

PGCD - PPCM

Théorèmes de Bézout et de GAUSS

Table des matières

1	Plus grand commun diviseur	2
1.1	Définition	2
1.2	Nombres premiers entre eux	2
1.3	Algorithme d'Euclide	3
2	Plus petit commun multiple	4
3	Théorème de Bézout	4
3.1	Égalité de Bézout	4
3.2	Théorème de Bézout	5
3.3	Algorithme de Bézout	6
3.4	Corollaire de Bézout	6
4	Le théorème de Gauss	7
4.1	Le théorème	7
4.2	Corollaire du théorème de Gauss	8
4.3	Propriétés	8

1 Plus grand commun diviseur

1.1 Définition

Définition 1 : Soit a et b deux entiers relatifs non nuls.

L'ensemble des diviseurs communs à a et b admet un plus grand élément D , appelé plus grand commun diviseur.

On note : $D = \text{pgcd}(a, b)$

Démonstration : *Existence*

L'ensemble des diviseurs communs à a et b est un ensemble fini car intersection de deux ensembles finis.

De plus 1 divise a et b donc l'ensemble des diviseurs communs à a et b est non vide.

Or tout ensemble fini non vide admet un plus grand élément donc D existe.

Exemples :

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

$$\text{pgcd}(60, 84) = 12$$

$$\text{pgcd}(150, 240) = 30$$

Propriétés :

- Si b divise a alors $\text{pgcd}(a, b) = |b|$
- Pour tout entier naturel k non nul, on a : $\text{pgcd}(ka, kb) = k \text{pgcd}(a, b)$.

1.2 Nombres premiers entre eux

Définition 2 : On dit que a et b sont premiers entre eux si et seulement si

$$\text{pgcd}(a, b) = 1$$

Exemple : $\text{pgcd}(15, 8) = 1$ donc 15 et 8 sont premiers entre eux.

⚠ Il ne faut pas confondre des nombres premiers entre eux et des nombres premiers. 15 et 8 ne sont pas premiers et pourtant ils sont premiers entre eux.

Par contre deux nombres premiers distincts sont nécessairement premiers entre eux.

1.3 Algorithme d'Euclide

Théorème 1 : Soit a et b deux naturels non nuls tels que b ne divise pas a .

La suite des divisions euclidiennes suivantes finit par s'arrêter. Le dernier reste non nul est alors le $\text{pgcd}(a, b)$

$$\begin{array}{lll}
 a \text{ par } b & a = b q_0 + r_0 & \text{avec } b > r_0 \geq 0 \\
 b \text{ par } r_0 & b = r_0 q_1 + r_1 & \text{avec } r_0 > r_1 \geq 0 \\
 r_0 \text{ par } r_1 & r_0 = r_1 q_2 + r_2 & \text{avec } r_1 > r_2 \geq 0 \\
 & \vdots & \\
 r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1} q_n + r_n & \text{avec } r_{n-1} > r_n \geq 0 \\
 r_{n-1} \text{ par } r_n & r_{n-1} = r_n q_{n+1} + 0 &
 \end{array}$$

On a alors $\text{pgcd}(a, b) = r_n$.

Démonstration :

- La suite des restes : $r_0, r_1, r_2, \dots, r_n$ est une suite strictement décroissante dans \mathbb{N} car $r_0 > r_1 > r_2 > \dots > r_n$.

Cette suite est donc finie. Il existe alors n tel que $r_{n+1} = 0$.

Montrons que $\text{pgcd}(a, b) = \text{pgcd}(b, r_0)$.

Soit $D = \text{pgcd}(a, b)$ et $d = \text{pgcd}(b, r_0)$.

