# Chapitre 3 : Arithmétique dans $\mathbb{Z}$

On a vu que $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre. De plus, on connait les idéaux de $\mathbb{Z}$ : ils sont de la forme $n\mathbb{Z}$ $(n \in \mathbb{N})$.
En d'autres termes, tous les idéaux de $\mathbb{Z}$ sont des idéaux principaux.

Rem Un anneau vérifiant de telles propriétés est appelé un anneau principal.

## I- Divisibilité

déf Etant donnés $a, b \in \mathbb{Z}$, on dit que $a$ divise $b$ (ou que $b$ est multiple de $a$) si :

$$\exists c \in \mathbb{Z}, \quad b = ac.$$

On note alors $a | b$.

Rem • L'idéal principal $a\mathbb{Z} = \{ak / k \in \mathbb{Z}\}$ est aussi l'ensemble des multiples de $a$. On a de plus :

$$a | b \iff b\mathbb{Z} \subseteq a\mathbb{Z}$$

• Les diviseurs de 1 sont les éléments inversibles de $\mathbb{Z}$, ie $\pm 1$.

prop (i) $(a|b$ et $a|c) \Rightarrow a | b+c$.
(ii) $a|b \Rightarrow a | bc$.
(iii) $(a|b$ et $b|a) \Rightarrow |a| = |b|$.
(iv) $(a|b$ et $c|d) \Rightarrow ac | bd$
(v) $ab|c \Rightarrow a|c$ et $b|c$ (la réc est fausse !)
(vi) $(\mathbb{N}, |)$ est un ensemble partiellement ordonné.

## 2. Division euclidienne et congruence

**Thm** Pour tout $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$, il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tq

$$a = qb + r \quad \text{et} \quad 0 \leqslant r < b.$$

**dém** * $a \in \mathbb{N}$ : par récurrence sur $a$.
* $a \in \mathbb{Z}_-$ : traiter le cas de $-a$.

**prop** Soient $a, m \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Alors il y a équivalence entre :
(i) $a$ et $m$ ont même reste dans la div eucl par $b$.
(ii) $a - m \in b\mathbb{Z}$, ie $b \mid a-m$.

**déf** Si $a$ et $m$ vérifient l'une de ces conditions, on dit que $a$ et $m$ sont congrus modulo $b$, et on notera $a \equiv m \,[b]$

**Rem** $a \in \mathbb{Z}$ est congru modulo $b$ à son reste dans la div euclidienne par $b$.

**prop** La relation de congruence est une relation d'équivalence.

**prop** $\forall x, y, x', y' \in \mathbb{Z}$, $\forall m \in \mathbb{N}^*$, $x \equiv x' \,[m]$ et $y \equiv y' \,[m]$. Alors :

$$x + y = x' + y' \,[m] \quad \text{et} \quad x \times y = x' \times y' \,[m].$$

**Application** critères de divisibilité dans $\mathbb{Z}$ :

* divisibilité par 3 : $10 \equiv 1 \,[3] \Rightarrow 10^k \equiv 1 \,[3]$. $\forall k \geqslant 1$.

et $a = 10^p a_p + 10^{p-1} a_{p-1} + \dots + 10 a_1 + a_0 \equiv a_p + \dots + a_1 + a_0 \,[3]$.

$\Rightarrow a$ divisible par 3 $\Leftrightarrow 3 \mid a_0 + \dots + a_p$.

* divisibilité par 9, par 11, ....

# 3. Anneau $\mathbb{Z}/n\mathbb{Z}$

**notation** On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation d'équivalence "congru modulo $n$".

**rem** Comme la classe d'un entier est égale à celle de son reste dans la div par $n$, on a :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

où $\bar{a} = \{b \in \mathbb{Z} / b \equiv a [n]\} = \{a + kn / k \in \mathbb{Z}\} = a + n\mathbb{Z}$.

**prop** Pour tout $\bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}$, on pose :

$$\bar{x} + \bar{y} = \overline{x+y} \qquad \bar{x} \times \bar{y} = \overline{x \times y}.$$

Alors $+$ et $\times$ sont des LCI bien définies sur $\mathbb{Z}/n\mathbb{Z}$.

