Terminale Maths expertes

PGCD. Théorèmes de Bézout et de Gauss

Cours

Dans tout le chapitre, les lettres a, b, c, d, k, n, q, r, u, v… désignent des **entiers relatifs**.

Remarques : rappels du chapitre 2 utilisés dans ce chapitre

• **Combinaisons linéaires :** si d divise a et d divise b, alors d divise $au + bv$ pour tous entiers u et v (en particulier $a + b$ et $a - b$).
• **Taille des diviseurs :** si d divise a et $a \neq 0$, alors $|d| \leqslant |a|$.
• **Division euclidienne :** pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple $(q\,;r)$ d'entiers tel que $a = bq + r$ et $0 \leqslant r < b$.
• **Bon ordre :** toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

I. PGCD de deux entiers

1. Diviseurs communs et PGCD

Exemple : diviseurs communs à 30 et à 48

• Diviseurs positifs de 30 : 1, 2, 3, 5, 6, 10, 15, 30.
• Diviseurs positifs de 48 : 1, 2, 3, 4, 6, 8, 12, 16, 24, 48.
• Diviseurs positifs communs à 30 et à 48 : 1, 2, 3, 6. Dans $\mathbb{Z}$, il faut leur ajouter leurs opposés -1, -2, -3, -6.
Le plus grand diviseur commun à 30 et à 48 est donc 6 : c'est leur PGCD, et on écrit $\text{PGCD}(30\,;48) = 6$.

Définition 1 : PGCD

Soit a et b deux entiers relatifs **non tous les deux nuls**.
L'ensemble des diviseurs communs à a et à b est fini et contient 1 : il admet donc un plus grand élément. Ce plus grand élément est appelé **plus grand commun diviseur** de a et b ; on le note

$$\text{PGCD}(a\,;b) \qquad \text{(ou parfois } a \wedge b\text{)}.$$

Comme 1 est un diviseur commun, on a toujours $\text{PGCD}(a\,;b) \geqslant 1$.

Remarques :

• L'ensemble des diviseurs communs est fini : si par exemple $a \neq 0$, tout diviseur d de a vérifie $-|a| \leqslant d \leqslant |a|$.
• $\text{PGCD}(0\,;0)$ n'est pas défini : tout entier divise 0, il n'y a donc pas de plus grand diviseur commun.

Propriété 1 : premières propriétés

Soit a et b deux entiers relatifs non tous les deux nuls.

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

b. Si $a \neq 0$: $\text{PGCD}(a\,;0) = |a|$ et $\text{PGCD}(a\,;1) = 1$.

c. Si $b \neq 0$ et si b divise a, alors $\text{PGCD}(a\,;b) = |b|$.

Démonstration

a. La définition ne dépend pas de l'ordre de a et b : les diviseurs communs à a et b sont les diviseurs communs à b et a.
De plus, un entier et son opposé ont les mêmes diviseurs ($a = kd \iff -a = (-k)d$). Donc a et $|a|$ ont les mêmes diviseurs, de même que b et $|b|$: les diviseurs communs sont les mêmes, et le plus grand aussi.

b. Tout entier divise 0 (car $0 = 0 \times d$). Les diviseurs communs à a et 0 sont donc exactement les diviseurs de a.
Or $|a|$ divise a, et tout diviseur d de a vérifie $d \leqslant |a|$ (car $a \neq 0$). Le plus grand diviseur de a est donc $|a|$:

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

Les diviseurs communs à a et 1 sont des diviseurs de 1, c'est-à-dire -1 ou 1. Le plus grand est 1 : $\text{PGCD}(a\,;1) = 1$.

c. $|b|$ divise b et, par hypothèse, $|b|$ divise a : $|b|$ est un diviseur commun à a et b.
Tout diviseur commun d divise en particulier $b \neq 0$, donc $d \leqslant |b|$.
$|b|$ est donc le plus grand des diviseurs communs : $\text{PGCD}(a\,;b) = |b|$.

Exemples :

• $\text{PGCD}(-30\,;48) = \text{PGCD}(30\,;48) = 6$. • $\text{PGCD}(-15\,;0) = 15$. • 12 divise 36, donc $\text{PGCD}(36\,;12) = 12$.

