

Chapitre n° 4 : PGCD, théorèmes de Bezout et de Gauss, Application aux équations diophantiennes

1 Plus grand commun diviseur, Algorithme d'Euclide

Définition 1: PGCD

Soit a et b deux entiers relatifs non tous nuls.

L'ensemble des diviseurs positifs communs à a et b est non vide (il contient 1) et est fini (il est majoré par $\max(|a|, |b|)$). Il admet donc un plus grand élément, appelé **plus grand commun diviseur**.

On le note : $\text{PGCD}(a, b)$.

Exemple 1: $\text{PGCD}(24, 18) = 6$, $\text{PGCD}(60, -84) = 12$, $\text{PGCD}(-150, -240) = 30$.

Propriété 1

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

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

$$\text{PGCD}(a, 0) =$$

$$\text{Si } b \text{ divise } a, \text{ alors } \text{PGCD}(a, b) =$$

$$\text{homogénéité du PGCD : } \forall k \in \mathbb{N}^*, \text{ PGCD}(ka, kb) =$$

Preuve 1: L'homogénéité du PGCD se démontre à l'aide de l'algorithme d'Euclide, voir 3

Exemple 2: $\text{PGCD}(82, 0) =$

$$\text{PGCD}(-24, -18) =$$

$$\text{PGCD}(30, 5) =$$

$$\text{PGCD}(240, 180) =$$

Définition 2: Nombres premiers entre eux

On dit que a et b sont premiers entre eux si $\text{PGCD}(a, b) = 1$.

Exemple 3:

- $\text{PGCD}(15, 8) = 1$ donc 15 et 8 sont premiers entre eux.
- $\text{PGCD}(a, 1) = 1$. Le nombre 1 est premier avec tout entier.

Remarque 1: Il ne faut pas confondre des nombres premiers entre eux et des nombres premiers. 15 et 8 ne sont pas premiers mais ils sont premiers entre eux.

En revanche, deux nombres premiers distincts sont nécessairement premiers entre eux.

Théorème 2: Algorithme d'Euclide

Soit a et b deux entiers naturels non nuls tels que b ne divise pas a .

La suite des divisions euclidiennes suivantes finit toujours par un reste nul et le dernier reste non nul est toujours le PGCD de a et de b :

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

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

Preuve 2:

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

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

On déduit de ces deux inégalités que $D = d$, d'où $\text{PGCD}(a, b) = \text{PGCD}(b, r_0)$.

- $r_0 > r_1 > r_2 > \dots > r_n$ donc la suite (r_k) des restes commence par être strictement décroissante dans \mathbb{N} . Mais toute suite décroissante **et à valeurs dans** \mathbb{N} est constante à partir d'un certain rang. donc il existe un rang n tel que $r_{n+1} = 0$.
- 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.

Méthode 1 (Calculer le PGCD de deux nombres):

Calculer $\text{PGCD}(123\,456\,789, 9\,876)$.

CORRECTION

D'après l'algorithme d'Euclide, on a		$123\,456\,789 = 9\,876 \times 12\,500 + 6\,789$	
		$9\,876 = 6\,789 \times 1 + 3\,087$	
		$6\,789 = 3\,087 \times 2 + 615$	
		$3\,087 = 615 \times 5 + 12$	
		$615 = 12 \times 51 + 3$	dernier reste non nul
		$12 = 3 \times 4 + 0$	

Preuve 3 (de 1): L'algorithme d'Euclide appliqué au couple (ka, kb) donne des divisions euclidiennes successives qui sont exactement celles provenant du couple (a, b) où tous les membres sont multipliés par k . Le dernier reste non nul est donc kr_n c'est-à-dire $k \times \text{PGCD}(a, b)$

2 Théorème de Bézout

Propriété 3: Identité de Bézout

Soit a et b deux entiers non nuls et $D = \text{PGCD}(a, b)$.
Il existe alors un couple (u, v) d'entiers relatifs telle que : $au + bv = D$.

