# Plus grand diviseur commun
# Théorèmes de Bézout et Gauss

## I] PGCD de deux entiers naturels :

### 1- Définition :

**Définition :** Soit $a$ et $b$ deux entiers relatifs non tous nuls.
L'ensemble des diviseurs communs à $a$ et $b$ admet un plus grand élément $d$, appelé **plus grand commun diviseur.**
On note : $d = \text{pgcd}(a, b)$

**Exemples :** $\text{pgcd}(36, 48) = 12$, $\text{pgcd}(100, 75) = 25$, $\text{pgcd}(42, 56) = 14$.

### 2- Propriétés du PGCD :

**Propriétés :**

- $\text{pgcd}(a, b) = \text{pgcd}(b, a)$.
- $\text{pgcd}(a, b) = \text{pgcd}(|\ a\ |, |\ b\ |)$.
- $\text{pgcd}(a, 0) = |\ a\ |$ car 0 est multiple de tout entier.
- Si $b$ divise $a$ alors $\text{pgcd}(a, b) = |\ b\ |$.
- Pour tout entier naturel $k$ non nul, on a : $\text{pgcd}(ka, kb) = k\text{pgcd}(a, b)$.

### 3- Nombres premiers entre eux :

**Définition :** Dire que deux entiers relatifs non nuls **a et b sont premiers entre eux** signifie que
**PGCD(a ; b) = 1**.

**Exemple :** 45 et 34 sont premiers entre eux car leur seul diviseur commun positif est 1.

## II] Algorithme d'Euclide :

**Théorème :** Soit $a$ et $b$ deux naturels non nuls tels que $b$ ne divise pas $a$.
La suite des divisions euclidiennes du diviseur par le reste de la division précédente finit par s'arrêter.
Le dernier reste non nul est alors le $\text{pgcd}(a, b)$

| | | |
|---|---|---|
| division de $a$ par $b$ : | $a = bq_0 + r_0$ | avec $b > r_0 \geq 0$ |
| division de $b$ par $r_0$ : | $b = r_0q_1 + r_1$ | avec $r_0 > r_1 \geq 0$ |
| division de $r_0$ par $r_1$ : | $r_0 = r_1q_2 + r_2$ | avec $r_1 > r_2 \geq 0$ |
| ⋮ | ⋮ | ⋮ |
| division de $r_{n-2}$ par $r_{n-1}$ : | $r_{n-2} = r_{n-1}q_n + r_n$ | avec $r_{n-1} > r_n \geq 0$ |
| division de $r_{n-1}$ par $r_n$ : | $r_{n-1} = r_n\, q_{n+1} + 0$ | |
| D'où $\text{pgcd}(a, b) = r_n$. | | |

**Démonstration :** Montrons que $pgcd(a, b) = pgcd(b, r_0)$ par une double inégalité.
Soit $D = pgcd(a, b)$ et $d = pgcd(b, r_0)$.
$D$ divise $a$ et $b$ donc divise toute combinaison linéaire de $a$ et $b$ et donc divise
$a - bq_0 = r_0$.

$D$ divise $b$ et $r_0$, par conséquent $D \leq d$.
$d$ divise $b$ et $r_0$ donc divise toute combinaison linéaire de $b$ et $r_0$ et donc divise

$$bq_0 + r_0 = a.$$

$d$ divise $a$ et $b$, par conséquent $d \leq D$.
On déduit de ces deux inégalités que $D = d$ soit $pgcd(a, b) = pgcd(b, r_0)$.

↳ La suite des restes $r_0, r_1, \dots, r_n$ est strictement décroissante dans $\mathbb{N}$. (car $r_0 > r_1 > \cdots > r_n \geq 0$.)

D'après le principe de la descente infinie (toute suite strictement décroissante dans $\mathbb{N}$ est finie), il existe alors $n$ tel que $r_{n+1} = 0$. (car tant que le reste est non nul on peut diviser).

↳ De proche en proche, on en déduit, avec $r_n$ divisé $r_{n-1}$, que :

$$pgcd(a, b) = pgcd(b, r_0) = \cdots = pgcd(r_{n-2}, r_{n-1}) = pgcd(r_{n-1}, r_n) = r_n$$

Conclusion : $pgcd(a, b) = r_n$. Le dernier reste non nul est le pgcd.

