

## THÉORÈME DE BÉZOUT DANS $\mathbb{Z}$

Dans tout ce document, on suppose  $(a, b) \in (\mathbb{Z}^*)^2$ .

### 1. Définition

On dit que  $a$  et  $b$  sont premiers entre eux lorsque  $a \wedge b = 1$

### 2. Théorème de Bézout

$$a \wedge b = 1 \Leftrightarrow \exists(u, v) \in \mathbb{Z}^2, au + bv = 1$$

Remarque : le couple  $(u, v)$  n'est pas unique. Par exemple, avec  $a = 7$  et  $b = 11$ , on a :

$$(-3) \times 7 + 2 \times 11 = 8 \times 7 - 5 \times 11 = 1$$

Démonstration du théorème de Bézout :

Implication  $\Rightarrow$  :

Supposons  $a \wedge b = 1$ .

D'après la définition du pgcd, on a alors :  $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z} = \mathbb{Z}$

Donc :  $\forall w \in \mathbb{Z}, \exists(u, v) \in \mathbb{Z}^2, au + bv = w$

En particulier avec  $w = 1$  :  $\exists(u, v) \in \mathbb{Z}^2, au + bv = 1$

Implication  $\Leftarrow$  :

Supposons :  $\exists(u, v) \in \mathbb{Z}^2, au + bv = 1$

Notons  $d = a \wedge b$ . Comme  $d$  divise  $a$ , il divise  $au$ . Comme  $d$  divise  $b$ , il divise  $bv$ .

Finalement  $d$  divise  $au + bv$  donc  $d$  divise 1, d'où :  $d = 1$

On a même un résultat un peu plus fort : si  $a$  et  $b$  sont premiers entre eux, alors  $au + bv$  "parcourt"  $\mathbb{Z}$ .

### 3. Détermination pratique d'une égalité de Bézout : algorithme d'**Euclide-Bézout**

Exemple avec  $a = 142$  et  $b = 38$ .

Première étape : on applique l'algorithme d'Euclide

$$\begin{array}{cccc} r_0 & q_1 & r_1 & r_2 \\ 142 & = & 3 \times 38 & + 28 \end{array}$$

$$\begin{array}{cccc} r_1 & q_2 & r_2 & r_3 \\ 38 & = & 1 \times 28 & + 10 \end{array}$$

$$\begin{array}{cccc} r_2 & q_3 & r_3 & r_4 \\ 28 & = & 2 \times 10 & + 8 \end{array}$$

$$\begin{array}{cccc} r_3 & q_4 & r_4 & r_5 \\ 10 & = & 1 \times 8 & + 2 \end{array}$$

$$\begin{array}{cccc} r_4 & q_5 & r_5 & r_6 \\ 8 & = & 4 \times 2 & + 0 \end{array}$$

Donc  $142 \wedge 38 = r_5 = 2$

Deuxième étape : on part de la relation contenant  $r_5$  (l'avant dernière) et par injections successives, on exprime  $r_5$  en fonction de  $r_0 = a$  et  $r_1 = b$  :

$$2 = 10 - 1 \times 8$$

$$\begin{aligned}
2 &= 10 - 1 \times (28 - 2 \times 10) = -1 \times 28 + 3 \times 10 \\
2 &= -1 \times 28 + 3 \times (38 - 1 \times 28) = 3 \times 38 - 4 \times 28 \\
2 &= 3 \times 38 - 4 \times (142 - 3 \times 38) = -4 \times 142 + 15 \times 38
\end{aligned}$$

Finalement, un couple  $(u, v)$  possible est  $(-4, 15)$ .

### Cas général

D'après l'algorithme d'Euclide, on a :

$$r_{k-1} = q_k r_k + r_{k+1} \quad \text{où} \quad \begin{cases} 0 \leq r_{k+1} < r_k \\ r_{k-1} \wedge r_k = r_k \wedge r_{k+1} \end{cases}$$

Ceci, pour tout entier  $k$  tel que  $1 \leq k \leq n$  où  $n$  est tel que  $r_{n+1} = 0$  et  $r_n = a \wedge b$ .

Montrons, par récurrence descendante finie sur  $k \in \llbracket 1, n-1 \rrbracket$ , la propriété :

$$\wp(k) : \exists (u_k, v_k) \in \mathbb{Z}^2, r_n = u_k r_k + v_k r_{k-1}$$

- Déjà, on a :  $r_{n-2} = r_{n-1} q_{n-1} + r_n$   
D'où :  $r_n = r_{n-1} q_{n-1} + r_{n-2}$   
En posant  $u_{n-1} = q_{n-1}$  et  $v_{n-1} = 1$ , on obtient  $\wp(n-1)$ .
- Montrons que, pour tout  $k \in \llbracket 2, n-1 \rrbracket$ ,  $\wp(k) \Rightarrow \wp(k-1)$ .

Soit  $k \in \llbracket 2, n-1 \rrbracket$  et supposons  $\wp(k)$  :

$$\exists (u_k, v_k) \in \mathbb{Z}^2, r_n = u_k r_k + v_k r_{k-1}$$

Or :  $r_{k-2} = r_{k-1} q_{k-1} + r_k$

D'où :  $r_n = u_k (r_{k-2} - r_{k-1} q_{k-1}) + v_k r_{k-1}$   
 $r_n = (-u_k q_{k-1} + v_k) r_{k-1} + u_k r_{k-2}$

On pose alors :  $u_{k-1} = -u_k q_{k-1} + v_k$  et  $v_{k-1} = u_k$

Ainsi, on obtient  $\wp(k-1)$ .

