

I. PGCD de deux entiers	1	III. Théorème de Bézout	3
II. Algorithme d'Euclide	2	IV. Théorème de Gauss	4

I. PGCD de deux entiers

PROPRIÉTÉ

Soient a et b deux entiers relatifs non tous nuls.

L'ensemble des diviseurs communs à a et b admet un plus grand élément.

DÉFINITION

On appelle cet élément le **plus grand diviseur commun à a et b** , que l'on note $\text{PGCD}(a;b)$.

Démonstration :

L'ensemble des diviseurs communs à a et b est non vide, puisqu'il contient 1.

Le plus grand élément de cet ensemble est majoré par a ou b , car le plus grand diviseur de a est a , de même pour b (avec a et b non tous nuls).

Or, toute partie non vide et majorée de \mathbb{N} (ici de \mathbb{Z}) admet un plus grand élément.

D'où l'existence d'un plus grand élément dans l'ensemble des diviseurs communs à a et b .

REMARQUE : les anglophones le notent $\text{GCD}(a;b)$ pour *Greatest Common Divisor* (GCD).

EXEMPLE C1

Déterminer l'ensemble des diviseurs de 24, noté D_{24} , ainsi que celui des diviseurs de 18, noté D_{18} .
En déduire $\text{PGCD}(24;18)$.

PROPRIÉTÉS (ÉVIDENTES)

- $\text{PGCD}(a;b) = \text{PGCD}(b;a)$
- $\text{PGCD}(a;b) = \text{PGCD}(|a|;|b|)$
- $\text{PGCD}(a;0) = a$
- Si b divise a , alors $\text{PGCD}(a;b) = |b|$.

DÉFINITION

Soient a et b deux entiers relatifs non tous nuls.

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

EXEMPLE C2

$5 \times 3 = 15$ et $2 \times 7 \times 7 = 98$ donc 15 et 98 sont premiers entre eux.

EXEMPLE A1

1. Déterminer tous les entiers naturels n tels que : $\text{PGCD}(n; 324) = 12$.
2. En déduire parmi eux les entiers naturels n inférieurs à 100.

EXEMPLE A2

Trouver tous les entiers naturels a et b avec $a < b$ tels que :
 $ab = 432$ et $\text{PGCD}(a; b) = 6$.

II. Algorithme d'Euclide

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls tels que b ne divise pas a .
D'après la division euclidienne : $a = bq + r$ avec $0 < r < b$.
Alors : $\text{PGCD}(a; b) = \text{PGCD}(b; r)$.

Démonstration :

THÉORÈME (ALGORITHME D'EUCLIDE)

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

On définit l'algorithme d'Euclide par la suite des divisions euclidiennes du diviseur par le reste de la division précédente, tant que ce reste est non nul :

Division de a par b :	$a = bq_0 + r_0$	avec	$0 < r_0 < b$
Division de b par r_0 :	$b = r_0q_1 + r_1$	avec	$0 \leq r_1 < r_0$
Si $r_1 \neq 0$, division de r_0 par r_1 :	$r_0 = r_1q_2 + r_2$	avec	$0 \leq r_2 < r_1$
...			
Si $r_n \neq 0$, division de r_{n-1} par r_n :	$r_{n-1} = r_nq_{n+1} + r_{n+1}$	avec	$0 \leq r_{n+1} < r_n$

$\text{PGCD}(a; b)$ est le dernier reste non nul dans cet algorithme.

Démonstration :

La suite des restes (r_n) est strictement décroissante dans \mathbb{N} .

Par conséquent, il existe un plus entier naturel m tel que $r_m = 0$.

D'après la propriété précédente : $\text{PGCD}(a; b) = \text{PGCD}(b; r_0) = \text{PGCD}(r_0; r_1) = \dots = \text{PGCD}(r_{m-1}; r_m)$.

Or, $r_m = 0$ donc $\text{PGCD}(r_{m-1}; r_m) = r_{m-1}$ d'où $\text{PGCD}(a; b) = r_{m-1}$ (le dernier reste non nul).

EXEMPLE C3

$$9945 = 3003 \times 3 + 936$$

$$3003 = 936 \times 3 + 195$$

$$936 = 195 \times 4 + 156$$

$$195 = 156 \times 1 + 39$$

$$156 = 39 \times 4 + 0$$

donc, d'après l'algorithme d'Euclide : $\text{PGCD}(9945; 3003) = 39$.

III. Théorème de Bézout

THÉORÈME (IDENTITÉ DE BÉZOUT)

Soient a et b deux entiers naturels non nuls. On note d le PGCD de a et b .

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

Démonstration :

On note $E = \{ au + bv, (u; v) \in \mathbb{Z}^2 \text{ et } au + bv > 0 \}$.

$E \neq \emptyset$ car $a \in E$ (prendre $u=1$ et $v=0$) avec $a > 0$.

E est donc une partie non vide de \mathbb{N} : E donc un plus petit élément, noté m : $m = au_0 + bv_0$.

Montrons que $m = d$:

• $d \mid a$ et $d \mid b$ donc $d \mid m$ (car m est une combinaison linéaire de a et b)

donc $d \leq m$.

