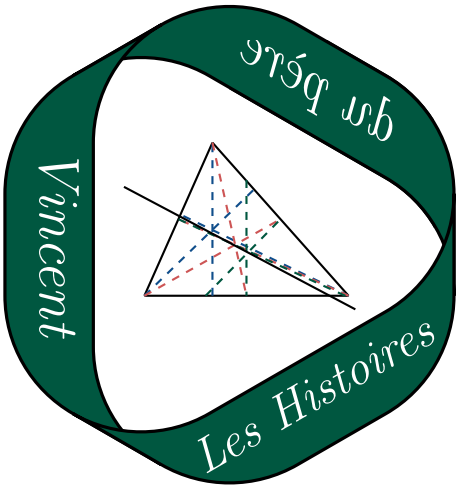
Lycée Lucie Aubrac - Terminale



Chapitre 6
Arithmétique
Nombres premiers

Table des matières

1 L'ensemble des nombres premiers

Définition 1

Un entier naturel est un **nombre premier** s'il admet exactement deux diviseurs positifs : 1 et lui même.

Exemples.
La liste des nombres premiers inférieurs à 30 est la suivante : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29.

Remarque.
L'entier 1 n'est pas un nombre premier car il n'admet qu'un seul diviseur.

Proposition 1

Tout entier naturel supérieur ou égal à 2 est divisible par un nombre premier.

Démonstration.
On va montrer par récurrence que la propriété $\mathcal{P}(n)$:« Tout entier naturel compris entre 2 et n est divisible par un nombre premier » est vraie pour tout entier $n \geqslant 2$.
Initialisation : Pour $n = 2$, la propriété est vraie car 2 est divisible par 2 qui est premier.
Hérédité : Supposons que $\mathcal{P}(n)$ soit vraie pour un certain entier $n \geqslant 2$ et montrons qu'alors $\mathcal{P}(n+1)$ est vraie.
Soit k un entier tel que $2 \leqslant k \leqslant n+1$. L'objectif est de montrer que k est divisible par un nombre premier.
Si $2 \leqslant k \leqslant n$, d'après $\mathcal{P}(n)$, il est clair que k est divisible par un nombre premier.
Si $k = n+1$, on distingue deux cas :

- Si k est premier, il est divisible par lui-même donc par un nombre premier.
- Si k n'est pas premier, cela signifie qu'il existe des entiers a et b tels que $k = ab$ et tels que $2 \leqslant a \leqslant n$ et $2 \leqslant b \leqslant n$.
  On peut alors appliquer l'hypothèse $\mathcal{P}(n)$ à l'entier a. Ainsi, a est divisible par un nombre premier p. Par conséquent, $p|a$ et $a|k$ donc, par transitivité, $p|k$.

Dans tous les cas, on a montré que $\mathcal{P}(n+1)$ est vraie. □

Remarque. La propriété de récurrence est ici un peu particulière. Elle concerne tout entier inférieur ou égal à n et pas seulement l'entier n. On dit qu'il s'agit d'une propriété de récurrence forte.

Proposition 2

Soit $n \geqslant 2$.

- Soit n est un nombre premier ;
- Soit n est divisible par un nombre premier compris entre 2 et $\sqrt{n}$.

Démonstration.
Soit $n \geqslant 2$. Supposons que n ne soit pas premier.

Cela signifie qu'il existe des entiers a et b, avec $a > 1$ et $b > 1$ tels que $n = ab$.
L'un des deux entiers a, ou b est inférieur ou égal à $\sqrt{n}$ car sinon, on aurait $ab > n$.
Supposons par exemple, que $a \leqslant \sqrt{n}$ (le cas $b \leqslant \sqrt{n}$ se traite de la même manière).
D'après la propriété 1, a est divisible par un nombre premier p. Comme $p|a$ et $a|n$, on en déduit, par transitivité que $p|n$. De plus, on a bien $p \leqslant \sqrt{n}$.

□

Méthode – Démontrer qu'un entier est premier

- Dresser la liste de tous les nombres premiers inférieurs ou égaux à $\sqrt{n}$.
- Vérifier qu'aucun de ces nombres ne divise n.

