Arithmétique et Algèbre Effectives - 10/09/24
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 =

$= \{\dots, -2, -1, 0, 1, 2, \dots\}$

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

$\mathbb{Z}_{>0} = \{1, 2, \dots\}$: 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 <u>a divise b</u>, 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 <u>diviseur</u> de b, que b est un <u>multiple</u> de a et que b est <u>divisible</u> 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 :

$$a \mid b \text{ et } b \mid a \iff a = \pm b$$

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 diviseur commun à a et b si $d \mid a$ et $d \mid b$.

On dit que $d \in \mathbb{Z}$ est le plus grand commun diviseur (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 $\operatorname{pgcd}(a,b) = 1$

Exemples

$\operatorname{pgcd}(24, 18) = 6$
$\operatorname{pgcd}(14, 49) = 7$
$\operatorname{pgcd}(2024, 0) = 2024$ $\Longrightarrow$ Remarque : $\forall\, a \in \mathbb{Z} \setminus \{0\}$ $\operatorname{pgcd}(a, 0) = a$.
Attention : $\operatorname{pgcd}(0,0)$ est indéfini.

Exercice : Calculer $\operatorname{pgcd}(1260, 462)$. (Résultat 42)

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

Un algorithme pour calculer le pgcd est détaillé dans la Proposition 2 du Livre VII des Éléments.

Euclide écrivait :

" **Proposition 2** : Étant donnés deux nombres qui ne sont pas premiers entre eux, calcule leur pgcd.

comme si les nombres étaient la longueur de segments

Soient AB et CD deux nombres donnés qui ne sont pas premiers entre eux... "

Exemple pratique de l'algorithme originaire proposé par Euclide :

Pgcd $(49, 14)$

l'entier plus petit — le différence entre le plus grand et le plus petit.

$\underline{14}$, $49-14=\underline{35}$

$\underline{14}$, $35-14=\underline{21}$

$\underline{14}$, $21-14=\underline{7}$

$\underline{7}$, $14-7=\underline{7}$: J'obtiens deux entiers égaux : ça est le pgcd

$\Downarrow$

$\mathrm{pgcd}(49,14)=7$.

Exercice : Écrire cet algorithme

Algorithme 1 : Algorithme d'Euclide version soustractive :

EUCLIDE SOUSTRACTIF (a,b)

Entrées : Deux entiers $a, b > 0$

Sortie : $\mathrm{pgcd}(a,b)$.

1. Si $a<b$: $(a,b) \leftarrow (b,a)$
2. Tant que $a \neq b$:
3. $\quad (a,b) \leftarrow (b, a-b)$
4. $\quad$ Si $a<b$: $(a,b) \leftarrow (b,a)$
5. Renvoyer a

Comment prouver que l'algorithme 1 est correcte ?

1) Il faut montrer qu'il termine.

2) Il faut montrer que la sortie est effectivement le $\mathrm{pgcd}(a,b)$.

Preuve

1) Preuve de terminaison

Si $a=b$, l'algorithme s'arrête.

Si $a \neq b$, à chaque étape la plus grande des deux valeurs diminue strictement.

Étant donné que les deux entiers sont positifs, on finit par attendre un point où $a=b$ et l'algorithme s'arrête.

2) Preuve de correction

Il suffit de montrer que $\text{pgcd}(a,b) = \text{pgcd}(b,a-b)$

<u>Dém</u> : D'après un résultat précédent, il suffit de montrer que :

$$\boxed{\text{pgcd}(a,b) \mid \text{pgcd}(b,a-b)} \ \underline{\text{et}} \ \boxed{\text{pgcd}(b,a-b) \mid \text{pgcd}(a,b)}$$

Puisque les pgcd sont positifs, cela implique que $\text{pgcd}(a,b) = \text{pgcd}(b,a-b)$

(1) Soit $d = \text{pgcd}(a,b) \Rightarrow d \mid a$ et $d \mid b$

$\Rightarrow d \mid -b$ et $d \mid a \Rightarrow d \mid a-b$ et $d \mid b$

$\Rightarrow d \mid \text{pgcd}(b, a-b)$.

