Définition 1 : nombre premier

Un entier naturel p est **premier** s'il admet exactement deux diviseurs, 1 et p.

Remarque

Un nombre qui n'est pas premier est dit **composé**.

Propriété 1 : Existence d'un diviseur premier

Tout entier naturel non nul n non premier admet un diviseur premier p tel que $p \leq \sqrt{n}$.

Remarque

On en déduit le **test de primalité** suivant : si un entier naturel n n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$, alors n est premier.

Théorème 1 : Euclide

Il existe une infinité de nombres premiers.

Remarque

Le plus grand nombre premier connu est $2^{82\,589\,933} - 1$, découvert en décembre 2018. Il possède 24 862 048 chiffres. Voir le projet `https://www.mersenne.org/`.

Théorème 2 : Théorème fondamental de l'arithmétique

Tout entier $n \geq 2$ peut se décomposer de **manière unique** en produit de nombres premiers.
Il existe des nombres premiers p_1, ..., p_m et des entiers naturels non nuls α_1, ..., α_m tels que :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$$

Propriété 2 : Diviseurs d'un entier

Un entier naturel d divise un entier naturel n si et seulement si les exposants des facteurs premiers de la factorisation de d sont au plus égaux à ceux de n.

Remarque

Le nombre $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$ a exactement $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_m + 1)$ diviseurs.

Propriété 3 : Petit théorème de Fermat

Si p est un nombre premier et si n est un entier non divisible par p, alors :

$$n^{p-1} \equiv 1 \, [p]$$

Remarque

Ce théorème nous donne un autre test de primalité : si pour tout n inférieur ou égal à p, n^{p-1} n'est pas congru à 1 modulo p alors p n'est pas premier.