# IDENTITÉ DE BÉZOUT

## I - PGCD DE DEUX ENTIERS

### Théorème et définition

Si a et b sont deux entiers non nuls alors il existe un unique entier naturel d qui vérifie les deux conditions suivantes :
1) d divise a et d divise b
2) Si un entier k divise a et b alors il divise d
L'entier d défini plus haut est noté $a \wedge b$ et appelé plus grand commun diviseur de a et b

### Conséquence

Pour tout $(a;b) \in \mathbb{Z}^* \times \mathbb{Z}^*$

- $a \wedge b > 0$
- $a \wedge b = |a| \wedge |b|$

### Propriétés

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

- Si b divise a alors $a \wedge b = |b|$
- Si b ne divise pas a et si r est le reste modulo b de a alors $a \wedge b = b \wedge r$
- $a \wedge b = b \wedge a$
- $\forall\ k \in \mathbb{Z}^*$ , $ka \wedge kb = |k|(a \wedge b)$
- $\forall\ c \in \mathbb{Z}^*$ , $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

## II - ENTIERS PREMIERS ENTRE EUX

### Définition

Deux entiers non nuls a et b sont premiers entre eux, si $a \wedge b = 1$

**Exemple**

Soit n un entier naturel, $a = n+1$ et $b = n+9$

1) Si d est un diviseur commun de a et b alors d divise $b - a = 8 \Rightarrow d \in \{-8;-4;-2;-1;1;2;4;8\}$

2) Si n est pair alors a et b sont impairs donc a et b ne sont pas divisible par $2, 4$ et $8$

$\Rightarrow a \wedge b = 1 \Rightarrow$ si n pair, a et b sont premiers entre eux

### Théorème

Soit a et b deux entiers non nuls. Alors il existe un unique couple $(a';b')$ d'entiers tel que $a = (a \wedge b)a'$ , $b = (a \wedge b)b'$ et $a' \wedge b' = 1$

**Démonstration :**

Soit a et b deux entiers non nuls. Posons $d = a \wedge b$

$d = a \wedge b \Rightarrow$ il existe $(a';b') \in \mathbb{Z}^* \times \mathbb{Z}^*$ tel que $a = da'$ et $b = db'$

On en déduit que $d = a \wedge b = da' \wedge db' = d(a' \wedge b') \Rightarrow a' \wedge b' = 1$. L'unicité est évidente

### Lemme de Gauss

Soit a, b et c trois entiers non nuls
Si $a \wedge b = 1$ et a divise bc alors a divise c

**Démonstration :**

Soit a, b et c trois entiers non nuls tels que $a \wedge b = 1$

On a : $ac \wedge bc = |c|(a \wedge b) = |c|$

a divise bc $\Rightarrow$ il existe $k \in \mathbb{Z}$ tel que $bc = ka$

Donc $ac \wedge bc = |c| \Rightarrow ac \wedge ka = |c| \Rightarrow |a|(c \wedge k) = |c| \Rightarrow |a|\, d = |c|$ où $d = c \wedge k$

$\Rightarrow |a|$ divise $|c| \Rightarrow$ a divise c

### Théorème

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

Si $\left.\begin{array}{l} n \equiv 0 \,(\text{mod } a) \\ n \equiv 0 \,(\text{mod } b) \\ a \wedge b = 1 \end{array}\right\}$ alors $n \equiv 0 \,(\text{mod } ab)$

**Démonstration :**

Soit $(a;b) \in \mathbb{N}^* \times \mathbb{N}^*$ et $n \in \mathbb{Z}$ tels que $n \equiv 0 \,(\text{mod } a)$, $n \equiv 0 \,(\text{mod } b)$ et $a \wedge b = 1$

$\left.\begin{array}{l} a \text{ divise } n \Rightarrow \text{il existe } q \in \mathbb{Z} \text{ tel que } n = aq \\ b \text{ divise } n \Rightarrow \text{il existe } q' \in \mathbb{Z} \text{ tel que } n = bq' \end{array}\right\} \Rightarrow aq = bq'$ alors :

$\left.\begin{array}{l} b \text{ divise } aq \\ a \wedge b = 1 \end{array}\right\} \Rightarrow b$ divise $q \Rightarrow$ il existe $k \in \mathbb{Z}$ tel que $q = kb$