D divise a et b donc D divise $a - bq_0 = r_0$, donc D divise b et r_0 donc : $D \leq d$
 d divise b et r_0 donc d divise $bq_0 + r_0 = a$, donc d divise a et b donc : $d \leq D$

On déduit de ces deux inégalités que $D = d$: $\text{pgcd}(a, b) = \text{pgcd}(b, r_0)$

- De proche en proche, on en déduit que :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = \dots = \text{pgcd}(r_{n-2}, r_{n-1}) = \text{pgcd}(r_{n-1}, r_n)$$

or r_n divise r_{n-1} , donc $\text{pgcd}(r_{n-1}, r_n) = r_n$

Conclusion : $\text{pgcd}(a, b) = r_n$. Le dernier reste non nul est le pgcd .

Exemple :

Calculer le $\text{pgcd}(4\,539, 1\,958)$.

On effectue les divisions euclidiennes suivantes :

$$4\,539 = 1\,958 \times 2 + 623$$

$$1\,958 = 623 \times 3 + 89$$

$$623 = 89 \times 7$$

Conclusion : $\text{pgcd}(4\,539, 1\,958) = 89$

Remarque : Le petit nombre d'étapes montre la performance de cet algorithme.

Algorithme : Voici un algorithme d'Euclide que l'on peut proposer pour trouver le pgcd de deux nombres. On pourrait éventuellement utiliser l'algorithme de la division euclidienne à l'intérieur du programme, mais pour les besoins de simplicité, on utilisera la partie entière pour trouver le quotient.

```

Variables :  $a, b, q, r$  entiers naturels
Entrées et initialisation
| Lire  $a, b$ 
|  $E(a/b) \rightarrow q$ 
|  $a - bq \rightarrow r$ 
Traitement
| tant que  $r \neq 0$  faire
|   |  $b \rightarrow a$ 
|   |  $r \rightarrow b$ 
|   |  $E(a/b) \rightarrow q$ 
|   |  $a - bq \rightarrow r$ 
| fin
Sorties : Afficher  $b$ 

```

2 Plus petit commun multiple

Définition 3 : Soit a et b deux entiers relatifs non nuls.

L'ensemble des multiples strictement positifs communs à a et à b admet un plus petit élément M , appelé plus petit commun multiple.

On le note : $M = \text{ppcm}(a, b)$.

Démonstration : *Existence*

L'ensemble des multiples strictement positifs à a et à b n'est pas vide. En effet $|ab|$ est un multiple positif de a et de b .

Toute partie non vide de \mathbb{N} admet un plus petit élément donc M existe.

Exemple :

$$\text{ppcm}(18, 12) = 36$$

$$\text{ppcm}(24, 40) = 120$$

Pour additionner deux fractions, on recherche le dénominateur commun le plus petit qui n'est autre que le ppcm.

Propriétés :

- Si b divise a alors $\text{ppcm}(a, b) = |a|$
- Si a et b sont premiers entre eux alors $\text{ppcm}(a, b) = |ab|$
- On a : $ab = \text{ppcm}(a, b) \times \text{pgcd}(a, b)$

3 Théorème de Bézout

3.1 Égalité de Bézout

Théorème 2 : Soit a et b deux entiers non nuls et $D = \text{pgcd}(a, b)$

Il existe alors un couple (u, v) d'entiers relatifs tels que :

$$au + bv = D$$

Démonstration :

Soit G l'ensemble formé par les entiers naturels strictement positifs de la forme $ma + nb$ où m et n sont des entiers relatifs.

G est une partie de \mathbb{N} non vide : on vérifie facilement que $|a| \in G$.

G admet donc un plus petit élément d tel que $d = au + bv$

- $D = \text{pgcd}(a, b)$ divise a et b donc D divise $au + bv = d$ et donc $\underline{D \leq d}$
- Montrons que d divise a

Divisons a par d , on a alors $a = dq + r$ avec $0 \leq r < d$.

On isole le reste et on remplace d par $au + bv$:

$$r = a - dq = a - auq - bvq = a(1 - uq) + b(-vq)$$

Donc $r = 0$. En effet si $r \neq 0$ alors $r \in G$, or $r < d$ et d est le plus petit élément de G , cela est absurde.