Exercice d'application 1 : lire un PGCD sur les diviseurs

a. Écrire la liste des diviseurs positifs de 84, puis celle des diviseurs positifs de 120.

.....

.....

b. En déduire les diviseurs positifs communs à 84 et à 120, puis $\text{PGCD}(84\,;120)$.

.....

.....

c. Donner, en justifiant à l'aide de la propriété 1 : $\text{PGCD}(-35\,;0)$, $\text{PGCD}(17\,;1)$ et $\text{PGCD}(45\,;-15)$.

.....

.....

.....

2. PGCD et division euclidienne

Pour deux entiers a et b, on note $\mathcal{D}(a\,;b)$ l'ensemble des diviseurs communs à a et à b.

Propriété 2 : PGCD et division

Soit a, b, q et r des entiers, avec $b \neq 0$, tels que

$$a = bq + r.$$

Alors a et b ont les mêmes diviseurs communs que b et r : $\mathcal{D}(a\,;b) = \mathcal{D}(b\,;r)$. En particulier :

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

C'est le cas lorsque q et r sont le quotient et le reste de la division euclidienne de a par b.

Démonstration

On montre que les deux ensembles sont égaux par **double inclusion**.

Tout diviseur commun à b et r divise a. Soit d un diviseur commun à b et r. Comme

$$a = b \times q + r \times 1,$$

a est une combinaison linéaire de b et de r : d divise donc a. Ainsi d divise a et b : $\mathcal{D}(b\,;r) \subset \mathcal{D}(a\,;b)$.

Tout diviseur commun à a et b divise r. Soit d un diviseur commun à a et b. Comme

$$r = a \times 1 + b \times (-q),$$

r est une combinaison linéaire de a et de b : d divise donc r. Ainsi d divise b et r : $\mathcal{D}(a\,;b) \subset \mathcal{D}(b\,;r)$.

Conclusion. Les deux ensembles de diviseurs communs sont égaux ; ils ont donc le même plus grand élément : $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r)$.

Remarque : on peut retrancher un multiple

La propriété 2 vaut pour **toute** écriture $a = bq + r$, même si r n'est pas le reste : on peut toujours retrancher à a un multiple de b sans changer le PGCD :

$$\text{PGCD}(a\,;b) = \text{PGCD}(b\,;a - bq).$$

Par exemple, pour tout $n \in \mathbb{N}^*$: $\text{PGCD}(2n+1\,;n) = \text{PGCD}(n\,;(2n+1) - 2n) = \text{PGCD}(n\,;1) = 1$.

3. L'algorithme d'Euclide

Théorème 1 : algorithme d'Euclide

Soit a et b deux entiers naturels non nuls. On effectue des divisions euclidiennes successives, en divisant à chaque étape le diviseur précédent par le reste obtenu :

$$\begin{aligned} a &= b\,q_1 + r_1, & 0 \leqslant r_1 < b \\ b &= r_1 q_2 + r_2, & 0 \leqslant r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, & 0 \leqslant r_3 < r_2 \\ &\vdots & \\ r_{n-1} &= r_n q_{n+1} + 0. & \end{aligned}$$

Les restes finissent par s'annuler, et **le PGCD de a et b est le dernier reste non nul** r_n (c'est b lorsque $r_1 = 0$).

Démonstration

1. L'algorithme s'arrête. Chaque reste est strictement plus petit que le diviseur qui l'a produit :

$$b > r_1 > r_2 > r_3 > \cdots \geqslant 0.$$

Les restes forment donc une suite d'entiers naturels strictement décroissante. Une telle suite ne peut pas comporter plus de $b+1$ termes (il n'y a que $b+1$ entiers entre 0 et b) : un reste finit par être nul. On note r_n le dernier reste non nul, de sorte que $r_{n+1} = 0$.

2. Le PGCD ne change pas d'une ligne à l'autre. Chaque ligne est de la forme « dividende = diviseur × quotient + reste ». D'après la propriété 2, appliquée à chaque ligne :

$$\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r_1) = \text{PGCD}(r_1\,;r_2) = \cdots = \text{PGCD}(r_{n-1}\,;r_n) = \text{PGCD}(r_n\,;0).$$

3. Conclusion. D'après la propriété 1 b., $\text{PGCD}(r_n\,;0) = r_n$ (car $r_n > 0$). Donc $\text{PGCD}(a\,;b) = r_n$.
Si $r_1 = 0$, alors b divise a et $\text{PGCD}(a\,;b) = b$ (propriété 1 c.).