Par suite $n = aq = kab \Rightarrow ab$ divise n

## III - PPCM DE DEUX ENTIERS

### Théorème et définition

Pour tous entiers non nuls a et b il existe un unique entier naturel non nul m qui vérifie les deux conditions suivantes :
1) m est un multiple de a et b
2) Tout multiple commun de a et b est un multiple de m
L'entier m ainsi défini est le plus petit commun multiple de a et b et est noté $a \vee b$

**Démonstration :**

Soit $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}^*$ et $d = a \wedge b$, a' et b' les entiers tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$

On pose $m = d|a'b'|$

- $m = d|a'b'| = d|a'||b'| = |da'||b'| = |a||b'| \Rightarrow$ m est un multiple de $|a| \Rightarrow$ m est un multiple de a
- $m = d|a'b'| = d|a'||b'| = |a'||db'| = |b||a'| \Rightarrow$ m est un multiple de $|b| \Rightarrow$ m est un multiple de b

Par suite m est un multiple commun de a et b

Soit x un multiple commun de a et b .Montrons que x est un multiple de m

$\left.\begin{array}{l} x \text{ est un multiple de } a \Rightarrow \text{il existe } q \in \mathbb{Z} \text{ tel que } x = qa \\ x \text{ est un multiple de } b \Rightarrow \text{il existe } q' \in \mathbb{Z} \text{ tel que } x = q'b \end{array}\right\} \Rightarrow qa = q'b \Rightarrow qa'd = q'b'd$

$\Rightarrow qa' = q'b' \Rightarrow a'$ divise $q'b'$ et puisque $a' \wedge b' = 1$ alors $a'$ divise $q'$

$\Rightarrow$ il existe $k \in \mathbb{Z}$ tel que $q' = ka'$ donc $x = q'b = q'db' = ka'db' = k(da'b') \Rightarrow |x| = |k|m$

$\Rightarrow$ x est un multiple de m

Par suite $m > 0$ et tout multiple commun de a et b est un multiple de m

**Conséquences**

- $\forall (a;b) \in \mathbb{Z}^* \times \mathbb{Z}^*, a \vee b = |a| \vee |b|$
- $\forall (a;b) \in \mathbb{Z}^* \times \mathbb{Z}^* \ (a \vee b) \times (a \wedge b) = |ab|$

**Propriétés**

Soit a et b deux entiers non nuls

- Si b divise a alors $a \vee b = |a|$
- $\forall k \in \mathbb{Z}^*, \ ka \vee kb = |k|(a \vee b)$
- $a \vee b = b \vee a$
- $a \vee (b \vee c) = (a \vee b) \vee c$

**Exercice**

Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ le système $S : \begin{cases} ab = -1176 \\ a \vee b = 84 \end{cases}$

**Solution :**

$$S : \begin{cases} ab = -1176 \\ a \vee b = 84 \end{cases} \Leftrightarrow \begin{cases} (a \vee b).(a \wedge b) = 1176 \\ a \vee b = 84 \ ; ab < 0 \end{cases} \Leftrightarrow \begin{cases} a \wedge b = 14 \\ a \vee b = 84 \ ; ab < 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} a = 14a', b = 14b' \text{ et } a' \wedge b' = 1 \\ 14(a' \vee b') = 84 \ ; a'b' < 0 \end{cases} \Leftrightarrow \begin{cases} a = 14a', b = 14b' \text{ et } a' \wedge b' = 1 \\ a' \vee b' = 6 \ ; a'b' < 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} a = 14a', b = 14b' \text{ et } a' \wedge b' = 1 \\ |a'b'| = 6 \ ; a'b' < 0 \end{cases} \Leftrightarrow \begin{cases} a = 14a', b = 14b' \text{ et } a' \wedge b' = 1 \\ a'b' = -6 \end{cases}$$

$$\Leftrightarrow \begin{cases} a = 14a' \text{ et } b = 14b' \\ (a';b') \in \{(1;-6);(-1;6);(6;-1);(-6;1);(2;-3);(-2;3);(3;-2);(-3;2)\} \end{cases}$$

$$\Leftrightarrow (a;b) \in \{(14;-84);(-14;84);(84;-14);(-84;14);(28;-42);(-28;42);(42;-28);(-42;28)\}$$

Donc $S_{\mathbb{Z}\times\mathbb{Z}} = \{(14;-84);(-14;84);(84;-14);(-84;14);(28;-42);(-28;42);(42;-28);(-42;28)\}$