Exemple.
Montrer que l'entier 71 est premier.

Solution :
Supposons par l'absurde que 71 ne soit pas premier.
Il existerait alors un diviseur premier de 71 compris entre 2 et $\sqrt{71}$.
Or $\sqrt{71} < 9$. Ainsi, 71 serait divisible par l'un des entiers suivants : 2, 3, 5, 7.

- D'après les critères de divisibilité, il est clair que 2, 3 et 5 ne divisent pas 71.
- De plus, 7 ne divise pas 71 car le reste de la division de 71 par 7 est 1.

Finalement, aucun de ces nombres ne divise 71, ce qui est absurde.
Cela signifie que 71 est premier.

Proposition 3

Il existe une infinité de nombres premiers.

Démonstration.
Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombre premiers.
On note p_1, p_2, $\ldots$, p_n ces nombres premiers. On considère alors l'entier $N = p_1 \times p_2 \times \ldots \times p_n + 1$.
D'après la propriété 1, N est divisible par l'un des nombres premiers.
Autrement dit, il existe $1 \leqslant i \leqslant n$ tel que p_i divise N.
On a donc $N \equiv 0\,[p_i]$
Or, $N \equiv p_1 \times p_2 \times \ldots \times p_n + 1 \equiv 1\,[p_i]$, ce qui est absurde. □

Histoire – Infinité des nombres premiers

L'infinité de l'ensemble des nombres premiers est énoncé et démontré dans les *Éléments* d'**Euclide**. Plus tard, les mathématiciens continuèrent d'étudier la répartition des nombres premiers. Par exemple, en utilisant les congruences, l'allemand **Gustav Lejeune Dirichlet (1805-1859)** a pu établir le théorème de progression arithmétique : si a et b sont premiers entre eux, il existe une infinité de nombres premiers de la forme $an + b$.

Dirichlet

2 Décomposition en produit de facteurs premiers

Proposition 4

Pour tout entier $n \geqslant 2$, il existe des nombres premiers distincts $p_1, p_2, \ldots, p_k$ et des entiers $\alpha_1, \alpha_2, \ldots, \alpha_k$ tels que $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$.
De plus, cette décomposition est unique à l'ordre des facteurs près.

Démonstration.
Démontration de l'existence : On va montrer par récurrence que la propriété $\mathcal{P}(n)$:« Pour entier naturel k compris entre 2 et n, k se décompose en produit de nombres premiers » est vraie pour tout entier $n \geqslant 2$.
Initialisation : Il est clair que $\mathcal{P}(2)$ est vraie.
Hérédité : Supposons que $\mathcal{P}(n)$ soit vraie pour un certain entier $n \geqslant 2$ et montrons qu'alors $\mathcal{P}(n+1)$ est vraie.
Pour montrer que $\mathcal{P}(n+1)$ est vraie, il suffit de montrer que $n+1$ admet une décomposition en produit de nombres premiers.
Si $n+1$ est un nombre premier, alors $\mathcal{P}(n+1)$ est vraie.
Sinon, d'après la propriété 1, $n+1$ admet un diviseur premier p. Par conséquent, il existe un entier k tel que $n+1 = kp$ (avec $2 \leqslant k \leqslant n$).
D'après l'hypothèse $\mathcal{P}(n)$, k se décompose en produit de nombres premiers et par conséquent, $n+1$ aussi. Ainsi, on a montré que $\mathcal{P}(n+1)$ est vraie.

Démontration de l'unicité : Soit $n \geqslant 2$. On suppose par l'absurde qu'un certain nombre premier p apparaît avec l'exposant α dans une décomposition de n et avec l'exposant β dans une autre décomposition de n (avec éventuellement $\beta = 0$ si p n'apparaît pas dans la deuxième décomposition).
Ainsi, il existe des entiers a et b premiers avec p tels que $n = p^\alpha a$ et $n = p^\beta b$.
Si $\alpha > \beta$, alors $a = p^{\alpha-\beta} b$. Par conséquent, $p|a$, ce qui est impossible.
De même si $\beta > \alpha$, alors $b = p^{\beta-\alpha} a$. Par conséquent, $p|b$, ce qui est impossible.
Finalement, on a montré que $\alpha = \beta$, ce qui prouve l'unicité de la décomposition. □