**Exemple :** On applique l'algorithme d'Euclide pour calculer le PGCD de 364 et 247.
$364 = 247 \times 1 + 117.$
$247 = 117 \times 2 + 13.$
$117 = 13 \times 9 + 0.$
On en déduit que PGCD(364 ; 247) = 13.

## II] Théorème de Bézout :

### 1- L'identité de Bézout :

**Théorème :** Soient a et b deux entiers naturels non nuls.
Il **existe alors un couple (u, v)** d'entiers relatifs que **au + bv = PGCD(a ; b)**

**Démonstration :**
Soit E l'ensemble des combinaisons linéaires strictement positives de a et b :

$$E = \{am + bm \in N^*, \text{ avec } m \in Z \text{ et } n \in Z\}$$

E est non vide car il contient a et b donc E admet un plus petit élément noté d. Il existe donc deux entiers relatifs u et v tels que au + bv = d.
Montrons que d = PGCD(a ; b). Pour cela, on va montrer que PGCD(a ; b) ⩽ d et que d ⩽ PGCD(a; b).

**1) PGCD(a ; b) ⩽ d :**
Comme le PGCD de a et b divise a et b, il divise toute combinaison linéaire de ces entiers.
En particulier, il divise d. On en déduit que PGCD(a; b) ⩽ d.

**2) d ⩽ PGCD(a ; b) :**
On effectue la division euclidienne de a par d. Il existe des entiers q et r tels que a = dq + r avec 0 ⩽ r < d.
Or : r = a − dq = a − (au + bv)q = a − auq − bvq = a(1 − uq) − bvq est une combinaison linéaire de a et b positive ou nulle.
Si r n'était pas nul, on aurait alors construit un élément de E strictement inférieur à d, ce qui est absurde. On en déduit que r est nul et par suite que d divise a.
On montre de même que d divise b.
d est donc un diviseur commun à a et b, et par définition du PGCD, on a donc d ⩽ PGCD(a; b).

**3) Conclusion :**
d = PGCD(a; b) et il existe donc bien une combinaison linéaire de a et b telle que au + bv = PGCD(a; b).

**Exemple :** PGCD(18; 60) = 6. On peut trouver un couple (u ; v) tel que 18u + 60v = 6, par exemple le couple (− 3 ; 1).

**Remarques :**

- Il n'y a pas d'unicité du couple (u; v) trouvé. Dans l'exemple précédent, le couple (7 ; −2) convient aussi. Pour déterminer l'ensemble de ces couples, il faut résoudre une équation diophantienne.

➢ La réciproque de cette propriété est fausse ! En effet, si d = au + bv, alors d n'est pas nécessairement le PGCD des entiers a et b.
**Contre-exemple :** 2 = 1 + 1 et pourtant 2 n'est pas le PGCD du couple (1; 1).

**Théorème :** Conséquence de l'identité de Bézout.
Tout diviseur commun à a et b **divise** le PGCD(a, b).

**Démonstration :** Soit d un diviseur commun à a et b :
d divise toute combinaison linaire de a et de b, donc d'après l'identité de Bézout, d divise au + bv = PGCD(a, b).

### 2- Théorème de Bézout :

**Théorème :** Soient a et b deux entiers naturels non nuls.
**a et b sont premiers entre eux** si, et seulement si, **il existe deux entiers relatifs u et v tels que au+bv = 1.**

$$\text{pgcd}(a,b) = 1 \iff \exists u, v \in \mathbb{Z}, au + bv = 1$$

**Démonstration :**
↳ a et b sont premiers entre eux, alors PGCD(a ; b) = 1, et d'après l'identité de Bézout, il existe alors deux entiers relatifs u et v tels que au + bv = 1.
↳ Réciproquement, si il existe deux entiers relatifs u et v tels que au + bv = 1, alors tout diviseur commun à a et b divise au + bv, donc 1. Donc PGCD(a ; b) = 1 et donc a et b sont premiers entre eux.

