

Théorèmes de Bezout et Gauss

1. PGCD de deux entiers

On notera dans la suite

- $\text{Div}(a)$ l'ensemble des diviseurs d'un entier a non nul ;
- $\text{Div}(a; b)$ l'ensemble des diviseurs communs de deux entiers a et b non tous nuls.

Clairement $(a; b) = \text{Div}(a) \cap \text{Div}(b)$.

Théorème - Définition. Soit a et b deux entiers non tous nuls.

$\text{Div}(a; b)$ est un ensemble fini non vide. Il possède un plus grand élément, appelé plus grand diviseur commun de a et b et noté $\text{PGCD}(a; b)$.

Démonstration. Supposons a non nul. $\text{Div}(a; b)$ est fini car il ne contient que des entiers entre $-a$ et a ; il est non vide car il contient 1. Il possède ainsi un plus grand élément. ■

Exemple

On a

$$\text{Div}(15) = \{-15; -5; -3; -1; 1; 3; 5; 15\} \text{ et } \text{Div}(6) = \{-6; -3; -2; -1; 1; 2; 3; 6\},$$

Donc

$$\text{Div}(15; 6) = \{-3; -1; 1; 3\}.$$

Il en résulte que $\text{PGCD}(15; 6) = 3$.

Exemple

Déterminons le PGCD m de 126 et 136. Soit d un diviseur commun de 126 et 136. Alors d divise $136 - 126 = 10$, donc $m \in \{1; 2; 5; 10\}$. Ni 10, ni 5 ne divise 126, en revanche 2 divise 126 et 136. Par conséquent $d = 2$.

Exemple

Déterminons le PGCD m de 414 et 630. À l'aide de la calculatrice, on constate que

$$414 = 9 \times 46 = 2 \times 9 \times 23 \text{ et } 630 = 7 \times 9 \times 2 \times 5.$$

Ainsi $m = 2 \times 9 = 18$ car 23 et 7×5 n'ont pas de « facteurs communs » (voir leçon sur les nombres premiers).

Théorème 1. Soit a et b deux entiers naturels non tous nuls.

1. $\text{Div}(a; b) = \text{Div}(b; a)$ et $\text{PGCD}(a; b) = \text{PGCD}(b; a)$.
2. $\text{Div}(a; 0) = \text{Div}(a)$ et $\text{PGCD}(a; 0) = a$.
3. Si b divise a , alors $\text{Div}(b) \subset \text{Div}(a)$ et $\text{PGCD}(a; b) = b$.
4. Pour tout entier k , on a $\text{Div}(a; b) = \text{Div}(a - kb; b)$ et $\text{PGCD}(a; b) = \text{PGCD}(a - kb; b)$.
5. Si $0 < b \leq a$, $\text{Div}(a; b) = \text{Div}(r; b)$ et $\text{PGCD}(a; b) = \text{PGCD}(r; b)$ où r est le reste de la division euclidienne de a par b .

Démonstration.

1. C'est évident.
2. L'ensemble des diviseurs de 0 est $\mathbb{Z}^*$, donc $\text{Div}(a; 0) = \text{Div}(a) \cap \mathbb{Z}^* = \text{Div}(a)$, ce qui montre que $\text{PGCD}(a; 0) = a$.

3. Si b divise a , tout diviseur de b est un diviseur de a , donc $\text{Div}(b) \subset \text{Div}(a)$. On en déduit que $\text{Div}(a; b) = \text{Div}(a) \cap \text{Div}(b) = \text{Div}(b)$, donc que $\text{PGCD}(a; b) = b$.
4. Si d divise a et b , alors d divise $a - kb$, donc d divise $a - kb$ et b , ce qui montre l'inclusion $\text{Div}(a; b) \subset \text{Div}(a - kb; b)$.
Si d divise $a - kb$ et b , alors d divise kb , donc aussi $(a - kb) + kb = a$. Finalement d divise a et b , d'où l'inclusion réciproque et l'égalité $\text{Div}(a; b) = \text{Div}(a - kb; b)$.
5. Écrivons la division euclidienne de a par b : $a = bq + r$. D'après la propriété précédente, $\text{PGCD}(a; b) = \text{PGCD}(a - bq; b) = \text{PGCD}(r; q)$. ■

Attention, $\text{Div}(a; b)$ n'est pas à égal $\text{Div}(ka + k'b; b)$ pour k et k' entier. En effet si c'était le cas, en prenant $k = b$ et $k' = -a$, on aurait $\text{Div}(a; b) = \text{Div}(0; b) = \text{Div}(b)$, ce qui est faux en général.

Exemple

Déterminons en fonction n le PGCD de $6n - 1$ et $4n + 1$.

Il divise toute combinaison linéaire de ceux-ci. Choisissons bien les coefficients pour faire disparaître n :

$$3(4n + 1) - 2(6n - 1) = 5.$$

Ainsi le PGCD ne peut être que 1 ou 5. Cherchons à l'aide d'un tableau si $4n + 1$ et $6n - 1$ peuvent être simultanément des multiples de 5.

