Soient a et b deux entiers relatifs non nuls, et soit δ leur PGCD :

L'ensemble des multiples de δ est identique à l'ensemble des entiers relatifs de la forme $au + bv$, pour toutes les valeurs de u et v prises dans $\mathbb{Z}$.

Autrement dit : $x = au + bv \Leftrightarrow x = k\delta$, avec $k , u , v \in \mathbb{Z}$ et $\delta = \text{PGCD}(|a| , |b|)$.

Preuve :

1) Soit $x = au + bv$, avec $u , v \in \mathbb{Z}$, montrons $x = k\delta$, avec $k \in \mathbb{Z}$:

$\delta \mid a \Rightarrow a = \delta a'$, $a' \in \mathbb{Z}$, $\delta \mid b \Rightarrow b = \delta b'$, $b' \in \mathbb{Z}$, d'où $x = au + bv = \delta(a'u + b'v) = k\delta$.

2) Soit $x = k\delta$, avec $k \in \mathbb{Z}$, montrons $x = au + bv$, avec $u , v \in \mathbb{Z}$:

Soit δ' le plus petit élément *strictement positif* de $E = \{ au + bv , \forall u , v \in \mathbb{Z} \}$, donc s'écrivant $au + bv$.

Montrons tout d'abord que α est diviseur de tous les termes de la forme $au + bv$, ou ce qui est totalement équivalent $|a|u + |b|v$:

Si α ne divise pas exactement un terme positif $x = |a|u + |b|v$, la *division euclidienne* de x par α donne :

$x = q\alpha + r$ avec $0 < r < \alpha$, soit $r = x - q\alpha = (|a|u + |b|v) - (|a|u' + |b|v')$ puisque α , qui appartient lui-même à E , s'écrit sous la forme $\alpha = |a|u' + |b|v'$.

(remarquer que si l'on avait choisi un $x < 0$, $x = |a|u + |b|v$, il serait l'opposé de $x' = -x = |a|(-u) + |b|(-v)$, et le raisonnement s'appliquerait à x').

Donc, $r = |a|(u' - u) + |b|(v' - v) \in E$, avec $r > 0$ et $r < \alpha$, ce qui est en contradiction avec le fait que α soit le plus petit entier positif de E .

On conclue $r = 0$, soit $x = q\alpha$.

Tout entier $au + bv$ est multiple de α , le plus petit entier positif de cette forme, soit $au + bv = k\alpha$, $k \in \mathbb{Z}$.

Nous avons vu au 1) que $au + bv = k\delta$, donc $\alpha = k\delta$, avec $\delta = \text{PGCD}(|a| , |b|)$.

$a = a.1 + b.0 \in E \Rightarrow a = K\alpha$ et $b = a.0 + b.1 \in E \Rightarrow b = K'\alpha$, donc α est diviseur commun de a et b , or: * Tout diviseur commun de a et b est diviseur de leur PGCD , δ , d'où $\delta = k'\alpha$.

$\alpha = k\delta$ et $\delta = k'\alpha$, avec $k , k' \in \mathbb{N}^* \Rightarrow \alpha = \delta$.

On conclue donc $x = k\delta = k\alpha = k(|a|u' + |b|v') = aU + bV$, avec $U , V \in \mathbb{Z}$.

Tout $x = k\delta$ s'écrit sous la forme $au + bv$, d'où le théorème initial.

Conséquence 1 : Théorème de Bézout :

Si δ = PGCD(a , b) , il existe u , $v \in \mathbb{Z}$ tels que $au + bv = \delta$.

C'est une conséquence de $\alpha = \delta$.

Conséquence 2 : Théorème de Gauss :

Si a divise exactement bc , alors que a est premier avec b , alors a divise exactement c .

Preuve :

a premier avec $b \Leftrightarrow$ PGCD (a , b) = 1 , noté $a \wedge b = 1 \Leftrightarrow \delta = 1$.

D'après le théorème de Bézout : Il existe u , $v \in \mathbb{Z}$ tels que $au + bv = \delta = 1$.

$au + bv = 1 \Rightarrow acu + bcv = c$.

Comme $a \mid ac$ (a divise exactement ac) et $a \mid bc$, par hypothèse , on déduit $a \mid c$.

Application : Résolution d'équations de la forme $au + bv = c$ avec a , b , c connus dans $\mathbb{Z}$, et u , v à déterminer dans $\mathbb{Z}$.

Résoudre : $4x + 12y = 23$ dans $\mathbb{Z}$.

2 divise $4x$ et $12y$, donc divise $4x + 12y$, alors que 2 ne divise pas 23. Il ne peut donc exister de solution.

Résoudre : $8x + 12y = 22$ dans $\mathbb{Z}$.

δ = PGCD (8 ; 12) = 4 .

4 divise $8x + 12y$, mais ne divise pas exactement $22 = 2 \times 11$. Il ne peut donc exister de solution.

Résoudre : $8x + 12y = 32$ dans $\mathbb{Z}$.

δ = PGCD (8 ; 12) = 4 .

a) *Simplifier préalablement par* PGCD($|a|$, $|b|$) :

L'équation devient : $2x + 3y = 8$

b) *Invoquer le Théorème de Bézout, selon lequel, il existe une solution* (u , v) *à* $au + bv = \delta$, puis :

Inventer *une solution particulière de* $2x + 3y = 1$:

(u , v) = (-1 ; +1) vérifie $2u + 3v = 1$.

c) *Soustraire la* **solution particulière** (u , v) *de* $2x + 3y = 1$ *de sa* **solution générale** (x , y) *:*

$\begin{cases} 2x + 3y = 1 \\ 2u + 3v = 1 \end{cases} \Rightarrow 2(x - u) - 3(y - v) = 0$, soit $2(x + 1) = 3(y - 1)$.

d) *Appliquer le Théorème de Gauss* :

$2 \mid 3(y - 1)$, or PGCD(2 ; 3) = 1 , donc $2 \mid y - 1 \Rightarrow y - 1$ multiple de $2 \Rightarrow y - 1 = 2k$, $k \in \mathbb{Z}$.

Report dans $2(x + 1) = 3(y - 1) \Rightarrow 2(x + 1) = 3(2k) \Rightarrow x + 1 = 3k$ (*remarquer qu'il s'agit du même k*)

Conclusion : $8x + 12y = 32$ admet une infinité de couples solutions $(x ; y) \in \mathbb{Z} \times \mathbb{Z}$, de la forme :

$x = -1 + 3k$, $y = 1 + 2k$ pour tout $k \in \mathbb{Z}$.