PGCD, PPCM DANS $\mathbb{Z}$. THÉORÈME DE BÉZOUT. APPLICATIONS

SOMMAIRE

Prérequis :

- Division euclidienne dans $\mathbb{Z}$. Propriétés de la divisibilité.
- Les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $(n\mathbb{Z}, +)$, $n \in \mathbb{N}$.
- $b \in a\mathbb{Z} \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z} \Leftrightarrow a \mid b$
- $a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = b$

1. PGCD, PPCM dans $\mathbb{Z}$

Dans tout ce paragraphe, on suppose $\boldsymbol{(a, b) \in \mathbb{Z} \times \mathbb{N}^*}$.

1.1. PPCM dans $\mathbb{Z}$

1.1.1. Proposition

$$\exists!\ n \in \mathbb{N},\ a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$$

Démonstration :

L'existence découle du fait que l'intersection de sous-groupes est un sous-groupe et du prérequis n°2.

Unicité : s'il existe $n' \in \mathbb{N}$ tel que : $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z} = n'\mathbb{Z}$

Alors $n \mid n'$ et $n' \mid n$

Donc : $n' = n$

1.1.2. Proposition

L'entier n ci-dessus vérifie :

- n est un multiple commun de a et de b
- **si n' est un multiple commun de a et de b, alors n' est un multiple de n.**

Démonstration :

- Comme $n\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, on a : $n\mathbb{Z} \subset a\mathbb{Z}$ et $n\mathbb{Z} \subset b\mathbb{Z}$

  D'où : $a \mid n$ et $b \mid n$

  n est un multiple commun de a et de b
- Si n' est un multiple commun de a et de b, alors :

  $$n' \in a\mathbb{Z} \cap b\mathbb{Z}$$

  $$n' \in n\mathbb{Z}$$

  Donc : $n \mid n'$

En conséquence, ***n* est le plus petit multiple commun de *a* et de *b***. On le note :

$$n = \text{ppcm}(a, b) \text{ ou } n = a \vee b$$

On a donc : $\boldsymbol{a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}}$

Remarque : la notion de ppcm peut se généraliser, par récurrence, à un nombre quelconque (mais fini) d'entiers :

$$\text{ppcm}(a_1, \ldots, a_n)\mathbb{Z} = a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z}$$

1.1.3. Propriétés de la loi $\vee$:

- Associativité : $(a \vee b) \vee c = a \vee (b \vee c)$
- Commutativité : $a \vee b = b \vee a$
- 1 est élément neutre : $1 \vee a = a \vee 1 = a$
- 0 est élément absorbant : $0 \vee a = a \vee 0 = 0$
- $a \mid b \Leftrightarrow a \vee b = b$
- Homogénéité $\boxed{m(a \vee b) = (ma) \vee (mb)}$

Noter l'analogie entre les symboles : $\vee$ et $\cap$

(Eh oui, la notation $\vee$ est malheureuse)

Démonstration :

- Associativité : elle découle de l'associativité de $\cap$

$$[(a \vee b) \vee c]\mathbb{Z} = (a \vee b)\mathbb{Z} \cap c\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \cap c\mathbb{Z} = a\mathbb{Z} \cap (b \vee c)\mathbb{Z} = [a \vee (b \vee c)]\mathbb{Z}$$

  Donc : $(a \vee b) \vee c = a \vee (b \vee c)$

- Commutativité : elle découle de la commutativité de $\cap$

$$(a \vee b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} = b\mathbb{Z} \cap a\mathbb{Z} = (b \vee a)\mathbb{Z}$$

  Donc : $a \vee b = b \vee a$

- Élément neutre : $(a \vee 1)\mathbb{Z} = a\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z}$ donc $a \vee 1 = a$

  Et (commutativité) : $1 \vee a = a$

- Élément absorbant : $(0 \vee a)\mathbb{Z} = 0\mathbb{Z} \cap a\mathbb{Z} = 0\mathbb{Z}$ donc $0 \vee a = 0$

  Et (commutativité) : $a \vee 0 = 0$

- Si $a \mid b$ alors $b \in a\mathbb{Z}$.

  En outre, $b \in b\mathbb{Z}$.

  Donc : $b \in a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$

  Donc : $a \vee b \mid b$

  Or, $a \vee b$ est un multiple de b donc : $a \vee b = b$

  Réciproquement, si : $a \vee b = b$

  Alors b est un multiple de a donc : $a \mid b$

- Homogénéité :

  Prouvons : $m(a \vee b)\mathbb{Z} = (ma \vee mb)\mathbb{Z}$

  Si $m = 0$, c'est évident. Supposons $m \neq 0$.

  Soit $x \in (ma \vee mb)\mathbb{Z} = ma\mathbb{Z} \cap mb\mathbb{Z}$. Alors,

$$\exists k, h \in \mathbb{Z},\ x = mak = mbh$$

  Alors $\frac{x}{m}$ est entier et : $\frac{x}{m} \in a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$

  Donc $\frac{x}{m}$ est un multiple de $a \vee b$.

  Autrement dit, x est un multiple de $m(a \vee b)$:

$$x \in m(a \vee b)\mathbb{Z} = m(a\mathbb{Z} \cap b\mathbb{Z})$$

  Donc : $(ma \vee mb)\mathbb{Z} \subset m(a \vee b)\mathbb{Z}$

Réciproquement, soit $x \in m(a \vee b)\mathbb{Z} = m(a\mathbb{Z} \cap b\mathbb{Z})$.

Alors : $\exists x' \in a\mathbb{Z} \cap b\mathbb{Z},\ x = mx'$

Or : $\exists h, k \in \mathbb{Z},\ x' = ah = bk$

Donc $x = mah = mbk$

D'où : $x \in ma\mathbb{Z} \cap mb\mathbb{Z} = (ma \vee mb)\mathbb{Z}$

Donc : $m(a \vee b)\mathbb{Z} \subset (ma \vee mb)\mathbb{Z}$

Finalement : $m(a \vee b)\mathbb{Z} = [(ma) \vee (mb)]\mathbb{Z}$

$$\boxed{m(a \vee b) = (ma) \vee (mb)}$$

1.2. PGCD dans $\mathbb{Z}$

1.2.1. Proposition

$$\exists!\ d \in \mathbb{N},\ a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

On verra plus loin (algorithme d'Euclide) comment déterminer l'entier d.

Démonstration :

Existence :

Il suffit de prouver que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$:

- il est non vide (contient 0)
- si x et y sont dans $a\mathbb{Z} + b\mathbb{Z}$, alors il existe des entiers p, q, r et s tels que :

$$x = ap + bq \text{ et } y = ar + bs$$

Donc : $x - y = a(p - r) + b(q - r) \in a\mathbb{Z} + b\mathbb{Z}$

Ce qui prouve bien que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$.