Si $n \equiv \dots [5]$	0	1	2	3	4
alors $4n + 1 \equiv \dots [5]$	1	0	4	4	2
et $6n - 1 \equiv \dots [5]$	4	0	1	2	3

En conclusion, $\text{PGCD}(4n + 1; 6n - 1)$ est égal à 5 si $n \equiv 1 [5]$ et à 1 sinon.

Exemple

Soit n un entier. Montrons que

$$\text{PGCD}(n^3 - n; n^2 + 1) = \text{PGCD}(n^2 + 1, 2) = \begin{cases} 1 & \text{si } n \text{ est pair} \\ 2 & \text{si } n \text{ est impair} \end{cases}$$

Remarquons déjà que $n^2 + 1$ n'est jamais nul, donc ce PGCD existe.

Puisque $n^3 - n - n(n^2 + 1) = -2n$, on en déduit que d'après la propriété 5.,

$$\text{PGCD}(n^3 - n; n^2 + 1) = \text{PGCD}(n^2 + 1, -2n) = \text{PGCD}(n^2 + 1, 2n).$$

La combinaison linéaire $2(n^2 + 1) - n \times 2n = 2$ ne permet pas de conclure que $\text{PGCD}(n^2 + 1, 2n) = \text{PGCD}(n^2 + 1, 2)$, il faut raisonner en deux temps.

Soit d un diviseur de $n^2 + 1$ et $2n$. Alors d divise $2(n^2 + 1) - n \times 2n = 2$ (et $n^2 + 1$), donc $\text{Div}(n^2 + 1, 2n) \subset \text{Div}(n^2 + 1, 2)$.

Réciproquement, si d divise $n^2 + 1$ et 2, alors d divise $2n$ (et $n^2 + 1$), d'où l'inclusion inverse $\text{Div}(n^2 + 1, 2) \subset \text{Div}(n^2 + 1, 2n)$ et finalement l'égalité de ces deux ensembles, ce qui prouve l'égalité des PGCD.

Si n est pair, $n^2 + 1$ est impair, donc $\text{PGCD}(n^2 + 1, 2) = 1$, tandis que si n est impair, $n^2 + 1$ est pair et $\text{PGCD}(n^2 + 1, 2) = 2$.

2. Algorithme d'Euclide

Théorème 2 (algorithme d'Euclide). Soit a et b deux entiers non tous nuls et d leur PGCD.

- Si $b = 0$, on a $d = a$ et l'algorithme s'arrête.
- Sinon, on effectue la division de a par b : $a = bq_1 + r_1$ avec $0 \leq r_1 < b$. D'après le théorème précédent, on a $\text{Div}(a; b) = \text{Div}(b; r_1)$.
- Si $r_1 = 0$, on conclut $d = b$.
- Sinon, on effectue la division de b par r_1 : $b = r_1q_2 + r_2$ avec $0 \leq r_2 < r_1$. On a donc $\text{Div}(a; b) = \text{Div}(b; r_1) = \text{Div}(r_1; r_2)$.
- Si $r_2 = 0$, on conclut : $d = r_1$.
- Sinon, ...
- En continuant ainsi, on est certain de tomber sur un reste nul, dans le cas contraire nous aurions construit une suite infinie strictement décroissante d'entiers naturels, ce qui est absurde. Soit r_n le dernier reste non nul. On a $r_{n-2} = r_{n-1}q_n + r_n$ et $\text{Div}(a; b) = \text{Div}(b; r_1) = \text{Div}(r_1; r_2) = \dots = \text{Div}(r_{n-1}; r_n) = \text{Div}(r_n; 0) = \text{Div}(r_n)$, ce qui montre que $d = r_n$.

$$\begin{array}{l}
 a = b \times q_1 + r_1 \\
 \swarrow \quad \searrow \\
 b = r_1 \times q_2 + r_2 \\
 \swarrow \quad \searrow \\
 r_1 = r_2 \times q_3 + r_3 \\
 \dots\dots\dots \\
 r_{n-2} = r_{n-1} \times q_n + r_n \\
 r_{n-1} = r_n \times q_{n+1} + 0
 \end{array}$$

On posera $r_{-1} = a$, $r_0 = b$ et $r_{n+1} = 0$, si bien que pour tout entier k vérifiant $0 \leq k \leq n$, on a l'égalité : $r_{k-1} = r_k q_{k+1} + r_{k+1}$ et de plus $0 = r_{n+1} < r_n < \dots < r_2 < r_1 < r_0$.

