

RAPPELS D'ARITHMETIQUE

Diviseur :

Un entier d non nul est un diviseur d'un entier n s'il existe un entier k tel que $n = kd$.

On dit aussi que d divise n , que n est un multiple de d . On note $d \mid n$.

Propriétés :

- Si n divise un entier, il divise tous ses multiples.
- Si n divise deux entiers a et b , il divise toute combinaison linéaire à coefficients entiers de a et b (en particulier leur somme).
- La relation \mid (divise) est une relation d'ordre partielle dans \mathbb{N} (réflexive, antisymétrique et transitive).

Attention : Dans \mathbb{Z} , la relation « divise » est réflexive et transitive, mais si $a \mid b$ et $b \mid a$ alors $b = \pm a$.

Diviseur commun :

Un entier d non nul un diviseur commun à deux entiers n et n' s'il divise à la fois de n et n' .

PGCD : Le PGCD de deux entiers n et n' est le plus grand diviseur commun à ces deux entiers (!).

On le note $\text{PGCD}(n, n')$ ou $n \wedge n'$.

PPCM : Le PPCM de deux entiers n et n' est le plus petit multiple positif commun de ces deux entiers (!).

On le note $\text{PPCM}(n, n')$ ou $n \vee n'$.

Propriétés :

- Si n et n' sont deux entiers, tout diviseur commun à n et n' est divisible par $n \wedge n'$.
- Si $(n, n', k) \in \mathbb{Z}^3$ avec $k > 0$ alors :

$$\text{PGCD}(kn, kn') = k \times \text{PGCD}(n, n') \quad \text{et} \quad \text{PPCM}(kn, kn') = k \times \text{PPCM}(n, n')$$

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

Division euclidienne :

Soient n et m deux entiers, m non nul. Il existe un unique couple (q, r) d'entiers tels que :

$$n = qm + r \quad \text{et} \quad 0 \leq r < |m|.$$

L'écriture $n = qm + r$ est la division euclidienne de n par m , q est le quotient, r est le reste.

Propriété (lemme d'Euclide) :

Si $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ et r est le reste de la division euclidienne de a par b , alors $\text{PGCD}(a, b) = \text{PGCD}(b, r)$.

Algorithme d'Euclide : Si $a \geq b > 0$ alors $d = \text{PGCD}(a, b)$ est le dernier reste non nul dans le tableau suivant :

A	B	Reste de A par B
a	b	r_1
b	r_1	r_2
r_1	r_2	r_3
\vdots	\vdots	\vdots
$r_{\alpha-2}$	$r_{\alpha-1}$	$r_\alpha = d$
$r_{\alpha-1}$	r_α	0

Théorème de Bézout :

Soient n et m sont deux entiers de PGCD d . Il existe une infinité de couples $(u, v) \in \mathbb{Z}^2$ tels que :

$$u \times n + v \times m = d.$$
Nombre premier :

Un entier naturel est premier s'il possède exactement deux diviseurs positifs : 1 et lui-même.

Propriété : Il y a une infinité de nombres premiers.

Théorème fondamental de l'arithmétique :

Tout nombre entier $N \geq 2$ se décompose de façon unique (à l'ordre près) en produit de nombres premiers.

Autrement dit : $\forall N \in \mathbb{N} \setminus \{0; 1\}$, il existe un unique entier $r \in \mathbb{N}^*$, un unique r -uplet (p_1, p_2, \dots, p_r) de nombres premiers tel que $p_1 < p_2 < \dots < p_r$ et un unique r -uplet (n_1, n_2, \dots, n_r) d'entiers strictement positifs tels que :

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

Les p_i pour $i \in \llbracket 1, r \rrbracket$ sont appelés facteurs ou diviseurs premiers de N .

Théorème de Gauss :

Soient a , b et c sont trois entiers non nuls tels que $\text{PGCD}(a, b) = 1$. Si a divise bc alors a divise c .

En particulier, si a est premier et ne divise pas b , alors a est un facteur premier de c .

Propriété : Soient a et b deux entiers naturels de décompositions $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ (les α_i et β_i pouvant ici être nuls). Alors :

$$\text{PGCD}(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_r^{\min(\alpha_r, \beta_r)} \quad \text{et} \quad \text{PPCM}(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_r^{\max(\alpha_r, \beta_r)}.$$

