Algèbre et Arithmétique Effectives - 09/09/25
Cours 1

On part de l'un des plus vieux algorithme de l'histroire :

L'ALGORITHME D'EUCLIDE (Livre VII des Éléments d'Euclide - 300 av. J.C.)

Il permet de calculer le plus grand commun diviseur (PGCD) de deux entiers.

Quelques rappels de divisibilité :

$\mathbb{Z}$ = ensemble des entiers relatifs =
$= \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$: entiers positifs ou nuls

$\mathbb{Z}_{>0} = \{1, 2, \ldots\}$: entiers positifs.

notre convention

Pour nous positif (resp. négatif) signifie strictement supérieur à zéro (resp. strictement inférieur à zéro).

Def : Soient $a, b \in \mathbb{Z}$. On dit que a divise b, et on écrit $a \mid b$, s'il existe $c \in \mathbb{Z}$ tel que :

$$b = ac.$$

Dans ce cas on dit que a est un diviseur de b, que b est un multiple de a et que b est divisible par a.

Si a ne divise pas b, on écrit $a \nmid b$.

Exemple

$\underset{a}{5} \mid \underset{b}{10}$ car $\exists\ \overset{c}{2} \in \mathbb{Z}$ tel que $10 = 5 \cdot 2$

$3 \nmid 5$ car $\forall\ c \in \mathbb{Z}$ $5 \neq 3 \cdot c$.

Remarque : $\forall\ a, b, c \in \mathbb{Z}$

- $a \mid a$, $1 \mid a$, $a \mid 0$
- $0 \mid a \iff a = 0$
- $a \mid b \iff -a \mid b \iff a \mid -b$
- $a \mid b$ et $a \mid c \Rightarrow a \mid b+c$ et $a \mid b-c$
- $a \mid b$ et $b \mid c \Rightarrow a \mid c$

Proposition : $\forall\ a, b \in \mathbb{Z}$ on a :

$a \mid b$ et $b \mid a \iff a = \pm b$

En particulier $\forall\ a \in \mathbb{Z}$

$a \mid 1 \iff a = \pm 1$.

Déf : Soient $a, b \in \mathbb{Z}$.

On dit que $d \in \mathbb{Z}$ est un <u>diviseur commun</u> à a et b si $d \mid a$ et $d \mid b$.

On dit que $d \in \mathbb{Z}$ est <u>le plus grand commun diviseur</u> (pgcd) si

- $d \geq 0$
- tout autre diviseur commun divise d.
(si $d' \mid a$ et $d' \mid b \Rightarrow d' \mid d$).

Déf : On dit que $a, b \in \mathbb{Z}$ sont **premiers entre eux** si $\text{pgcd}(a,b) = 1$

Exemples

1) $\text{pgcd}(24, 18) = 6$

diviseurs de 24 : 1, 2, 3, 4, 6, 8, 12, 24

diviseurs de 18 : 1, 2, 3, 6, 9, 18

$\Rightarrow \text{pgcd}(18,24) = 6$

2) $\text{pgcd}(2025, 0) = 2025 \Longrightarrow$ Remarque : $\forall a \in \mathbb{Z}\setminus\{0\}$ $\text{pgcd}(a,0) = a$.

Attention : $\text{pgcd}(0,0)$ est indéfini.

Théorème : Soient $a, b \in \mathbb{Z}$ tels que $a \neq 0$ ou $b \neq 0$. Alors il existe $d \in \mathbb{Z}_{>0}$ tel que $\text{pgcd}(a,b) = d$.

Dém

Si $a = 0 \Rightarrow \text{pgcd}(a,b) = b$.

Si $b = 0 \Rightarrow \text{pgcd}(a,b) = a$.

Puisque $\text{pgcd}(a,b) = \text{pgcd}(\pm a, \pm b)$ il suffit de démontrer le théorème $\forall a, b \in \mathbb{Z}_{>0}$.

La démonstration se base alors sur l'algorithme d'Euclide du calcul du PGCD.

On en décrit d'abord la version originale détaillée dans la Proposition 2 du livre VII des Éléments.

Algorithme 1 : Algorithme d'Euclide version soustractive

EUCLIDE SOUSTRACTIF (a,b)

Entrées : Deux entiers $a, b > 0$
Sortie : pgcd (a,b)

```
1.  Tant que a ≠ b faire
2.      Si a > b alors
3.          a := a - b
4.      Sinon
5.          b := b - a
6.  Renvoyer a
```

Exemple

pgcd (49, 14)

$\begin{matrix} a=49 \\ b=14 \end{matrix} \longrightarrow \begin{matrix} a=35 \\ b=14 \end{matrix} \longrightarrow \begin{matrix} a=21 \\ b=14 \end{matrix} \longrightarrow \begin{matrix} a=7 \\ b=14 \end{matrix} \longrightarrow \begin{matrix} a=7 \\ b=7 \end{matrix} \Longrightarrow$

$\Rightarrow$ pgcd (49, 14) = 7.

Pour compléter la démonstration il suffit donc de démontrer la correction de cet algorithme :

1) Il faut montrer qu'il termine.

2) Il faut montrer que la sortie est effectivement le pgcd (a,b)

→ Exercice 2 du TD 1

Remarque : L'algorithme 1 réalise automatiquement des divisions euclidiennes

$\begin{matrix} a=49 \\ b=14 \end{matrix} \xrightarrow{1} \begin{matrix} a=35 \\ b=14 \end{matrix} \xrightarrow{2} \begin{matrix} a=21 \\ b=14 \end{matrix} \xrightarrow{3} \begin{matrix} \boxed{a=7} \\ b=14 \end{matrix} \longrightarrow \begin{matrix} a=7 \\ b=7 \end{matrix} \Longrightarrow$

$a > b$ $\qquad\qquad\qquad\qquad$ $a < b$

$\Longrightarrow 49 = 3 \cdot 14 + 7$

Théorème (Division Euclidienne)

Soient $a, b \in \mathbb{Z}$, $b \neq 0$. Alors il existe un unique couple d'entiers (q, r) tel que

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

On appelle q le quotient et r le reste de la division. On note le reste $a \bmod b$.

Algorithme 2 : Algorithme d'Euclide classique

EUCLIDE (a, b)

Entrées : Deux entiers $a, b > 0$
Sortie : $\text{pgcd}(a, b)$

1. Tant que $b \neq 0$ faire
2. $c = b$
3. $b = a \bmod b$
4. $a = c$
5. Renvoyer a

$(a, b) \leftarrow (b, a \bmod b)$

Algorithme d'Euclide Étendu

Théorème (identité de Bézout)

Soient $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$, et soit $d = \text{pgcd}(a, b)$. Alors il existe un couple d'entiers (u, v) tels que

$$\boxed{au + bv = d}$$

identité de Bézout.

Exemple :

$a = 87$, $b = 24$

$87 = 24 \cdot 3 + 15$

$24 = 15 \cdot 1 + 9$

$15 = 9 \cdot 1 + 6$

$\boxed{9 = 6 \cdot 1 + 3}$ $= \mathrm{pgcd}(87, 24)$

$6 = 3 \cdot 2 + 0$

$$3 = 9 - 6 \cdot 1 = 9 - (15 - 9) =$$
$$= 9 \cdot 2 - 15 = (24 - 15) \cdot 2 - 15 =$$
$$= 24 \cdot 2 - 15 \cdot 3 = 24 \cdot 2 - (87 - 24 \cdot 3) \cdot 3 =$$
$$= \underbrace{-3}_{u} \cdot \underbrace{87}_{a} + \underbrace{11}_{v} \cdot \underbrace{24}_{b}$$