Méthode 1 : calculer un PGCD avec l'algorithme d'Euclide

Énoncé. Déterminer PGCD(1 636 ; 1 128).

Solution. On divise le plus grand par le plus petit, puis le diviseur par le reste, jusqu'à obtenir un reste nul.

dividende	diviseur	quotient	reste	égalité
1 636	1 128	1	508	$1\,636 = 1\,128 \times 1 + 508$
1 128	508	2	112	$1\,128 = 508 \times 2 + 112$
508	112	4	60	$508 = 112 \times 4 + 60$
112	60	1	52	$112 = 60 \times 1 + 52$
60	52	1	8	$60 = 52 \times 1 + 8$
52	8	6	**4**	$52 = 8 \times 6 + 4$
8	4	2	0	$8 = 4 \times 2 + 0$

Le dernier reste non nul est 4. Donc :

$$\text{PGCD}(1\,636\,;1\,128) = \text{PGCD}(1\,128\,;508) = \cdots = \text{PGCD}(8\,;4) = \text{PGCD}(4\,;0) = 4.$$

Exercice d'application 2 : utiliser l'algorithme d'Euclide

a. Déterminer PGCD(2 431 ; 1 001) à l'aide de l'algorithme d'Euclide.

.....

.....

.....

.....

b. En déduire la forme irréductible de la fraction $\frac{1\,001}{2\,431}$.

.....

.....

c. Soit n un entier naturel non nul. Montrer que $\text{PGCD}(n+6\,;n) = \text{PGCD}(n\,;6)$. Quelles sont les valeurs possibles de $\text{PGCD}(n+6\,;n)$?

.....

.....

.....

.....

4. Diviseurs communs et diviseurs du PGCD

Propriété 3 : diviseurs communs

Soit a et b deux entiers non tous les deux nuls. **Les diviseurs communs à a et à b sont exactement les diviseurs de leur PGCD** :

$$d \mid a \text{ et } d \mid b \iff d \mid \text{PGCD}(a\,;b).$$

Démonstration

Cas de deux entiers naturels non nuls. On reprend les notations de l'algorithme d'Euclide. La propriété 2, appliquée à chaque ligne, donne non seulement l'égalité des PGCD, mais aussi l'**égalité des ensembles** de diviseurs communs :

$$\mathcal{D}(a\,;b) = \mathcal{D}(b\,;r_1) = \mathcal{D}(r_1\,;r_2) = \cdots = \mathcal{D}(r_{n-1}\,;r_n) = \mathcal{D}(r_n\,;0).$$

Or tout entier divise 0 : les diviseurs communs à r_n et 0 sont exactement les diviseurs de r_n. Comme $r_n = \text{PGCD}(a\,;b)$, les diviseurs communs à a et b sont les diviseurs de $\text{PGCD}(a\,;b)$.

Cas général. a et $|a|$ ont les mêmes diviseurs, de même que b et $|b|$: on se ramène au cas précédent. Si l'un des deux est nul, par exemple $b = 0$ et $a \neq 0$, les diviseurs communs sont les diviseurs de a, c'est-à-dire ceux de $|a| = \text{PGCD}(a\,;0)$.

Exemple : diviseurs communs à 2 730 et à 5 610

L'algorithme d'Euclide donne : $5\,610 = 2\,730 \times 2 + 150$, $2\,730 = 150 \times 18 + 30$, $150 = 30 \times 5 + 0$.
Donc $\text{PGCD}(5\,610\,;2\,730) = 30$.
Les diviseurs positifs communs à 2 730 et à 5 610 sont donc les diviseurs de 30 : 1, 2, 3, 5, 6, 10, 15 et 30.

Remarque

Le PGCD est donc le plus grand diviseur commun en deux sens : il est plus grand que tous les autres, et **tous les autres le divisent**.

