Feuille de cours 8 : algorithme d'Euclide

Pour deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, on note $\mathcal{D}(a) \cap \mathcal{D}(b)$ l'ensemble des diviseurs communs à a et b. Lorsque ces entiers ne sont pas tous les deux nuls, cet ensemble est non vide, fini et admet donc un plus grand élément : le PGCD de a et b noté $PGCD(a, b)$.

Rappelons que la division euclidienne d'un entier $a \in \mathbb{Z}$ par un entier $b \in \mathbb{N}^*$ assure l'existence et l'unicité d'un couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ vérifiant :

$$a = \qquad\qquad \text{avec} \quad 0 \leq r <$$

1 Lemme fondamental de division

Pour déterminer le PGCD de deux entiers sans avoir à expliciter l'ensemble de tous leurs diviseurs, le résultat fondamental repose sur la conservation des diviseurs communs lors d'une division euclidienne :

Proposition 1 (Lemme d'Euclide)
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. En notant r le reste de la division euclidienne de a par b, on a :

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$$

démonstration : On écrit la division euclidienne de a par b : $a = bq + r$ avec $0 \leq r < b$.

- Inclusion directe ($\subset$) : Soit $d \in$
  Alors $d \mid a$ et $d \mid b$. Par combinaison linéaire à coefficients entiers, on a donc :

  $$d \mid a - bq \quad \text{c'est-à-dire} \quad d \mid$$

  Ainsi, d est un diviseur commun à b et r, donc
- Inclusion réciproque ($\supset$) : Soit $d \in \mathcal{D}(b) \cap \mathcal{D}(r)$.
  Alors $d \mid b$ et $d \mid r$. Par combinaison linéaire :

  $$d \mid \qquad\qquad \text{c'est-à-dire} \quad d \mid a$$

  Ainsi, d est un diviseur commun à a et b, d'où $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$.

Par double inclusion, on a bien $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$.

□

Conséquence immédiate : Deux ensembles d'entiers égaux ayant le même plus grand élément, on en déduit que :

$$PGCD(a, b) = PGCD(b, r)$$

Exercice 1
Sans poser l'ensemble de tous les diviseurs, déterminer $PGCD(105, 30)$ en utilisant une seule division euclidienne et la propriété précédente.

2 L'algorithme d'Euclide

Le principe de l'algorithme consiste à réitérer ce lemme : on remplace le calcul du PGCD de deux entiers par celui du plus petit d'entre eux et du reste obtenu, jusqu'à parvenir à un reste nul.

Proposition 2 (Algorithme d'Euclide)
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. On définit par récurrence la suite finie (r_k) par :

- $r_0 = a$ et $r_1 = b$,
- pour tout $k \in \mathbb{N}^*$ tel que $r_k \neq 0$, r_{k+1} est le reste dans la division euclidienne de r_{k-1} par r_k, c'est-à-dire :

Alors il existe un entier $N \in \mathbb{N}$ tel que $r_N \neq 0$ et $r_{N+1} = 0$, et $PGCD(a, b) = r_N$.

démonstration :

- $b \neq 0$, donc r_2 est défini comme le reste dans la division euclidienne de r_0 par r_1, et l'on a $0 \leq r_2 < r_1$.
- Si $r_2 \neq 0$, r_3 est le reste dans la division euclidienne de r_1 par r_2, donc $0 \leq r_3 < r_2 < r_1$.
- En réitérant, tant que les restes sont non nuls, on construit une suite d'entiers strictement décroissante :
$$r_1 > r_2 > r_3 > \cdots \geq 0$$

Si la suite ne s'annulait jamais, on obtiendrait une suite infinie d'entiers naturels strictement décroissante, ce qui est impossible. Il existe donc nécessairement un premier rang où elle s'annule, noté $N + 1$, vérifiant $r_N \neq 0$ et $r_{N+1} = 0$.
D'après le lemme fondamental :

$$\begin{aligned}\mathcal{D}(a) \cap \mathcal{D}(b) &= \mathcal{D}(r_0) \cap \mathcal{D}(r_1) \\ &= \mathcal{D}(r_1) \cap \mathcal{D}(r_2) \\ &= \dots \\ &= \mathcal{D}(r_N) \cap \mathcal{D}(r_{N+1}) \\ &= \mathcal{D}(r_N) \cap \mathcal{D}(0).\end{aligned}$$

Or l'ensemble des diviseurs de 0 est $\mathcal{D}(0) =$ donc $\mathcal{D}(r_N) \cap \mathcal{D}(0) = \mathcal{D}(r_N)$, ensemble dont le plus grand élément n'est autre que r_N. Finalement, le plus grand élément de $\mathcal{D}(a) \cap \mathcal{D}(b)$ est $PGCD(a, b) = r_N$.

□

À retenir : Le $PGCD(a, b)$ est le **dernier reste non nul** dans la suite des divisions euclidiennes successives de l'algorithme d'Euclide.

3 Exemples

Calculons le $PGCD(207, 162)$ en organisant les divisions successives dans un tableau :

r_{k-1}	r_k	Division euclidienne : $r_{k-1} = r_k q + r_{k+1}$	Égalité ensembles des diviseurs
162	45	$162 = 45 \times 3 + 27$	$\mathcal{D}(162) \cap \mathcal{D}(45) = \mathcal{D}(45) \cap \mathcal{D}(27)$
45	27	$45 =$	
		$27 = 18 \times 1 + 9$	$\mathcal{D}(27) \cap \mathcal{D}(18) = \mathcal{D}(18) \cap \mathcal{D}(9)$
18	9	$18 = 9 \times 2 + 0$	$\mathcal{D}(18) \cap \mathcal{D}(9) =$

Le dernier reste non nul est , donc $PGCD(207, 162) =$.

Exercice 2
En utilisant l'algorithme d'Euclide sous forme de divisions successives, calculer $PGCD(420, 154)$.

Exercice 3
Les entiers 119 et 72 sont-ils premiers entre eux ?