Unicité :

S'il existe $d' \in \mathbb{N}$ tel que : $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} = d'\mathbb{Z}$

Alors $d \mid d'$ et $d' \mid d$

Donc : $d' = d$

1.2.2. Proposition

L'entier d ci-dessus vérifie :

- d diviseur commun de a et de b
- **si d' est un diviseur commun de a et de b, alors d' est un diviseur de d.**

Démonstration :

- Notons : $\Gamma_{ab} = a\mathbb{Z} + b\mathbb{Z} = \{am + bn, (m, n) \in \mathbb{Z}^2\} = d\mathbb{Z}$

  En particularisant $m = 1$ et $n = 0$, on voit que : $a \in d\mathbb{Z}$

  En particularisant $m = 0$ et $n = 1$, on voit que : $b \in d\mathbb{Z}$

  D'où : $d \mid a$ et $d \mid b$

- Puisque $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, il existe un couple $(u, v) \in \mathbb{Z}^2$ tels que :

$$au + bv = d \times 1 = d$$

Attention : (u, v) n'est pas unique. (Voir 2.2.) On verra (en 2.3.) comment déterminer un tel couple (u, v).

On voit alors que tout diviseur commun d' de a et de b est aussi un diviseur de d.

En conséquence, ***d* est le plus grand diviseur commun de *a* et de *b***. On le note :

$$d = \text{pgcd}(a, b) \text{ ou } d = a \wedge b \text{ ou encore } d = (a, b)$$

On a donc : $$\boldsymbol{a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}}$$

1.2.3. Définition

Une égalité du type $au + bv = d$ où $d = a \wedge b$ est appelée égalité de Bézout.

Remarque : la notion de pgcd peut se généraliser, par récurrence, à un nombre quelconque (mais fini) d'entiers :

$$\text{pgcd}(a_1, \ldots, a_n)\mathbb{Z} = a_1\mathbb{Z} + a_2\mathbb{Z} + \ldots + a_n\mathbb{Z}$$

1.2.4. Propriétés de la loi $\wedge$:

- Associativité : $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
- Commutativité : $a \wedge b = b \wedge a$
- 0 est élément neutre : $0 \wedge a = a \wedge 0 = a$
- 1 est élément absorbant : $1 \vee a = a \vee 1 = 1$
- $a \mid b \Leftrightarrow a \wedge b = a$
- Homogénéité $\boxed{m(a \wedge b) = (ma) \wedge (mb)}$

Noter l'analogie entre les symboles : $\wedge$ et $\cup$

(Eh oui, la notation $\wedge$ est malheureuse)

Démonstration :

- Associativité : elle découle de l'associativité de la loi + dans $\mathbb{Z}$

$$[(a \wedge b) \wedge c]\mathbb{Z} = (a \wedge b)\mathbb{Z} + c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z} = a\mathbb{Z} + (b \wedge c)\mathbb{Z} = [a \wedge (b \wedge c)]\mathbb{Z}$$

  Donc : $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

- Commutativité : elle découle de la commutativité de la loi + dans $\mathbb{Z}$

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

  Donc : $a \wedge b = b \wedge a$

- Élément neutre : $(a \wedge 0)\mathbb{Z} = a\mathbb{Z} + 0\mathbb{Z} = a\mathbb{Z}$ donc $a \wedge 0 = a$

  Et (commutativité) : $0 \wedge a = a$

- Élément absorbant : $(1 \wedge a)\mathbb{Z} = 1\mathbb{Z} + a\mathbb{Z} = \mathbb{Z}$ donc $1 \wedge a = 1$

  Et (commutativité) : $a \wedge 1 = 1$

- Si $a \mid b$ alors $b \in a\mathbb{Z}$: $\exists \alpha \in \mathbb{Z}, b = a\alpha$

  Alors : $\forall u, v \in \mathbb{Z}^2, au + bv = a(u + \alpha v) \in a\mathbb{Z}$

  Autrement dit : $a\mathbb{Z} + b\mathbb{Z} \subset a\mathbb{Z}$

  C'est-à-dire : $(a \wedge b)\mathbb{Z} \subset a\mathbb{Z}$

  Donc : $a \mid a \wedge b$

  Et comme $a \wedge b \mid a$, il vient : $a = a \wedge b$

  Réciproquement, si : $a \wedge b = a$

Alors a est un diviseur de b : $a \mid b$

- Homogénéité :

  Prouvons : $ma\mathbb{Z} + mb\mathbb{Z} = m(a\mathbb{Z} + b\mathbb{Z})$

  Si $m = 0$, c'est évident. Supposons $m \neq 0$.

  Soit $x \in ma\mathbb{Z} + mb\mathbb{Z}$:

  $$\exists k, h \in \mathbb{Z},\ x = mak + mbh$$

  Alors $\frac{x}{m}$ est entier et : $\frac{x}{m} \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$

  Donc $\frac{x}{m}$ est un multiple de $a \wedge b$.

  Autrement dit, x est un multiple de $m(a \wedge b)$:

  $$x \in m(a \wedge b)\mathbb{Z}$$

  $$ma\mathbb{Z} + mb\mathbb{Z} \subset m(a \wedge b)\mathbb{Z}$$

  Réciproquement, soit $x \in m(a\mathbb{Z} + b\mathbb{Z})$.

  Alors : $\exists x' \in a\mathbb{Z} + b\mathbb{Z},\ x = mx'$

  Or : $\exists h, k \in \mathbb{Z},\ x' = ah + bk$

  Donc $x = mah + mbk$

  D'où : $x \in ma\mathbb{Z} + mb\mathbb{Z}$

  Donc : $m(a\mathbb{Z} + b\mathbb{Z}) \subset ma\mathbb{Z} + mb\mathbb{Z}$

  Finalement : $m(a\mathbb{Z} \cap b\mathbb{Z}) = ma\mathbb{Z} \cap mb\mathbb{Z}$

  $$m(a \wedge b)\mathbb{Z} = [(ma) \wedge (mb)]\mathbb{Z}$$

  D'où : $\boxed{m(a \wedge b) = (ma) \wedge (mb)}$

1.2.5. Corollaire

Si $d = a \wedge b$, alors : $\frac{a}{d} \wedge \frac{b}{d} = 1$

Remarquons qu'un pgcd n'est jamais nul. En effet, il est au moins égal à 1 puisque 1 divise a et 1 divise b.

Démonstration :

D'après la relation $m(a \wedge b) = (ma) \wedge (mb)$, on peut écrire :

$$d\left(\frac{a}{d} \wedge \frac{b}{d}\right) = a \wedge b = d$$

D'où : $\frac{a}{d} \wedge \frac{b}{d} = 1$

1.3. Algorithme d'Euclide

1.3.1. Propriétés

- $a \wedge b = a \wedge (a - b)$
- Si q et r sont respectivement le quotient et le reste de la division euclidienne de a par b ($a = bq + r$, $0 \leqslant r < b$) alors : $\boldsymbol{a \wedge b = b \wedge r}$

Ce résultat est la base de l'algorithme d'Euclide.

Démonstration :

- Notons $d = a \wedge b$ et $d' = a \wedge (a - b)$.

  Comme $d \mid a$ et $d \mid b$, il est clair que $d \mid (a - b)$.