Voici deux traductions algorithmiques, avec et sans usage des couples. L'introduction de r et r' est superflue, elle améliore juste la lisibilité de l'algorithme.

```

(r, r') ← (a, b)
Tant que r' ≠ 0 faire
    (r, r') ← (r', reste de r par r')
Fin Tant que
Renvoyer r
    
```

```

r ← a
r' ← b
Tant que r' ≠ 0 faire
    w ← reste de r par r'
    r ← r'
    r' ← w
Fin Tant que
Renvoyer r
    
```

Exemple

Déterminons le PGCD de 374 et 297. On a
 $374 = 297 \times 1 + 77$
 $297 = 77 \times 3 + 66$
 $77 = 66 \times 1 + 11$
 $66 = 11 \times 6 + 0$
 Le dernier reste non nul est 11, donc $\text{PGCD}(374; 297) = 11$.

Théorème 3. Soit a et b deux entiers non tous nuls. Les diviseurs communs de a et b sont les diviseurs de leur PGCD.

Démonstration. Cela résulte de la démonstration de l'algorithme d'Euclide :

$$\text{Div}(a; b) = \text{Div}(r_n) = \text{Div}(\text{PGCD}(a; b)). \blacksquare$$

Pour $a = 0$ et $b = 0$, on peut dire que les diviseurs communs de a et b sont ceux de 0 (tous les entiers). Cela incite à poser $\text{PGCD}(0; 0) = 0$, ce que nous ferons dans la suite.

Théorème 4. Soit a, b et k trois entiers. Alors

$$\text{PGCD}(ka; kb) = k \times \text{PGCD}(a; b).$$

Démonstration. Il suffit de multiplier par k toutes les lignes de l'algorithme d'Euclide effectuées pour a et b . ■

❖ Algorithme d'Euclide étendu

On reprend les notations du théorème précédent.

Théorème 5 (algorithme d'Euclide étendu). Pour tout entier k vérifiant $-1 \leq k \leq n + 1$, il existe deux entiers u_k et v_k tels que $r_k = au_k + bv_k$.

Démonstration. Pour $k = -1$ et $k = 0$ la propriété est vraie car

$$r_{-1} = a = a \times 1 + b \times 0 \text{ et } r_0 = b = a \times 0 + b \times 1,$$

il suffit donc de poser $u_{-1} = 1, v_{-1} = 0, u_0 = 0$ et $v_0 = 1$.

Pour un entier k tel que $0 \leq k \leq n$, supposons les entiers $u_{-1}, u_0, \dots, u_k$ et $v_{-1}, v_0, \dots, v_k$ construits. Alors

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_{k+1} = au_{k-1} + bv_{k-1} - (au_k + bv_k)q_{k+1} \\ &= (u_{k-1} - q_{k+1}u_k)a + (v_{k-1} - q_{k+1}v_k)b \end{aligned}$$

d'où l'existence de u_{k+1} et v_{k+1} en prenant :

$$u_{k+1} = u_{k-1} - q_{k+1}u_k \text{ et } v_{k+1} = v_{k-1} - q_{k+1}v_k. \quad \blacksquare$$

Exemple

On a déterminé précédemment le PGCD de 374 et 297 par l'algorithme d'Euclide.

- On peut écrire $374 = 1 \times 374 + 0 \times 297$ et $297 = 0 \times 374 + 1 \times 297$.
- De $374 = 297 \times 1 + 77$, on déduit $77 = 1 \times 374 - 1 \times 297$.
- On a $66 = 297 - 3 \times 77 = 297 - 3(1 \times 374 - 1 \times 297) = -3 \times 374 + 4 \times 297$.
- On a $11 = 77 - 66 \times 1 = 77 = (1 \times 374 - 1 \times 297) - (-3 \times 374 + 4 \times 297) = 4 \times 374 - 5 \times 297$.
- Enfin on a $0 = 66 - 11 \times 6 = (-3 \times 374 + 4 \times 297) - (4 \times 374 - 5 \times 297) \times 6 = -27 \times 374 + 34 \times 297$.

Théorème 6 (propriétés des entiers u_k et v_k).

1. Pour tout entier k vérifiant $1 \leq k \leq n + 1$, on a $u_k > 0$ et $v_k < 0$ si k est impair et $u_k < 0$ et $v_k > 0$ si k est pair.

En particulier, u_k et v_k sont de signe opposé.

2. $(|u_k|)_{1 \leq k \leq n+1}$ et $(|v_k|)_{1 \leq k \leq n+1}$ sont des suites strictement croissantes.

3. $u_{n+1} = (-1)^n \frac{b}{d}$ et $v_{n+1} = (-1)^{n+1} \frac{a}{d}$.

4. $|u_n| < \frac{b}{2d}$ et $|v_n| < \frac{a}{2d}$.

Démonstration.

Remarquons tout d'abord pour tout entier k tel que $0 \leq k \leq n$, $q_{k+1} \geq 1$. En effet, si l'on avait $q_{k+1} = 0$ pour un entier k , on aurait $r_{k-1} = r_{k+1}$ et la suite des restes ne serait pas strictement décroissante.