**Exemples :**
1) Démontrer que, pour tout entier naturel n, 5n + 7 et 3n + 4 sont premiers entre eux.
↳ **3(5n + 7) − 5(3n + 4) = 1 donc P GCD(5n + 7 ; 3n + 4) = 1.**

2) a. Justifier qu'il existe deux entiers u et v tels que 29u + 12v = 1.
↳ **9 et 12 sont premiers entre eux, donc d'après le théorème de Bézout, il existe bien deux entiers u et v tels que 29u + 12v = 1.**

b. En utilisant l'algorithme d'Euclide, déterminer un couple (u ; v) possible.
↳ **D'après l'algorithme d'Euclide, on a :**
**29 = 12 × 2 + 5 ;**
**12 = 5 × 2 + 2 ;**
**5 = 2 × 2 + 1.**
**En remontant l'algorithme d'Euclide, on a alors :**
**1 = 5 − 2 × 2 = 5 − 2 × (12 − 5 × 2) = 5 × 5 − 2 × 12.**
**Et ainsi, 1 = 5 × (29 − 12 × 2) − 2 × 12 = 29 × 5 + 12 × (−12)**
**Ainsi, le couple (u ; v) = (5 ; −12) convient.**

## III] Théorème de Gauss :

### 1- Théorème :

**Théorème :** Soient a, b et c trois entiers naturels non nuls.
**Si a | bc** et **si a et b sont premiers entre eux**, **alors a | c**.

**Démonstration :**
a | bc, donc il existe un entier k tel que bc = ka.
a et b sont premiers entre eux. D'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que au + bv = 1.

En multipliant cette égalité par c, on obtient $auc + bvc = c$ et par suite, comme $bc = ka$, l'égalité devient $auc + kav = c$, soit en factorisant $a(uc + kv) = c$.
Ainsi, $a \mid c$.

**Exemple :** Si 4 divise $3^{10} \times n$, comme 4 et $3^{10}$ sont premiers entre eux, on sait alors que 4 divise n.

**Remarque :** La condition « **a et b premiers entre eux** » est **essentielle** dans le théorème et la propriété qui en découle.
On peut proposer deux contre-exemples :
- 6 divise $8 \times 9 = 72$ mais 6 ne divise ni 8 ni 9.
- 4 et 6 divisent 12 mais $4 \times 6$ ne divise pas 12.

## III] Equation diophantienne :

### 1- Définition :

**Définition :** Une **équation diophantienne (E) de la forme : $ax + by = c$** est une **équation linéaire à deux inconnue du premier degré.**
D'après le corollaire du théorème de Bézout, **(E) admet des solutions si, et seulement si, c est un multiple de pgcd(a, b)**

### 2- Résoudre une équation diophantienne :

**Exemple :** Résoudre dans $Z^2$ l'équation $14x - 17y = 4$.

- **Vérifions que l'équation admet des solutions :**

14 et 17 sont premiers entre eux et 4 est un multiple de 1, donc d'après l'identité de Bézout, l'équation $14x - 17y = 4$ admet des solutions.
(14 et 17 étant premiers entre eux, l'équation n'est pas simplifiable)

- **Déterminons une solution particulière en remontant l'algorithme d'Euclide :**

$17 = 14 \times 1 + 3$ donc $3 = 17 - 14$
$14 = 3 \times 4 + 2$ donc $2 = 14 - 3 \times 4$
$3 = 2 \times 1 + 1$ donc $1 = 3 - 2$.

Ainsi, on a : $1 = 3 - 2$
Donc : $1 = 3 - (14 - 3 \times 4) = 3 \times 5 - 14$
Donc : $1 = (17 - 14) \times 5 - 14 = 14 \times (-6) + 17 \times 5$
On multiplie chaque membre de l'égalité par 4 :
$4 = 14 \times (-24) + 17 \times 20$ soit $14 \times (-24) - 17 \times (-20) = 4$.
Ainsi, **une solution particulière** de l'équation $14x - 17y = 4$ est **$(-24 ; -20)$.**

