Proposition : *(Identité de Bézout)*

Soit a et b deux entiers relatifs non-nuls. On note d le *PGCD* de a e de b :
$d = \text{pgcd}\,(a\,;b)$.
Il existe au moins un couple d'entiers relatifs $(u\,;v)$ tel que : $u{\cdot}a + v{\cdot}b = d$

Démonstration :

Soit E l'ensemble formé par l'ensemble des nombres de la forme : $u{\cdot}a + v{\cdot}b$ où $u{\in}\mathbb{Z}$ et $v{\in}\mathbb{Z}$.
On peut noter l'ensemble E sous la forme :
$E = \left\{u{\cdot}a{+}v{\cdot}b \;\middle|\; u{\in}\mathbb{Z},\, v{\in}\mathbb{Z}\right\}$

On note F l'ensemble des nombres strictement positifs contenus dans E. C'est-à-dire : $F = E \cap \mathbb{N}^*$.

Montrons que F n'est pas vide. Effectuons une disjonction de cas sur le signe de a *(a est non nul)* :

- Si $a > 0$ alors $1{\cdot}a + 0{\cdot}b > 0$
  Ainsi, $a{\in}F$: F est non-vide.
- Si $a < 0$ alors $(-1){\cdot}a + 0{\cdot}b > 0$
  Ainsi, $-a{\in}F$: F est non-vide.

F est un sous-ensemble non vide de $\mathbb{N}$. On admet alors qu'il possède un plus petit élément. Notons k ce plus petit élément et $(u_0\,;v_0)$ le couple d'entiers relatifs définissant k comme un élément de E : $k = u_0{\cdot}a + v_0{\cdot}b$

Nous alllons montrer que ce plus petit élément est $\text{pgcd}\,(a\,;b)$. C'est à dire que $k{=}d$.

- La division euclidienne de a par k donne l'existence d'un couple d'entiers relatifs $(q\,;r)$ vérifiant :
  $a = q{\cdot}k + r \quad ; \quad 0{\leqslant}r{<}k$.
  On a les égalités suivantes :
  $$a = q{\cdot}k + r \implies a = q{\cdot}\left(u_0{\cdot}a + v_0{\cdot}b\right) + r$$
  $$\implies a - q{\cdot}u_0{\cdot}a - q{\cdot}v_0{\cdot}b = r$$
  $$\implies (1 - q{\cdot}u_0){\cdot}a + (-q{\cdot}v_0){\cdot}b = r$$
  On vient de montrer que $r{\in}E$.
  Montrons que l'entier r est nul par un raisonnement par l'absurde :
  > Supposons que $r{>}0$. Ainsi, on a $r{\in}F$ et il vérifie $r{<}k$. Ces résultat contredisent le fait que k est le plus petit élément de F.

  On en déduit que : $r{\leqslant}0$. Ainsi, on vient de montrer que $r{=}0$.
  Le reste de la division euclidienne de a par k étant nul : l'entier k divise a.
  Par un raisonnement similaire sur l'entier b, on montre que l'entier k divise b.
  k étant un diviseur commun aux entiers a et b, on en déduit que k divise $\text{pgcd}\,(a\,;b)$: **k divise d**.
- d est le *PGCD* des entiers a et b. Ainsi, on a :
  - d divise $a \implies d$ divise $u_0{\cdot}a$;
  - d divise $b \implies d$ divise $v_0{\cdot}b$;

  Ainsi, d divise $u_0{\cdot}a + v_0{\cdot}b$: **d divise k**.

On vient de montrer que "k divise d" et que "d divise k".
On en déduit : $d = k = a{\cdot}u_0 + b{\cdot}v_0$

Ce qui montre l'existence du couple d'entiers relatifs recherché.

Théorème : *(de Bézout)*

Soit a et b deux entiers relatifs non-nuls.
$\text{pgcd}\,(a\,;b) = 1$ si, et seulement si, il existe un couple d'entiers relatifs $(u\,;v)$ tel que : $u{\cdot}a + v{\cdot}b = 1$.

Démonstration :

- $\text{pgcd}\,(a\,;b) = 1 \implies \exists\,(u\,;v)\,,\ u{\cdot}a{+}v{\cdot}b{=}1$
  Cette implication est établie par l'identité de Bézout.
- $\exists\,(u\,;v)\,,\ u{\cdot}a{+}v{\cdot}b{=}1 \implies \text{pgcd}\,(a\,;b) = 1$
  Supposons l'existence du couple $(u\,;v){\in}\mathbb{Z}{\times}\mathbb{Z}$ tel que : $u{\cdot}a + v{\cdot}b = 1$
  Notons $d{=}\text{pgcd}\,(a\,;b)$. Il existe k et k' deux entiers relatifs vérifiant : $a = k{\cdot}d \quad ; \quad b = k'{\cdot}d$
  On a les égalités suivantes :
  $$u{\cdot}a + v{\cdot}b = 1 \implies u{\cdot}\left(k{\cdot}d\right) + v{\cdot}\left(k'{\cdot}d\right) = 1$$
  $$\implies d{\cdot}\left(k{\cdot}u + k'{\cdot}v\right) = 1$$
  On en déduit que d divise 1. Donc $d{=}1$.
  Ce qui établit l'implication réciproque.

Théorème : *(de Gauss)*

Soit a, b et c trois entiers relatifs non-nuls.
Si a divise $b{\cdot}c$ et si a et b sont premiers entre eux alors a divise c

Démonstration :

a divise $b{\cdot}c$. On en déduit l'existence d'un entier relatif k tels que : $b{\cdot}c = k{\cdot}a$

a et b étant premiers entre eux : $\text{pgcd}\,(a\,;b) = 1$.
D'après l'identité de Bézout, on en déduit l'existence d'un couple d'entiers $(u\,;v)$ vérifiant : $a{\cdot}u{+}b{\cdot}v = 1$

On a les égalités suivantes :
$$a{\cdot}u + b{\cdot}v = 1 \implies c{\cdot}\left(a{\cdot}u + b{\cdot}v\right) = c$$
$$\implies a{\cdot}(u{\cdot}c) + (b{\cdot}c){\cdot}v = c$$
D'après la première remarque :
$$\implies a{\cdot}(u{\cdot}c) + (k{\cdot}a){\cdot}v = c \implies a{\cdot}(u{\cdot}c + v) = c$$
L'égalité précédente montre que l'entier a divise c.

Corollaire :

Soit a, b et c trois entiers relatifs non-nuls.
Si $\text{pgcd}\,(a\,;b) = 1$ et si a et b divisent c alors $a{\cdot}b$ divise c.

Preuve :

Puisque a divise c, il existe un entier relatif k vérifiant :
$c = k{\cdot}a$
Puisque b divise c, alors b divise $k{\cdot}a$.

Or, a et b sont premiers entre eux et b divise le produit $k{\cdot}a$. D'après le théorème de Gauss, on en déduit que b divise k.
On en déduit l'existence d'un entier relatif k' vérifiant :
$b = k'{\cdot}k$.

Ainsi, on a les égalités suivantes :
$$c = k{\cdot}a \implies c = \left(k'{\cdot}b\right){\cdot}a \implies c = k'{\cdot}\left(a{\cdot}b\right)$$
On vient de montrer que $a{\cdot}b$ divise l'entier relatif c.