Voici pour la suite un tableau réunissant les ingrédients nécessaires à la compréhension de la démonstration.

r_k	u_k	v_k
$r_{-1} = a$	$u_{-1} = 1$	$v_{-1} = 0$
$r_0 = b$	$u_0 = 0$	$v_0 = 1$
r_1	$u_1 = 1$	$v_1 = -q_1$
r_2	$u_2 = -q_2$	$v_2 = 1 + q_1 q_2$
...	...	...
r_{k+1}	$u_{k+1} = u_{k-1} - q_{k+1} u_k$	v_{k+1}
r_{k+2}	$u_{k+2} = u_k - q_{k+2} u_{k+1}$	v_{k+2}
...	...	...
$r_n = d$	u_n	v_n
$r_{n+1} = 0$	u_{n+1}	v_{n+1}

On démontre les propriétés pour u_k , la démonstration est analogue pour v_k .

1. Montrons par récurrence sur $k \geq 1$ la propriété : « $u_{2k-1} > 0$ et $u_{2k} < 0$ ».

Pour $k = 1$, on a $u_1 = 1 > 0$ et $u_2 = -q_2 < 0$.

Supposons la propriété vraie pour k et montrons-la pour $k + 1$:

$$u_{2(k+1)-1} = u_{2k+1} = u_{2k-1} - q_{2k+1} u_{2k} > u_{2k+1} > 0$$

et

$$u_{2(k+1)} = u_{2k+2} = u_{2k} - q_{2k+2} u_{2k+1} < u_{2k} < 0.$$

2. Si k est un entier pair, avec $k \geq 2$,

$$|u_{k+1}| - |u_k| = u_{k+1} + u_k = u_{k-1} - q_{k+1} u_k + u_k = u_{k-1} - (q_{k+1} - 1) u_k \geq u_{k-1} > 0,$$

L'avant-dernière inégalité résultant de $q_{k+1} \geq 1$, et de $u_k < 0$.

Si k est un entier impair avec $k \geq 2$,

$$\begin{aligned} |u_{k+1}| - |u_k| &= -u_{k+1} - u_k = -u_{k-1} + q_{k+1} u_k - u_k = -u_{k-1} + (q_{k+1} - 1) u_k \\ &\geq -u_{k-1} > 0. \end{aligned}$$

Cela montre que la suite $(|u_k|)_{1 \leq k \leq n+1}$ est strictement croissante.

3. Montrons par récurrence sur k , avec $-1 \leq k \leq n$, que

$$r_k u_{k+1} - r_{k+1} u_k = (-1)^k b.$$

Pour $k = -1$, on a bien $r_{-1} u_0 - r_0 u_{-1} = a \times 0 - b \times (-1) = -b$.

Supposons la propriété vraie pour un entier k vérifiant $-1 \leq k \leq n - 1$. Alors

$$\begin{aligned} r_{k+1} u_{k+2} - r_{k+2} u_{k+1} &= r_{k+1} (u_k - q_{k+2} u_{k+1}) - (r_k - r_{k+1} q_{k+2}) u_{k+1} \\ &= r_{k+1} u_k - r_k u_{k+1} = -(-1)^k b = (-1)^{k+1} b. \end{aligned}$$

En particulier, pour $k = n$, on obtient $r_n u_{n+1} - r_{n+1} u_n = (-1)^n b$ et comme $r_{n+1} = 0$ et $r_n = d$, il vient $du_{n+1} = (-1)^n b$, soit $u_{n+1} = (-1)^n \frac{b}{d}$.

L'égalité $au_{n+1} + bv_{n+1} = d$ conduit alors à $v_{n+1} = (-1)^{n+1} \frac{a}{d}$.

4. Comme $r_{n-1} = r_n q_{n+1} + r_{n+1} = r_n q_{n+1}$ et que $r_n < r_{n-1}$, on a $q_{n+1} \geq 2$.

$$\text{De } u_{n+1} = u_{n-1} - q_{n+1} u_n, \text{ on déduit } |u_n| = \frac{|u_{n+1} - u_{n-1}|}{|q_{n+1}|} \leq \frac{|u_{n+1} - u_{n-1}|}{2}.$$

Comme u_{n+1} et u_{n-1} ont le même signe, sont non nuls et que $|u_{n-1}| < |u_{n+1}|$, deux cas se présentent :

- S'ils sont positifs, $u_{n-1} < u_{n+1}$, donc $|u_{n+1} - u_{n-1}| = u_{n+1} - u_{n-1} < u_{n+1} = |u_{n+1}|$.
- S'ils sont négatifs, $-u_{n-1} < -u_{n+1}$, d'où $u_{n-1} > u_{n+1}$, donc

$$|u_{n+1} - u_{n-1}| = -u_{n+1} + u_{n-1} < -u_{n+1} = |u_{n+1}|.$$

Dans les deux cas, on a prouvé que $|u_{n+1} - u_{n-1}| < |u_{n+1}|$. D'après le 3., il vient

$$|u_n| \leq \frac{|u_{n+1} - u_{n-1}|}{2} < \frac{|u_{n+1}|}{2} = \frac{1}{2} \left| (-1)^n \frac{b}{d} \right| = \frac{b}{2d}. \quad \blacksquare$$

3. Théorème de Bezout

Théorème 7 (identité de Bezout). Soit deux entiers a et b et $d = \text{PGCD}(a; b)$.