**prop** Pour tout $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif dont les éléments neutres sont $\bar{0}$ et $\bar{1}$.

**rem**
- si $n = 0$, $a \equiv b [0] \Leftrightarrow 0 | a-b$, i.e. $a = b \Rightarrow \mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$
- si $n = 1$, $a \equiv b [1] \Leftrightarrow 1 | a-b$, ce qui est tjr vérifié.

Ainsi, $\mathbb{Z}/1\mathbb{Z} = \{\bar{0}\}$.

**exple**
- Calculer la table des opérations de l'anneau $\mathbb{Z}/4\mathbb{Z}$.
- Comparer la table de $(\mathbb{Z}/4\mathbb{Z}, +)$ et celle de $(U_4, \times)$.

**rem** L'anneau $(\mathbb{Z}/4\mathbb{Z}, +, \times)$ n'est pas intègre.

On montrera que : $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow n$ première.

et même $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow n$ première.

**déf** On appelle morphisme canonique de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ l'application $j_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \to \bar{x}$.

**prop** $j_n$ est un morphe d'anneaux surjectif.

## 4. PGCD et PPCM

### 4.1. Définition du PGCD

On note $D(a) = \{x \in \mathbb{Z} / x|a\}$ = ens des diviseurs de $a$.

$\forall a, b \in \mathbb{Z}^*$, $D(a) \cap D(b) \cap \mathbb{N}$ est une partie non vide de $\mathbb{N}$ et finie. Elle admet un plus grand élément.

**déf** On appelle pgcd de $a$ et $b$ le plus grand élément de $D(a) \cap D(b) \cap \mathbb{N}$. On le note $a \wedge b$, ou $\text{pgcd}(a,b)$.

**convention** $a \wedge 0 = a$, $0 \wedge 0 = 0$.

**prop** $a \wedge b$ est aussi le plus grand élément de $D(a) \cap D(b) \cap \mathbb{N}$ pour l'ordre partiel $|$, ie :

- $a \wedge b$ divise $a$ et $b$.
- Tout diviseur de $a$ et $b$ divise $a \wedge b$.

### 4.2. Algorithme d'Euclide

**prop** $a, b \in \mathbb{N}$, $b \neq 0$. $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$ Alors :

$$D(a) \cap D(b) = D(b) \cap D(r).$$

En particulier $a \wedge b = b \wedge r$.

**Algorithme d'Euclide** $r_0 = a$, $r_1 = b$ ...

$\left| \begin{array}{l} r_0 = r_1 q + r \\ 0 \leqslant r < r_1 \end{array} \right.$ $\Rightarrow$ On pose $r_2 = r$.

On recommence : $r_k$, $r_{k+1}$ donnés : $r_{k+2}$ : Reste de la div eucl de $r_k$ par $r_{k+1}$

③ Alors $(r_k)_{k\geq 2}$ est une suite de $\mathbb{N}$ strictement $\searrow$ :

$\exists\, r_s$ tq $r_s = 0$.

Dès lors : $a \wedge b = r_0 \wedge r_1 \overset{\text{Prop}}{=} r_1 \wedge r_2 = \dots = r_{s-1} \wedge r_s$

$= r_{s-1} \wedge 0 = r_{s-1}$.

**Prop** Le pgcd de $a$ et $b$ est le dernier reste non-nul quand on effectue les div. eucl. successives.

**exple** Calcul de $162 \wedge 207$.

**Exercice** Ecrire un algo calculant le Reste de la div eucl de $a$ par $b$.

## 4.3 Coefficients de Bezout

**Prop** Pour tout couple $(a,b) \in \mathbb{Z}^2$, on a :

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}.$$

**Cor** $\forall (a,b) \in \mathbb{Z}^2$, $\exists (u,v) \in \mathbb{Z}$ tq

$$au + bv = a \wedge b.$$

On dit que $(u,v)$ est un couple de Bezout.

Il n'est pas unique !

**exple** $4 \wedge 6 = 2$ $\quad 4 \times (-1) + 6 \times (1) = 2$.

$207 \wedge 162$.

Algo d'Euclide

$207 = 162 + 45$

$162 = 3 \times 45 + 27$

$45 = 27 \times 1 + 18$.

