

Le théorème de Bézout

Théorème de Bézout : a et b sont des entiers non nuls. Il existe deux entiers u et v tels que $au + bv = \text{PGCD}(a; b)$.

Exemples : Le PGCD de 22 et de 4 est 2. On peut écrire que $-4 \times 5 + 1 \times 22 = 2$.

Le PGCD de 875 et de 215 est 5. On peut écrire que $-14 \times 875 + 57 \times 215 = 5$.

Démonstration : considérons les $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.

Les naturels de cette forme constituent une partie non vide de $\mathbb{N}$ qui admet donc un plus petit élément.

Soit n ce plus petit élément.

n est le plus petit entier non nul tel que $n = au + bv$ ($u \in \mathbb{Z}$ et $v \in \mathbb{Z}$).

Montrons que $n = \text{PGCD}(a; b)$.

$\text{PGCD}(a; b)$ divise a et b donc $\text{PGCD}(a; b)$ divise $au + bv$ donc $\text{PGCD}(a; b) \leq n$.

Montrons que n divise a et b . Pour cela on va montrer que le reste de la division de a par n est 0.

Divisons a par n : $a = nq + r$ ($0 \leq r < n$) donc $r = a - nq = a - (au + bv)q = a(1 - uq) - bvq$

r est donc sous la forme $au + bv$ donc $r = 0$ (car $r < n$ et car n est le plus petit entier non nul sous la forme $au + bv$).

donc n divise a .

On montre de même que n divise b donc n divise $\text{PGCD}(a; b)$ donc $n \leq \text{PGCD}(a; b)$.

Finalement $n = \text{PGCD}(a; b)$.

Conséquence immédiate : si a et b sont premiers entre eux, alors il existe deux entiers u et v tels que $au + bv = 1$.

Propriété : la réciproque est vraie : s'il existe deux entiers u et v tels que $au + bv = 1$, alors a et b sont premiers entre eux.

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

$\text{PGCD}(a; b)$ divise a et b donc $\text{PGCD}(a; b)$ divise $au + bv$ donc $\text{PGCD}(a; b)$ divise 1 donc $\text{PGCD}(a; b) = 1$ donc a et b sont premiers entre eux.

Il n'y a pas d'unicité : quand on a deux coefficients u et v , on peut en trouver d'autres :

$$au + bv = au + ab - ab + bv = a(u + b) + b(v - a).$$

$$\text{Exemple : } 1 = -7 \times 2 + 3 \times 5 = -7 \times 2 - 7 \times 3 + 7 \times 3 + 3 \times 5 = -7 \times 5 + 3 \times 12$$

$$= -7 \times 5 - 7 \times 3 + 7 \times 3 + 3 \times 12 = -7 \times 8 + 3 \times 19 \text{ etc.}$$

Comment trouver les coefficients a et b ?

Le PGCD de 4 et de 22 est 2. Trouver les deux entiers u et v tels que $4u + 22v = 2$.

Il suffit de diviser 22 par 4 : $22 = 4 \times 5 + 2$ donc $-4 \times 5 + 22 = 2$.

$$u = -5 \text{ et } v = 1.$$

Le PGCD de 9 et de 21 est 3. Trouver les deux entiers u et v tels que $9u + 21v = 3$.

Il suffit de diviser 21 par 9 : $21 = 2 \times 9 + 3$ donc $-2 \times 9 + 21 = 3$.

$$u = -2 \text{ et } v = 1.$$

Le PGCD de 875 et de 215 est 5. Trouver les deux entiers u et v tels que $875u + 215v = 5$.

Divisons 875 par 215 : $875 = 4 \times 215 + 15$ donc $875 - 4 \times 215 = 15$.

Ça ne va pas, on veut 5 et on a 15.

Appliquons l'algorithme d'Euclide :

$$875 = 4 \times 215 + 15 \qquad \text{donc } 15 = 875 - 4 \times 215$$

$$215 = 14 \times 15 + 5 \qquad \text{donc } 5 = 215 - 14 \times 15$$

$$15 = 3 \times 5 \qquad \text{donc PGCD}(875 ; 215) = 5$$

$$5 = 215 - 14 \times 15 = 215 - 14 \times (875 - 4 \times 215) = -14 \times 875 + 57 \times 215.$$

Voilà, on a trouvé : $-14 \times 875 + 57 \times 215 = 5$.

$$u = -14 \text{ et } v = 57.$$

Même chose avec 238 et 105.

Appliquons l'algorithme d'Euclide :

$$238 = 2 \times 105 + 28 \quad \text{donc } 28 = 238 - 2 \times 105$$

$$105 = 3 \times 28 + 21 \quad \text{donc } 21 = 105 - 3 \times 28$$

$$28 = 1 \times 21 + 7 \quad \text{donc } 7 = 28 - 21$$

$$21 = 3 \times 7 \quad \text{donc PGCD}(238; 105) = 7$$

$$7 = 28 - 21 = 28 - (105 - 3 \times 28) = 4 \times 28 - 105 = 4 \times (238 - 2 \times 105) - 105 = 4 \times 238 - 9 \times 105.$$

Voilà, on a trouvé : $4 \times 238 - 9 \times 105 = 7$.

$u = 4$ et $v = -9$.

On peut aussi essayer avec des nombres premiers entre eux, par exemple 50 et 39.

Appliquons l'algorithme d'Euclide :

$$50 = 1 \times 39 + 11 \quad \text{donc } 11 = 50 - 39$$

$$39 = 3 \times 11 + 6 \quad \text{donc } 6 = 39 - 3 \times 11$$

$$11 = 1 \times 6 + 5 \quad \text{donc } 5 = 11 - 6$$

$$6 = 1 \times 5 + 1 \quad \text{donc } 1 = 6 - 5$$

$$5 = 5 \times 1 \quad \text{donc PGCD}(50; 39) = 1$$

$$1 = 6 - 5 = 6 - (11 - 6) = 2 \times 6 - 11 = 2 \times (39 - 3 \times 11) - 11 = -7 \times 11 + 2 \times 39$$

$$= -7 \times (50 - 39) + 2 \times 39 = 9 \times 39 - 7 \times 50$$

Voilà, on a trouvé : $9 \times 39 - 7 \times 50 = 1$.

$u = -7$ et $v = 9$.