1. Il existe deux entiers u et v tels que $au + bv = d$.
2. L'ensemble des combinaisons linéaires de a et b (c'est-à-dire les entiers de la forme $au + bv$, u et v entiers) est l'ensemble des multiples de d .

Exemple

Le PGCD de 12 et 28 est 4. On a par exemple $-2 \times 12 + 28 = 4$. La relation n'est pas unique ; on a aussi $5 \times 12 - 2 \times 28 = 4$ ou encore $-9 \times 12 + 28 \times 4 = 4$.

Le théorème précédent n'admet pas de réciproque. Par exemple on a $2 \times 1 + 3 \times 1 = 5$ mais 5 n'est pas le PGCD de 2 et 3.

Démonstration.

Si $a = b = 0$, le théorème est trivial avec le fait que $\text{PGCD}(0; 0) = 0$. Supposons à présent a et b non tous nuls.

1. L'algorithme d'Euclide étendu pour $k = n$ donne le résultat :

$$d = r_n = au_n + bv_n.$$

Voici une seconde démonstration, « abstraite ».

Soit l'ensemble $E = \{ax + by ; (x; y) \in \mathbb{Z}^2 \text{ et } ax + by \geq 1\}$.

E un sous-ensemble de $\mathbb{N}$ et il est non vide car $|a| \in E$ ou $|b| \in E$. Il admet donc un plus petit élément $d \geq 1$ pour un certain choix de u et v .

Si d ne divisait pas a , la division euclidienne de a par d donnerait

$$a = dq + r \text{ avec } 1 \leq r < d$$

d'où

$$r = a - dq = a - q(au + bv) = a(1 - q) + b(-qv),$$

ce qui impliquerait $r \in E$. Cela contredirait le caractère minimal de d . Ainsi d divise a et avec le même argument on montre qu'il divise b . Il en résulte que d divise $\text{PGCD}(a; b)$, en particulier $d \leq \text{PGCD}(a; b)$.

Par ailleurs $\text{PGCD}(a; b)$ divise a et b , donc il divise $au + bv = d$, d'où $\text{PGCD}(a; b) \leq d$.

Finalement $d \leq \text{PGCD}(a; b) \leq d$, ce qui montre que $d = \text{PGCD}(a; b)$.

2. Soit $n = au + bv$ avec u et v entiers. Comme d divise a et b , d divise $au + bv = n$, donc n est un multiple de d .

Soit n un multiple de d . On peut écrire $n = kd$, avec k entier. Comme il existe u et v tels que $au + bv = d$, on en déduit $n = kd = (ku)a + (kv)b$, ce qui montre que n est une combinaison linéaire de u et v . ■

Pour déterminer une identité de Bezout, on utilise les égalités obtenues dans l'algorithme d'Euclide.

Exemple

On a déterminé précédemment le PGCD de 374 et 297 par l'algorithme d'Euclide. Alors

$$\begin{aligned} 11 &= 77 - 66 \times 1 \text{ car } 77 = 66 \times 1 + 11 \\ &= 77 - (297 - 77 \times 3) \times 1 \text{ car } 297 = 77 \times 3 + 66 \\ &= 77 \times 4 - 297 \times 1 \\ &= (374 - 297) \times 4 - 297 \times 1 \text{ car } 374 = 297 \times 1 + 77 \\ &= 374 \times 4 - 297 \times 5 \end{aligned}$$

Voici l'algorithme d'Euclide étendu qui prend deux entiers a et b et renvoie, dans cet ordre, le PGCD de a et b et les coefficients u et v tels que $au + bv = \text{PGCD}(a; b)$.

Les variables u, v, u', v', r et r' jouent le rôle de $u_k, v_k, u_{k+1}, v_{k+1}, r_k$ et r_{k+1} . On a vu que

$$u_0 = 1, v_0 = 0, u_1 = 0, v_1 = 1, u_{k+1} = u_{k-1} - q_{k+1}u_k \text{ et } v_{k+1} = v_{k-1} - q_{k+1}v_k$$

où q_{k+1} est le quotient de la division euclidienne de r_{k-1} par r_k .

On donne deux versions, l'une utilisant les n -uplets et l'autre non.

```
(r, r') ← (a, b)
(u, v, u', v') ← (1, 0, 0, 1)
Tant que r' ≠ 0 faire
  q ← quotient de r par r'
  (u, v, u', v') = (u', v', u - qu', v - qv')
  (r, r') ← (r', reste de r par r')
Fin Tant que
Renvoyer r, u, v
```

```
r ← a ; r' ← b
u ← 1 ; v ← 0 ; u' ← 0 ; v' ← 1
Tant que r' ≠ 0 faire
  q ← quotient de r par r'
  c ← u ; d ← v ; u ← u' ; v ← v'
  u' ← c - qu' ; v' ← d - qv'
  w ← reste de r par r'
  r ← r' ; r' ← w
Fin Tant que
Renvoyer r, u, v
```

❖ Entiers premiers entre eux

Définition. On dit que deux entiers a et b sont premiers entre eux (ou étrangers) si leur PGCD est égal à 1.

