

1 Arithmétique

1.1 Division euclidienne et pgcd

Soient $a, b \in \mathbb{Z}$. On dit que b **divise** a et on note $b|a$ s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Théorème (Division euclidienne). Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$. Il **existe** des entiers $q, r \in \mathbb{Z}$ tels que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b$$

De plus q et r sont **uniques**.

Terminologie : q est le **quotient** et r est le **reste**.

Nous avons donc l'équivalence : $r = 0$ si et seulement si b divise a .

Pgcd de deux entiers

Soient $a, b \in \mathbb{Z}$ deux entiers, non tous les deux nuls. Le plus grand entier qui divise à la fois a et b s'appelle le **plus grand diviseur commun** de a, b et se note $\text{pgcd}(a, b)$.

Algorithme d'Euclide

Lemme. Soient $a, b \in \mathbb{N}^*$. Écrivons la division euclidienne $a = bq + r$. Alors

$$\text{pgcd}(a, b) = \text{pgcd}(b, r)$$

Algorithme d'Euclide.

On souhaite calculer le pgcd de $a, b \in \mathbb{N}^*$. On peut supposer $a \geq b$. On calcule des divisions euclidiennes successives. Le pgcd sera le dernier reste non nul :

- division de a par b , $a = bq_1 + r_1$. Par le lemme, $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$ et si $r_1 = 0$ alors $\text{pgcd}(a, b) = b$ sinon on continue :
- $b = r_1q_2 + r_2$, $\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$,
- $r_1 = r_2q_3 + r_3$, $\text{pgcd}(a, b) = \text{pgcd}(r_2, r_3)$,
- ...

Nombres premiers entre eux

Deux entiers a, b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$.

Si deux entiers $a, b \in \mathbb{Z}$ ne sont pas premiers entre eux, on peut s'y ramener en divisant par $d = \text{pgcd}(a, b)$.

$$\begin{cases} a &= a'd \\ b &= b'd \end{cases} \quad \text{avec} \quad a', b' \in \mathbb{Z} \text{ et } \text{pgcd}(a', b') = 1$$

1.2 Théorème de Bézout

Théorème (Théorème de Bézout). Soient a, b des entiers. Il existe des entiers $u, v \in \mathbb{Z}$ tels que

$$au + bv = \text{pgcd}(a, b)$$

Les entiers u, v sont des **coefficients de Bézout**. Ils s'obtiennent en « remon- tant » l'algorithme d'Euclide.

Corollaire. Si $d|a$ et $d|b$ alors $d|\text{pgcd}(a, b)$.

Corollaire. Soient a, b deux entiers. a et b sont premiers entre eux **si et seule- ment** si il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = 1$$

Remarque. Si on trouve deux entiers u', v' tels que $au' + bv' = d$, cela n'im- plique **pas** que $d = \text{pgcd}(a, b)$. On sait seulement alors que $\text{pgcd}(a, b)|d$.

Corollaire (Lemme de Gauss). Soient $a, b, c \in \mathbb{Z}$.

$$\text{Si } a|bc \text{ et } \text{pgcd}(a, b) = 1 \text{ alors } a|c$$

Équations $ax + by = c$

Proposition. Considérons l'équation

$$ax + by = c \quad (\text{E})$$

où $a, b, c \in \mathbb{Z}$.

1. L'équation (E) possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $\text{pgcd}(a, b)|c$.

2. Si $\text{pgcd}(a, b)|c$ alors il existe même une infinité de solutions entières et elles sont exactement les $(x, y) = (x_0 + \alpha k, y_0 + \beta k)$ avec $x_0, y_0, \alpha, \beta \in \mathbb{Z}$ fixés et k parcourant \mathbb{Z} .

ppcm

Le $\text{ppcm}(a, b)$ (**plus petit multiple commun**) est le plus petit entier ≥ 0 divisible par a et par b .

Proposition. Si a, b sont des entiers (non tous les deux nuls) alors

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|$$

Proposition. Si $a|c$ et $b|c$ alors $\text{ppcm}(a, b)|c$.

1.3 Nombres premiers

Un **nombre premier** p est un entier ≥ 2 dont les seuls diviseurs positifs sont 1 et p .

Proposition. Il existe une infinité de nombres premiers.

Remarque. Si un nombre n n'est pas premier alors un de ses facteurs est $\leq \sqrt{n}$.

Proposition (Lemme d'Euclide). Soit p un nombre premier. Si $p|ab$ alors $p|a$ ou $p|b$.

Théorème (Décomposition en facteurs premiers). Soit $n \geq 2$ un entier. Il existe des nombres premiers $p_1 < p_2 < \dots < p_r$ et des exposants entiers $\alpha_1, \alpha_2, \dots, \alpha_r \geq 1$ tels que :

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

De plus les p_i et les α_i ($i = 1, \dots, r$) sont uniques.

1.4 Congruences

Soit $n \geq 2$ un entier. On dit que a est **congru** à b **modulo** n , si n divise $b - a$. On note alors

$$a \equiv b \pmod{n}.$$

On note aussi parfois $a = b \pmod{n}$ ou $a \equiv b[n]$. Une autre formulation est

$$a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z} \quad a = b + kn.$$

Remarquez que n divise a si et seulement si $a \equiv 0 \pmod{n}$.

Proposition.

1. La relation « congru modulo n » est une relation d'équivalence :
 - (Réflexivité) $a \equiv a \pmod{n}$,
 - (Symétrie) si $a \equiv b \pmod{n}$ alors $b \equiv a \pmod{n}$,
 - (Transitivité) si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors $a \equiv c \pmod{n}$.
2. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a + c \equiv b + d \pmod{n}$.
3. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a \times c \equiv b \times d \pmod{n}$.
4. Si $a \equiv b \pmod{n}$ alors pour tout $k \geq 0$, $a^k \equiv b^k \pmod{n}$.

Équation de congruence $ax \equiv b \pmod{n}$

Proposition. Soit $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$ fixés et $n \geq 2$. Considérons l'équation $ax \equiv b \pmod{n}$ d'inconnue $x \in \mathbb{Z}$:

1. Il existe des solutions si et seulement si $\text{pgcd}(a, n)|b$.
2. Les solutions sont de la forme $x = x_0 + \ell \frac{n}{\text{pgcd}(a, n)}$, $\ell \in \mathbb{Z}$ où x_0 est une solution particulière. Il existe donc $\text{pgcd}(a, n)$ classes de solutions.

Théorème (Petit théorème de Fermat). Si p est un nombre premier et $a \in \mathbb{Z}$ alors

$$a^p \equiv a \pmod{p}$$

Corollaire. Si p ne divise pas a alors

$$a^{p-1} \equiv 1 \pmod{p}$$