  Comme $d \mid a$ et $d \mid (a - b)$, il s'en suit que : $d \mid d'$

  Comme $d' \mid a$ et $d' \mid (a - b)$, il est clair que $d' \mid b$

  Comme $d' \mid a$ et $d' \mid b$, il s'en suit que : $d' \mid d$

  Finalement : $d = d'$

$$a \wedge b = a \wedge (a - b)$$

- Il suffit d'appliquer $|q|$ fois la propriété précédente :

$$a \wedge b = (bq + r) \wedge b = ... = (bq + r - kb) \wedge b = ... = r \wedge b = b \wedge r \quad (1 \leqslant |k| \leqslant |q|)$$

1.3.2. Conséquence : **algorithme d'Euclide (permettant de calculer le pgcd de deux entiers *a* et *b*)**

On suppose ici que : **a et b sont éléments de $\mathbb{N}^*$ avec $a > b$ et b ne divise pas a.**

Rappel :
Si b divise a, alors :
$a \wedge b = b$
L'algorithme ci-contre est alors sans intérêt.

Posons : $r_0 = a$ et $r_1 = b$ (donc $r_0 > r_1$)

Effectuons la division euclidienne de $r_0 = a$ par $r_1 = b$:

$$\exists!(q_1, r_2) \in \mathbb{N}^2,\ r_0 = q_1 r_1 + r_2 \text{ où } \begin{cases} 0 \leqslant r_2 < r_1 \\ r_0 \wedge r_1 = r_1 \wedge r_2 \end{cases}$$

Si $r_2 = 0$ alors $a \wedge b = r_0 \wedge r_1 = r_1 \wedge 0 = r_1$.

Sinon, on réitère en effectuant la division euclidienne de r_1 par r_2.

Supposons maintenant que, pour $k \geqslant 2$, on ait :

$$r_{k-1} = q_k r_k + r_{k+1} \text{ où } \begin{cases} 0 \leqslant r_{k+1} < r_k \\ r_{k-1} \wedge r_k = r_k \wedge r_{k+1} \end{cases}$$

Éviter de parler de "suite d'entiers strictement décroissante" donc "nulle à partir d'un certain rang"...

On obtient alors des restes (à savoir $r_0, r_1, ..., r_k$) rangés dans un ordre décroissant strict :

$$r_0 > r_1 > r_2 > ... > r_k$$

Par conséquent, il existe un rang n tel que $r_{n+1} = 0$.

On a alors : $r_{n-1} = q_n r_n + 0$ où $r_{n-1} \wedge r_n = r_n \wedge 0 = r_n$

On en déduit : $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = ... = r_n \wedge 0 = r_n$

Conclusion :

le pgcd est le dernier reste non nul dans les divisions euclidiennes successives de r_{k-1} par r_k ($k \geqslant 1$)

Exemple : calculer le pgcd de 142 et 38 avec l'algorithme d'Euclide :

$$\begin{matrix} r_0 & q_1 & r_1 & r_2 \end{matrix}$$
$$142 = 3 \times 38 + 28$$

$$\begin{matrix} r_1 & q_2 & r_2 & r_3 \end{matrix}$$
$$38 = 1 \times 28 + 10$$

$$\begin{matrix} r_2 & q_3 & r_3 & r_4 \end{matrix}$$
$$28 = 2 \times 10 + 8$$

$$\begin{matrix} r_3 & q_4 & r_4 & r_5 \end{matrix}$$
$$10 = 1 \times 8 + \mathbf{2}$$

$$\begin{matrix} r_4 & q_5 & r_5 & r_6 \end{matrix}$$
$$8 = 4 \times 2 + 0$$

Donc $142 \wedge 38 = r_5 = 2$

Présentation de l'algorithme en vue de sa programmation :

```
Répéter
    q := a div b
    r := a mod b
    a := b
    b := r
Jusqu'à r = 0
pgcd := a
```

Illustration avec $a = 142$ et $b = 38$

$q = 4$ $r = 10$ $a = 38$ $b = 10$

$q = 3$ $r = 8$ $a = 10$ $b = 8$

$q = 1$ $r = 2$ $a = 8$ $b = 2$

$q = 4$ $r = \mathbf{0}$ $a = 2$ $b = 0$

pgcd = $a = 2$

Remarque : on peut étendre l'algorithme d'Euclide à $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Par exemple :

$$-142 = (-4) \times 38 + 10$$
$$38 = 3 \times 10 + 8$$
$$10 = 1 \times 8 + 2$$
$$8 = 4 \times 2 + 0$$

D'où : $(-142) \wedge 38 = 2$.

Mais cela est peu utile car, dans $\mathbb{Z}$, on définit :

$$\mathbf{pgcd}(a, b) = \mathbf{pgcd}(|a|, |b|)$$

2. Théorème de Bézout et quelques conséquences

Dans tout ce paragraphe, on suppose $(a, b) \in \left(\mathbb{Z}^*\right)^2$.

2.1. Définition

On dit que a et b sont premiers entre eux lorsque $a \wedge b = 1$

2.2. Théorème de **Bézout**

$$a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1$$

Remarque : le couple (u, v) n'est pas unique. Par exemple, avec $a = 7$ et $b = 11$, on a :

$$(-3) \times 7 + 2 \times 11 = 8 \times 7 - 5 \times 11 = 1$$

Démonstration du théorème de Bézout :

Implication $\Rightarrow$:

Supposons $a \wedge b = 1$.

D'après la définition du pgcd, on a alors : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z} = \mathbb{Z}$

Donc : $\forall w \in \mathbb{Z}, \exists (u, v) \in \mathbb{Z}^2,\ au + bv = w$

En particulier avec $w = 1$: $\exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1$

> On a même un résultat un peu plus fort : si a et b sont premiers entre eux, alors $au + bv$ "parcourt" $\mathbb{Z}$.

Implication $\Leftarrow$:

Supposons : $\exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1$

Notons $d = a \wedge b$. Comme d divise a, il divise au. Comme d divise b, il divise bv.

Finalement d divise $au + bv$ donc d divise 1, d'où : $d = 1$

2.3. Détermination pratique **d'une égalité de Bézout** : algorithme d'**Euclide-Bézout**

Exemple avec $a = 142$ et $b = 38$.

Première étape : on applique l'algorithme d'Euclide

$$\begin{matrix} r_0 & q_1 & r_1 & r_2 \\ 142 = 3 \times 38 + 28 \end{matrix}$$

$$\begin{matrix} r_1 & q_2 & r_2 & r_3 \\ 38 = 1 \times 28 + 10 \end{matrix}$$

$$\begin{matrix} r_2 & q_3 & r_3 & r_4 \\ 28 = 2 \times 10 + 8 \end{matrix}$$

$$\begin{matrix} r_3 & q_4 & r_4 & r_5 \\ 10 = 1 \times 8 + \mathbf{2} \end{matrix}$$

$$\begin{matrix} r_4 & q_5 & r_5 & r_6 \\ 8 = 4 \times 2 + 0 \end{matrix}$$

Donc $142 \wedge 38 = r_5 = 2$

Deuxième étape : on part de la relation contenant r_5 (l'avant dernière) et par injections successives, on exprime r_5 en fonction de $r_0 = a$ et $r_1 = b$:

$$2 = 10 - 1 \times 8$$

$$2 = 10 - 1 \times (28 - 2 \times 10) = -1 \times 28 + 3 \times 10$$

$$2 = -1 \times 28 + 3 \times (38 - 1 \times 28) = 3 \times 38 - 4 \times 28$$

$$2 = 3 \times 38 - 4 \times (142 - 3 \times 38) = -4 \times 142 + 15 \times 38$$

Finalement, un couple (u, v) possible est $(-4, 15)$.