5. PGCD et multiplication

Propriété 4 : homogénéité du PGCD

Soit a, b et k trois entiers naturels non nuls. Alors :

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

Démonstration

Une division multipliée par k reste une division euclidienne. Si $a = bq + r$ avec $0 \leqslant r < b$, alors en multipliant par $k > 0$:

$$ka = (kb)\,q + kr \qquad \text{avec} \qquad 0 \leqslant kr < kb.$$

Par unicité de la division euclidienne, c'est la division euclidienne de ka par kb : le quotient est le même, q, et le reste est multiplié par k.

Conséquence sur l'algorithme d'Euclide. En appliquant ce résultat à chaque ligne de l'algorithme d'Euclide pour a et b, l'algorithme pour ka et kb a les mêmes quotients et les restes $kr_1, kr_2, \ldots, kr_n, 0$. Son dernier reste non nul est donc kr_n :

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

Exemple

$420 = 20 \times 21$ et $540 = 20 \times 27$. Comme $\text{PGCD}(21\,;27) = 3$ (car $27 = 21 \times 1 + 6$ et $21 = 6 \times 3 + 3$, puis $6 = 3 \times 2$), on obtient

$$\text{PGCD}(420\,;540) = 20 \times \text{PGCD}(21\,;27) = 20 \times 3 = 60.$$

Exercice d'application 3 : diviseurs communs et homogénéité

a. Calculer PGCD$(252\,;180)$. Combien d'entiers naturels divisent à la fois 252 et 180 ? Les citer.

.....

.....

.....

.....

b. Sans algorithme, à l'aide de la propriété 4, calculer PGCD$(4\,200\,;3\,500)$.

.....

.....

c. Un confiseur dispose de 252 dragées et de 180 chocolats. Il veut confectionner le plus grand nombre possible de sachets identiques en utilisant toutes les friandises. Combien de sachets fera-t-il ? Quelle sera la composition de chaque sachet ?

.....

.....

.....

.....

II. Nombres premiers entre eux. Théorème de Bézout

1. Nombres premiers entre eux

Définition 2 : entiers premiers entre eux

Deux entiers a et b non tous les deux nuls sont **premiers entre eux** lorsque

$$\text{PGCD}(a\,;b) = 1,$$

c'est-à-dire lorsque leur seul diviseur commun positif est 1.

Exemples :

• $42 = 2 \times 3 \times 7$ et $55 = 5 \times 11$ n'ont aucun diviseur positif commun autre que 1 : ils sont premiers entre eux.
• Deux entiers consécutifs n et $n+1$ sont toujours premiers entre eux : un diviseur commun divise leur différence $(n+1) - n = 1$.
• 6 et 9 ne sont pas premiers entre eux : 3 les divise tous les deux.

Attention

Ne pas confondre « premiers entre eux » et « premiers » : 8 et 15 sont premiers entre eux, alors qu'aucun des deux n'est un nombre premier.

Propriété 5 : simplifier par le PGCD

Soit a et b deux entiers naturels non nuls et $d = \text{PGCD}(a\,;b)$. Il existe deux entiers naturels non nuls a' et b' **premiers entre eux** tels que

$$a = d\,a' \qquad \text{et} \qquad b = d\,b'.$$

Démonstration

d divise a et b : il existe donc des entiers a' et b' tels que $a = da'$ et $b = db'$. Comme a, b et d sont strictement positifs, a' et b' le sont aussi.
D'après la propriété 4 (homogénéité) :

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

En divisant par $d \neq 0$: $\text{PGCD}(a'\,;b') = 1$. a' et b' sont premiers entre eux.