Proposition 5 – Corollaire

Soit $n \geqslant 2$ un entier dont la décomposition en produit de nombres premiers est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$. Alors,

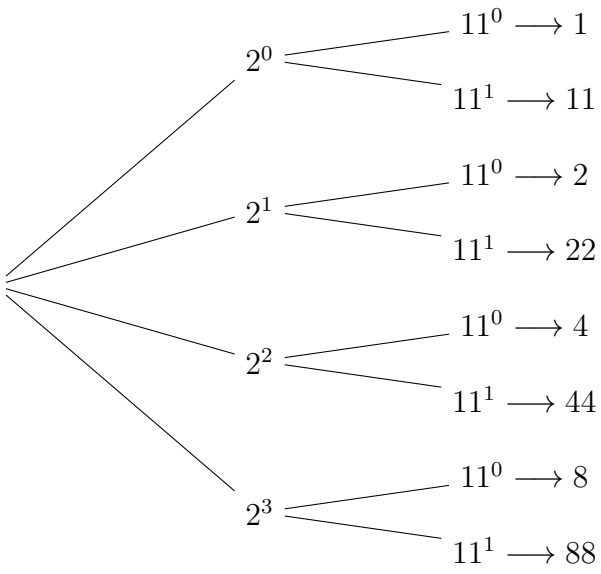
- les diviseurs de n sont les nombres de la forme :
$$n = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k} \quad (\text{avec } 0 \leqslant \beta_i \leqslant \alpha_i, \text{ pour tout } i).$$
- le nombre de diviseurs de n est $(\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1)$.

Méthode – Déterminer l'ensemble des diviseurs d'un entier

- Décomposer l'entier en produit de nombres premiers.
- Énumérer les diviseurs en utilisant un arbre permettant de lister les différentes possibilités.

Exemple.
Déterminer l'ensemble des diviseurs de 88.

Solution :
$88 = 2^3 \times 11$ donc ses diviseurs sont de la forme $2^{\beta_1} \times 11^{\beta_2}$, avec $0 \leqslant \beta_1 \leqslant 3$ et $0 \leqslant \beta_2 \leqslant 1$.
L'arbre suivant permet d'énumérer toutes les possibilités.



Ainsi, les diviseurs de 88 sont 1, 2, 4, 8, 11, 22, 44 et 88.

Proposition 6

Soient n et m deux entiers naturels supérieurs ou égaux à 2. On suppose, quitte à utiliser des exposants nuls, que m et n peuvent s'écrire sous forme de produit de nombres premiers de la manière suivante :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k} \quad \text{et} \quad m = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}.$$

On a alors :
- $\text{PGCD}(n\,;m) = p_1^{\min(\alpha_1\,\beta_1)} \times p_2^{\min(\alpha_2\,\beta_2)} \times \ldots \times p_k^{\min(\alpha_k\,\beta_k)}$
- $\text{PPCM}(n\,;m) = p_1^{\max(\alpha_1\,\beta_1)} \times p_2^{\max(\alpha_2\,\beta_2)} \times \ldots \times p_k^{\max(\alpha_k\,\beta_k)}$

Exemple.
Les décompositions de 126 et 196 sont $126 = 2 \times 3^2 \times 7$ et $196 = 2^2 \times 3^0 \times 7^2$.
Par conséquent, $\text{PGCD}(126\,;196) = 2^1 \times 3^0 \times 7^1 = 14$.
De plus, $\text{PPCM}(126\,;196) = 2^2 \times 3^2 \times 7^2 = 1764$.

Remarque.
En pratique, pour des grands nombres, la décomposition en produit de nombres premiers est difficile à obtenir. La meilleure méthode pour déterminer un PGCD reste donc l'algorithme d'Euclide. La propriété 6 ci-dessus peut néanmoins avoir un intérêt pour résoudre des questions d'ordre théorique.

3 Petit théorème de Fermat

Proposition 7 – Lemme

Si p est un nombre premier et k un entier tel que $1 \leqslant k \leqslant p-1$, alors p divise $\binom{p}{k}$.

