# Mathématiques expertes
# Arithmétique 3

Serge Bays

Lycée les Eucalyptus

17 mars 2022

## Définition

On appelle nombre premier tout entier naturel $p$, $p \geq 2$, dont les seuls diviseurs dans $\mathbb{N}$ sont exactement 1 et $p$.

**Exemples**
2, 3, 5, 7, 11, 13 sont des nombres premiers.

0, 1 et tous les nombres pairs différents de 2 ne sont pas des nombres premiers.

**Théorème**

Tout entier naturel différent de 0 et de 1 admet un diviseur premier.

**Propriété**

Si un entier naturel $n \geq 4$ n'est divisible par aucun nombre premier $p$ tel que $p \leq \sqrt{n}$ ; alors $n$ est premier.

**Théorème**

Il existe une infinité de nombres premiers

**Démonstration**

Supposons que l'ensemble des nombres premiers est fini. Soit $p_1, p_2, \ldots, p_k$ les seuls nombres premiers existants.
Considérons alors $n = p_1 p_2 \ldots, p_k + 1$.
Pour tout $i$, $n \equiv 1 \mod p_i$. Mais $n$ admet un diviseur premier qui ne peut être l'un des $p_i$ d'où une contradiction. On vérifie que chaque $p_i$ divise $p_1 p_2 \ldots, p_k$ et s'il divise $n$, il doit donc diviser la différence $n - p_1 p_2 \ldots, p_k$ qui vaut 1.

**Théorème**

Soit $p$ un nombre premier et $n$ un entier.
Si $p$ ne divise pas $n$, alors $p$ et $n$ sont premiers entre eux.

**Conséquence** : deux nombres premiers distincts sont premiers entre eux

**Théorème fondamental de l'arithmétique**

Tout entier naturel $n$ , $n \geq 2$, s'écrit comme un produit de facteurs premiers et cette décomposition est unique à l'ordre près des facteurs.

## Démonstration

Existence
$n$ admet un diviseur premier : soit $p_1$ avec $n = p_1 \times n_1$ et $n_1 < n$.
Si $n_1 = 1$, c'est terminé, sinon, on recommence le même raisonnement :
$n_1$ admet un diviseur premier ; soit $p_2$ avec $n_1 = p_2 \times n_2$ et $n_2 < n_1$.
Si $n_2 = 1$, c'est terminé, sinon, on poursuit le même raisonnement.
On construit ainsi une suite strictement décroissante d'entiers naturels $(n_1, n_2, \ldots)$.
Cette construction s'arrête à une étape $r$ et alors $n = p_1 p_2, \ldots, p_r$.

**Unicité**

Elle découle du théorème de Gauss et du théorème disant que deux nombres premiers distincts sont premiers entre eux.

En regroupant les facteurs qui ne sont pas distincts, on obtient :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

où les $p_i$ sont des nombres premiers distincts et les $\alpha_i$ des entiers naturels non nuls.

**Application**

Recherche de diviseurs

Les diviseurs entiers naturels de $n$ sont de la forme :

$p_1^{d_1} p_2^{d_2} \dots p_r^{d_r}$ où chaque $d_i$ vérifie $0 \leq d_i \leq \alpha_i$

Cette propriété permet en particulier de déterminer le pgcd de deux entiers.

**Crible d'Eratosthène**

C'est une méthode permettant de dresser la liste des nombres premiers inférieurs à un nombre donné.

Exemple : on veut dresser la liste de tous les nombres premiers compris entre 1 et 100.
On écrit la liste des nombres entiers compris entre 1 et 100.
On barre le 1.
On barre tous les multiples de 2 autres que 2.
On barre tous les multiples de 3 autres que 3.
Remarque : Lorsqu'on a éliminé tous les multiples d'un entier $p$ autre que p, le plus petit entier restant est forcément premier.
On barre tous les multiples de 5 autres que 5, tous les multiples de 7 autres que 7.
Le plus petit entier restant est 11. Or on a déjà éliminé tous les multiples de 11 de la forme $11k$ où $k < 11$. $100 < 11^2$, donc il n'y a plus rien à éliminer ; c'est terminé.

Soient $p$ un nombre premier et $a$ un entier naturel non divisible par $p$ :
alors $a^{p-1} - 1$ est divisible par $p$.

Autrement dit : $a^{p-1} \equiv 1 \ [p]$

### Conséquence

Soient $p$ un nombre premier et $a$ un entier naturel :
alors $a^p - a$ est divisible par $p$.

Autrement dit : $a^p \equiv a\,[p]$

## Démonstration

Déterminer si les nombres suivants sont premiers : 103 ; 119 ; 137 ; 211.

Décomposer en facteurs premiers les nombres suivants : 120 ; 126 ; 336 ; 735.

En utilisant la décomposition en facteurs premiers, mettre les fractions suivantes sous forme irréductible : $\frac{126}{588}$ ; $\frac{504}{336}$ ; $\frac{3825}{300}$.

En utilisant la décomposition en facteurs premiers, dresser la liste des diviseurs des nombres suivants : 90 ; 120 ; 245.