Exemple : fraction irréductible

$\text{PGCD}(1\,636\,;1\,128) = 4$ (méthode 1), avec $1\,636 = 4 \times 409$ et $1\,128 = 4 \times 282$. D'après la propriété 5, 409 et 282 sont premiers entre eux :

$$\frac{1\,636}{1\,128} = \frac{409}{282} \quad \text{est la forme irréductible.}$$

2. Identité de Bézout

Théorème 2 : identité de Bézout

Soit a et b deux entiers non tous les deux nuls, et $d = \text{PGCD}(a\,;b)$. Il existe deux entiers relatifs u et v tels que

$$au + bv = d.$$

Démonstration

On considère l'ensemble E des entiers **strictement positifs** qui s'écrivent comme combinaison linéaire de a et b :

$$E = \{am + bn \ : \ m \in \mathbb{Z},\ n \in \mathbb{Z} \ \text{ et } \ am + bn > 0\}.$$

Étape 1 : E admet un plus petit élément. a et b ne sont pas tous les deux nuls ; si par exemple $a \neq 0$, alors $|a| = a \times (\pm 1) + b \times 0$ est strictement positif, donc $|a| \in E$ (si $a = 0$, on raisonne de même avec $|b|$). Ainsi E est une partie non vide de $\mathbb{N}$: elle admet un plus petit élément, que l'on note δ. Il existe donc des entiers u et v tels que

$$\delta = au + bv.$$

Étape 2 : δ divise a et b. On effectue la division euclidienne de a par δ : $a = \delta q + r$ avec $0 \leqslant r < \delta$. Alors

$$r = a - \delta q = a - (au + bv)\, q = a\,(1 - uq) + b\,(-vq).$$

r est donc une combinaison linéaire de a et b. Si on avait $r > 0$, alors r appartiendrait à E tout en étant strictement plus petit que δ : c'est impossible puisque δ est le plus petit élément de E. Donc $r = 0$ et δ divise a.
On montre de la même façon que δ divise b.

Étape 3 : $\delta = d$.
• δ est un diviseur commun à a et b (étape 2), donc $\delta \leqslant d$ puisque d est le plus grand d'entre eux.
• d divise a et b, donc d divise la combinaison linéaire $au + bv = \delta$. Comme $\delta > 0$, on en déduit $d \leqslant \delta$.
Donc $\delta = d$, c'est-à-dire : $au + bv = d$.

Remarque

Le couple $(u\,;v)$ n'est pas unique. Par exemple $\text{PGCD}(54\,;42) = 6$ et

$$54 \times (-3) + 42 \times 4 = -162 + 168 = 6, \qquad 54 \times 4 + 42 \times (-5) = 216 - 210 = 6.$$

Méthode 2 : trouver u et v en « remontant » l'algorithme d'Euclide

Énoncé. Déterminer deux entiers u et v tels que $54u + 42v = \text{PGCD}(54\,;42)$.

Solution. On écrit l'algorithme d'Euclide en isolant chaque reste :

$$\begin{array}{lll} 54 = 42 \times 1 + 12 & \text{donc} & 12 = 54 - 42 \times 1 \\ 42 = 12 \times 3 + \mathbf{6} & \text{donc} & 6 = 42 - 12 \times 3 \\ 12 = 6 \times 2 + 0 & & \end{array}$$

Le dernier reste non nul est 6 : $\text{PGCD}(54\,;42) = 6$.

On part de la dernière égalité et on remplace les restes un par un :

$$6 = 42 - 12 \times 3 = 42 - (54 - 42) \times 3 = 42 - 54 \times 3 + 42 \times 3 = 54 \times (-3) + 42 \times 4.$$

Le couple $(u\,;v) = (-3\,;4)$ convient. **Vérification :** $54 \times (-3) + 42 \times 4 = -162 + 168 = 6$.

Propriété 6 : équations $ax + by = c$ — existence de solutions

Soit a et b deux entiers non tous les deux nuls, $d = \text{PGCD}(a\,;b)$, et c un entier. L'équation

$$ax + by = c$$

admet au moins un couple solution d'entiers $(x\,;y)$ **si, et seulement si,** d **divise** c.

Démonstration

Si l'équation a une solution $(x_0\,;y_0)$. d divise a et b, donc il divise la combinaison linéaire $ax_0 + by_0 = c$.

Réciproquement, si d divise c. On écrit $c = dk$ avec $k \in \mathbb{Z}$. D'après l'identité de Bézout, il existe u et v tels que $au + bv = d$. En multipliant par k :

$$a\,(uk) + b\,(vk) = dk = c.$$

Le couple $(uk\,;vk)$ est une solution de l'équation.