Exemple

Pour tout entier n , $2n - 1$ et $3n - 2$ sont premiers entre eux car un diviseur commun doit diviser la combinaison linéaire

$$3(2n - 1) - 2(3n - 2) = 1.$$

Ce ne peut donc être que -1 ou 1 .

Théorème 8. Soit a et b deux entiers naturels non tous nuls et d un entier naturel. Alors $d = \text{PGCD}(a; b)$ si et seulement si $a = da'$ et $b = db'$ avec a' et b' premiers entre eux.

Démonstration. Si $d = \text{PGCD}(a; b)$, il existe a' et b' entiers tels que $a = da'$ et $b = db'$. Alors $d = \text{PGCD}(a; b) = \text{PGCD}(da'; db') = d \times \text{PGCD}(a'; b')$, d'où en simplifiant par d , $\text{PGCD}(a'; b') = 1$.

Réciproquement, si $a = da'$ et $b = db'$ avec a' et b' premiers entre eux, alors

$$d = d \times \text{PGCD}(a'; b') = \text{PGCD}(da'; db') = \text{PGCD}(a; b). \blacksquare$$

Théorème 9 (de Bezout). Deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $au + bv = 1$.

Démonstration. Si $\text{PGCD}(a; b) = 1$, alors l'égalité $au + bv = 1$ est une conséquence du théorème précédent.

Réciproquement, s'il existe deux entiers u et v tels que $au + bv = 1$, le PGCD de a et b divise a et b , donc également $au + bv = 1$. Ainsi $\text{PGCD}(a; b) = 1$. $\blacksquare$

En complément, citons ce résultat d'unicité.

Théorème 10. Soit a et b deux entiers premiers entre eux et supérieurs ou égaux à 2. Il existe un unique couple $(u; v)$ tel que $au - bv = 1$ avec $0 < u < b$ et $0 < v < a$.

Démonstration. Existence d'une solution. D'après le théorème de Bezout, il existe un couple $(u_0; v_0)$ vérifiant $au_0 - bv_0 = 1$.

Effectuons la division euclidienne de u_0 par b : il existe u et q tel que $u_0 = bq + u$ avec $0 \leq u < b$. Supposons que $u = 0$. On aurait alors $au_0 - bv_0 = abq - bv_0 = 1$, d'où l'on déduit $b(aq - v_0) = 1$, ce qui contredit $b \geq 2$. Ainsi $0 < u < b$. Alors

$$au_0 - bv_0 = 1 \Leftrightarrow a(bq + u) - bv_0 = 1 \Leftrightarrow au - (v_0 - aq)b = 1,$$

ce qui montre, en posant $v = v_0 - aq$ que le couple (u, v) vérifie $au - bv = 1$.

Il reste à montrer que v vérifie $0 < v < a$.

- Supposons $v \geq a$. On aurait $-bv \leq -ba$, puis $au - bv \leq au - ba$, soit $1 \leq au - ba$. Or $u < b$, donc $au < ab$ et $au - ba < 0$, ce qui entraînerait $1 < 0$. Ainsi $v < a$.
- Supposons $v \leq 0$. Alors $-bv \geq 0$, donc $au - bv \geq au$, soit $1 \geq au$. Or $a \geq 2$ et $u \geq 1$, donc $au \geq 2$, d'où $1 \geq 2$, ce qui est absurde. Ainsi $v > 0$.

Unicité. Supposons qu'il existe deux couples (u, v) et (u', v') vérifiant

$$0 < u < b, 0 < v < a, au - bv = 1 \text{ et } 0 < u' < b, 0 < v' < a, au' - bv' = 1.$$

Alors $au - bv = 1 = au' - bv'$, d'où $a(u - u') = b(v - v')$. Ainsi b divise $a(u - u')$ et comme a et b sont premiers entre eux, b divise $u - u'$, autrement dit $u - u'$ est un multiple de b . Mais les inégalités $0 < u < b$ et $0 < u' < b$ implique $-b < u - u' < b$, et le seul multiple de b à vérifier cette inégalité est 0, ce qui donne $u - u' = 0$ et $u = u'$.

Il vient alors $au - bv = 1 = au - bv'$, d'où $-bv = -bv'$ et $v = v'$.

Cela montre que $(u, v) = (u', v')$, ce qui est l'unicité annoncée. ■

4. Théorème de Gauss

Théorème 11 (de Gauss). Soit a, b, c des entiers.

Si a divise bc et si a est premier avec b , alors a divise c .

Démonstration. Si a est premier avec b , il existe d'après le théorème de Bezout deux entiers u et v tels que $au + bv = 1$.