$27 = 18 \times 1 + 9$.

$18 = 9 \times 2 + 0$

Ainsi $207 \wedge 162 = 9$

Et $9 = 27 - 18 = 27 - (45 - 27) = 2 \times 27 - 45$

$= 2 \times (162 - 3 \times 45) - 45 = 2 \times 162 - 7 \times 45$.

$= 2 \times 162 - 7(207 - 162) = (-7) \times 207 + (9) \times 162$

Exercice Écrire un algorithme qui à $(a,b) \in \mathbb{Z}^2$ renvoie $a \wedge b$ et un couple de Bezout $(u,v)$.

## 4.4. Nombres premiers entre eux

**déf** $a$ et $b \in \mathbb{Z}$ sont dit premier entre eux si

$$a \wedge b = 1.$$

**exple** $17 \wedge 19 = 1$, $5 \wedge 6 = 1$, $n \wedge (n+1) = 1$.

**Thm** (Bezout) Soient $a, b \in \mathbb{Z}$, on a l'équivalence

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z} : au + bv = 1.$$

**COR** (Thm de Gauss) Soient $a, b, c \in \mathbb{Z}$. Si

$$\left.\begin{array}{l} a \mid bc \\ a \wedge b = 1 \end{array}\right\} \Rightarrow a \mid c.$$

**COR** Si

$$\left.\begin{array}{l} a \mid c \\ b \mid c \\ a \wedge b = 1 \end{array}\right\} \text{ alors } ab \mid c.$$

**rem** Si $a \wedge b \neq 1$, c'est faux en gl : 4/12, 6/12, mais 24/12

**COR** Soient $a, b, c \in \mathbb{Z}$.

$$\left.\begin{array}{l} a \wedge c = 1 \\ b \wedge c = 1 \end{array}\right\} \Rightarrow ab \wedge c = 1.$$

**prop** Caractérisation du PGCD :

Soient $a, b \in \mathbb{Z}$, $d \in \mathbb{Z}$.

$$d = a \wedge b \iff \left\{\begin{array}{l} \exists a' \in \mathbb{Z} : a = da' \\ \exists b' \in \mathbb{Z} : b = db' \\ a' \wedge b' = 1. \end{array}\right.$$

(4) × Equations diophantiennes. On cherche l'ens des solutions $(u,v)$ de l'équation :

$$au + bv = c. \quad \text{avec } a,b \neq 0.$$

× Existence de solutions : $(\exists (u,v) \in \mathbb{Z}^2 : au+bv=c) \Leftrightarrow (a \wedge b \text{ divise } c)$

× Recherche de l'ens des solutions

→ On simplifie l'équation : $\left(\frac{a}{a\wedge b}\right)u + \left(\frac{b}{a\wedge b}\right)v = \left(\frac{c}{a\wedge b}\right)$

D'après la prop précédente, on se ramène ainsi à la situation

$$a'u + b'v = c' \quad \text{avec } a' \wedge b' = 1.$$

→ On détermine un couple de Bezout $(u_0, v_0)$ :

$$a'u_0 + b'v_0 = c'.$$

Alors si $(u,v)$ autre solution, ie $a'u + b'v = c'$

Par différence on a : $a'(u-u_0) = b'(v_0 - v)$ (*)

$\rightsquigarrow a' \mid b'(v_0 - v)$ $\overset{\text{Gauss}}{\Rightarrow}$ $\exists k$ tq $(v_0 - v) = a'k$.

$a' \wedge b' = 1$

En reportant dans (*), $u - u_0 = b'k$.

Les solutions sont donc $u = u_0 + kb'$, $v = v_0 - a'k$, $k \in \mathbb{Z}$

Exple Résolution de $8u + 13v = 2$.

## 4.5. PPCM de deux entiers

$\forall a,b \in \mathbb{Z}^*$, $(a\mathbb{Z}) \cap (b\mathbb{Z}) \cap \mathbb{N}$ est une partie non-vide de $\mathbb{N}$

Elle admet donc un plus petit élément.

Déf On appelle PPCM de $a$ et $b$ ce plus petit élément.

On le note $a \vee b$, ou $\text{PPCM}(a,b)$.

