Rappel des définitions et propriétés de d'arithmétique

Tous les nombres mentionnés sont entiers naturels (la plupart des définitions et propriétés s'étendent q=aux entiers relatifs).

Diviseur : d (non nul) est un diviseur de n si $\frac{n}{d}$ est entier.

Diviseur commun : d (non nul) est un diviseur commun à n et n' si c'est un diviseur de n et de n' (!).

PGCD : Le PGCD de deux nombres n et m est le plus grand diviseur commun à ces deux nombres (!).
On note PGCD(n ; m).

PPCM : Le PPCM de deux nombres est le plus petit multiple positif commun de ces deux nombres (!).
On note PPCM(n ; m).

Nombres premiers entre eux : Deux nombres sont premiers entre eux si leur PGCD est 1.

Nombre premier : Un nombre est premier s'il possède exactement deux diviseurs : 1 et lui-même.

Remarques : Tout nombre est divisible par 1 et lui-même.
1 n'est pas premier (il n'a qu'un seul diviseur : 1)

Théorème fondamental de l'arithmétique :

Tout nombre entier supérieur ou égal à 2 se décompose de façon unique (à l'ordre près) en produit de nombres premiers.

Autrement dit : $\forall$ N $\in$ $\mathbb{N}\backslash\{0 ; 1\}$,

$$N = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$$

avec $p_1 < p_2 < \ldots < p_r$ premiers et uniques et $n_1, n_2, \ldots, n_r$ entiers et uniques.
Les p_i (i = 1 ; 2 ; … ; r) sont appelés **facteurs premiers** de N.

Division euclidienne : n et m sont deux entiers, m non nul.
Il existe un unique couple (q ; r) d'entiers tels que n = qm + r avec $0 \leq r < m$.
q est le **quotient**, r et le **reste** de la division euclidienne de n par m.

Complément

Théorème de Gauss : a, b et c sont trois entiers non nuls.
Si a divise bc et a et b sont premiers entre eux alors a divise c.