Exemples :

• $\text{PGCD}(12\,;18) = 6$ et 6 ne divise pas 7 : l'équation $12x + 18y = 7$ n'a **aucune** solution entière.
• $\text{PGCD}(54\,;42) = 6$ divise 30 : en multipliant par 5 l'égalité de la méthode 2,
$54 \times (-15) + 42 \times 20 = 30$.

3. Théorème de Bézout

Théorème 3 : théorème de Bézout

Deux entiers a et b non tous les deux nuls sont **premiers entre eux** si, et seulement si, il existe deux entiers relatifs u et v tels que

$$au + bv = 1.$$

Démonstration

Sens direct. Si a et b sont premiers entre eux, alors $\text{PGCD}(a\,;b) = 1$, et l'identité de Bézout (théorème 2) donne directement deux entiers u et v tels que $au + bv = 1$.

Réciproque. On suppose qu'il existe u et v tels que $au + bv = 1$, et on note $d = \text{PGCD}(a\,;b)$.
d divise a et b, donc d divise la combinaison linéaire $au + bv = 1$.
Or $d \geqslant 1$, et le seul diviseur positif de 1 est 1 : donc $d = 1$. a et b sont premiers entre eux.

Attention

Seule la valeur 1 permet de conclure. Une égalité $au + bv = d$ avec $d > 1$ prouve seulement que $\text{PGCD}(a\,;b)$ **divise** d, et non qu'il est égal à d : par exemple $2 \times 4 + 3 \times (-2) = 2$, alors que $\text{PGCD}(2\,;3) = 1$.

Méthode 3 : prouver que deux expressions sont premières entre elles

Énoncé. Démontrer que, pour tout entier naturel n, les entiers $2n+3$ et $5n+7$ sont premiers entre eux.

Solution. On cherche des coefficients qui **éliminent** n : on multiplie $2n+3$ par 5 et $5n+7$ par 2, puis on soustrait :

$$5\,(2n+3) - 2\,(5n+7) = 10n + 15 - 10n - 14 = 1.$$

On a trouvé deux entiers $u = 5$ et $v = -2$ tels que $(2n+3)\,u + (5n+7)\,v = 1$. D'après le théorème de Bézout, $2n+3$ et $5n+7$ sont premiers entre eux.

Exercice d'application 4 : coefficients de Bézout

a. Appliquer l'algorithme d'Euclide à 47 et 30. Que peut-on dire de ces deux entiers ?

.....

.....

.....

.....

b. En remontant l'algorithme, déterminer deux entiers u et v tels que $47u + 30v = 1$. Vérifier.

.....

.....

.....

.....

.....

c. Déterminer deux entiers u et v tels que $84u + 120v = 12$.

.....

.....

.....

.....

Exercice d'application 5 : théorème de Bézout

a. Démontrer que, pour tout entier naturel n, les entiers $2n+1$ et $3n+2$ sont premiers entre eux.

.....

.....

.....

b. Démontrer que, pour tout entier naturel non nul n, les entiers n et $2n+1$ sont premiers entre eux.

.....

.....

c. Trouver deux entiers u et v tels que $7u+12v=1$. En déduire un entier x tel que $7x \equiv 1\ [12]$, puis un entier x tel que $7x \equiv 3\ [12]$.

.....

.....

.....

.....

.....

III. Théorème de Gauss

1. Le théorème

Théorème 4 : théorème de Gauss

Soit a, b et c trois entiers non nuls.

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

Démonstration

On utilise Bézout. a et b sont premiers entre eux : d'après le théorème de Bézout, il existe deux entiers u et v tels que

$$au+bv=1.$$

On multiplie par c. $acu+bcv=c$.

On montre que a divise chaque terme.
• $acu = a\times(cu)$ est un multiple de a ;
• a divise bc par hypothèse, donc a divise aussi $bc\times v$.
a divise donc la somme $acu+bcv$, c'est-à-dire c.

Attention : l'hypothèse « premiers entre eux » est indispensable

6 divise $4\times 3=12$, mais 6 ne divise ni 4 ni 3 : le théorème ne s'applique pas car $\text{PGCD}(6\,;4)=2\neq 1$.

