Arithmétique

Une fiche de cours de Stéphane Pasquet - Mise à jour : 28 janvier 2026

(https://courspasquet.fr) (https://mathweb.fr)

Dans ce qui suit, sauf indication contraire, a, b, c et n sont des entiers relatifs.

Divisibilité

Notation

a divise $b \iff a \mid b \iff \exists n \in \mathbb{Z},\ b = a \times n$

Propriétés

Transitivité	Combinaison linéaire
$\begin{cases} a \mid b \\ b \mid c \end{cases} \implies a \mid c$	$\begin{cases} a \mid b \\ a \mid c \end{cases} \implies \forall (\lambda, \mu) \in \mathbb{Z},\ a \mid (\lambda b + \mu c)$

Division euclidienne

$\forall (a; b) \in \mathbb{N} \times \mathbb{N},\ \exists !\ (q; r) \in \mathbb{N} \times \mathbb{N},\ a = bq + r, \quad 0 \leqslant r < b$

Congruences

a est congru à b modulo $c \iff a = b + nc\ (0 \leqslant b < c) \iff a \equiv b \mod c$

- $a \equiv b \mod n \iff n \mid (a - b)$
- $\begin{cases} a \equiv c \mod n \\ c \equiv b \mod n \end{cases} \iff a \equiv b \mod n$
- $a \equiv b \mod n \iff \forall k \in \mathbb{Z},\ \begin{cases} a + k \equiv b + k \mod n \\ ka \equiv kb \mod n \\ a^k \equiv b^k \mod n \quad (k \in \mathbb{N}) \end{cases}$
- $\begin{cases} a \equiv b \mod n \\ a' \equiv b' \mod n \end{cases} \iff \begin{cases} a + a' \equiv b + b' \mod n \\ aa' \equiv bb' \mod n \end{cases}$

PGCD

Propriétés

- $a = bq + r,\ 0 \leqslant r < b,\ q \in \mathbb{Z} \iff \text{pgcd}\,(a\,;\,b) = \text{pgcd}\,(b\,;\,r)$
- Les diviseurs communs à a et b divisent $\text{pgcd}\,(a\,;\,b)$
- $\begin{cases} d \mid a \\ d \mid b \end{cases} \implies d \mid \text{pgcd}\,(a\,;\,b)$
- $\exists (a', b') \in \mathbb{Z} \times \mathbb{Z},\ \begin{cases} a = a' \times \text{pgcd}\,(a\,;\,b) \\ b = b' \times \text{pgcd}\,(a\,;\,b) \end{cases}$ avec $\text{pgcd}\,(a'\,;\,b') = 1$.
- a et b premiers entre eux $\iff \text{pgcd}\,(a\,;\,b) = 1$

Théorème de Bézout

$\text{pgcd}\,(a\,;\,b) = 1 \iff \exists\,(u;v) \in \mathbb{Z}^2,\ au + bv = 1$

Corollaire

$$\text{pgcd}\,(a\,;\,b) = d \iff \begin{cases} d \mid a \text{ et } d \mid b \\ \exists\ (u\,;v) \in \mathbb{Z}^2,\ au + bv = d. \end{cases}$$

Théorème de Gauss

$$\begin{cases} a \mid bc \\ \text{pgcd}\,(a\,;\,b) = 1 \end{cases} \implies a \mid c$$

Nombres premiers

Un entier naturel est premier s'il n'est divisible que par 1 et lui-même.
L'ensemble des nombres premiers est souvent noté $\mathbb{P}$.

Théorèmes

- $\mathbb{P}$ est infini.
- $n \in \mathbb{N}^*$ n'est divisible par aucun nombre premier inférieur à $\sqrt{n} \implies n \in \mathbb{P}$.

Exemple : $\sqrt{137} \approx 11,7$ et 137 n'admet aucun diviseurs premiers inférieurs à 11,7 donc 137 est un nombre premier.

Décomposition en produit de facteurs premiers

Tout entier naturel n supérieur ou égal à 2 peut s'écrire sous la forme :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$$

où k est un entier naturel non nul et $p_i \in \mathbb{P}$ pour $1 \leqslant i \leqslant k$.

Petit théorème de Fermat

$$\begin{cases} p \in \mathbb{P} \\ a \in \mathbb{N},\ a \not\equiv 0 \mod p \end{cases} \implies a^{p-1} \equiv 1 \mod p$$

Exemple : $a = 27$, $p = 5$. p est premier et a n'est pas divisible par p donc $27^{5-1} \equiv 1 \mod 5$.