

Plus grand commun diviseur (pgcd) Théorèmes de Bézout et de GAUSS

Table des matières

1 Plus grand commun diviseur (pgcd)	2
1.1 Définition	2
1.2 Nombres premiers entre eux	2
1.3 Algorithme d'Euclide	3
2 Théorème de Bézout	4
2.1 Identité de Bézout	4
2.2 Théorème de Bézout	5
2.2.1 Déterminer un couple d'entiers de Bézout	5
2.2.2 Algorithme de Bézout	6
2.3 Corollaire de Bézout	6
3 Le théorème de Gauss	7
3.1 Le théorème	7
3.2 Corollaire du théorème de Gauss	7
3.3 Équations diophantiennes	7

1 Plus grand commun diviseur (pgcd)

1.1 Définition

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

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

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

Remarque : On note aussi $\text{pgcd}(a, b) = a \wedge b$.

Cette notation est plutôt réservée à l'enseignement supérieur.

Démonstration : Existence et unicité

L'ensemble des diviseurs communs à a et b est un ensemble fini car intersection de deux ensembles dont l'un au moins est fini (non tous nuls).

L'ensemble des diviseurs communs à a et b est non vide car 1 divise a et b .

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

Exemples : $\text{pgcd}(24, 18) = 6$, $\text{pgcd}(60, 84) = 12$, $\text{pgcd}(150, 240) = 30$

Propriété 1 : Propriétés du pgcd

- $\text{pgcd}(a, b) = \text{pgcd}(b, a)$.
- $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$.
- $\text{pgcd}(a, 0) = |a|$ car 0 est multiple de tout entier.
- Si b divise a alors $\text{pgcd}(a, b) = |b|$
- Pour tout entier naturel k non nul, on a : $\text{pgcd}(ka, kb) = k \text{pgcd}(a, b)$.

Exemples : $\text{pgcd}(30, 75) = \text{pgcd}(75, 30)$ et $\text{pgcd}(-24, -18) = \text{pgcd}(24, 18)$
 $\text{pgcd}(82, 0) = 82$, $\text{pgcd}(30, 5) = 5$ et $\text{pgcd}(240, 180) = 10 \text{pgcd}(24, 18) = 60$.

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.

⚠ Ne pas confondre « nombres premiers entre eux » et « nombres premiers ».

15 et 8 ne sont pas premiers et mais sont premiers entre eux.

Par contre deux nombres premiers distincts sont premiers entre eux.

Remarque : Une fraction irréductible q s'écrit :

$$q = \frac{a}{b} \text{ avec } a \in \mathbb{Z}, b \in \mathbb{N}^* \text{ et } \text{pgcd}(a, b) = 1.$$

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 du diviseur par le reste de la division précédente finit par s'arrêter. Le dernier reste non nul est alors le $\text{pgcd}(a, b)$

$$\begin{array}{lll}
 \text{division de } a \text{ par } b : & a = b q_0 + r_0 & \text{avec } b > r_0 \geq 0 \\
 \text{division de } b \text{ par } r_0 : & b = r_0 q_1 + r_1 & \text{avec } r_0 > r_1 \geq 0 \\
 \text{division de } r_0 \text{ par } r_1 : & r_0 = r_1 q_2 + r_2 & \text{avec } r_1 > r_2 \geq 0 \\
 \vdots & \vdots & \vdots \\
 \text{division de } r_{n-2} \text{ par } r_{n-1} : & r_{n-2} = r_{n-1} q_n + r_n & \text{avec } r_{n-1} > r_n \geq 0 \\
 \text{division de } r_{n-1} \text{ par } r_n : & r_{n-1} = r_n q_{n+1} + 0 & \\
 \text{D'où } & \text{pgcd}(a, b) = r_n. &
 \end{array}$$

Démonstration :

- Montrons que $\text{pgcd}(a, b) = \text{pgcd}(b, r_0)$ par une double inégalité.

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

D divise a et b donc divise toute combinaison linéaire de a et b et donc divise $a - bq_0 = r_0$. D divise b et r_0 , par conséquent $D \leq d$.

d divise b et r_0 donc divise toute combinaison linéaire de b et r_0 et donc divise $bq_0 + r_0 = a$. d divise a et b , par conséquent $d \leq D$.

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

- La suite des restes r_0, r_1, \dots, r_n est strictement décroissante dans \mathbb{N} .
(car $r_0 > r_1 > \dots > r_n \geq 0$.)

D'après le principe de la descente infinie (toute suite strictement décroissante dans \mathbb{N} est finie), il existe alors n tel que $r_{n+1} = 0$

(car tant que le reste est non nul on peut diviser).

