

## PGCD ET PPCM DANS $\mathbb{Z}$ . Algorithme d'Euclide dans $\mathbb{Z}$

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

### 1. PPCM dans $\mathbb{Z}$

#### 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.

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

Alors  $n | n'$  et  $n' | n$

Donc :  $n' = n$

#### 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 :  $a | n$  et  $b | n$

$n$  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 :  $n | n'$

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

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

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

#### 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 :  $0 \vee a = a \vee 0 = 0$

- $a | b \Leftrightarrow a \vee b = b$

- Homogénéité :  $m(a \vee b) = (ma) \vee (mb)$

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

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

## 2. PGCD dans $\mathbb{Z}$

### 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 :

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

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

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 :

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

$$\text{Alors } d \mid d' \text{ et } d' \mid d$$

$$\text{Donc : } d' = d$$

### 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 :

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

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

En particulierisant  $m = 0$  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.

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 :

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

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

### 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 :

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

#### 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 :  $m(a \wedge b) = (ma) \wedge (mb)$

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  $m(a \wedge b)$  :

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

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

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 :  $m(a \wedge b) = (ma) \wedge (mb)$

### 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 :  $\frac{a}{d} \wedge \frac{b}{d} = 1$

## 3. Algorithme d'Euclide

### 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  $b$  ( $a = bq + r, 0 \leq r < b$ ) alors :  $a \wedge b = b \wedge r$

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 :

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

### 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  $a$ .

Posons :

$$r_0 = a \text{ et } r_1 = b \text{ (donc } r_0 > r_1)$$

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

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

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  $k \geq 2$ , on ait :

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

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

$$r_0 > r_1 > r_2 > \dots > r_k$$

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

On a alors :

$$r_{n-1} = q_n r_n + 0 \text{ où } r_{n-1} \wedge r_n = r_n \wedge 0 = r_n$$

On en déduit :

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \dots = r_n \wedge 0 = r_n$$

Conclusion :

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

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

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

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

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

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

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

Donc  $142 \wedge 38 = r_5 = 2$

Présentation de l'algorithme en vue de sa programmation :

Répéter
$q := a \text{ div } b$
$r := a \text{ mod } b$
$a := b$
$b := r$
Jusqu'à $r = 0$
pgcd := a

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

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

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

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

$$q = 4 \quad r = 0 \quad a = 2 \quad b = 0$$

$$\text{pgcd} = a = 2$$

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 :

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