## IV- INVERSE MODULO B

**Théorème**

Soit a et b deux entiers naturels non nuls tels que $b \geq 2$ et $a \wedge b = 1$
Alors il existe un unique entier non nul u appartenant à $\{0,1,2,3,...,b-1\}$ tel que $au \equiv 1 (\text{mod } b)$ .On dit que u est un inverse de a modulo b

**Démonstration :**

Soit n et p deux entiers

$na \equiv pa (\text{mod } b) \Leftrightarrow (n-p)a \equiv 0 (\text{mod } b)$ et puisque $a \wedge b = 1$ alors :

$(n-p)a \equiv 0 (\text{mod } b) \Leftrightarrow$ b divise $n-p$ (*)

Soit i et j deux entiers tels que $0 \leq i < j \leq b-1$

$0 < j-i < b \Rightarrow$ b ne divise pas $j-i$ On déduit alors de (*) que ia et ja ont nécessairement des reste modulo b distincts

Par suite, à chaque élément ia de $E = \{0,a,2a,...,(b-1)a\}$ il correspond un unique reste appartenant $\{0,1,2,...,b-1\}$ donc la relation $au \equiv 1 (\text{mod } b)$ possède une unique solution dans $\{0,1,2,...,b-1\}$

**Exemple**

Déterminons un inverse de 3 modulo 5

| Reste modulo 5 de a | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Reste modulo 5 de 3a | 0 | 3 | 1 | 4 | 2 |

Alors 2 est un inverse de 3 modulo 5

Si x est une solution de $3x \equiv 1(\text{mod}\,5) \Rightarrow 3x \equiv 3\times 2(\text{mod}\,5) \Rightarrow 3(x-2) \equiv 0(\text{mod}\,5) \Rightarrow$ 5 divise $3(x-2)$ et comme 5 ne divise pas 3 alors 5 divise $x-2 \Rightarrow x \equiv 2(\text{mod}\,5)$

Réciproquement : Si $x \equiv 2(\text{mod}\,5) \Rightarrow 3x \equiv 1(\text{mod}\,5)$

Donc les solutions dans $\mathbb{Z}$ de l'équation $3x \equiv 1\ (\text{mod}\,5)$ sont tous les entiers $x = 5k+2, k \in \mathbb{Z}$

## V- IDENTITÉ DE BÉZOUT

### Théorème

> Deux entiers a et b sont premiers entre eux, si et seulement si il existe deux entier u et v tels que $au + bv = 1$

**Démonstration**

**1er cas** : Si a et b sont deux entiers naturels tels que $a \wedge b = 1$

- Si $b = 1$ alors $a\times 0 + b\times 1 = 1$ et les entiers 0 et 1 conviennent
- Si $b > 1$ alors la relation $au \equiv 1(\text{mod}\,b)$ admet une unique solution w dans $\{0;1;...;b-1\}$

Alors il existe un entier k tel que $aw = 1 + kb \Rightarrow aw - kb = 1$

Il suffit donc de prendre $u = w$ et $v = -k$

Réciproquement :

Supposons qu'il existe deux entiers u et v tels que $au + bv = 1$ alors tout diviseur d commun à a et b divise $1 \Rightarrow a \wedge b = 1$

**2ème cas** : Si $a \in \mathbb{Z}^*_-$ et $b \in \mathbb{N}^*$ alors $(-a) \in \mathbb{N}^*$

$a \wedge b = 1 \Leftrightarrow (-a) \wedge b = 1$ donc d'après le 1er cas : $(-a) \wedge b = 1 \Leftrightarrow$ il existe deux entiers u et v tels que $(-a)u + bv = 1 \Leftrightarrow a(-u) + bv = 1$ ce qui prouve le théorème

**3ème cas** : Si $b \in \mathbb{Z}^*_-$ et $a \in \mathbb{N}^*$ alors $(-b) \in \mathbb{N}^*$

$a \wedge b = 1 \Leftrightarrow a \wedge (-b) = 1$ donc d'après le 1er cas $a \wedge (-b) = 1 \Leftrightarrow$ il existe deux entiers u et v tels que $au + (-b)v = 1 \Leftrightarrow au + b(-v) = 1$ ce qui prouve le théorème

**4ème cas** : Si $a \in \mathbb{Z}^*_-$ et $b \in \mathbb{Z}^*_-$ alors $(-a) \in \mathbb{N}^*$ et $(-b) \in \mathbb{N}^*$