$r = 0$ donc d divise a . En faisant le même raisonnement, on montrerait que d divise aussi b .

d divise a et b donc $\underline{d \leq D}$

- conclusion : $D \leq d$ et $d \leq D$ donc $D = d$.

Conséquence : Tout diviseur commun à a et b divise leur pgcd.

3.2 Théorème de Bézout

Théorème 3 : Deux entiers relatifs a et b sont premiers entre eux si et seulement si, il existe deux entiers relatifs u et v tels que :

$$au + bv = 1$$

ROC

Démonstration :

Dans le sens \Rightarrow : Immédiat grâce à l'égalité de Bézout.

Dans le sens \Leftarrow : (réciproquement)

On suppose qu'il existe deux entiers u et v tels que : $au + bv = 1$.

Si $D = \text{pgcd}(a, b)$ alors D divise a et b donc D divise $au + bv$.

Donc D divise 1. On a bien $D = 1$.

Exemple : Montrer que $(2n + 1)$ et $(3n + 2)$ sont premiers entre eux $\forall n \in \mathbb{N}$.

Il s'agit de trouver des coefficients u et v pour que $u(2n + 1) + v(3n + 2) = 1$.

$$-3(2n + 1) + 2(3n + 2) = -6n - 3 + 6n + 4 = 1$$

$\forall n \in \mathbb{N}$, il existe $u = -3$ et $v = 2$ tel que $u(2n + 1) + v(3n + 2) = 1$.

Les entiers $(2n + 1)$ et $(3n + 2)$ sont premiers entre eux.

Exemple : Montrer que 59 et 27 sont premiers entre eux puis déterminer un couple (x, y) tel que : $59x + 27y = 1$

Pour montrer que 59 et 27 sont premiers entre eux on effectue l'algorithme d'Euclide et pour déterminer un couple (x, y) , on remonte l'algorithme d'Euclide :

$$59 = 27 \times 2 + 5 \quad (1)$$

$$27 = 5 \times 5 + 2 \quad (2)$$

$$5 = 2 \times 2 + 1 \quad (3)$$

59 et 27 sont premiers entre eux.

On remonte l'algorithme d'Euclide :

$$2 \times 2 = 5 - 1$$

On multiplie l'égalité (2) par 2

$$27 \times 2 = 5 \times 10 + 2 \times 2$$

$$27 \times 2 = 5 \times 10 + 5 - 1$$

$$27 \times 2 = 5 \times 11 - 1$$

$$5 \times 11 = 27 \times 2 + 1$$

on multiplie l'égalité (1) par 11

$$59 \times 11 = 27 \times 22 + 5 \times 11$$

$$59 \times 11 = 27 \times 22 + 27 \times 2 + 1$$

$$59 \times 11 = 27 \times 24 + 1$$

$$\text{On a donc : } 59 \times 11 + 27 \times (-24) = 1$$

3.3 Algorithme de Bézout

Il s'agit de déterminer un couple $(u; v)$ d'entiers relatifs sachant que les entiers a et b sont premiers entre eux. On doit donc avoir : $au + bv = 1$

On isole le premier terme :

$$au = b(-v) + r$$

On teste, en incrémentant u , le reste de la division de $m = au$ par b . Tant que le reste est différent de 1, on réitère la division.

On analysera de plus si le réel b est positif ou non pour déterminer le quotient.

Une fois u trouvé, on détermine v :

$$v = \frac{1 - m}{b}$$

On teste ce programme avec : $a = 59$ et $b = 27$

On trouve alors : $u = 11$ et $v = -24$

Variables : a, b, u, v, m, r entiers

Entrées et initialisation

Lire a, b

$0 \rightarrow r$

$0 \rightarrow u$

Traitement

tant que $r \neq 1$ **faire**

$u + 1 \rightarrow u$

$au \rightarrow m$

si $b > 0$ **alors**

$m - E\left(\frac{m}{b}\right) \times b \rightarrow r$

sinon

$m - E\left(\frac{m}{b} + 1\right) \times b \rightarrow r$

fin

fin

$\frac{1 - m}{b} \rightarrow v$

Sorties : Afficher u et v

3.4 Corollaire de Bézout

Théorème 4 : L'équation $ax + by = c$ admet des solutions entières si et seulement si c est un multiple du $\text{pgcd}(a, b)$.