Cas général

D'après l'algorithme d'Euclide, on a :

$$r_{k-1} = q_k r_k + r_{k+1} \text{ où } \begin{cases} 0 \leqslant r_{k+1} < r_k \\ r_{k-1} \wedge r_k = r_k \wedge r_{k+1} \end{cases}$$

Ceci, pour tout entier k tel que $1 \leqslant k \leqslant n$ où n est tel que $r_{n+1} = 0$ et $r_n = a \wedge b$.

Montrons, par récurrence descendante finie sur $k \in [\![1, n-1]\!]$, la propriété :

$$\wp(k) : \exists (u_k, v_k) \in \mathbb{Z}^2,\ r_n = u_k r_k + v_k r_{k-1}$$

- Déjà, on a : $r_{n-2} = r_{n-1} q_{n-1} + r_n$

  D'où : $r_n = r_{n-1} q_{n-1} + r_{n-2}$

  En posant $u_{n-1} = q_{n-1}$ et $v_{n-1} = 1$, on obtient $\wp(n-1)$.

- Montrons que, pour tout $k \in [\![2, n-1]\!]$, $\wp(k) \Rightarrow \wp(k-1)$.

  Soit $k \in [\![2, n-1]\!]$ et supposons $\wp(k)$:

  $$\exists (u_k, v_k) \in \mathbb{Z}^2,\ r_n = u_k r_k + v_k r_{k-1}$$

  Or : $r_{k-2} = r_{k-1} q_{k-1} + r_k$

  D'où : $r_n = u_k (r_{k-2} - r_{k-1} q_{k-1}) + v_k r_{k-1}$

  $r_n = (-u_k q_{k-1} + v_k) r_{k-1} + u_k r_{k-2}$

  On pose alors : $u_{k-1} = -u_k q_{k-1} + v_k$ et $v_{k-1} = u_k$

  Ainsi, on obtient $\wp(k-1)$.

Du principe de raisonnement par récurrence, on déduit :

$$\forall k \in [\![1, n-1]\!],\ \wp(k)$$

En particulier, on a $\wp(1)$: $a \wedge b = r_n = u_1 r_1 + v_1 r_0 = v_1 a + u_1 b$

Le couple (v_1, u_1) fournit une égalité de Bézout pour $a = r_0$ et $b = r_1$.

De plus, cet algorithme prouve une nouvelle fois le théorème de Bézout par récurrence.

Les suites finies (u_k) et (v_k) se prêtent facilement à la programmation. Elles sont simultanément récurrentes et définies par :

$$\begin{cases} u_{n-1} = q_{n-1} \text{ (connu)} \\ u_k = v_{k-1} \ 1 \leqslant k \leqslant n-2 \end{cases} \quad \text{et} \quad \begin{cases} v_{n-1} = 1 \\ v_k = u_k q_{k-1} + u_{k-1} \ 1 \leqslant k \leqslant n-2 \end{cases}$$

2.4. Conséquences : théorèmes de **Gauss** (et variantes)

Soit $(a, b, c) \in \left(\mathbb{Z}^*\right)^3$.

1. $(a \wedge b = 1 \text{ et } a \mid bc) \Rightarrow a \mid c$
2. $(a \mid c,\ b \mid c \text{ et } a \wedge b = 1) \Rightarrow ab \mid c$
3. $(a \wedge b = 1 \text{ et } a \wedge c = 1) \Rightarrow a \wedge bc = 1$
4. $(p \text{ premier et } p \mid ab) \Rightarrow (p \mid a \text{ ou } p \mid b)$

Remarques :

- Le résultat 1 est très utile. Il sert dans la résolution des équations Diophantiennes et dans la preuve de l'unicité de la décomposition en facteurs premiers.
- Le résultat 2 est utile dans la résolution des systèmes de congruences.
- Le résultat 3 est utile pour montrer que la fonction indicatrice φ d'Euler est multiplicative.

Démonstration :

1. Comme $a \wedge b = 1$, le théorème de Bézout permet d'affirmer que :

$$\exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1$$

En multipliant par c : $acu + bcv = c$

Or, $a \mid acu$ et par hypothèse $a \mid bcv$. Donc : $a \mid c$

2. Comme $a \mid c$: $\exists k \in \mathbb{Z},\ c = ka$

Comme $b \mid c$, on en déduit : $b \mid ka$

Or, $a \wedge b = 1$. Donc, d'après 1. : $b \mid k$

$ab \mid ak$

$ab \mid c$

Preuve directe :

Comme $a \mid c$: $\exists k \in \mathbb{Z},\ c = ka$

Comme $b \mid c$: $\exists h \in \mathbb{Z},\ c = hb$

Comme $a \wedge b = 1$, le théorème de Bézout permet d'affirmer que :

$$\exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1$$

En multipliant par c : $acu + bcv = c$

$a(hb)u + b(ka)v = c$

$ab(hu + kv) = c$

$ab \mid c$

3. Comme $a \wedge b = 1$: $\exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1$

Comme $a \wedge c = 1$: $\exists (u', v') \in \mathbb{Z}^2,\ au' + cv' = 1$

En multipliant membre à membre : $(au + bv)(au' + cv') = 1$

On développe : $a^2uu' + aucv' + bvau' + bvcv' = 1$

$a(auu' + ucv' + bvu') + bc(vv') = 1$

Et d'après le théorème de Bézout : $a \wedge bc = 1$

4. Si $p \mid a$, il n'y a rien d'autre à démontrer.

Si p ne divise pas a alors p étant premier, on a : $p \wedge a = 1$

Par ailleurs : $p \mid ab$

Et d'après la propriété 1 : $p \mid b$

On a donc bien : $p \mid a$ ou $p \mid b$

2.5. Liens PPCM-PGCD

2.5.1. Théorème

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$

Si $a \wedge b = 1$, alors $a \vee b = |ab|$

Démonstration :

Soit m un multiple de a et de b :

$$\exists (a, a') \in \mathbb{Z}^2,\ m = aa' = bb'$$

Comme ($a \mid bb'$ et $a \wedge b = 1$), d'après le théorème de Gauss, on déduit :

$$a \mid b'$$

Donc : $$\exists a'' \in \mathbb{Z},\ b' = aa''$$

D'où : $$m = baa''$$

Donc m est un multiple de ab.

On a montré que tout multiple de a et de b est un multiple de ab.

Donc $|ab|$ est le plus petit multiple commun (positif) de a et de b :

$$a \vee b = |ab|$$

2.5.2. Théorème

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$

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

Démonstration :

Posons $d = \text{pgcd}(a, b)$.