• \rightarrow Division euclidienne de a par m : $a = mq + r$ avec $0 \leq r < m$.

$$\text{Donc : } r = a - mq = a - (au_0 + bv_0)q = \dots = a(1 - u_0q) + b(-v_0q).$$

Si $r \neq 0$, alors $r \in E$ et donc, puisque m est le plus petit élément de E : $r \geq m$.

Ceci est absurde, puisque $0 \leq r < m$.

On a donc (raisonnement par l'absurde) : $r = 0$.

D'où $m \mid a$.

\rightarrow De même, on démontrerait que $m \mid b$.

$\rightarrow d$ étant le plus grand diviseur commun à a et b , on a donc $m \leq d$.

• On a donc : $d = m$.

THÉORÈME DE BÉZOUT

Soient a et b deux entiers naturels non nuls.

a et b sont premiers entre eux si, et seulement si, il existe $(u; v) \in \mathbb{Z}^2$, $au + bv = 1$.

Démonstration :

\Rightarrow : c'est l'identité de Bézout dans le cas où $\text{PGCD}(a; b) = 1$

\Leftarrow : supposons que $au + bv = 1$.

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

DÉFINITION

Dans les théorèmes ci-dessus, on appelle *coefficients de Bézout* les entiers u et v .

EXEMPLE C4

Pour déterminer les coefficients de Bézout, on utilise l'algorithme d'Euclide.

$$\begin{aligned} \text{Algorithme d'Euclide pour 600 et 124 :} & \quad (1) \quad 600 = 124 \times 4 + 104 \\ & \quad (2) \quad 124 = 104 \times 1 + 20 \\ & \quad (3) \quad 104 = 20 \times 5 + 4 \\ & \quad (4) \quad 20 = 4 \times 5 + 0 \end{aligned}$$

M
E
T
H
O
D
E
1

Puis on « remonte » ces égalités en ayant pour objectif de trouver u et v tels que $600u + 124v = 4$. L'idée est de remplacer le reste de la ligne précédente en partant de la dernière ligne où le reste est non nul.

$$\begin{aligned} (3) \quad 4 &= 104 - 20 \times 5 \\ (2) \quad &= 104 - (124 - 104 \times 1) \times 5 \\ &= 124 \times (-5) + 104 \times 6 \\ (1) \quad &= 124 \times (-5) + (600 - 124 \times 4) \times 6 \\ &= 600 \times 6 + 124 \times (-29) \end{aligned}$$

Donc $u=6$ et $v=-29$ conviennent.

M
E
T
H
O
D
E
2

On peut aussi partir de la première ligne, et exprimer chaque fois le reste en fonction des autres nombres :

$$\begin{aligned} (1) \quad 104 &= 600 - 124 \times 4 \\ (2) \quad 20 &= 124 - 104 \times 1 \\ &= 124 - (600 - 124 \times 4) \times 1 \\ &= 600 \times (-1) + 124 \times 5 \\ (3) \quad 4 &= 104 - 20 \times 5 \\ &= (600 - 124 \times 4) - (600 \times (-1) + 124 \times 5) \times 5 \\ &= 600 \times 6 + 124 \times (-29) \end{aligned}$$

Donc $u=6$ et $v=-29$ conviennent.

EXEMPLE A3

1. Montrer que 59 et 27 sont premiers entre eux.
2. Déterminer un couple d'entiers relatifs $(x; y)$ tel que : $59x + 27y = 1$.
3. Montrer que pour tout entier relatif n , $2n+1$ et $3n+2$ sont premiers entre eux.



p. 113 méthode 4

IV. Théorème de Gauss

THÉORÈME DE GAUSS

Soient a, b et c trois entiers naturels non nuls.

Si $a \mid bc$ et $\text{PGCD}(a; b) = 1$, alors $a \mid c$.

Démonstration :

Si $a \mid bc$ alors : il existe un entier relatif q tel que $bc = aq$.

Or, $\text{PGCD}(a; b) = 1$ donc, d'après le théorème de Bézout, il existe un couple d'entiers naturels $(u; v)$ tel que : $au + bv = 1$.

Alors : $(au + bv)c = c$ ie $auc + vbc = c$ ie $auc + vaq = c$ ie $a(uc + vq) = c$

d'où $a \mid c$.

EXEMPLE A4

1. Trouver tous les couples d'entiers relatifs $(x; y)$ tels que : $5(x-1) = 7y$.
2. En déduire les couples d'entiers relatifs $(x; y)$ tels que : $5x + 7y = 5$.

COROLLAIRE DU THÉORÈME DE GAUSS

Soient a, b et c trois entiers naturels non nuls.

Si $b \mid a, c \mid a$ et $\text{PGCD}(b; c) = 1$, alors $bc \mid a$.

Démonstration :

|

EXEMPLE A5

Soit x un entier relatif. Montrer que si $x \equiv 0 [8]$ et $x \equiv 0 [9]$ alors $x \equiv 0 [72]$.

→ BILAN DU CHAPITRE & TRAVAIL EN AUTONOMIE ←



- Fiche bilan → p.125
- QCM 10 questions corrigées → p.126
- Exercices corrigés → 106 à 118 p.127
- Exercices types corrigés → méthodes 7 et 8 p.117