Preuve 4:

Soit G l'ensemble formé des entiers 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

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

Montrons que $d = \text{PGCD}(a, b) = D$.

et donc $D \leq d$ (car $d > 0$).

Montrons que d divise a .

Donc $r = 0$ par conséquent d divise a .

En faisant le même raisonnement, on montre que d divise aussi b .

d divise a et b , donc $d \leq D$.

Conclusion : $D \leq d$ et $d \leq D$ donc $D = d$.

Corollaire 1

Tout diviseur commun à a et b divise leur PGCD.

Preuve 5:

Tout diviseur commun à a et b divise toute

Or d'après l'identité de Bézout, $\text{PGCD}(a, b)$ est une

Donc tout diviseur commun à a et b divise leur PGCD.

Corollaire 2: Théorème de Bézout

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

$$au + bv = 1$$

Preuve 6:

① Si $\text{PGCD}(a, b) = 1$ alors l'identité de Bézout donne l'existence des entiers relatifs a et b tels que $au + bv = 1$

② Réciproquement, a et b sont deux entiers relatifs tels qu'il existe deux entiers relatifs tels que $au + bv = 1$.

Corollaire 3: caractérisation du PGCD

$\text{PGCD}(a; b) = D$, si, et seulement si, il existe $(a'; b') \in \mathbb{Z}^2$ tel que :
 $a = Da'$ et $b = Db'$ et $\text{PGCD}(a'; b') = 1$.

Preuve 7: Démontrons le sens direct.

Démontrons la réciproque.

il existe $(a'; b'; k') \in \mathbb{Z}^3$ tel que $a = ka'$ et $b = kb'$ et $\text{PGCD}(a'; b') = 1$.

Méthode 2 (Montrer que deux nombres sont premiers entre eux):

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

CORRECTION

Soit $n \in \mathbb{N}$.

Il suffit de prouver qu'il existe des entiers u et v tels que $u(2n + 1) + v(3n + 2) = 1$.

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

Il existe $u = -3$ et $v = 2$ tels que $u(2n + 1) + v(3n + 2) = 1$.

D'après le théorème de Bézout, les entiers $(2n + 1)$ et $(3n + 2)$ sont donc premiers entre eux.

Méthode 3 (Déterminer un couple $(u; v)$ tel que $au + bv = 1$):

Montrer que 59 et 27 sont premiers entre eux.

CORRECTION

Pour cela, il suffit de déterminer un couple d'entiers relatifs (x, y) tel que : $59x + 27y = 1$.

On applique l'algorithme d'Euclide étendu, qui consiste à exprimer chaque reste des divisions euclidiennes successives en fonction de a et b :

$$59 = 27 \times 2 + 5 \quad \text{donc} \quad 5 = 59 - 2 \times 27$$

$$\begin{aligned} 27 &= 5 \times 5 + 2 \quad \text{donc} \quad 2 = 27 - 5 \times 5 \\ & \quad 2 = 27 - 5(59 - 2 \times 27) \\ & \quad 2 = 11 \times 27 - 5 \times 59 \end{aligned}$$

$$\begin{aligned} 5 &= 2 \times 2 + 1 \quad \text{donc} \quad 1 = 5 - 2 \times 2 \\ & \quad 1 = 59 - 2 \times 27 - 2(11 \times 27 - 5 \times 59) \\ & \quad 1 = 11 \times 59 - 24 \times 27 \end{aligned}$$

Corollaire 4: Corollaire de Bézout

Soit $(a; b; c) \in \mathbb{Z}^3$.

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

Preuve 8:

- *Dans le sens direct* : Supposons que l'équation $ax + by = c$ admette une solution $(x_0 ; y_0)$ et notons $D = \text{PGCD}(a, b)$.

- *Réciproquement* : Soit c un multiple de $D = \text{PGCD}(a, b)$.

