# Nombres premiers

## 1. Nombres premiers et nombres composés

**Définition.** *Un entier naturel différent de 1 est dit premier si ses seuls diviseurs positifs sont 1 et lui-même. Il est dit composé dans le cas contraire.*
*Les diviseurs d'un entier composé différents de 1 et lui-même sont appelés diviseurs stricts.*

**Exemple**

Les nombres premiers inférieurs à 20 sont 2, 3, 5, 7, 11, 13, 17 et 19.

**Théorème 1.**
**1.** S'il existe deux entiers $a$ et $b$ tels que $n = ab$ avec $a \geq 2$ et $b \geq 2$, alors $n$ est composé.
**2.** Si $n$ est composé, il existe deux entiers $a$ et $b$ tels que $n = ab$ avec
$$2 \leq a < n \text{ et } 2 \leq b < n.$$

**Démonstration.**
**1.** Puisque $a \geq 2$, on a $b = \frac{n}{a} \leq \frac{n}{2} < n$, et comme de plus $b \geq 2$, cela montre que $b$ est un diviseur de $n$ autre que 1 et $n$, donc $n$ est composé.
**2.** Si $n$ est composé, il existe un diviseur strict $a$ de $n$, donc vérifiant $2 \leq a < n$ et $n = ab$ pour un entier $b$. Mais $b = \frac{n}{a}$, d'où
$$2 \leq a < n \Rightarrow \frac{1}{n} < \frac{1}{a} \leq \frac{1}{2} \Rightarrow 1 < \frac{n}{a} \leq \frac{n}{2} \Rightarrow 2 \leq b < n. \quad \blacksquare$$

**Exemple**

Démontrons que si la somme de deux entiers naturels non nuls $a$ et $b$ est un nombre premier, alors $a$ et $b$ sont premiers entre eux.
On raisonne par contraposée. Soit $a$ et $b$ deux entiers naturels non nuls qui ne sont pas premiers entre eux ; il existe un entier $k \geq 2$ divisant $a$ et $b$, donc divisant $a + b$.
Par ailleurs on a $k \leq a$ et $k \leq b$, d'où $2k \leq a + b$, puis $k \leq \frac{a+b}{2} < a + b$ car $a + b > 0$.
Il existe donc un diviseur $k$ de $a + b$ vérifiant $2 \leq k < a + b$, ce qui montre que $a + b$ n'est pas premier.

**Théorème 2.** Soit $n \geq 2$ un entier naturel. Le plus petit diviseur de $n$ compris entre 2 et $n$ est premier.

**Démonstration.** Soit $p$ le plus petit des diviseurs de $n$ compris entre 2 et $n$ (l'ensemble de ces diviseurs n'est pas vide, il contient $n$).
Si $p$ n'était pas premier, il admettrait un diviseur $d$ vérifiant $1 < d < p$, donc $d$ serait un diviseur de $n$ strictement inférieur à $p$, ce qui contredirait le caractère minimal de $p$. $\blacksquare$

**Corollaire 3.** Soit $n \geq 2$ un entier naturel.
**1.** Si $n$ est composé, alors il admet un diviseur premier inférieur ou égal à $\sqrt{n}$.
**2.** Si aucun des entiers premiers compris entre 2 et $\sqrt{n}$ ne divise $n$, alors $n$ est premier.

**Démonstration.** Soit $n$ un entier naturel composé et $d$ son plus petit diviseur strict, qui est premier d'après le théorème précédent. On a donc $n = dd'$ avec $d \leq d'$, d'où l'on déduit $dd \leq dd'$, soit $d^2 \leq n$, et enfin $d \leq \sqrt{n}$.
Le deuxième point est la contraposée du premier. ■

❖ **Infinitude des nombres premiers**

**Théorème 4.** Il existe une infinité de nombres premiers.

**Démonstration.** Supposons qu'il n'existe qu'un nombre fini $k$ de nombres premiers

$$p_1, p_2, \ldots, p_k$$

et considérons leur produit $A = p_1 p_2 \ldots p_k$. Alors l'entier $A + 1$ n'est pas premier car pour tout $1 \leq i \leq k$, on a $A + 1 > p_i$ (et les $p_i$ sont les seuls nombres premiers !), donc d'après le corollaire 2, il admet un diviseur premier strictement inférieur à $A + 1$, donc l'un des $p_i$. Or $A + 1$ n'est divisible par aucun des $p_i$ car sinon $p_i$ diviserait la différence

$$(A + 1) - A = 1.$$

On a donc prouvé par l'absurde qu'il existe une infinité de nombres premiers. ■

## 2. Recherche de nombres premiers

❖ **Test de primalité**

Le corollaire 3 donne un moyen pratique de déterminer si un nombre est premier ou pas.