Exemple

On cherche les entiers x tels que 28 divise $15x$. Comme $28=2^2\times 7$ et $15=3\times 5$, on a $\text{PGCD}(28\,;15)=1$.
D'après le théorème de Gauss, 28 divise x. Réciproquement, si x est un multiple de 28, $15x$ aussi. Les solutions sont les multiples de 28.

2. Une conséquence : diviser par un produit

Propriété 7 : corollaire du théorème de Gauss

Soit a, b et c trois entiers non nuls.

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

Démonstration

a divise c : il existe un entier k tel que $c = ak$.
b divise $c = ak$, et b est premier avec a : d'après le théorème de Gauss, b divise k. Il existe donc un entier k' tel que $k = bk'$.
En remplaçant : $c = ak = a\,b\,k' = (ab)\,k'$. Donc ab divise c.

Exemples :

• 6 et 11 divisent 660, et 6 et 11 sont premiers entre eux : donc $6 \times 11 = 66$ divise 660.
• Un entier divisible par 4 et par 9 est divisible par 36, car $\text{PGCD}(4\,;9) = 1$.
• **Contre-exemple :** 6 et 9 divisent 18, mais $6 \times 9 = 54$ ne divise pas 18 : 6 et 9 ne sont pas premiers entre eux.

Exercice d'application 6 : théorème de Gauss et corollaire

a. Déterminer tous les couples d'entiers $(x\,;y)$ tels que $4x = 9y$.

.....

.....

.....

.....

b. Démontrer que, pour tout entier n, le produit $n(n+1)(n+2)$ est divisible par 2, par 3, puis par 6.

.....

.....

.....

.....

.....

c. Déterminer les entiers n tels que 7 divise $3n$.

.....

.....

3. Résoudre une équation $ax + by = c$

Propriété 8 : solutions de $ax + by = c$

Soit a et b deux entiers non nuls **premiers entre eux**, c un entier, et $(x_0\,;y_0)$ un couple d'entiers solution de l'équation $ax + by = c$. Les solutions entières de cette équation sont les couples

$$(x\,;y) = (x_0 + bk\,;\ y_0 - ak) \qquad \text{avec} \qquad k \in \mathbb{Z}.$$

Démonstration

On se ramène à une égalité de produits. Comme $ax_0 + by_0 = c$, un couple $(x\,;y)$ est solution si, et seulement si, $ax + by = ax_0 + by_0$, c'est-à-dire :

$$a\,(x - x_0) = b\,(y_0 - y).$$

Toute solution est de la forme annoncée. Soit $(x\,;y)$ une solution.
a divise $b\,(y_0 - y)$ et a est premier avec b : d'après le théorème de Gauss, a divise $y_0 - y$. Il existe donc un entier k tel que $y_0 - y = ak$, soit $y = y_0 - ak$.
En remplaçant dans l'égalité : $a\,(x - x_0) = b \times ak$, et comme $a \neq 0$: $x - x_0 = bk$, soit $x = x_0 + bk$.

Réciproquement, ces couples sont solutions. Pour tout entier k :

$$a\,(x_0 + bk) + b\,(y_0 - ak) = ax_0 + abk + by_0 - abk = ax_0 + by_0 = c.$$

Méthode 4 : résoudre une équation $ax + by = c$ dans $\mathbb{Z}^2$

Énoncé. Résoudre dans $\mathbb{Z}^2$: **a.** $5x + 7y = 1$; **b.** $5x + 7y = 12$.

Solution. a. Existence. $\text{PGCD}(5\,;7) = 1$: 5 et 7 sont premiers entre eux, l'équation a des solutions (propriété 6).

Solution particulière. On cherche x pour que $y = \dfrac{1 - 5x}{7}$ soit entier : $x = -4$ donne $y = \dfrac{21}{7} = 3$. Le couple $(-4\,;3)$ est solution : $5 \times (-4) + 7 \times 3 = -20 + 21 = 1$.
Égalité de produits. $(x\,;y)$ est solution $\iff 5x + 7y = 5 \times (-4) + 7 \times 3 \iff 5\,(x + 4) = 7\,(3 - y)$.
Gauss. Si $(x\,;y)$ est solution : 5 divise $7\,(3 - y)$ et $\text{PGCD}(5\,;7) = 1$, donc 5 divise $3 - y$: il existe $k \in \mathbb{Z}$ tel que $3 - y = 5k$. En remplaçant : $5\,(x + 4) = 7 \times 5k$, donc $x + 4 = 7k$.
Réciproque. Pour $x = -4 + 7k$ et $y = 3 - 5k$: $5\,(-4 + 7k) + 7\,(3 - 5k) = -20 + 35k + 21 - 35k = 1$.
Conclusion. Les solutions sont les couples $(-4 + 7k\,;\ 3 - 5k)$, avec $k \in \mathbb{Z}$.