Démonstration :

Dans le sens \Rightarrow

$ax + by = c$ admet une solution (x_0, y_0) .

Comme $D = \text{pgcd}(a, b)$ divise a et b il divise $ax_0 + by_0$.

D divise donc c

Dans le sens \Leftarrow (réciproquement)

c est un multiple de $D = \text{pgcd}(a, b)$.

Donc il existe un entier relatif k tel que : $c = kd$

De l'égalité de Bézout, il existe deux entiers relatifs u et v tels que :

$$au + bv = D$$

En multipliant par k , on obtient :

$$auk + bvk = kD \Leftrightarrow a(uk) + b(vk) = c$$

Donc il existe $x_0 = uk$ et $y_0 = vk$ tels que $ax_0 + by_0 = c$

Exemple : L'équation $4x + 9y = 2$ admet des solutions car $\text{pgcd}(4, 9) = 1$ et 2 multiple de 1

L'équation $9x - 15y = 2$ n'admet pas de solution car $\text{pgcd}(9, 15) = 3$ et 2 non multiple de 3

4 Le théorème de Gauss

4.1 Le théorème

Théorème 5 : Soit a, b et c trois entiers relatifs non nuls.

Si a divise le produit bc et si a et b sont premiers entre eux alors a divise c .

ROC

Si a divise le produit bc , alors il existe un entier k tel que : $bc = ka$

Si a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que : $au + bv = 1$

En multipliant par c , on a :

$$\begin{aligned} acu + bcv &= c & \text{or } bc &= ka, \text{ donc :} \\ acu + kav &= c \\ a(cu + kv) &= c \end{aligned}$$

Donc a divise c .

Exemple : Trouver les solutions dans \mathbb{Z}^2 de l'équation : $5(x - 1) = 7y$

5 divise $7y$, or $\text{pgcd}(5, 7) = 1$, donc d'après le théorème de Gauss 5 divise y . On a donc : $y = 5k$

En remplaçant dans l'équation, on a :

$$5(x - 1) = 7 \times 5k \Leftrightarrow x - 1 = 7k \Leftrightarrow x = 7k + 1$$

Les solutions sont donc de la forme : $\begin{cases} x = 7k + 1 \\ y = 5k \end{cases} \quad k \in \mathbb{Z}$

4.2 Corollaire du théorème de Gauss

Théorème 6 : Si b et c divisent a et si b et c sont premiers entre eux alors bc divise a .

ROC

Démonstration : Si b et c divisent a , alors il existe k et k' entiers relatifs tels que :

$$a = kb \quad \text{et} \quad a = k'c \quad \text{donc} : \quad kb = k'c$$

b divise $k'c$, or $\text{pgcd}(b, c) = 1$ donc d'après le théorème de Gauss b divise k' donc : $k' = k''b$

$$a = k'c = k''bc$$

Donc bc divise a .

Exemple : Si 5 et 12 divisent a , comme 5 et 12 sont premiers entre eux, $5 \times 12 = 60$ divise a .

4.3 Propriétés

Ces propriétés découlent du théorème de Bézout et de Gauss.

Propriété 1 : Soit a et b deux entiers non nuls, D leur pgcd et M leur ppcm.

- Il existe deux entiers a' et b' premiers entre eux tels que :

$$a = Da' \quad \text{et} \quad b = Db'$$

- On a les relations suivantes :

$$M = Da'b' \quad \text{et} \quad ab = MD$$