**Exemple**

89 est premier car $\sqrt{89} < 10$ et ni 2, ni 3, ni 5, ni 7 ne divise 89.

L'algorithme suivant prend en entrée un entier $n$ et teste s'il existe un diviseur de $n$ compris entre 2 et $\sqrt{n}$.

```
Pour d de 2 à partie entière de √n
  Si d divise n
    Afficher « Non premier »
    Stopper le programme
  Fin Si
Fin Pour
Afficher « Premier »
```

Une version plus efficace de ce programme consisterait à ne tester que les diviseurs premiers inférieurs à $\sqrt{n}$, mais encore faut en connaître la liste…

❖ **Crible d'Ératosthène**

Le crible d'Ératosthène est un algorithme permettant de déterminer la liste des nombres premiers inférieurs ou égaux à un entier $n \geq 2$.
On écrit la liste des entiers de 2 à $n$, on raye les multiples de 2, puis à chaque fois on raye les multiples du plus petit entier restant (sauf l'entier lui-même).
On peut s'arrêter lorsque le carré du plus petit entier restant est supérieur à $n$.

Voici un exemple pour $n = 25$.

| | | | | |
|---|---|---|---|---|
| | 2 | 3 | | 5 |
| | 7 | | 9 | |
| 11 | | 13 | | 15 |
| | 17 | | 19 | |
| 21 | | 23 | | 25 |

Suppression des multiples de 2

| | | | | |
|---|---|---|---|---|
| | 2 | 3 | | 5 |
| | 7 | | | |
| 11 | | 13 | | |
| | 17 | | 19 | |
| | | 23 | | 25 |

Suppression des multiples de 3

| | | | | |
|---|---|---|---|---|
| | 2 | 3 | | 5 |
| | 7 | | | |
| 11 | | 13 | | |
| | 17 | | 19 | |
| | | 23 | | |

Suppression des multiples de 5

L'algorithme suivant renvoie la liste $L$ des nombres premiers compris entre 2 et $n$.

```
L est la liste des entiers de 2 à n
d ← 2
Tant que d ≤ √n
  Supprimer de L les multiples de d strictement supérieurs à d
  d ← le successeur de d dans L
```

## 3. Nombres premiers et divisibilité

**Lemme 5.** Soit $p$ un nombre premier et $a$ un entier.
Alors $a$ et $p$ sont premiers entre eux si et seulement si $p$ ne divise pas $a$.

**Démonstration.** Comme $p$ est premier, $\text{Div}(p) = \{1; p\}$. Par conséquent

$$\text{Div}(a; p) \subset \{1; p\}.$$

Il y a donc deux possibilités :

- $\text{Div}(a; p) = \{1\}$ et dans ce cas $a$ et $p$ sont premiers entre eux ;
- $\text{Div}(a; p) = \{1; p\}$, dans ce cas $p \in \text{Div}(a)$, ce qui montre que $p$ divise $a$. ■

**Corollaire 6.** Si un entier premier divise un produit de facteurs $ab$, alors il divise au moins l'un des facteurs $a$ ou $b$.

**Démonstration.** Soit $p$ un nombre premier divisant le produit $ab$.
Si $p$ divise $a$, la conclusion est acquise.
Si $p$ ne divise pas $a$, alors comme $p$ est premier, $a$ et $p$ sont premiers entre eux d'après le lemme 5. Du théorème de Gauss, il résulte que $p$ divise $b$. ■

**Corollaire 7.** Si un entier $p$ premier divise un produit de nombres premiers, alors $p$ est égal à l'un d'eux.

**Démonstration.** Soit $p$, $a$, $b$ trois nombres premiers tel que $p$ divise $ab$.
Puisque $a$ et $p$ sont premiers, alors d'après le lemme 5, il y a deux possibilités :

- soit $p$ divise $a$, ce qui revient à dire $p = a$ puisque $a$ est premier et la conclusion est acquise ;
- soit $p$ est premier avec $a$, alors d'après le théorème de Gauss, $p$ divise $b$. Comme $b$ est premier, on conclut que $p = b$. ■

## 4. Décomposition en facteurs premiers

**Théorème 8.** Tout entier naturel $n \geq 2$ s'écrit de façon unique comme produit de nombres premiers.

Précisons l'énoncé. Pour tout entier naturel $n \geq 2$,

- il existe $k$ entiers premiers distincts $p_1$, $p_2$, …, $p_k$ et $k$ entiers naturels strictement positifs $\alpha_1$, $\alpha_2$, …, $\alpha_k$ tels que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ;
- il y a unicité de cette décomposition à l'ordre des facteurs près. Autrement dit, si
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \dots q_\ell^{\beta_\ell},$$
alors $k = \ell$ et $\{p_1; p_2; \dots; p_k\} = \{q_1; q_2; \dots; q_k\}$.