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

Exemple 4:

- L'équation $4x + 9y = 2$ admet des solutions car $\text{PGCD}(4, 9) = 1$ et 2 est multiple de 1.
En effet, si $x = -4$ et $y = 2$, on a : $4(-4) + 9(2) = -16 + 18 = 2$.
- L'équation $9x - 15y = 2$ n'admet pas de solution car $\text{PGCD}(9, 15) = 3$ et 2 n'est pas multiple de 3.

3 Le théorème de Gauss et son corollaire**Théorème 4: Théorème de Gauss**

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 .

Preuve 9:

Exemple 5: Pour trouver les solutions dans \mathbb{Z}^2 de l'équation $5(x - 1) = 7y$, on sait que :

5 divise $7y$. Or $\text{PGCD}(5, 7) = 1$, donc, d'après le théorème de Gauss, 5 divise y .

Il existe donc $k \in \mathbb{Z}$ tel que $y = 5k$.

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 : $\begin{cases} x = 7k + 1 \\ y = 5k \end{cases}, k \in \mathbb{Z}.$

Réciproquement, ces solutions vérifient effectivement l'équation.

Propriété 5: Corollaire de Gauss

Si b et c divisent a et si b et c sont premiers entre eux, alors bc divise a .

Preuve 10:

Exemple 6: Si 5 et 12 divisent a , alors 60 divise a , car 5 et 12 sont premiers entre eux.

4 Équation diophantienne $ax + by = c$

Définition 3

Une **équation diophantienne** est une équation à **coefficients entiers** dont on cherche les **solutions entières**.

Les équations diophantiennes du premier degré à deux inconnues sont du type :
 $ax + by = c$, où a , b et c sont trois entiers relatifs donnés.

Propriété 6: critère d'existence de solution

Une équation diophantienne de la forme $ax + by = c$, admet des solutions si, et seulement si, c est un multiple du PGCD(a, b).

Méthode 4 (Résoudre une équation du type $ax + by = c$):

EXERCICE 1

On cherche à résoudre l'équation diophantienne :

$$48x + 18y = -5 \quad (E)$$

Le PGCD de 48 et de 18 vaut 6.

Le PGCD de 48 et 18 ne divise pas -5 , donc l'équation (E) n'admet aucune solution.

EXERCICE 2

On cherche à résoudre l'équation diophantienne :

$$3x + 4y = 1 \quad (E)$$

D'après l'algorithme d'Euclide :
$$\left\{ \begin{array}{l} 3 = 4 \times 0 + 3 \\ 4 = 3 \times 1 + 1 \\ 3 = 1 \times 3 + 0 \end{array} \right. \Rightarrow \text{PGCD}(3; 4) = 1.$$

Les entiers 3 et 4 sont premiers entre eux, donc l'équation (E) admet une infinité de solutions.
On détermine une solution particulière de (E) :

$$3 \times (-1) + 4 \times 1 = 1 \quad (E_0)$$

Par soustraction :

$$\begin{array}{rrcr} 3 \times & x & + 4 \times & y & = 1 \\ - & 3 \times (-1) & + 4 \times & 1 & = 1 \\ \hline & 3 \times (x + 1) & + 4 \times (y - 1) & = 0 \end{array}$$

On en déduit que $3 \times \underbrace{(x + 1)}_{\text{entier}} = -4 \times (y - 1)$, et donc que $3 \mid -4 \times (y - 1)$.

Or 3 et 4 sont premiers entre eux, donc d'après le théorème de Gauss, on a $3 \mid y - 1$.

Il existe donc un entier k tel que $y - 1 = 3 \times k$, ce qui donne $y = 1 + 3k$.

