Contents

1. Définition du PGCD

Soit $a, b \in \mathbb{Z}^*$.

Le plus **grand entier** qui divise à la fois a et b s'appelle le **plus grand commun diviseur** ou **PGCD** de a et b.

On le note **PGCD(a,b)** ou $a \wedge b$.

Exercice 1

Donner en partant de la définition :

- PGCD(12,36)
- PGCD(13,43)
- PGCD(57,9)

Remarque :

$\text{PGCD }(a, b) = \text{PGCD }(|a|, |b|)$.

1.a. Propriété du PGCD

Soit $a, b \in \mathbb{Z}^*$. Si a divise b alors $\text{PGCD }(a, b) = |a|$.

Exercice 2

Soit a un entier relatif.

Déterminer le PGCD d des entiers $m = 14a + 3$ et $n = 21a + 4$ et trouver des entiers u et v tels que $um + vn = d$.

2. Algorithme d'Euclide

2.a. Principe de base

Soit $a, b \in \mathbb{Z}^*$.

S'il existe des entiers k et s avec $s \neq 0$ tels que $a = bk + s$ alors les diviseurs communs à a et b sont exactement les diviseurs communs à b et s, et $\text{PGCD }(a, b) = \text{PGCD }(b, s)$.

2.b. Algorithme d'Euclide

Soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$. On cherche $d = \text{PGCD }(a, b)$. On note $r_0 = b$.

On effectue des divisions euclidiennes successives tant que le reste est non nul.

$$\begin{aligned}
a &= r_0 q_1 + r_1 && 0 < r_1 < r_0 \\
b &= r_1 q_2 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} && 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0 && r_{n+1} = 0
\end{aligned}$$

$(r_k)_{k\in\mathbb{N}}$ est une suite strictement décroissante d'entiers naturels donc, *au bout d'un certain temps*, on obtient un reste nul et l'algorithme s'arrête.

Si $r_{n+1} = 0$ alors r_n divise r_{n-1}, donc

$$\text{PGCD }(r_{n-1}, r_n) = r_n$$

.

2.b.i. Théorème

Le PGCD de a et b est le dernier reste non nul obtenu par l'algorithme d'Euclide. (ci-dessus, c'est r_n).

Remarque :

Si $r_1 = 0$, c'est que b divise a, donc PGCD $(a, b) = b = r_0$. (l'algorithme s'arrête immédiatement).

Exercice 3

Calculer $PGCD(8820; 3150)$ avec l'algorithme d'Euclide.

Propriétés :

Soit $a, b \in \mathbb{Z}^*$. Si d divise a et b alors d divise PGCD (a, b).

$$\begin{cases} d \mid a \\ d \mid b \end{cases} \Longrightarrow d \mid PGCD(a,b)$$

Remarque :

On peut définir le PGCD de 3 entiers ou plus. On peut utiliser la propriété suivante :

si $d = \text{PGCD }(a, b)$ alors PGCD $(a, b, c) =$ PGCD (d, c).

Exemple :

$PGCD(12, 28, 18) = PGCD(4, 18) = 2$

3. Nombres premiers entre eux

3.a. Définition

Soit a et b deux entiers non nuls.

On dit que a et b sont **premiers entre eux** si PGCD $(a, b) = 1$.

On dit aussi que a **est premier avec** b.

3.b. Propriétés

Soit $a, b \in \mathbb{Z}^*$ et $d = PGCD(a, b)$.

$$\frac{a}{d} \text{ et } \frac{b}{d} \text{ sont premiers entre eux}$$

Une fraction est irréductible si le numérateur et le dénominateur sont premiers entre eux. Pour obtenir une fraction irréductible égale à $\frac{p}{q}$, il suffit de simplifier par le PGCD .

4. Théorème de Bachet-Bézout (ou Identité de Bézout)

Soient a et b deux entiers relatifs.

Si d est le PGCD de a et b, **alors** il existe deux entiers relatifs x et y tels que $ax + by = d$.