- De proche en proche, on en déduit, avec r_n divise r_{n-1} , que :

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

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

Exemple : Déterminer le $\text{pgcd}(4\,539, 1\,958)$.

On effectue les divisions successives suivantes :

$$\begin{array}{ll}
 4\,539 = 1\,958 \times 2 + 623 & \text{pgcd}(4\,539, 1\,958) = 89 \\
 1\,958 = 623 \times 3 + 89 & \\
 623 = 89 \times 7 &
 \end{array}$$

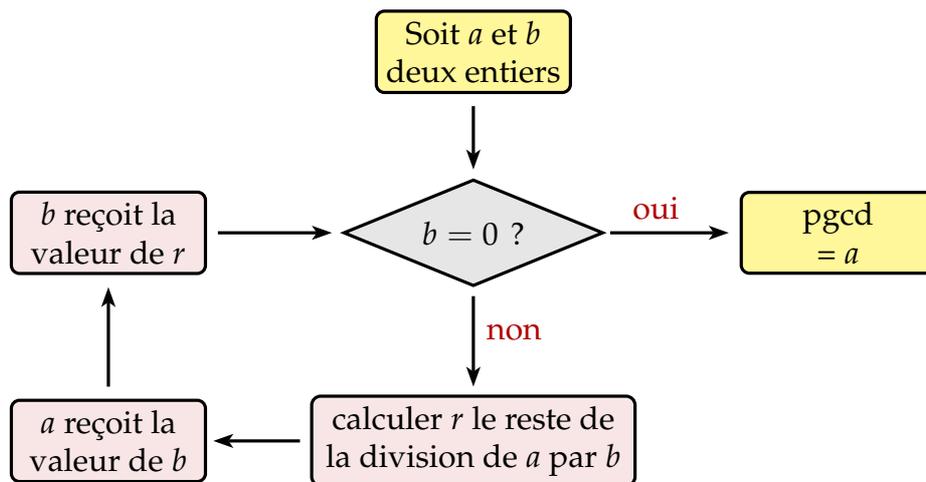
Remarque : Le petit nombre d'étapes montre la performance de cet algorithme.

Algorithme : On crée en Python 🐍 la fonction $\text{pgcd}(a,b)$ en initialisant le reste. Par une boucle conditionnelle tant que le reste est non nul, on divise, puis on réactualise les valeurs de a et b .

On obtient alors pour $\text{pgcd}(4\,539, 1\,958)$: 89

```
def pgcd(a, b):
    r = a % b
    while r != 0:
        a = b
        b = r
        r = a % b
    return b
```

L'algorithme d'Euclide peut être présenté sous la forme d'un organigramme. On pose la question « est-ce que $b = 0$? ». Si oui, le pgcd est égal à a . Si non, on part dans la boucle « non ». On revient à la question avec les nouvelles valeurs de a et b .



2 Théorème de Bézout

2.1 Identité 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 des combinaisons linéaires strictement positives de a et de b .

G n'est pas vide car il contient par exemple $|a|$.

Du principe du bon ordre, G admet un plus petit élément $d = au + bv$ avec $d > 0$.

Notons $D = \text{pgcd}(a, b)$ et montrons que $d = D$ par double inégalité.

- D divise a et b donc divise toute combinaison linéaire de a et de b et donc divise $au + bv = d$ d'où $D \leq d$
- Divisons a par d : $a = dq + r$ avec $0 \leq r < d$.
Isolons le reste r et remplaçons d par $au + bv$:

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

Si $r \neq 0$ alors $r \in G$, or d est le plus petit élément de G donc $r \geq d$.

Impossible car $r < d$, d'où $r = 0$ et par conséquent d divise a .

- Par un raisonnement identique, on montre que d divise b .
- d divise a et b donc $d \leq D$
- Par double inégalité, on a donc $D = d$.

Théorème 3 : Conséquence de l'identité de Bézout.

Tout diviseur commun à a et b divise $D = \text{pgcd}(a, b)$.

Démonstration : Soit d un diviseur commun à a et b :

d divise toute combinaison linéaire de a et de b donc d'après l'identité de Bézout, d divise $au + bv = D$.

