

II Théorème de BÉZOUT - Théorème de GAUSS

Propriété:

Soient a et b 2 entiers relatifs non simultanément nuls

Soit $d = \text{PGCD}(a, b)$

1. Il existe 2 entiers relatifs u et v tels que $au + bv = d$

2. L'ensemble des entiers $au + bv$ (u et v entiers relatifs) est l'ensemble des multiples de d .

Démonstration:

1. Existence à l'aide de l'algorithme d'Euclide

$$a = bq_0 + r_0 \Rightarrow r_0 = a - bq_0 = au_0 + bv_0 \quad (u_0 = 1 \text{ et } v_0 = -q_0)$$

$$\begin{aligned} b &= q_1 r_0 + r_1 \Rightarrow r_1 = b - q_1 r_0 = b - q_1 (au_0 + bv_0) \\ &= a(-u_0 q_1) + b(1 - q_1 v_0) \\ &= au_1 + bv_1 \quad (u_1 = -u_0 q_1 \quad v_1 = 1 - q_1 v_0) \end{aligned}$$

etc ... jusqu'au dernier reste non nul qui est d

2. $\Rightarrow$ Soit $n = au + bv$ un entier

$$\begin{cases} d \mid a \\ d \mid b \end{cases} \Rightarrow d \mid au + bv \Leftrightarrow d \mid n$$

donc n est un multiple de d

$\Rightarrow$ Réciproquement

si n est un multiple de d Alors il existe $k \in \mathbb{Z}$ tel que $n = kd$
on sait d'après 1. il existe u et v tels que $d = au + bv$

$$\text{donc } n = k(au + bv) = aku + bkv = aU + bV$$

$$\text{avec } U = ku \text{ et } V = kv$$

donc n s'écrit comme combinaison linéaire entière de a et b

Théorème de BÉZOUT

Deux entiers relatifs a et b sont premiers entre eux

[ssi] il existe des entiers relatifs u et v tels que $au + bv = 1$

Démonstration:

$\Rightarrow$ / a et b sont premiers entre eux $\Rightarrow \text{PGCD}(a, b) = 1$

$\Rightarrow$ il existe u et v tels que $au + bv = 1$ (propriété précédente)

$\Leftarrow$ / Il existe 2 entiers tels que $au + bv = 1$

soit d'un diviseur commun de a et b

$$\begin{cases} d \mid a \\ d \mid b \end{cases} \Rightarrow d \mid au + bv \Rightarrow d \mid 1 \Rightarrow d = 1 \text{ ou } d = -1$$

donc $\text{PGCD}(a, b) = 1$

Théorème de GAUSS

Soient a, b et c 3 entiers non nuls

[Si] a divise bc [et si] a et b sont premiers entre eux

[Alors] a divise c

Démonstration:

• $a \mid bc \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $bc = ka$

• $\text{PGCD}(a, b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$ (BÉZOUT)

donc $c au + cbv = c$

$$\Rightarrow cau + k av = c$$

$$\Rightarrow a(cu + kv) = c \quad \text{donc } a \mid c$$

Conséquence:

[Si] $a \mid c$ et $b \mid c$ avec $\text{PGCD}(a, b) = 1$

[Alors] $ab \mid c$

Démonstration: $a \mid c \Rightarrow c = ka$

$b \mid c \Rightarrow b \mid ka \xrightarrow{\text{GAUSS}} b \mid k \Rightarrow k = kb \Rightarrow c = kba \Rightarrow ab \mid c$