En multipliant par c on a donc $acu + bcv = c$. Or a divise acu et bcv , par conséquent il divise $acu + bcv = c$. ■

Corollaire 1. Si un entier n est divisible par deux entiers a et b premier entre eux alors il est divisible par ab .

Démonstration. Comme n est divisible par a et b , il existe deux entiers k et k' tels que $n = ka = k'b$, ce qui montre que a divise $k'b$. Mais comme a et b sont premiers entre eux, le théorème de Gauss implique que a divise k' , d'où l'existence d'un entier q tel que $k' = aq$.

On en déduit $n = qab$, ce qui montre que ab divise n . ■

Exemple

L'entier $n(n^2 - 1)$ est le produit des trois entiers consécutifs $n - 1$, n et $n + 1$. Parmi ces entiers, il en existe au moins divisible par 2 et au moins un divisible par 3. Comme 2 et 3 sont premiers entre eux, $n(n^2 - 1)$ est divisible par leur produit, 6.

Corollaire 2. Un entier p est premier avec les entiers a et b si et seulement si p est premier avec ab .

Démonstration. Soit p un entier premier avec a et b . Il existe des entiers u, v, u', v' tels que
$$pu + av = 1 \text{ et } pu' + bv' = 1.$$

En faisant le produit de ces égalités, il vient

$$p(puu' + buv' + au'v) + ab \times vv' = 1.$$

Cela montre que p et ab sont premiers entre eux.

Réciproquement, si p est premier avec ab , il existe deux entiers u et v tels que

$$pu + abv = 1.$$

Cette égalité peut se lire $pu + a \times bv = 1$, ce qui montre que p et a sont premiers entre eux d'après le théorème de Bezout. Il en est de même de p et b . ■

Exemple

9 est premier avec 11 et avec 16, donc 9 est premier avec $11 \times 16 = 176$.

Corollaire 3. Soit a et b deux entiers premiers entre eux.

Alors pour tous entiers k et ℓ , les entiers a^k et b^ℓ sont premiers entre eux.

Démonstration. Montrons d'abord par récurrence que pour tout $\ell \in \mathbb{N}$, a et b^ℓ sont premiers entre eux.

- Pour $\ell = 1$, c'est l'hypothèse du corollaire.
- Supposons la propriété vraie pour un entier ℓ . D'après le corollaire 2 appliqué au triplet $(p, a, b) = (a, b, b^\ell)$, il vient que a et $b^{\ell+1}$ sont premiers entre eux.

Soit ℓ un entier fixé. D'après ce qu'on vient de montrer, a et b^ℓ sont premiers entre eux. Par conséquent, la première partie de la démonstration s'applique au couple $(b^\ell; a)$ à la place de $(a; b)$ et montre que pour tout $k \in \mathbb{N}$, b^ℓ et a^k sont premiers entre eux. ■

5. Équation diophantienne $ax + by = c$

Exemple

Réolvons les équations suivantes, d'inconnues x et y entières.

1. $9x + 15y = 7$

2. $7x - 4y = 1$

3. $7x - 4y = 3$

1. Comme 3 divise $9x + 15y$ mais pas 7, cette équation n'a pas de solution.

2. Réolvons l'équation $7x - 4y = 1$. D'après le théorème de Bezout cette équation admet des solutions car $\text{PGCD}(7; 4) = 1$.

Une identité de Bezout n'est pas bien difficile à trouver : $7 \times 3 - 4 \times 5 = 1$.

L'équation peut donc s'écrire $7x - 4y = 7 \times 3 - 4 \times 5$, ou encore

$$7(x - 3) = 4(y - 5).$$

Soit $(x; y)$ un couple de solutions. Comme 7 et 4 sont premiers entre eux, le théorème de Gauss montre que 7 divise $y - 5$, donc qu'il existe un entier k tel que $y - 5 = 7k$, ou encore $y = 5 + 7k$. On en déduit $7(x - 3) = 4 \times 7k$, soit $x - 3 = 4k$ et finalement $x = 3 + 4k$.

Réciproquement les couples $(3 + 4k; 5 + 7k)$ sont solutions car

$$7(3 + 4k) - 4(5 + 7k) = 21 + 28k - 20 - 28k = 1.$$

Finalement les solutions de cette équation sont les couples $(3 + 4k; 5 + 7k)$ avec k entier. Par exemple $(3; 5)$, $(7; 12)$, $(-1; -2)$.

3. Puisque 3 est un multiple de $\text{PGCD}(7; 4) = 1$, cette équation a des solutions. Une solution particulière peut se construire à partir d'une solution particulière de l'équation 2 : comme $7 \times 3 - 4 \times 5 = 1$, en multipliant par 3 on a $7 \times 9 - 4 \times 15 = 3$, ce qui montre que $(9; 15)$ est une solution particulière. Une solution plus simple est $(1; 1)$. L'équation devient

$$7x - 4y = 7 - 4 \Leftrightarrow 7(x - 1) = 4(y - 1).$$

Le raisonnement est ensuite identique. On conclut que les solutions sont les couples de la forme $(1 + 4k; 1 + 7k)$, k entier.