2.2 Théorème de Bézout

Théorème 4 : Deux entiers relatifs a et b sont premiers entre eux **si et seulement si**, il existe un couple d'entiers relatifs (u, v) tel que : $au + bv = 1$.

$$\text{pgcd}(a, b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}, au + bv = 1$$

Démonstration : Par double implication

- Si $\text{pgcd}(a, b) = 1$, d'après l'identité de Bézout, il existe un couple d'entiers relatifs (u, v) tel que $au + bv = 1$
- Réciproquement, il existe un couple d'entiers relatifs (u, v) tel que : $au + bv = 1$.
Si $D = \text{pgcd}(a, b)$ alors D divise a et b , donc divise toute combinaison linéaire de a et de b , et donc D divise $au + bv$ d'où D divise 1 et donc $D = 1$

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

Soit $a = 2n + 1$ et $b = 3n + 2$ on a alors :

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

Il existe donc $(u, v) = (-3, 2) \in \mathbb{Z}^2$ tel que $au + bv = 1$, d'après le th. de Bézout :

$$\text{pgcd}(2n + 1, 3n + 2) = 1.$$

2.2.1 Déterminer un couple d'entiers de Bézout

Montrer que 59 et 27 sont premiers entre eux.

En déduire un couple $(x, y) \in \mathbb{Z}^2$ tel que : $59x + 27y = 1$

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

$$\begin{aligned} 59 &= 27 \times 2 + 5 & L_1 & & 59 \text{ et } 27 \text{ sont premiers entre eux.} \\ 27 &= 5 \times 5 + 2 & L_2 & & \\ 5 &= 2 \times 2 + 1 & L_3 & & \end{aligned}$$

On remonte l'algorithme d'Euclide de L_3 jusqu'à l'égalité L_1 :

$$\begin{aligned} \text{de } L_3 : & 2 \times 2 = 5 - 1 & L_4 & & \\ L_2 \times 2 : & 27 \times 2 = 5 \times 10 + \underbrace{2 \times 2}_{L_4} & L_1 \times 11 : & 59 \times 11 = 27 \times 22 + \underbrace{5 \times 11}_{L_5} \\ & 27 \times 2 = 5 \times 10 + 5 - 1 & & 59 \times 11 = 27 \times 22 + 27 \times 2 + 1 \\ & 27 \times 2 = 5 \times 11 - 1 & & 59 \times 11 = 27 \times 24 + 1 \\ & 5 \times 11 = 27 \times 2 + 1 & L_5 & & \text{Donc } 59 \times 11 + 27 \times (-24) = 1 \end{aligned}$$

Le couple d'entiers de Bézout est donc $(11, -24)$

2.2.2 Algorithme de Bézout

La fonction Python  `bezout(a,b)`, avec $a > 0$ et a premier avec b , détermine un couple d'entiers relatifs (u, v) tel que :

$$au + bv = 1 \Leftrightarrow au = b(-v) + r$$

La fonction teste, en incrémentant u , le reste, r , de la division de au par b si $b > 0$ et $(-b)$ si $b < 0$. Tant que $r \neq 1$, on réitère la division.

Une fois u trouvé, on détermine $v = \frac{1 - au}{b}$.

`besout(59,27)` donne alors $u = 11$ et $v = -24$

```
def bezout(a,b):
    r=0
    u=0
    while r!=1:
        u+=1
        if b>0:
            r=a*u%b
        else:
            r=a*u%(-b)
    v=int((1-a*u)/b)
    return u,v
```

2.3 Corollaire de Bézout

Théorème 5 : L'équation $ax + by = c$ admet des solutions entières si et seulement si c est un multiple du $\text{pgcd}(a, b)$.

Démonstration : Par double implication

- $ax + by = c$ admet une solution (x_0, y_0) .
Comme $D = \text{pgcd}(a, b)$ divise a et b , D divise toute combinaison linéaire de a et de b , donc D divise $ax_0 + by_0 = c$.
- Réciproquement c est un multiple de $D = \text{pgcd}(a, b)$.
Donc il existe $k \in \mathbb{Z}$ tel que : $c = kD$, d'après l'identité de Bézout, il existe deux entiers relatifs u et v tels que : $au + bv = D$.
En multipliant par k , on obtient : $auk + bvk = kD \Leftrightarrow a(uk) + b(vk) = c$.
Il existe donc $x_0 = uk$ et $y_0 = vk$ tels que $ax_0 + by_0 = c$

Exemple : $4x + 9y = 2$ admet des solutions car $\text{pgcd}(4, 9) = 1$ et 2 multiple de 1.
 $9x - 15y = 2$ n'admet pas de solution car $\text{pgcd}(9, 15) = 3$ et 2 non multiple de 3.

3 Le théorème de Gauss

3.1 Le théorème

Théorème 6 : 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 .

Démonstration : Par le théorème de Bézout.

- a divise bc , alors il existe un entier k tel que : $bc = ka$
- a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que : $au + bv = 1$ (E)
- (E) $\times c$: $acu + bcv = c \stackrel{bc=ka}{\Leftrightarrow} acu + kav = c \Leftrightarrow a(cu + kv) = c \Rightarrow a$ divise c .