**Exemple**

- $45 = 3^2 \times 5$ ;
- 19 est sa propre décomposition.

**Démonstration.**

**Existence.** On va démontrer pour récurrence sur $n \geq 2$ la propriété « tout entier $k$ compris entre 2 et $n$ possède une décomposition en facteurs premiers ».

La propriété est vraie pour $n = 2$ car le seul entier $k$ concerné est 2 qui est bien un produit de nombre premier.

Supposons la propriété vraie pour un entier $n$.

Si $n + 1$ est premier, la conclusion est atteinte, sinon $n + 1$ possède un diviseur premier strict $p$ vérifiant $1 < p < n + 1$. On a alors $1 < \frac{n+1}{p} < n + 1$, soit $2 \leq \frac{n+1}{p} \leq n$, donc d'après l'hypothèse de récurrence $\frac{n+1}{p}$ possède une décomposition en facteurs premiers $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, d'où l'on déduit $n + 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} p$.

**Unicité.** Raisonnons par l'absurde, soit $n$ le plus petit entier tel qu'il existe deux décompositions distinctes $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \dots q_\ell^{\beta_\ell}$.

L'entier $p_1$ divise $q_1^{\beta_1} q_2^{\beta_2} \dots q_\ell^{\beta_\ell}$, donc, par le corollaire 7, il est égal à l'un des $q_i$, par exemple $p_1 = q_1$, et en simplifiant :
$$\frac{n}{p_1} = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = q_1^{\beta_1 - 1} q_2^{\beta_2} \dots q_\ell^{\beta_\ell}.$$
On a éventuellement $\alpha_1 - 1 = 0$ ou $\beta_1 - 1 = 0$, ce qui signifie que $p_1$ ou $q_1$ n'apparaissent plus dans la décomposition.

Comme $\frac{n}{p_1} < n$, par minimalité de $n$ ces deux décompositions de $\frac{n}{p_1}$ sont identiques. En multipliant par $p_1$, on en déduit que celles de $n$ aussi, ce qui est absurde. ■

**Exemple**

Montrons que $\sum_{k=1}^{n} \frac{1}{k}$ n'est jamais un entier.

Soit $p$ l'unique entier tel que $2^p \leq n < 2^{p+1}$. Les entiers $k$ compris entre 1 et $n$ et distincts de $2^p$ admettent au plus $p - 1$ facteurs 2 dans leur décomposition en facteurs premiers. La somme de leurs inverses se réduit au même dénominateur sous la forme $\frac{N}{2^{p-1} m}$ avec $m$ impair.

Ainsi $\sum_{k=1}^{n} \frac{1}{k} = \frac{1}{2^p} + \frac{N}{2^{p-1}m} = \frac{m+2N}{2^p m}$ n'est pas un entier puisque le numérateur est impair et le dénominateur pair.

**Théorème 9.** Il existe une infinité de nombres premiers de la forme $4n-1$, $n \in \mathbb{N}^*$

**Démonstration.** Supposons qu'il n'existe qu'un nombre fini de nombres premiers

$$p_1, p_2, \ldots, p_k$$

de la forme $4n-1$ ; considérons $P = p_1 p_2 \ldots p_k$ leur produit ainsi que $Q = 4P - 1$.
Pour tout $1 \leq i \leq k$, on a $P \geq p_i$, donc $Q = 4P - 1 \geq 4p_i - 1 > 4p_i > p_i$, ainsi $Q$ n'est pas premier puisqu'il est de la forme $4n-1$ et supérieur à tous les $p_i$.
$Q$ est impair donc si un nombre premier $p$ le divise, il est nécessairement de la forme $4k-1$ ou $4k+1$ (car $4k$ et $4k+2$ sont pairs). Mais si $p$ était de la forme $4k-1$, ce serait l'un des $p_i$ et comme il divise $P$, il diviserait $Q - 4P = -1$, ce qui est absurde.
Ainsi la décomposition en facteurs premiers de $Q$ ne comporte que des nombres premiers $p$ vérifiant $p \equiv 1\ [4]$, donc par produit $Q \equiv 1\ [4]$ d'après les propriétés sur les congruences. C'est en contradiction avec $Q = 4P - 1 \equiv -1\ [4]$.
Ainsi il existe une infinité de nombres premiers de la forme $4k-1$. ■