D'après l'homogénéité du ppcm (1.1.3.) :

$$\text{ppcm}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}\,\text{ppcm}(a, b)$$

Or, d'après 2.5.1. : $$\text{ppcm}\left(\frac{a}{d}, \frac{b}{d}\right) = \left|\frac{ab}{d^2}\right|$$

D'où : $$|ab| = d \times \text{ppcm}(a, b)$$

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

3. Applications

3.1. Étude de deux suites d'entiers premiers entre eux

Soient (a_n) et (b_n) les suites définies par :

$$\forall n \in \mathbb{N},\ \left(1+\sqrt{2}\right)^n = a_n + b_n\sqrt{2}$$

Démontrer que (a_n) et (b_n) sont des suites d'entiers et que :

$$\forall n \in \mathbb{N},\ a_n \wedge b_n = 1$$

Preuve :

D'après la formule du binôme :

$$\forall n \in \mathbb{N},\ \left(1+\sqrt{2}\right)^n = \sum_{k=0}^{n} C_n^k \left(\sqrt{2}\right)^k$$

Donc : $$a_n = \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} C_n^k \left(\sqrt{2}\right)^k \overset{k=2p}{=} \sum_{p=0}^{E(n/2)} C_n^{2p} 2^p$$

$$\sqrt{2}\, b_n = \sum_{\substack{k=0 \\ k \text{ impair}}}^{n} C_n^k \left(\sqrt{2}\right)^k \overset{k=2p+1}{=} \sum_{p=0}^{E((n-1)/2)} C_n^{2p+1} \left(\sqrt{2}\right)^{2p+1}$$

$$b_n = \sum_{p=0}^{E((n-1)/2)} C_n^{2p+1} 2^p$$

Ce qui prouve que (a_n) et (b_n) sont bien des suites d'entiers.

On montre par un calcul similaire que : $\forall n \in \mathbb{N},\ \left(1-\sqrt{2}\right)^n = a_n - b_n\sqrt{2}$

On a alors : $\forall n \in \mathbb{N},\ \left(a_n + b_n\sqrt{2}\right)\left(a_n - b_n\sqrt{2}\right) = (-1)^n$

$$\forall n \in \mathbb{N},\ a_n^2 - 2\,b_n^2 = (-1)^n$$

On en déduit : $\forall n \in \mathbb{N},\ a_n((-1)^n a_n) + b_n(-2\times(-1)^n b_n) = 1$

D'après le théorème de Bézout : $\forall n \in \mathbb{N},\ a_n \wedge b_n = 1$

3.2. Application aux racines de l'unité

Pour tout $n \in \mathbb{N}$, on note : $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$

Soient a et b des entiers naturels. Démontrer que :

$$\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_{\text{pgcd}(a,\,b)}$$

En déduire que : $\text{pgcd}(X^a - 1, X^b - 1) = X^{\text{pgcd}(a,\,b)} - 1$

Preuve :

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

Montrons : $\mathbb{U}_a \cap \mathbb{U}_b \subset \mathbb{U}_d$

Soit $z \in \mathbb{U}_a \cap \mathbb{U}_b$.

On sait que : $\exists (u, v) \in \mathbb{Z}^2,\ au + bv = d$

On a alors : $z^d = z^{au+bv} = (z^a)^u \times (z^b)^v = 1 \times 1 = 1$

Donc $z \in \mathbb{U}_d$.

Montrons : $\mathbb{U}_d \subset \mathbb{U}_a \cap \mathbb{U}_b$

Soit $z \in \mathbb{U}_d$. Donc : $z^d = 1$

Or, $d \mid a$, d'où : $z^a = z^{kd} = 1$

De même, $d \mid b$, d'où : $z^b = 1$

D'où : $z \in \mathbb{U}_a \cap \mathbb{U}_b$

Finalement : $\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_{\text{pgcd}(a,\,b)}$

On sait que : $X^a - 1 = \prod_{\alpha \in \mathbb{U}_a} (X - \alpha)$ et $X^b - 1 = \prod_{\alpha \in \mathbb{U}_b} (X - \alpha)$

Donc : $\text{pgcd}(X^a - 1, X^b - 1) = \prod_{\alpha \in \mathbb{U}_a \cap \mathbb{U}_b} (X - \alpha) = \prod_{\alpha \in \mathbb{U}_d} (X - \alpha) = X^d - 1 = X^{\text{pgcd}(a,\,b)} - 1$

3.3. Éléments inversible de $\mathbb{Z}/n\mathbb{Z}$

Théorème

Soit $n \in \mathbb{N}^*$. Alors : $\bar{x} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^* \Leftrightarrow \text{pgcd}(x, n) = 1$

Preuve :

On a équivalence des assertions suivantes :

$$\bar{x} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}$$

$$\exists\, \bar{y} \in \mathbb{Z}/n\mathbb{Z},\ \bar{x}\,\bar{y} = \bar{1}$$

$$\exists y \in \mathbb{Z},\ xy = 1\ [n]$$

$$\exists (y, k) \in \mathbb{Z}^2,\ xy - kn = 1$$

$$\text{pgcd}(x, n) = 1$$

Conséquence : $\mathbb{Z}/n\mathbb{Z}$ est un corps (i.e. tous les éléments non nuls sont inversibles) si et seulement si n est premier.

La dernière équivalence étant le théorème de Bézout.

Application : résoudre, dans $\mathbb{Z}/20\mathbb{Z}$, le système : $\begin{cases} \bar{4}\bar{x} + \bar{7}\bar{y} = \bar{10} \\ \bar{5}\bar{x} + \bar{14}\bar{y} = \bar{18} \end{cases}$

Le déterminant du système est : $\bar{4} \times \bar{14} - \bar{5} \times \bar{7} = \bar{1}$

Or, $\bar{1}$ est inversible dans $\mathbb{Z}/20\mathbb{Z}$. Donc le système admet une unique solution.

On peut le résoudre par substitution :

$$\bar{7}\ \bar{y} = \bar{10} - \bar{4}\ \bar{x}$$

En remplaçant dans l'autre équation : $\bar{5}\ \bar{x} + 2(\bar{10} - \bar{4}\ \bar{x}) = \bar{18}$

$$-\bar{3}\ \bar{x} + \bar{20} = \bar{18}$$

$$\bar{3}\ \bar{x} = \bar{2}$$

Pour calculer l'inverse d'un élément $\bar{a}$ dans $\mathbb{Z}/n\mathbb{Z}$, on peut par exemple, utiliser le théorème d'Euler :
si pgcd(a, n) = 1, alors $a^{\varphi(n)} = 1\ [n]$
En conséquence :
$a \times a^{\varphi(n)-1} = 1\ [n]$
L'inverse de $\bar{a}$ est donc $\bar{a}^{\varphi(n)-1}$

Or, $\bar{3}$ est inversible $\mathbb{Z}/20\mathbb{Z}$ et $\bar{3} \times \bar{7} = \bar{21} = \bar{1}$.

D'où : $\bar{x} = \bar{2} \times \bar{7} = \bar{14}$

D'où : $\bar{7}\ \bar{y} = \bar{10} - \bar{4} \times \bar{14} = \bar{14}$

Or, $\bar{7}$ est inversible $\mathbb{Z}/20\mathbb{Z}$ et $\bar{3} \times \bar{7} = \bar{21} = \bar{1}$.

