen***, le nombre de diviseurs d'un entier compris entre 1 et n est $\ln n$.
Par exemple, en calculant la moyenne exacte du nombre de diviseurs des entiers inférieurs ou égaux à 100 000, on trouve $\frac{1166750}{100000}=11{,}6675$ et $\ln(100000)\approx 11{,}51$.
Mais qu'en est-il du nombre moyen de facteurs premiers ?
En 1917, Hardy et Ramanujan ont montré qu'en ordre moyen, le nombre de facteurs premiers distincts d'un entier inférieur ou égal à n est $\ln\ln n$.
Il est donc possible d'avoir une information sur la moyenne de facteurs premiers distincts d'un entier… mais cela ne nous dit rien sur la plupart des entiers ! En effet, dire qu'une classe a obtenu 12,3 de moyenne à un devoir surveillé ne donne aucune indication sur la répartition des notes : il se peut que la plupart des élèves ait eu entre 11 et 13, comme il se peut que les notes soient très dispersées entre 1 et 20.
Voilà pourquoi Hardy et Ramanujan ont introduit la notion d'***ordre normal***, et ont démontré que « la plupart des entiers » n ont $\ln\ln n$ facteurs premiers distincts… Pour en savoir davantage et découvrir notamment le théorème de Erdös-Kac (1939) :

https://www.mathemathieu.fr/33-theorie-probabiliste-nombres-thm-fondateurs

III. Petit théorème de Fermat

PETIT THÉORÈME DE FERMAT

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

***Démonstration** sous forme d'exercice* : → correction disponible sur mathemathieu.fr/1711

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* $N=(p-1)!\,a^{p-1}$.

On note r_k le reste de la division euclidienne de ka par p (pour tout entier k de 1 à $p-1$).
Alors $N\equiv r_1r_2r_3\ldots r_{p-1}\ [p]$.

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.

Une simple conséquence de ce théorème est :

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

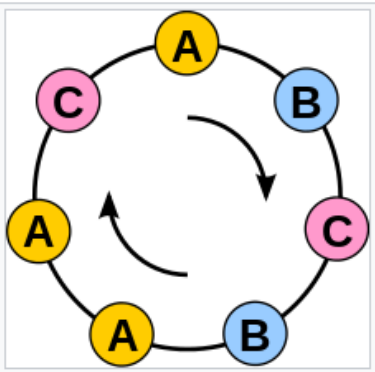
COROLLAIRE DU PETIT THÉORÈME DE FERMAT

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

Démonstrations : *voir* mathemathieu.fr/1712 *pour la démonstration classique,*
et mathemathieu.fr/1713 *pour une démonstration par récurrence.*

Exercice intéressant : démontrer que le petit théorème de Fermat, sa conséquence et son corollaire ci-dessus sont des énoncés équivalents.

On peut aussi démontrer ce corollaire par double dénombrement, comme on le trouve sur Wikipédia :



Collier représentant 7 mots différents.

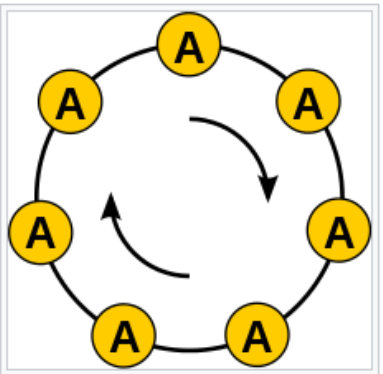
Soit p un nombre premier et a un nombre entier. Considérons un alphabet constitué de a symboles. Comptons les n mots de longueur p dans lesquels il y a au moins deux symboles distincts.

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.

EXEMPLE A2

p. 141 méthode 5

Montrer que pour tout $n \in \mathbb{N}$, $3^{6n}-1$ est divisible par 7.

→ BILAN DU CHAPITRE & TRAVAIL EN AUTONOMIE ←

- Fiche bilan → p.153
- QCM 8 questions corrigées → p.153
- Exercices corrigés → 113 à 122 p.155
- Exercices types corrigés → méthodes 6 et 7 p.142/143

→ Fils d'un riche marchand, Pierre de Fermat (première décennie du XVII^{e} siècle - 1665) naît à Beaumont-de-Lomagne (Tarn-et-Garonne), près de Montauban. Il suit des études de droit à Toulouse, Bordeaux et Orléans puis 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 unique de deux carrés.

→ 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 par contre 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).

→ 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. Mais il fut sans aucun doute l''un des mathématiciens les plus féconds de son époque, et 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 $n>2$, 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.