- **On modifie l'équation en utilisant cette solution particulière :**

$14x - 17y = 4 \Leftrightarrow 14x - 17y = 14 \times (-24) - 17 \times (-20)$
$\Leftrightarrow 14x + 14 \times 24 = 17y + 17 \times 20$
$\Leftrightarrow$ **$14(x + 24) = 17(y + 20)$**

**On termine la résolution de l'équation en déterminant toutes ses solutions :**
$14(x + 24) = 17(y + 20)$ donc 14 divise $17(y + 20)$, or 14 et 17 sont premiers entre eux, donc d'après le théorème de Gauss, 14 divise $y + 20$, donc il existe $k \in Z$ tel que $y + 20 = 14k$, d'où **$y = -20 + 14k$.**
Or $14(x + 24) = 17(y + 20)$, donc $14(x + 24) = 17 \times 14k$, d'où $x + 24 = 17k$ donc **$x = -24 + 17k$.**

**Réciproquement :**
Pour tout $k \in Z$, si $x = -24 + 17k$ et $y = -20 + 14k$, alors :

$14x - 17y = 14(-24 + 17k) - 17(-20 + 14k) = -14 \times 24 + 14 \times 17k + 17 \times 20 - 17 \times 14k = -336 + 340 = 4$
Donc (x ; y) est bien une solution de l'équation $14x - 17y = 4$.
**Conclusion :**
Les solutions de l'équation $14x - 17y = 4$ dans Z2 sont tous les couples d'entiers relatifs de la forme **$(-24 + 17k ; -20 + 14k)$, pour tout $k \in Z$**.

## 2- Inverse modulo n.

**Définition :** Soit a un entier relatif et soit n entier naturel supérieur ou égal à 2.
**a admet un inverse modulo n $\Leftrightarrow$ il existe un entier b tel que $ab \equiv 1$ [n].**
On dit que b est un inverse de a modulo n.
**Exemple :** $4 \times 3 = 12 = 11 + 1$, donc $4 \times 3 - 1 = 12$, donc $4 \times 3 \equiv 1$ [12]. Donc 4 est un inverse de 3 modulo 11.
**Propriété :** Soit a un entier relatif et soit n entier naturel supérieur ou égal à 2.
**a admet un inverse modulo n $\Leftrightarrow$ a et n sont premiers entre eux**.

**Démonstration :**
a admet un inverse modulo n $\Leftrightarrow$ il existe un entier b tel que $ab \equiv 1$ [n]
$\Leftrightarrow$ il existe deux entiers b et k tels que $ab - 1 = kn$
$\Leftrightarrow$il existe deux entiers b et k tels que $ab + (-k)n = 1$
$\Leftrightarrow$ a et n sont premiers entre eux (d'après le théorème de Bézout)

**Remarque :** Si a est inversible alors il possède un inverse unique entre 1 et $n - 1$, et une infinité d'inverses car ils sont tous définis modulo n.

**Exemples :**
1) Montrer que 7 possède un inverse modulo 22 puis donner celui compris entre 1 et 21.
- **7 et 22 sont premiers entre eux donc d'après la propriété précédente, 7 possède un inverse modulo 22. On cherche alors l'entier a compris entre 0 et 22 tel que $7a \equiv 1$ [22].**
**$22 = 7 \times 3 + 1$, donc $7 \times 3 \equiv -1$ [22] donc $7 \times (-3) \equiv 1$ [22], donc $-3$ est un inverse de 7 modulo 22, donc $-3 + 22 = 19$ aussi.**

2) Résoudre dans Z : $7x \equiv 5$ [22].
- **$7x \equiv 5$ [22] $\Leftrightarrow\Rightarrow -3 \times 7x \equiv 5 \times (-3)$ [22] (il y a bien équivalence grâce à l'inverse modulo).**
**Or $-3 \times 7 \equiv 1$ [22], donc $7x \equiv 5$ [22] $\Leftrightarrow\Rightarrow x \equiv -15$ [22] $\Leftrightarrow\Rightarrow x \equiv 7$ [22].**
**Les solutions de l'équation $7x \equiv 5$ [22] sont donc les entiers $x = 7 + 22k$, avec $k \in Z$.**