Exemple :

26 et 34 admettent 2 comme PGCD, il existe donc deux entiers relatifs u et v tels que

$$26u + 34v = 2$$

5. Théorème de Bézout

Deux entiers non nuls a et b sont premiers entre eux **si et seulement si**, il existe des entiers u et v tels que: $au + bv = 1$

Trouver une relation de Bezout pour a et b, c'est trouver des entiers u et v tels que $au + bv = pgcd(a, b)$.

Pour cela :

- On applique l'algorithme d'Euclide a et b.
- On part de l'égalité donnant le pgcd, et on **"remonte"** l'algorithme.

$$a = 116, b = 10 \qquad \begin{aligned} 116 &= 11 \times 10 + 6 \\ 10 &= 1 \times 6 + 4 \\ 6 &= 1 \times 4 + 2 \\ 4 &= 2 \times 2 + 0 \end{aligned}$$

On remonte maintenant en remplaçant systématiquement le reste de la ligne précédente.

$$\begin{aligned} 2 &= 6 - 1 \times 4 \\ 2 &= 6 - 1 \times (10 - 6) = 2 \times 6 - 10 \\ 2 &= 2 \times (116 - 10 \times 11) - 10 = 2 \times 116 - 23 \times 10 \end{aligned}$$

$2a - 23b = 2$ est une relation de Bezout pour $a = 116$ et $b = 10$ ($u = 2, v = -23$).

- Une fois qu'on a calculé u et v, il est facile de vérifier que $au + bv = PGCD(a, b)$.
- u et v ne sont pas uniques.

$7a - 81b = 2$ est une autre relation de Bezout pour $a = 116$ et $b = 10$.

Exercice 4

- A l'aide de l'algorithme d'Euclide, déterminer le PGCD de 420 et 637, puis exprimer ce PGCD comme combinaison linéaire de ces deux nombres.
- Même question pour 152 et 184
- Montrer que $\forall n \in \mathbb{N}, (2n + 1)$ et $(3n + 2)$ sont premiers entre eux.

5.a. Conséquences du théorème de Bézout

Le théorème de Bézout permet de démontrer *facilement* des théorèmes arithmétiques importants.

Exercice 5

Si un nombre n est divisible par a et par b et que ces deux nombres sont premiers entre eux, il est divisible par $a \times b$.

Démonstration guidée

D'après les hypothèses, on peut trouver des entiers k et l tels que :

$n =$ ... et $n =$ ....

De plus, d'après le théorème de Bézout, on peut trouver u et v tels que $\cdots$.

On a alors

$$\begin{aligned} n &= 1 \times n \\ &= \\ &= \\ &= \\ &= ab \times (ul + vk) \end{aligned}$$

qui est bien divisible par $a \times b$.

Exercice 6

Comment reconnaître facilement qu'un nombre est un multiple de 45 ?

Par exemple, est-ce que 4 685 368 545 est un multiple de 45 ?

Exercice 7

a et b sont deux entiers naturels non nuls.

Démontrer que $\mathrm{PGCD}\ (3a + 4b; 4a + 5b) = \mathrm{PGCD}\ (a; b)$.

6. Lemme de Gauss

Soit a, b et c trois nombres entiers tels que **a divise bc**. Si a est premier avec b, alors a divise c.

Démonstration à connaître

On écrit une relation de Bézout pour a et b :
il existe des entiers u et v tels que

$$au + bv = 1$$

La relation de divisibilité indique qu'il existe un entier k tel que

$$ak = bc.$$

On a alors

$$\begin{aligned} akv &= bcv \\ akv &= c \times bv \\ akv &= c(1 - au) \\ akv &= c - acu \\ akv - acu &= c \\ a(kv - cu) &= c \end{aligned}$$

ce qui montre que c est un multiple de a.

Exercice 8

Donner un contre-exemple illustrant le fait que la **seconde hypothèse du lemme de Gauss est indispensable**.