Convention $a \vee 0 = 0$ $\quad 0 \vee 0 = 0$

**prop** $a \vee b$ est aussi le plus petit élément de $(a\mathbb{Z}) \cap (b\mathbb{Z}) \cap \mathbb{N}$ pour l'ordre partiel $|$, ie :

- $a \vee b$ est multiple de $a$ et $b$.
- si $m$ est multiple de $a$ et de $b$, $m$ est aussi multiple de $a \vee b$.

**prop** Pour tout $a, b \in \mathbb{Z}$, on a :

$$(a \vee b) \times (a \wedge b) = |a| \cdot |b|.$$

## 4.6. Généralisation aux PGCD et PPCM de plusieurs entiers

Soient $a_1, \dots, a_n \in \mathbb{Z}$. $(n \geq 2)$

$a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$ idéal de $\mathbb{Z}$ $\Rightarrow \exists ! \delta \in \mathbb{N}$ tq $\delta\mathbb{Z} = a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$.

$\bigcap a_i\mathbb{Z}$ idéal de $\mathbb{Z}$ $\Rightarrow \exists ! \mu \in \mathbb{N}$ tq $\mu\mathbb{Z} = \bigcap a_i\mathbb{Z}$.

**déf** On appelle pgcd de $a_1, \dots, a_n$ (resp ppcm de $a_1, \dots, a_n$) l'entier naturel $\delta$ (resp $\mu$). On le note $a_1 \wedge \dots \wedge a_n$ (resp $a_1 \vee \dots \vee a_n$)

**prop** (i) Caract du PGCD. Soit $\delta \in \mathbb{N}$.

$$\delta = a_1 \wedge \dots \wedge a_n \iff \begin{cases} \cdot\ \delta \text{ divise } a_1, \dots, a_n. \\ \cdot\ \text{Pour tout } d \text{ diviseur de } a_1, \dots, a_n, \ d \mid \delta. \end{cases}$$

(ii) Caract du PPCM : Soit $\mu \in \mathbb{N}$

$$\mu = a_1 \vee \dots \vee a_n \iff \begin{cases} a_1, \dots, a_n \text{ divisent } \mu. \\ \text{Tout multiple de } a_1, \dots, a_n \text{ est multiple de } \mu. \end{cases}$$

**prop** (i) Commutativité : $\forall \sigma \in S_n$.

$$a_{\sigma(1)} \wedge \dots \wedge a_{\sigma(n)} = a_1 \wedge \dots \wedge a_n.$$

$$a_{\sigma(1)} \vee \dots \vee a_{\sigma(n)} = a_1 \vee \dots \vee a_n$$

(ii) Homogénéité : $\forall n \in \mathbb{Z}^*$ :

$$(a_1 n) \wedge \dots \wedge (a_m n) = |n| (a_1 \wedge \dots \wedge a_m)$$
$$(a_1 n) \vee \dots \vee (a_m n) = |n| (a_1 \vee \dots \vee a_m)$$

(iii) Associativité : $[\![1, m]\!] = \bigcup_{j=1}^{k} I_j$ tq $I_j \cap I_i = \emptyset$ $j \neq i$.

$a_1 \wedge \dots \wedge a_m = \mathrm{pgcd}(\mathrm{pgcd}\{a_j, j \in I_1\}, \dots, \mathrm{pgcd}\{a_j, j \in I_k\})$

$a_1 \vee \dots \vee a_m = \mathrm{ppcm}(\quad)$

**Prop** (Bezout) Soient $a_1, \dots, a_n \in \mathbb{Z}$. $\exists (u_1, \dots, u_n) \in \mathbb{Z}$ tq

$$a_1 u_1 + \dots + a_n u_n = a_1 \wedge \dots \wedge a_n.$$

**déf** Soient $a_1, \dots, a_k \in \mathbb{Z}^*$.

(i) $a_1, \dots, a_k$ sont $1^{\text{ers}}$ entre eux dans leur ensemble si :

$$a_1 \wedge \dots \wedge a_k = 1.$$

(ii) $a_1, \dots, a_k$ sont $1^{\text{ers}}$ entre eux deux à deux si

$$a_i \wedge a_j = 1 \quad \forall i, j \quad i \neq j.$$

**Rem** × 6, 10, 15 sont premiers entre eux dans leur ens, mais pas deux à deux.

× Par contre, si $a_1, \dots, a_n$ sont $1^{\text{ers}}$ entre eux deux à deux, $a_1 \wedge \dots \wedge a_n = 1$.