D'où : $\bar{y} = \bar{3} \times \bar{14} = \bar{2}$

Conclusion : $S = \{(\bar{14}\,;\,\bar{2})\}$

3.4. Équation Diophantienne $ax + by = c$ avec $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$

a) Déterminer une condition nécessaire et suffisante pour que l'équation admette au moins une solution.
b) Déterminer, dans ce cas, l'ensemble de toutes les solutions.
c) Application : en multipliant mon jour de naissance par 12 et mon mois de naissance par 31, j'obtiens 442.
Quelle est ma date de naissance ? (On ne demande pas l'année, ouf !)

Solution :

a) Posons $d = \text{pgcd}(a, b)$.

Soient a' et b' tels que : $a = da'$ et $b = db'$

D'après 1.2.5. on a alors : $a' \wedge b' = 1$

L'équation s'écrit : $d(a'x + b'y) = c$

Si d ne divise pas c, alors l'équation n'a pas de solutions.

Si d divise c, alors on pose $c = dc'$. Il vient alors :

$$a'x + b'y = 1$$

Comme $a' \wedge b' = 1$, le théorème de Bézout assure l'existence d'un couple (u, v) solution de $a'x + b'y = 1$.

En multipliant par c', on a alors : $a'c'u + b'c'v = c'$

Le couple $(c'u, c'v)$ est donc une solution particulière de l'équation Diophantienne $ax + by = c$.

Une condition nécessaire et suffisante d'existence de solution est : <u>le pgcd de a et b divise c</u>.

b) On suppose désormais que le pgcd de a et b divise c.

Nous connaissons maintenant une solution particulière $(c'u, c'v)$.

On peut en déduire l'ensemble des solutions. Soit (x, y) une solution quelconque de l'équation $ax + by = c$.

On a alors : $\begin{cases} a'x + b'y = c' \\ a'c'u + b'c'v = c' \end{cases}$

Par différence, il vient : $a'(x - c'u) + b'(y - c'v) = 0$

En conséquence : $a' \mid b'(y - c'v)$

Et comme $a' \wedge b' = 1$, on a, d'après le théorème de Gauss :

$$a' \mid (y - c'v)$$

Donc : $\exists k \in \mathbb{Z}, y = ka' + c'v$

En remplaçant : $a'(x - c'u) + b'ka' = 0$

Et comme $a' \neq 0$: $x = -b'k + c'u$

Réciproquement, on vérifie que, pour tout $k \in \mathbb{Z}$, le couple $(-b'k + c'u, ka' + c'v)$ est bien solution de l'équation Diophantienne.

<u>Bilan</u> : les couples (x, y) solutions de l'équation $ax + by = c$ (lorsque pgcd(a, b) divise c) sont de la forme :

$$(x, y) = (-b'k + c'u, ka' + c'v), \ k \in \mathbb{Z}$$

c) Notons J et M mon jour et mon mois de naissance respectivement.

On a donc : $12J + 31M = 442$

Comme $12 \wedge 31 = 1$, l'équation admet des solutions. (Donc je suis bien né !)

On recherche une solution particulière en appliquant l'algorithme d'Euclide-Bézout :

$r_0 \quad q_1 \quad r_1 \quad r_2$
$31 = 2 \times 12 + 7$

$r_1 \quad q_2 \quad r_2 \quad r_3$
$12 = 1 \times 7 + 5$

$r_2 \quad q_3 \quad r_3 \quad r_4$
$7 = 1 \times 5 + 2$

$r_3 \quad q_4 \quad r_4 \quad r_5$
$5 = 2 \times 2 + 1$

$r_4 \quad q_5 \quad r_5 \quad r_6$
$2 = 2 \times 1 + 0$

Puis, on exprime le pgcd (à savoir 1) en fonction des restes précédents :

$$1 = 5 - 2 \times 2$$

$$1 = 5 - 2 \times (7 - 5) = -2 \times 7 + 3 \times 5$$

$$1 = -2 \times 7 + 3 \times (12 - 7) = 3 \times 12 - 5 \times 7$$

$$2 = 3 \times 12 - 5 \times (31 - 2 \times 12) = -5 \times 31 + 13 \times 12$$

Finalement, un couple (u, v) possible est $(-5, 13)$.

On a donc : $-5 \times 31 + 13 \times 12 = 1$

En multipliant par 442 : $-2210 \times 31 + 5746 \times 12 = 442$

Donc le couple $(J_0, M_0) = (5742, -2210)$ est une solution particulière de l'équation $12J + 31M = 442$.

On recherche maintenant l'ensemble de toutes les solutions. Soit (J, M) une solution quelconque.

$$\begin{cases} 12J + 31M = 442 \\ 5746 \times 12 - 2210 \times 31 = 442 \end{cases}$$

Par différence, il vient : $12(J - 5746) + 31(M + 2210) = 0$

En conséquence : $31 \mid 12(J - 5746)$

Et comme $12 \wedge 31 = 1$, on a, d'après le théorème de Gauss :

$$31 \mid J - 5746$$

Donc : $\exists k \in \mathbb{Z}, J = 31k + 5746$

Or, évidemment $J \in [\![1, 31]\!]$: $1 \leqslant 31k + 5746 \leqslant 31$

$$-5745 \leqslant 31k \leqslant -5715$$

$$k = -185$$

$$J = 11$$

On en déduit : $M = 10$

Je suis donc né un 11 octobre.

3.5. Théorème Chinois et applications

3.5.1. Théorème Chinois

Soit $(m, n) \in \left(\mathbb{N}^*\right)^2$.

Si $m \wedge n = 1$, alors $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Démonstration :

1. Un morphisme de groupe injectif remarquable

Soient $(m, n) \in (\mathbb{N}^*)^2$.

Considérons l'application f qui à tout entier relatif x associe un couple constitué de sa classe modulo m et de sa classe modulo n :

$$\begin{array}{rcl} f : \mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & ([x]_m, [x]_n) \end{array}$$

Où : $[x]_m = \{y \in \mathbb{Z} \mid y - x \in m\mathbb{Z}\}$

Montrons que f est un **morphisme de groupes additifs** :

$\forall (x, y) \in (\mathbb{N})^2$, $f(x + y) = ([x + y]_m, [x + y]_n)$

Et d'après les lois sur les classes :

$$f(x + y) = ([x]_m + [y]_m, [x]_n + [y]_n)$$

Et par propriétés des couples :

$$f(x+y) = ([x]_m , [x]_n) + ([y]_m , [y]_n) = f(x) + f(y)$$

Ce qui prouve que f est un morphisme du groupe $(\mathbb{Z}, +)$ sur le groupe produit $\left(\mathbb{Z}/m\mathbb{Z},+\right)\times\left(\mathbb{Z}/n\mathbb{Z},+\right)$.

C'est même un morphisme d'anneaux (car $f(xy) = ([xy]_m , [xy]_n) = ([x]_m , [x]_n) \times ([y]_m , [y]_n) = f(x) \times f(y)$ et $f(1) = ([1]_m , [1]_n)$

Déterminons **le noyau de f** :

$$\text{Ker}(f) = \{x \in \mathbb{Z} \mid f(x) = ([0]_m , [0]_n)\} = \{ x \in \mathbb{Z} \mid [x]_m = [0]_m \text{ et } [x]_n = [0]_n\} = m\mathbb{Z} \cap n\mathbb{Z}$$

Or, on sait que : $m\mathbb{Z} \cap n\mathbb{Z} = p\mathbb{Z}$ où $p = \text{ppcm}(m, n)$

Donc : $\text{Ker}(f) = p\mathbb{Z}$ où $\text{ppcm}(m, n)$

On a donc $\text{Ker}(f) \neq \{0\}$ et f n'est pas un morphisme injectif.