De façon plus générale, on a le résultat suivant, que l'on n'appliquera pas le jour du bac !

Théorème 12. Soit a , b , c trois entiers relatifs et soit (E) l'équation $ax + by = c$, d'inconnues x et y , deux entiers relatifs. Posons $d = \text{PGCD}(a; b)$.

- Si c n'est pas un multiple de d , l'équation n'a pas de solution ;
- Si c est un multiple de d , l'équation admet pour solutions les couples d'entiers

$$\left(x_0 + \frac{b}{d}k; y_0 - \frac{a}{d}k\right) \text{ avec } k \in \mathbb{Z}$$

où $(x_0; y_0)$ désigne une solution particulière de (E) .

Démonstration. D'après le théorème 7 (identité de Bezout), les combinaisons linéaires de a et b sont les multiples de d , par conséquent l'équation n'a pas de solution si c n'est pas un multiple de d .

Supposons à présent que c soit un multiple de d . D'après ce même théorème 7, l'équation $ax + by = c$ admet une solution $(x_0; y_0)$ qui vérifie donc $ax_0 + by_0 = c$.

Soit $(x; y)$ une solution de l'équation. On a donc $ax + by = c = ax_0 + by_0$, d'où

$$a(x - x_0) = b(y_0 - y)$$

soit, en divisant a et b par leur PGCD d :

$$a'(x - x_0) = b'(y_0 - y), \text{ avec } a' = \frac{a}{d} \text{ et } b' = \frac{b}{d}.$$

Comme a' et b' sont premiers entre eux, le théorème de Gauss montre que b' divise $x - x_0$, d'où l'existence de $k \in \mathbb{Z}$ tel que $x - x_0 = kb'$, ce qui donne

$$x = x_0 + kb' = x_0 + k \frac{b}{d}.$$

Enfin, de l'égalité $a'(x - x_0) = b'(y_0 - y)$, on déduit $a'kb' = b'(y_0 - y)$, puis en simplifiant, $a'k = y_0 - y$ et finalement $y = y_0 - \frac{a}{d}k$.

Réciproquement, si $(x_0; y_0)$ est un couple de solution, alors $\left(x_0 + \frac{b}{d}k; y_0 - \frac{a}{d}k\right)$ est un couple de solution car

$$a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}k\right) = ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k = ax_0 + by_0 = c. \blacksquare$$

En pratique, comme a' et b' sont premiers entre eux, l'algorithme d'Euclide permet de trouver u et v tel que $a'u + b'v = 1$, d'où $a'(uc) + b'(vc) = c$, ce qui donne comme couple particulier $(x_0; y_0)$ de solution $(uc; vc)$.

En complément, voici un théorème la « taille » des couples de solutions.

Définition. Un couple de solutions $(u_0; v_0)$ de l'équation $ax + by = c$ sera dit minimal si pour tout couple de solutions $(u; v)$ on a $|u_0| + |v_0| \leq |u| + |v|$.

Théorème 13. Soit a et b deux entiers naturels.

Le couple $(u_n; v_n)$ fourni par l'algorithme d'Euclide étendu est l'unique solution minimale de l'équation $ax + by = d$, où $d = \text{PGCD}(a; b)$.

Démonstration. D'après le théorème précédent, les couples de solutions de l'équation $ax + by = d$ sont ceux de la forme $(u_n + \frac{b}{d}k; v_n - \frac{a}{d}k)$, où (u_n, v_n) est le couple fourni par l'algorithme d'Euclide étendu.

On utilise l'inégalité $|a + b| \geq ||a| - |b||$ dont la démonstration est la suivante :

$$|a + b| \geq ||a| - |b|| \Leftrightarrow (a + b)^2 \geq (|a| - |b|)^2 \Leftrightarrow a^2 + 2ab + b^2 \geq |a|^2 - 2|a||b| + |b|^2 \\ \Leftrightarrow 2ab \geq -2|ab| \Leftrightarrow ab \geq -|ab|$$

et cette dernière inégalité est vraie (distinguer $ab \leq 0$ et $ab \geq 0$).

D'après le théorème 6, $|u_n| < \frac{b}{2a}$. Si k est un entier non nul, on a $1 \leq |k|$ d'où

$$2|u_n| < \frac{b}{a} \leq \frac{b}{a}|k| = \left| \frac{b}{a}k \right|,$$

et aussi $|u_n| < \left| \frac{b}{a}k \right|$ car $|u_n| > 0$. Cela implique en utilisant ces deux inégalités

$$\left| u_n + \frac{b}{a}k \right| \geq \left| |u_n| - \left| \frac{b}{a}k \right| \right| = \left| \frac{b}{a}k \right| - |u_n| > 2|u_n| - |u_n| = |u_n|.$$

On montrerait de même que $\left| u_n - \frac{a}{b}k \right| > |v_n|$

Cela montre que la solution minimale est obtenu pour $k = 0$ ■