## 5. Nombres premiers

**déf** Un entier $p \in \mathbb{N} \setminus \{0, 1\}$ est dit premier si

$$\mathcal{D}(p) = \{\pm 1, \pm p\}.$$

On note $\mathbb{P}$ l'ens des nbs premiers

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}.$$

**Rem** • Un seul nb premier pair : 2
• $n$ n'est pas premier $\Leftrightarrow \exists a,b \geq 2$ tq $n = ab$.

**prop** L'ens des nb premiers est infini.

**prop** • $p \in \mathbb{P}$, $a \in \mathbb{Z}$. Alors soit $p|a$, soit $p \wedge a = 1$
• $p \in \mathbb{P}$. $p|ab \Rightarrow p|a$ ou $p|b$.

**prop** Si $p > 1$, les CSSE :
(i) $p$ est premier
(ii) $p$ premier avec tout entier qu'il ne divise pas
(iii) $p$ premier avec tout entier $n \in [\![1, p-1]\!]$.
(iv) $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre.

**prop** $p$ est premier $\Leftrightarrow$ $\mathbb{Z}/p\mathbb{Z}$ est un corps

**Thm** [Décomposition en facteurs premiers]
Soit $n \in \mathbb{N} \setminus \{0,1\}$. Alors $n$ se décompose de manière unique (à l'ordre des facteurs près) en produit de nb premiers.
Plus précisément : $\exists k \geq 1$, $p_1, \dots, p_k \in \mathbb{P}^k$ deux à deux distincts, et $(\alpha_1, \dots, \alpha_k) \in (\mathbb{N}^*)^k$ tels que :

$$n = \prod_{j=1}^{k} p_j^{\alpha_j}.$$

Les $p_j$ s'appellent les facteurs premiers, et les $\alpha_j$ s'appellent les multiplicités des $p_j$ dans $n$.

**prop** Soient $a, b \in \mathbb{N} \setminus \{0,1\}$,

$$a = \prod_{p \in \mathbb{P}} p^{\alpha(p)} \qquad b = \prod_{p \in \mathbb{P}} p^{\beta(p)}$$

(6) (i) $a \mid b \iff \forall p \in \mathbb{P},\ \alpha(p) \leq \beta(p)$

(ii) $a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(\alpha(p), \beta(p))}$

(iii) $a \vee b = \prod_{p \in \mathbb{P}} p^{\max(\alpha(p), \beta(p))}$

## 6. Pour la culture

× Exemple de nombres premiers

→ Nombres de Fermat de la forme $2^{2^n} + 1 = F_n$

Fermat a mq $F_n$ est premier pour $n = 0, \dots, 4$, et pensait que $F_n \in \mathbb{P}, \forall n$.
Euler montra que $2^{2^5} + 1 = 641 \times 6700417$.
Jusqu'aujourd'hui, on a trouvé aucun autre nb de Fermat premier.
On ne sait même pas s'il y en a.

× Répartition des nb premiers

→ Crible d'Eratosthène.
Un enjeu : comprendre mieux cette répartition :
× intervalle sans nb premier
× nb premiers jumeaux

Thm (Hadamard - De la Vallée Poussin 1896) Si $\forall x > 0$, $\pi(x)$ est le nb de $p \in \mathbb{P}$ tq $p \leq x$, On a :

$$\pi(x) \underset{+\infty}{\sim} \frac{x}{\ln(x)}$$

× Problème de factorisation en nb premiers fonction à sens unique, cryptographie RSA.

× Equations à solutions entières $x^n + y^n = z^n$
Fermat énonça en 1637 : $\forall n \geq 3$, pas de solution $(x, y, z) \in (\mathbb{Z}^*)^3$.
Il affirmait qu'il en avait une démo (jamais trouvée).
Démonstration complète en 1994 par Andrew Wiles