Démonstration.
Soit p un nombre premier et k un entier tel que $1 \leqslant k \leqslant p-1$. On a $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$.
Par conséquent, $k!\binom{p}{k} = \dfrac{p!}{(p-k)!}$.
Comme $k \geqslant 1$, on voit que p divise $\dfrac{p!}{(p-k)!}$.
Cela signifie que p divise $k!\binom{p}{k}$.
Or, comme $k \leqslant p-1$, $k!$ et p sont premiers entre eux.
D'après le théorème de Gauss, on en déduit donc que p divise $\binom{p}{k}$. □

Proposition 8

Si p est un nombre premier alors pour tout entier a, $a^p \equiv a\,[p]$.

Démonstration.
Soit p un nombre premier.
Montrons par récurrence que la propriété $\mathcal{P}(a)$:« $a^p \equiv a\,[p]$ » est vraie pour tout entier $a \geqslant 0$.
Initialisation : Il est clair que $\mathcal{P}(0)$ est vraie.
Hérédité : Supposons que $\mathcal{P}(a)$ soit vraie pour un certain entier $a \geqslant 0$ et montrons qu'alors $\mathcal{P}(a+1)$ est vraie.
On a :

$$\begin{aligned}
(a+1)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k \\
&= 1 + \left(\sum_{k=1}^{p-1} \binom{p}{k} a^k \right) + a^p \\
&\equiv 1 + a^p\,[p] \quad \left(\text{car pour tout } 1 \leqslant k \leqslant p-1,\ p \text{ divise } \binom{p}{k} \right) \\
&\equiv 1 + a\,[p] \quad (\text{d'après l'hypothèse } \mathcal{P}(a))
\end{aligned}$$

Ainsi, on a montré que $(a+1)^p = a+1$ donc $\mathcal{P}(a)+1$ est vraie.

□

Proposition 9 – Petit théorème de Fermat

Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} \equiv 1\,[p]$.

Remarque.
Dans le cas où a est divisible par p, on a $a^{p-1} \equiv 0\,[p]$.

Démonstration.
Soit p un nombre premier et a un entier non divisible par p.
D'après la propriété précédente, $a^p \equiv a\,[p]$ $\quad(\star)$.
Or, comme p est premier et ne divise pas a, p est donc premier avec a.
Par conséquent, a est inversible modulo p.
En multipliant l'égalité $(\star)$ par l'inverse de a, on obtient $a^{p-1} \equiv 1\,[p]$. □

Exemple.
29 est un nombre premier et 250 n'est pas divisible par 29. On a donc $250^{28} \equiv 1\,[29]$.

Histoire – Grand théorème de Fermat

Le petit théorème de Fermat est à distinguer du grand théorème de Fermat, beaucoup plus difficile à démontrer. Ce théorème indique que l'équation $x^n + y^n = z^n$ (où n est un entier supérieur ou égal à 3) admet aucune solution entière et non nulle. Dans un ouvrage publié au XVII^{e} siècle, **Pierre de Fermat** avait énoncé ce résultat en ajoutant : « j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir ». Il s'était vraisemblablement trompé et de nombreux mathématiciens ont cherché à démontré ce résultat depuis. En particulier, au XIX^{e} siècle, **Sophie Germain (1776-1831)** a démontré le théorème pour une certaine classe d'exposants (les nombres premiers dits de Sophie Germain). Finalement, ce n'est qu'en 1994, plus de 350 ans après que Fermat ait énoncé le théorème, que le britannique **Andrew Wiles** parvient à une démonstration complète.

Andrew Wiles

Savoir-faire du chapitre

- Déterminer si un nombre est premier ou non.
- Dresser la liste des nombre premiers inférieurs à un nombre donné.
- Décomposer un nombre en produit de facteurs premiers.
- Déterminer les diviseurs d'un entier à partir de la décomposition en facteurs premiers.
- Déterminer le PGCD et le PPCM de deux entiers à partir de la décomposition en facteurs premiers.
- Cacluler des puissances modulo un nombre premier en utilisant le petit théorème de Fermat.
- Utiliser un raisonnement par récurrence forte.

QCM d'entrainement