En remplaçant, on obtient :

$$\begin{aligned} 3 \times (x + 1) &= -4 \times (y - 1) \implies 3 \times (x + 1) = -4 \times (\underbrace{1 + 3k - 1}_y) \\ &\implies 3 \times (x + 1) = -4 \times (3k) \\ &\implies x + 1 = -4k \\ &\implies x = -1 - 4k \end{aligned}$$

Ainsi, si x et y sont solutions de (E) , alors il existe un entier k tel que $x = -1 - 4k$ et $y = 1 + 3k$.

Réciproquement, soit k un entier quelconque :

$$\begin{aligned} 3 \times (-1 - 4k) + 4 \times (1 + 3k) &= 3 \times (-1) + \cancel{3 \times (-4)k} + 4 \times 1 + \cancel{4 \times 3k} \\ &= \underbrace{3 \times (-1) + 4 \times 1}_{= 1 \text{ d'après } (E_0)} \\ &= 1 \end{aligned}$$

On en déduit que $(-1 - 4k; 1 + 3k)$ est solution de (E) .

En conclusion, les solutions de (E) sont donc les couples $(-1 - 4k; 1 + 3k)$, avec k un entier relatif.

EXERCICE 3

On cherche à résoudre l'équation diophantienne :

$$48u + 18v = 12$$

D'après l'algorithme d'Euclide : $\left\{ \begin{array}{l} 48 = 18 \times 2 + 12 \\ 18 = 12 \times 1 + 6 \\ 12 = 6 \times 2 + 0 \end{array} \right. \Rightarrow \text{PGCD}(48; 18) = 6.$

Le PGCD de 48 et 18 divise 12, donc on peut simplifier l'équation diophantienne par 6.

$$48u + 18v = 12 \xLeftrightarrow{\div 6} 8u + 3v = 2 \quad (E)$$

Les entiers 8 et 3 sont premiers entre eux, donc l'équation (E) admet une infinité de solutions.

On détermine une solution particulière de (E) :

$$8 \times (-1) + 3 \times 3 = 1 \xRightarrow{\times 2} 8 \times (-2) + 3 \times 6 = 2 \quad (E_0)$$

Par soustraction :

$$\begin{array}{rcl} 8 \times u & + & 3 \times v = 2 \\ - & 8 \times (-2) & + 3 \times 6 = 2 \\ \hline 8 \times (u + 2) & + & 3 \times (v - 6) = 0 \end{array}$$

On en déduit que $8 \times \underbrace{(u + 2)}_{\text{entier}} = -3 \times (v - 6)$, et donc que $8 \mid -3 \times (v - 6)$.

Or 8 et 3 sont premiers entre eux, donc d'après le théorème de Gauss, on a $8 \mid v - 6$.

Il existe donc un entier l tel que $v - 6 = 8 \times l$, ce qui donne $\boxed{v = 6 + 8l}$.

En remplaçant, on obtient :

$$\begin{aligned} 8 \times (u + 2) &= -3 \times (v - 6) \implies 8 \times (u + 2) = -3 \times (\underbrace{6 + 8l}_v - 6) \\ &\implies 8 \times (u + 2) = -3 \times (8l) \\ &\implies u + 2 = -3l \\ &\implies \boxed{u = -2 - 3l} \end{aligned}$$

Ainsi, si u et v sont solutions de (E) , alors il existe un entier l tel que $u = -2 - 3l$ et $v = 6 + 8l$.

Réciproquement, soit l un entier quelconque :

$$\begin{aligned}8 \times (-2 - 3l) + 3 \times (6 + 8l) &= 8 \times (-2) + \cancel{8 \times (-3)l} + 3 \times 6 + \cancel{3 \times 8l} \\&= \underbrace{8 \times (-2) + 3 \times 6}_{= 2 \text{ d'après } (E_0)} \\&= 2\end{aligned}$$

On en déduit que $(-2 - 3l; 6 + 8l)$ est solution de (E) .

En conclusion, les solutions de (E) sont donc les couples $(-2 - 3l; 6 + 8l)$, avec l un entier relatif.