(2) Soit $d' = \text{pgcd}(b,a-b) \Rightarrow d' \mid b$ et $d' \mid a-b$

$\Rightarrow d' \mid b$ et $d' \mid b+(a-b) \Rightarrow d' \mid a$ et $d' \mid b$

$\Rightarrow d' \mid \text{pgcd}(a,b)$

Donc $d \mid d'$ et $d' \mid d \underset{d,d'>0}{\Longrightarrow} d = d'$.

Cela implique que à chaque étape on ne change pas le pgcd. Pour conclure il suffit de remarquer que $\text{pgcd}(a,a) = a$, $\forall a \in \mathbb{Z} \setminus \{0\}$. Donc la sortie de notre algorithme est le pgcd des entrées.

Remarque : PGCD(32,6)

0	6	32
1	6	26
2	6	20
3	6	14
4	6	8
5	6	2

c'est le reste

le nombre d'itérations est le quotient de la division euclidienne

$$32 = 6 \cdot \underset{\text{quotient}}{5} + \underset{\text{reste}}{2}$$

Donc l'algorithme 1 réalise automatiquement des divisions euclidiennes.

Rappel :

Théorème (Division euclidienne)

Soient $a, b \in \mathbb{Z}$, $b > 0$. 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 de la division et on le note a quo b (ou $\lfloor \frac{a}{b} \rfloor$).

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

Exemple : $a = 47$ et $b = 8$

a quo $b = 5$ $\qquad$ $a \bmod b = 7$

Algorithme 2 : Division Euclidienne

Division Euclidienne(a,b)

Entrées : $a, b \in \mathbb{Z}$ tels que $a \geq 0$ et $b > 0$

Sortie : le couple (q, r) tel que $a = bq + r$ avec $0 \leq r < b$.

```
(q, r) ← (0, a)
Tant que r ≥ b :
        r ← r - b
        q ← q + 1
Renvoyer (q, r)
```

Algorithme 3 : Algorithme d'Euclide classique

Euclide(a,b)

Entrées : $a, b \in \mathbb{Z}$ tels que $a, b > 0$

Sortie : pgcd(a,b).

```
si a < b : (a, b) ← (b, a)
Tant que b > 0 :
        (a, b) ← (b, a mod b)
Renvoyer a
```

< b car c'est le reste de la division

Exercice

Démontrer les assertions suivantes :

1) $\forall a, b, c \in \mathbb{Z}$, $a | b$ et $a | c \Rightarrow a | b + c$.

2) $\forall a, b, c \in \mathbb{Z}, \quad a \mid b$ et $b \mid c \Rightarrow a \mid c$

3) $\forall a, b \in \mathbb{Z}$, si $a \mid b$ et $b \mid a \Rightarrow a = \pm b$.

<u>Démo</u>

1) Puisque $a \mid b$, $\exists\, d \in \mathbb{Z}$ tel que $b = ad$

Puisque $a \mid c$, $\exists\, d' \in \mathbb{Z}$ tel que $c = ad'$

Donc :

$$b + c = ad + ad' = a\underbrace{(d + d')}_{\in \mathbb{Z}}$$

$\Rightarrow a \mid b + c$.

2) Puisque $a \mid b$, $\exists\, d \in \mathbb{Z}$ tel que $b = ad$

Puisque $b \mid c$, $\exists\, d' \in \mathbb{Z}$ tel que $c = bd'$

Donc :

$$c = bd' = \underbrace{add'}_{\in \mathbb{Z}} \Rightarrow a \mid c.$$

3) Si $a = 0$ ou $b = 0$, l'énoncé est vrai
Donc on peut supposer $b \neq 0$

Puisque $a \mid b$, $\exists\, d \in \mathbb{Z}$ tel que $b = ad$.

Puisque $b \mid a$, $\exists\, d' \in \mathbb{Z}$ tel que $a = bd'$

Donc :

$$b = ad = bdd' \Rightarrow \overset{b \neq 0}{\cancel{b}} = \cancel{b}dd' \Rightarrow dd' = 1$$

$$\Rightarrow d, d' = \pm 1 \Rightarrow a = \pm b.$$