Exemple : Résoudre l'équation (E) dans \mathbb{Z}^2 : $5(x - 1) = 7y$

7 divise $5(x - 1)$, or $\text{pgcd}(5, 7) = 1$, d'après le théorème de Gauss 7 divise $(x - 1)$.

Donc : $x - 1 = 7k, k \in \mathbb{Z}$. En remplaçant dans (E) : $5 \times 7k = 7y \Leftrightarrow y = 5k$.

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

3.2 Corollaire du théorème de Gauss

Théorème 7 : Si b et c , premiers entre eux, divisent a alors bc divise a .

Démonstration : :

b et c divisent a , alors il existe $k, k' \in \mathbb{Z}$ tels que : $a = kb$ et $a = k'c$

On a alors $kb = k'c$, donc b divise $k'c$, or $\text{pgcd}(b, c) = 1$, d'après le théorème de Gauss, b divise k' donc il existe $k'' \in \mathbb{Z}$ tel que : $k' = k''b$.

On a alors : $a = k'c = k''bc$. bc divise a .

Exemple : Si 5 et 12 divisent a comme $\text{pgcd}(5, 12) = 1$, d'après le corollaire du théorème de Gauss $5 \times 12 = 60$ divise a .

3.3 Équations diophantiennes

Définition 3 : Équation diophantienne

Équation polynomiale, à une ou plusieurs inconnues, à coefficients entiers dont on cherche les solutions parmi les nombres entiers.

Une équation diophantienne (E) de la forme : $ax + by = c$ est une équation linéaire à deux inconnues du premier degré.

D'après le corollaire du théorème de Bézout, (E) admet des solutions si, et seulement si, c est un multiple de $\text{pgcd}(a, b)$.

Remarque : Diophante d'Alexandrie, mathématicien grec du III^e siècle.

Si c est multiple du $\text{pgcd}(a, b)$, on peut alors ramener $ax + by = c$, en divisant par $\text{pgcd}(a, b)$, à la forme $a'x + b'y = c'$ avec $\text{pgcd}(a', b') = 1$.

Résolution d'une équation (E) du type : $ax + by = c$ avec $\text{pgcd}(a, b) = 1$

- On cherche une solution particulière (x_0, y_0) à l'équation (E).
Si cette solution n'est pas immédiate, on cherche alors une solution (x_1, y_1) à l'équation $ax + by = 1$ en remontant l'algorithme d'Euclide.
Une solution de (E) est alors $(x_0, y_0) = (cx_1, cy_1)$.
- Soit (x, y) une solution de (E), on soustrait terme à terme dans l'équation la solution (x, y) à la solution particulière (x_0, y_0) .
- On applique le théorème de Gauss pour déterminer l'expression de (x, y) .
- On vérifie que les solutions trouvées vérifient bien l'équation (E).

Exemple : Déterminer l'ensemble des solutions de l'équation (E) $17x - 33y = 1$.

- On cherche une solution particulière de (E).
Solution évidente (2,1) : $17 \times 2 - 33 \times 1 = 34 - 33 = 1$.
- Soit (x, y) une solution (E).

On a :
$$\begin{cases} 17x - 33y = 1 \\ 17(2) - 33(1) = 1 \end{cases}$$
 par soustraction terme à terme, on obtient :

$$17(x - 2) - 33(y - 1) = 0 \Leftrightarrow 17(x - 2) = 33(y - 1) \quad (E')$$

33 divise $17(x - 2)$ or $\text{pgcd}(17, 33) = 1$, d'après le th. de Gauss, 33 divise $(x - 2)$.

On a donc : $x - 2 = 33k$, $k \in \mathbb{Z}$.

En remplaçant dans (E'), on trouve $y - 1 = 17k$.

- Les solutions de (E) sont de la forme :
$$\begin{cases} x = 2 + 33k \\ y = 1 + 17k \end{cases}, k \in \mathbb{Z}$$
- Vérification : $17(2 + 33k) - 33(1 + 17k) = 34 + 561k - 33 - 561k = 1$

⚠ La **vérification est essentielle** car on raisonne par implication.

Remarque : Si l'on cherche à résoudre (E_1) : $17x - 33y = 5$.

- Une solution particulière de (E_1) est la solution (2,1) de (E) multipliée par 5, soit $(2 \times 5, 1 \times 5) = (10, 5)$.
- Les solutions de (E_1) sont alors de la forme :
$$\begin{cases} x = 10 + 33k \\ y = 5 + 17k \end{cases}, k \in \mathbb{Z}$$