Nous allons maintenant définir un nouveau morphisme $\overline{f}$ sur $\mathbb{Z}/p\mathbb{Z}$ qui aura même image que f.

Pour cela, il suffit de constater que l'image, par f, d'une classe est indépendante du représentant choisi dans cette classe :

On a : $f(x_1) = f(x_2) \Rightarrow f(x_1 - x_2) = ([0]_m , [0]_n)$

Ce qui signifie que $x_1 - x_2$ est un multiple commun de m et n donc multiple de $p = \text{ppcm}(m, n)$.

Donc $[x_1 - x_2]_p = [0]_p$, c'est-à-dire $[x_1]_p = [x_2]_p$.

Nous pouvons donc légitimement définir l'application :

$$\begin{aligned} \overline{f} : \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [x]_p &\mapsto ([x]_m , [x]_n) \end{aligned}$$

On a donc, plus simplement : $\overline{f}([x]_p) = f(x)$.

Il est clair que $\overline{f}$ **est un morphisme de groupes additifs** :

$\forall([x]_p , [y]_p) \in \left(\mathbb{Z}/p\mathbb{Z}\right)^2$:

$$\overline{f}([x]_p + [y]_p) = \overline{f}([x+y]_p) = f(x+y) = f(x) + f(y) = \overline{f}([x]_p) + \overline{f}([y]_p)$$

(Puisque f est un morphisme)

C'est même un isomorphisme d'anneaux car f l'est.

Montrons que $\overline{f}$ **est un morphisme injectif** :

$$\text{Ker}(\overline{f}) = \{ [x]_p \in \mathbb{Z}/p\mathbb{Z} \mid \overline{f}([x]_p) = 0\} = \{ [x]_p \in \mathbb{Z}/p\mathbb{Z} \mid f(x) = 0\} = \{ [x]_p \in \mathbb{Z}/p\mathbb{Z} \mid x \in \text{Ker}(f)\}$$

$$\text{Ker}(\overline{f}) = \{ [x]_p \in \mathbb{Z}/p\mathbb{Z} \mid x \in p\mathbb{Z}\} = \{[0]_p\}$$

Remarque : on dit que l'on a factorisé f : $f = \overline{f} \circ s$ où s est la surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z}$.

Bilan :

Pour tous m et n entiers naturels non nuls, il existe un morphisme injectif $\overline{f}$ entre

$$\mathbb{Z}/\text{ppcm}(m,n)\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

qui, à toute classe $[x]_{\text{ppcm}(m, n)}$ fait correspondre le couple $([x]_m , [x]_n)$.

2. Un cas particulier important

Supposons maintenant que m et n soient premiers entre eux. Dans ce cas : ppcm(m, n) = mn.

Dans ce cas, comme card$\left(\mathbb{Z}/_{mn\,\mathbb{Z}}\right) = mn = \text{card}\left(\mathbb{Z}/_{m\,\mathbb{Z}} \times \mathbb{Z}/_{n\,\mathbb{Z}}\right)$, le morphisme $\overline{f}$ est également **bijectif**.

C'est le **théorème Chinois :**

> Si $m \wedge n = 1$, alors $\mathbb{Z}/_{mn\,\mathbb{Z}} \cong \mathbb{Z}/_{m\,\mathbb{Z}} \times \mathbb{Z}/_{n\,\mathbb{Z}}$

Exemple : $\mathbb{Z}/_{6\,\mathbb{Z}} \cong \mathbb{Z}/_{2\,\mathbb{Z}} \times \mathbb{Z}/_{3\,\mathbb{Z}}$

3.5.2. Application 1 : systèmes de congruences

Des entiers a, b, m et n étant donnés, on considère le système suivant :

$$(S)\ \begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$$

Deux questions se posent :

1) À quelle condition, nécessaire et suffisante, le système admet des solutions.
2) Comment déterminer ces solutions.

Il y a un cas royal, c'est $m \wedge n = 1$. Dans ce cas, la surjectivité du morphisme $\overline{f}$ assure l'existence de solutions (qui seront, de plus, de la forme $x = x_0 + kmn$).

Voici un procédé algorithmique permettant de les trouver :

D'après le théorème de Bézout : $\exists (u, v) \in \mathbb{Z}^2$ tels que : $mu + nv = 1$

Posons $x_0 = bmu + anv$.

On a clairement : $x_0 \equiv anv\ [m]$

Or, $anv = a - amu$, donc : $x_0 \equiv a\ [m]$

On montre, de même, que : $x_0 \equiv b\ [n]$

On a donc une solution particulière x_0.

Soit x une solution quelconque. On a alors : $\begin{cases} x - x_0 \equiv 0\ [m] \\ x - x_0 \equiv 0\ [n] \end{cases}$

Donc $m \mid (x - x_0)$ et $n \mid (x - x_0)$

Or, $m \wedge n = 1$, donc $mn \mid (x - x_0)$.

> $(a \mid c$ et $b \mid c$ et $a \wedge b = 1) \Rightarrow ab \mid c$
>
> Preuve : on a $c = aa'$ et $b \mid aa'$.
>
> Or, $a \wedge b = 1$ donc $b \mid a'$ donc $ab \mid c$.

D'où : $\boldsymbol{x = x_0 + kmn}$.

Mais peut-il exister des solutions même si $m \wedge n \neq 1$? Quel procédé pour les trouver ?

Remarquons que le système (S) est équivalent à :

$$\exists (k, h) \in \mathbb{Z}^2 \text{ tels que } \begin{cases} x = a + km \\ x = b + hn \end{cases}$$

$$\exists (k, h) \in \mathbb{Z}^2 \text{ tels que } \begin{cases} x = a + km \\ a + km = b + hn \end{cases}$$

$$\exists (k, h) \in \mathbb{Z}^2 \text{ tels que } \begin{cases} x = a + km \\ km - hn = b - a \end{cases}$$

Or, l'équation d'inconnues h et k : $km - hn = b - a$ est une équation de Diophante. On sait qu'une telle équation admet des solutions si et seulement si $m \wedge n$ divise $b - a$.

On énonce donc :

Le système $\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$ admet des solutions si et seulement si $m \wedge n$ divise $b - a$.

(C'est évidement le cas lorsque $m \wedge n = 1$)

En résolvant l'équation de Diophante, on trouve h (ou k) et donc x.

Exemple :

Un régiment comporte entre 50 et 100 soldats.
Si on les range en 4 colonnes, il en reste 3.
Si on les range en 5 colonnes, il en reste 4.
Si on les range en 3 colonnes, il en reste 1.
Combien y a-t-il de soldats dans ce régiment ?