$a \wedge b = 1 \Leftrightarrow (-a) \wedge (-b) = 1$ donc d'après le 1er cas $(-a) \wedge (-b) = 1 \Leftrightarrow$ il existe deux entiers u et v tels que $(-a)u + (-b)v = 1 \Leftrightarrow a(-u) + b(-v) = 1$ ce qui prouve le théorème

### Corollaire

> Soit a et b deux entiers non nuls et $d = a \wedge b$ .Alors il existe deux entiers u et v tels que $au + bv = d$

**Démonstration :**

$a \wedge b = d \Rightarrow$ il existe deux entiers a' et b'tels que $a = da'$ , $b = db'$ et $a' \wedge b' = 1$

D'après le théorème de Bézout il existe deux entiers u et v tels que

$a'u + b'v = 1 \Leftrightarrow da'u + db'v = d \Leftrightarrow au + bv = d$

## VI- EXEMPLES D'ÉQUATIONS DE LA FORME $ax + by = c$ ; a, b et c entiers

### Théorème

> Soit a, b et c trois entiers et $d = a \wedge b$ .Alors l'équation $ax + by = c$ admet des solutions dans $\mathbb{Z}\times\mathbb{Z}$ si et seulement si d divise c

**Démonstration**

Soit a, b et c trois entiers et $d = a \wedge b$.

On considère dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $(E): ax + by = c$

$a \wedge b = d \Rightarrow$ il existe deux entiers a' et b' tels que $a = da'$ , $b = db'$ et $a' \wedge b' = 1$

Si d divise c alors il existe un entier c' tel que $c = dc'$

Donc l'équation (E) est équivalente à l'équation $a'x + b'y = c'$

Et puisque $a' \wedge b' = 1$, d'après le théorème de Bézout il existe deux entiers u et v tels que

$a'u + b'v = 1 \Rightarrow a'c'u + b'c'v = c'$ donc le couple $(c'u, c'v)$ est une solution de (E) dans $\mathbb{Z}\times\mathbb{Z}$

Réciproquement : Si $(x_0; y_0)$ est une solution de (E) dans $\mathbb{Z}\times\mathbb{Z}$ alors

$ax_0 + by_0 = c \Rightarrow d(a'x_0 + b'y_0) = c \Rightarrow$ d divise c

**Exercice**

Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $1075x + 64y = 9$

**Solution :**

Déterminons $1075 \wedge 64$ en utilisant l'algorithme d'Euclide

$1075 = 64\times16 + 51$

$64 = 51\times1 + 13$

$51 = 13\times3 + 12$ Alors $1075 \wedge 64 = 1$ divise $9 \Rightarrow$ (E) admet des solutions dans $\mathbb{Z}\times\mathbb{Z}$

$13 = 12\times1 + 1$

$12 = 12\times1 + 0$

Cherchons une solution particulière de (E)

Soit $a = 1075$ et $b = 64$

On a : $51 = 1075 - 16\times64 = a - 16b$

$13 = 64 - 51\times1 = b - (a - 16b)$

$12 = 51 - 3\times13 = a - 16b - 3\big(b - (a - 16b)\big)$

$1 = 13 - 12\times1 = b - (a - 16b) - \big(a - 16b - 3\big(b - (a - 16b)\big)\big) = -5a + 84b$

Donc $-45a + 756b = 9 \Rightarrow (-45; 765)$ est une solution particulière de (E) dans $\mathbb{Z}\times\mathbb{Z}$

Ainsi $\begin{cases} 1075x + 64y = 9 \\ -45\times1075 + 756\times64 = 9 \end{cases} \Rightarrow 1075(x + 45) + 64(y - 756) = 0$

$\Rightarrow 1075(x + 45) = -64(y - 756)$

$\Rightarrow 64$ divise $1075(x + 45)$ et puisque $64 \wedge 1075 = 1$ alors 64 divise $x + 45$

$\Rightarrow$ il existe $k \in \mathbb{Z}$ tel que $x = 64k - 45$

Donc $\begin{cases} 1075(x + 45) = -64(y - 756) \\ x = 64k - 45 \text{ , } k \in \mathbb{Z} \end{cases} \Rightarrow \begin{cases} y = -1075k + 756 \\ x = 64k - 45 \end{cases}$ , $k \in \mathbb{Z}$

Réciproquement : pour tout entier k

$1075(64k - 45) + 64(-1075k + 756) = -1075\times45 + 64\times756 = 9$

Alors $S_{\mathbb{Z}\times\mathbb{Z}} = \{(64k - 45; -1075k + 756) \ ; k \in \mathbb{Z}\}$