# Nombres premiers

\*\*\*

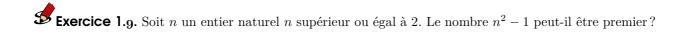
## I. Définition d'un nombre premier

#### Définition.

Un entier naturel n est dit **premier** s'il possède **exactement** deux diviseurs dans  $\mathbb{N}$ : 1 et lui même. Enfin, si cet entier naturel n, distinct de 1, est non premier, on dira qu'il est **composé**.

#### Exemples, contre-exemples.

- 2 est **premier** car ses seuls diviseurs positifs sont 1 et 2.
- 0 n'est pas premier car il possède une infinité de diviseurs positifs.
- 1 n'est pas premier car il de possède qu'un seul diviseur, lui-même!



#### Théorème.

Il existe une infinité de nombres premiers.

#### **Démonstration**

Raisonnons par l'absurde : supposons qu'il existe un nombre fini de nombres premiers. Soit p le plus grand d'entre eux.

Soit N le produit de tous ces nombres premiers.

$$N = 2 \times 3 \times \ldots \times p.$$

Posons 
$$N' = N + 1$$
.

Alors, pour tout nombre premier d, la division euclidienne de N' par d a pour reste 1 car  $N' = d \times q + 1$ .

Donc N' n'est divisible par aucun d'entre eux, donc N' est premier.

Mais N' > p, ce qui est impossible car p est le plus grand nombre premier.

Donc il n'existe pas un nombre fini de nombres premiers

#### Théorème.

- Tout entier naturel n supérieur ou égal à 2 admet un diviseur premier.
- Tout entier naturel  $n \ge 2$ , non premier, admet un diviseur premier inférieur ou égal à  $\sqrt{n}$ .

#### **Démonstration**

Soit n un entier  $n \ge 2$ .

- $\bullet$  Si n est premier, il est un diviseur premier de lui-même.
- Si n n'est pas premier, il admet un diviseur positif autre que 1 et lui-même. L'ensemble E des diviseurs positifs, autres que 1 et n, est donc un ensemble d'entiers naturels non vide : il a donc un plus petit élément que l'on note p. Si p n'était pas premier, il existerait un diviseur propre d de p qui serait plus petit que

p; comme d diviserait n avec p qui divise n, d diviserait n donc d serait un élément de E plus petit que p ce qui est impossible.

Ainsi p est premier et divise n; par suite il existe un entier q tel que n=pq avec 1 < q < n.

Donc q est un diviseur propre de n et par conséquent  $p\leqslant q.$ 

On en déduit que  $p^2 \leqslant pq$  soit  $p^2 \leqslant n$  et donc  $p \leqslant \sqrt{n}$ 

#### Propriété.

Soit n un entier supérieur à 2.

Si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à  $\sqrt{n}$  alors n est un nombre premier.

#### **Démonstration**

Si n n'est pas premier, il admet un diviseur premier inférieur ou égal à  $\sqrt{n}$  d'après le premier théorème. Cette propriété est donc la contraposée du second théorème.

**Exemple.** Démontrons que 139 est un nombre premier.

## II. Deux théorèmes fondamentaux

#### 1. Décomposition en produit de facteurs premiers

#### Théorème.

Tout entier naturel  $n \ge 2$  se décompose en un produit de nombres premiers.

Cette décomposition est unique à l'ordre des facteurs près.

On écrira  $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$  où  $n\geqslant 2,\ p_1,\ p_2,\dots,\ p_k$  sont des nombres premiers deux à deux distincts et  $\alpha_1,\ \alpha_2,\ \dots,\ \alpha_k$  sont des entiers naturels non nuls.

**Exemple.** Décomposer 140 en produit de facteurs premiers et en déduire la liste des diviseurs de 140.

## Propriété.

Si n est un entier naturel supérieur ou égal à 2, admettant pour décomposition en produit de facteurs premiers  $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$  admet alors n possède

exactement  $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \ldots \times (\alpha_k + 1)$  diviseurs positifs.

**Exemple.** Déterminer le nombre de diviseurs positifs de 72.

## 2. Petit théorème de Fermat

### Théorème.

Soit n un nombre entier.

Si p est un nombre premier ne divisant pas n alors  $n^{p-1} \equiv 1$  [p].

Conséquence : si p est un nombre premier et n un entier, alors  $n^p \equiv n$  [p].

**Exercice 2.9.** Montrer, que pour tout entier naturel n,  $n^{13} - n$  est divisible par 26.