Il s'agit ici de résoudre le système de congruences suivant :

$$\begin{cases} x \equiv 3[4] \\ x \equiv 4[5] \\ x \equiv 1[3] \end{cases}$$

On résout déjà le système : $\begin{cases} x \equiv 3[4] \\ x \equiv 4[5] \end{cases}$

Comme $4 \wedge 5 = 1$, le théorème chinois nous assure de l'existence de solutions. On cherche un couple (u, v) vérifiant : $4u + 5v = 1$

Le couple $(-1, 1)$ convient. On en déduit une solution particulière :

$$x_0 = bmu + anv = 4 \times 4 \times (-1) + 3 \times 5 \times 1 = -1$$

D'où : $x \equiv 19\ [20]$

On a donc l'équivalence : $\begin{cases} x \equiv 3[4] \\ x \equiv 4[5] \\ x \equiv 1[3] \end{cases} \Leftrightarrow \begin{cases} x \equiv 19[20] \\ x \equiv 1[3] \end{cases}$

Comme ci-dessus, on trouve cette fois : $x \equiv 19\ [60]$

Comme le régiment comporte entre 50 et 100 soldats, on conclut :

$x = 79$ soldats

3.5.3. Application 2 : l'indicatrice d'Euler φ est une fonction multiplicative

On rappelle que : $\varphi(n) = \text{Card}\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \{m \in [\![1, n-1]\!],\ m \wedge n = 1\}$

On suppose que $m \wedge n = 1$. Reprenons notre isomorphisme :

$$\begin{aligned} \overline{f} : \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [x]_{mn} &\mapsto ([x]_m, [x]_n) \end{aligned}$$

Soit $[x]_{mn} \in \left(\mathbb{Z}/mn\mathbb{Z}\right)^*$. Notons $[y]_{mn}$ son inverse.

On a : $([1]_m, [1]_n) = f([1]_{mn}) = f([x]_{mn}[y]_{mn}) = f([x]_{mn})\ f([y]_{mn})$

Donc $f([x]_{mn})$ est inversible dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

Réciproquement, si $f([x]_{mn})$ est inversible dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ alors $x \wedge m = 1$ et $x \wedge n = 1$

Donc $x \wedge mn = 1$ (d'après les variantes du théorème de Gauss 2.4.) et donc $[x]_{mn} \in \left(\mathbb{Z}/mn\mathbb{Z}\right)^*$.

On a donc un isomorphisme (induit par $\overline{f}$) entre $\left(\mathbb{Z}/mn\mathbb{Z}\right)^*$ et $\left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

On en déduit : si $m \wedge n = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$

Application : comme $\varphi(p) = p - 1$ et $\varphi(p^r) = p^r - p^{r-1}$ pour tout premier p, si $n = \prod_i p_i^{r_i}$ alors :

$$\varphi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$$

3.6. Équation du premier degré dans $\mathbb{Z}/n\mathbb{Z}$

Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}/n\mathbb{Z}$.

On considère l'équation : $\overline{a}\ \overline{x} + \overline{b} = \overline{0}$

CAS 1 :

Si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (i.e. $a \wedge n = 1$) alors, la résolution est immédiate :

$$\overline{x} = -\overline{a}^{-1}\overline{b}$$

Exemple : $\overline{6}\ \overline{x} + \overline{7} = \overline{0}$ dans $\mathbb{Z}/35\mathbb{Z}$.

Comme $6 \wedge 35 = 1$, $\overline{6}$ est inversible dans $\mathbb{Z}/35\mathbb{Z}$ et $\overline{6}^{-1} = \overline{6}$.

D'où : $\overline{x} = -\overline{6} \times \overline{7} = \overline{28}$

Remarque : si on cherche les solutions dans $\mathbb{Z}$, on obtient : $x = 28 + 35k$, $k \in \mathbb{Z}$.

CAS 2 :

Si $a \wedge n$ divise b, alors l'équation admet encore des solutions. En effet, on a :

$$\overline{a}\ \overline{x} + \overline{b} = \overline{0} \iff \exists y \in \mathbb{Z},\ ax + b = ny$$

On récupère alors une équation de Diophante dont on sait qu'elle a des solutions (puisque $a \wedge n$ divise b).

Notons (x_0, y_0) une solution particulière, $d = a \wedge n$, $a = a'd$ et $n = n'd$. On a alors :

$$x = x_0 - kn' \text{ et } y = y_0 + ka',\ k \in \mathbb{Z}$$

En choisissant x_0 dans $[\![0, n' - 1]\!]$, on a alors :

$$S = \{\ \overline{x_0}\ ;\ \overline{x_0 + n'}\ ;\ \ldots\ ;\ \overline{x_0 + (d-1)n'}\ \}$$

(Au total, d classes solutions)

Exemple : $\overline{12}\ \overline{x} - \overline{6} = \overline{0}$ dans $\mathbb{Z}/18\mathbb{Z}$.

$\overline{12}$ n'est pas inversible dans $\mathbb{Z}/18\mathbb{Z}$. Dans $\mathbb{Z}$, l'équation s'écrit :

$$12x - 6 = 18y$$

On détermine une solution particulière : $(x_0, y_0) = (2, 1)$

D'où : $x = x_0 + n'k = 2 + 3k,\ k \in \mathbb{Z}$

On en déduit : $S = \{ \overline{2} ; \overline{5} ; \overline{8} ; \overline{11} ; \overline{14} ; \overline{17} \}$

CAS 3

Si $a \wedge n$ ne divise pas b, alors l'équation n'admet pas de solutions. En effet, dans ce cas, l'équation de Diophante $ax + b = ny$ n'en admet pas.

3.7. Équation du second degré dans $\mathbb{Z}/n\mathbb{Z}$

On ne traite pas la théorie générale. On donne juste des exemples.

Exemple 1 : si n est un nombre premier p alors $\mathbb{Z}/p\mathbb{Z}$ est un corps et on calcule "normalement" :

$$\overline{x}^2 + \overline{x} + \overline{7} = \overline{0} \text{ dans } \mathbb{Z}/13\mathbb{Z}$$

$$\overline{x}^2 + \overline{14}\,\overline{x} + \overline{7} = \overline{0}$$

On canonise : $$(\overline{x} + \overline{7})^2 - \overline{42} = \overline{0}$$

$$(\overline{x} + \overline{7})^2 - \overline{4}^2 = \overline{0}$$

$$(\overline{x} + \overline{3})(\overline{x} + \overline{11}) = \overline{0}$$

Et comme $\mathbb{Z}/p\mathbb{Z}$ est intègre : $$\overline{x} = \overline{10} \text{ ou } \overline{x} = \overline{2}$$

Exemple 2 : $$\overline{x}^2 - 4\overline{x} + \overline{3} = \overline{0} \text{ dans } \mathbb{Z}/12\mathbb{Z}$$

On canonise : $$(\overline{x} - \overline{2})^2 = \overline{1}$$

On calcule les carrés dans $\mathbb{Z}/12\mathbb{Z}$:

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{x}^2$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{9}$	$\overline{4}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{9}$	$\overline{4}$	$\overline{1}$

D'où : $$\overline{x} - \overline{2} = \overline{1} \text{ ou } \overline{x} - \overline{2} = \overline{5} \text{ ou } \overline{x} - \overline{2} = \overline{7} \text{ ou } \overline{x} - \overline{2} = \overline{11}$$

$$S = \{ \overline{1} ; \overline{3} ; \overline{7} ; \overline{9} \}$$