Du principe de raisonnement par récurrence, on déduit :

$$\forall k \in \llbracket 1, n-1 \rrbracket, \wp(k)$$

En particulier, on a  $\wp(1)$  :  $a \wedge b = r_n = u_1 r_1 + v_1 r_0 = v_1 a + u_1 b$

Le couple  $(v_1, u_1)$  fournit une égalité de Bézout pour  $a = r_0$  et  $b = r_1$ .

De plus, cet algorithme prouve une nouvelle fois le théorème de Bézout par récurrence.

Les suites finies  $(u_k)$  et  $(v_k)$  se prêtent facilement à la programmation. Elles sont simultanément récurrentes et définies par :

$$\begin{cases} u_{n-1} = q_{n-1} \text{ (connu)} \\ u_k = v_{k-1} \quad 1 \leq k \leq n-2 \end{cases} \quad \text{et} \quad \begin{cases} v_{n-1} = 1 \\ v_k = u_k q_{k-1} + u_{k-1} \quad 1 \leq k \leq n-2 \end{cases}$$

#### 4. Conséquences : théorèmes de Gauss (et variantes)

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

1.  $(a \wedge b = 1 \text{ et } a \mid bc) \Rightarrow a \mid c$
2.  $(a \mid c, b \mid c \text{ et } a \wedge b = 1) \Rightarrow ab \mid c$
3.  $(a \wedge b = 1 \text{ et } a \wedge c = 1) \Rightarrow a \wedge bc = 1$
4.  $(p \text{ premier et } p \mid ab) \Rightarrow (p \mid a \text{ ou } p \mid b)$

#### Remarques :

- Le résultat 1 est très utile. Il sert dans la résolution des équations Diophantiennes et dans la preuve de l'unicité de la décomposition en facteurs premiers.
- Le résultat 2 est utile dans la résolution des systèmes de congruences.
- Le résultat 3 est utile pour montrer que la fonction  $\phi$  d'Euler est multiplicative.

#### Démonstration :

1. Comme  $a \wedge b = 1$ , le théorème de Bézout permet d'affirmer que :

$$\exists(u, v) \in \mathbb{Z}^2, au + bv = 1$$

En multipliant par  $c$  :  $acu + bcv = c$

Or,  $a \mid acu$  et par hypothèse  $a \mid bcv$ . Donc :  $a \mid c$

2. Comme  $a \mid c$  :  $\exists k \in \mathbb{Z}, c = ka$

Comme  $b \mid c$ , on en déduit :  $b \mid ka$

Or,  $a \wedge b = 1$ . Donc, d'après 1. :  $b \mid k$

$$ab \mid ak$$

$$ab \mid c$$

Preuve directe :

Comme  $a \mid c$  :  $\exists k \in \mathbb{Z}, c = ka$

Comme  $b \mid c$  :  $\exists h \in \mathbb{Z}, c = hb$

Comme  $a \wedge b = 1$ , le théorème de Bézout permet d'affirmer que :

$$\exists(u, v) \in \mathbb{Z}^2, au + bv = 1$$

En multipliant par  $c$  :  $acu + bcv = c$

$$a(hb)u + b(ka)v = c$$

$$ab(hu + kv) = c$$

$$ab \mid c$$

3. Comme  $a \wedge b = 1$  :  $\exists(u, v) \in \mathbb{Z}^2, au + bv = 1$

Comme  $a \wedge c = 1$  :  $\exists(u', v') \in \mathbb{Z}^2, au' + cv' = 1$

En multipliant membre à membre :  $(au + bv)(au' + cv') = 1$

On développe :  $a^2uu' + aucv' + bvau' + bvcv' = 1$

$$a(auu' + ucv' + bv u') + bc(vv') = 1$$

Et d'après le théorème de Bézout :  $a \wedge bc = 1$

4. Si  $p \mid a$ , il n'y a rien d'autre à démontrer.

Si  $p$  ne divise pas  $a$  alors  $p$  étant premier, on a :  $p \wedge a = 1$

Par ailleurs :  $p \mid ab$

Et d'après la propriété 1 :  $p \mid b$

On a donc bien :  $p \mid a$  ou  $p \mid b$

## 5. Liens PPCM-PGCD

### 5.1. Théorème

Soit  $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$

$$\text{Si } a \wedge b = 1, \text{ alors } a \vee b = |ab|$$

Démonstration :

Soit  $m$  un multiple de  $a$  et de  $b$  :

$$\exists (a', b') \in \mathbb{Z}^2, m = aa' = bb'$$

Comme  $(a \mid bb'$  et  $a \wedge b = 1)$ , d'après le théorème de Gauss, on déduit :

$$a \mid b'$$

Donc :  $\exists a'' \in \mathbb{Z}, b' = aa''$

D'où :  $m = baa''$

Donc  $m$  est un multiple de  $ab$ .

On a montré que tout multiple de  $a$  et de  $b$  est un multiple de  $ab$ .

Donc  $|ab|$  est le plus petit multiple commun (positif) de  $a$  et de  $b$  :

$$a \vee b = |ab|$$

### 5.2. Théorème

Soit  $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$

$$\text{ppcm}(a, b) \times \text{pgcd}(a, b) = |ab|$$

Démonstration :

Posons  $d = \text{pgcd}(a, b)$ .

D'après l'homogénéité du ppcm (1.1.3.) :

$$\text{ppcm}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \text{ppcm}(a, b)$$

Or, d'après 5.1. :

$$\text{ppcm}\left(\frac{a}{d}, \frac{b}{d}\right) = \left| \frac{ab}{d^2} \right|$$

D'où :

$$|ab| = d \times \text{ppcm}(a, b)$$

$$\text{ppcm}(a, b) \times \text{pgcd}(a, b) = |ab|$$