b. Solution particulière. On multiplie par 12 l'égalité $5 \times (-4) + 7 \times 3 = 1$: $5 \times (-48) + 7 \times 36 = 12$.
Le couple $(-48\,;36)$ est solution.
En reprenant la même démarche (ou d'après la propriété 8), les solutions sont les couples

$$(-48 + 7k\,;\ 36 - 5k), \qquad k \in \mathbb{Z}.$$

Remarque : lorsque a et b ne sont pas premiers entre eux

On note $d = \text{PGCD}(a\,;b)$. Si d ne divise pas c, il n'y a aucune solution (propriété 6). Si d divise c, on divise toute l'équation par d : on obtient une équation équivalente $a'x + b'y = c'$ avec a' et b' premiers entre eux (propriété 5).
Exemple : $12x + 18y = 30 \iff 2x + 3y = 5$ (on a divisé par 6).

Exercice d'application 7 : équations $ax + by = c$

a. Justifier que l'équation $11x + 4y = 1$ admet des solutions entières, en trouver une, puis les déterminer toutes.

.....

.....

.....

.....

.....

.....

.....

b. En déduire les solutions entières de l'équation $11x + 4y = 5$.

.....

.....

.....

c. Résoudre dans $\mathbb{Z}^2$ l'équation $12x + 18y = 30$.

.....

.....

.....

.....

d. L'équation $12x + 18y = 7$ a-t-elle des solutions entières ? Justifier.

.....

.....

IV. Algorithmique

L'algorithme d'Euclide se programme en quelques lignes : tant que le diviseur n'est pas nul, on remplace le couple $(a\,;b)$ par $(b\,;r)$, où r est le reste de a par b (propriété 2). La version « étendue » calcule en plus des coefficients de Bézout, en remontant les divisions comme dans la méthode 2.

Python

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

print(pgcd(1636, 1128))    # 4
```

Python

```
def bezout(a, b):
    # renvoie (d, u, v) avec a*u + b*v = d
    if b == 0:
        return (a, 1, 0)
    d, u, v = bezout(b, a % b)
    return (d, v, u - (a // b) * v)

print(bezout(54, 42))      # (6, -3, 4)
print(bezout(5, 7))        # (1, 3, -2)
```

Remarque

Dans la fonction `bezout`, si $bu' + rv' = d$ avec $r = a - bq$, alors $bu' + (a - bq)v' = d$, soit $a\,v' + b\,(u' - qv') = d$: c'est exactement le calcul « en remontant » de la méthode 2. Le module `math` de Python propose aussi la fonction `gcd`.

L'essentiel du chapitre

PGCD	Plus grand diviseur commun à a et b (non tous deux nuls). $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r)$ si $a = bq + r$.
Euclide	Le PGCD est le dernier reste non nul des divisions euclidiennes successives.
Diviseurs	Les diviseurs communs à a et b sont les diviseurs de $\text{PGCD}(a\,;b)$. $\text{PGCD}(ka\,;kb) = k\ \text{PGCD}(a\,;b)$.
Bézout	Il existe u, v tels que $au + bv = \text{PGCD}(a\,;b)$. a et b premiers entre eux $\iff$ il existe u, v tels que $au + bv = 1$.
Gauss	Si $a \mid bc$ et $\text{PGCD}(a\,;b) = 1$, alors $a \mid c$. Si $a \mid c$, $b \mid c$ et $\text{PGCD}(a\,;b) = 1$, alors $ab \mid c$.
$ax + by = c$	Solutions $\iff$ $\text{PGCD}(a\,;b) \mid c$. Si $\text{PGCD}(a\,;b) = 1$: solution particulière, égalité de produits, Gauss, réciproque.