

# PGCD - PPCD BÉZOUT ET GAUSS

## IPGCD

### 1°) Ensembles de diviseurs

Notation: Soit  $a$  un entier relatif,

on note  $D(a)$  l'ensemble des diviseurs de  $a$

exps :

$$\bullet D(6) = \{1, 2, 3, 6, -1, -2, -3, -6\}$$

$$\bullet D(0) = \mathbb{Z}^*$$

$$\bullet D(1) = \{1, -1\}$$

### Propriété:

Soient  $a$  et  $b$  2 entiers relatifs.

On note  $D(a, b)$  l'ensemble des diviseurs communs à  $a$  et  $b$

On a alors  $D(a, b) = D(a-b, b) = D(a-kb, b) \quad \forall k \in \mathbb{Z}$

Démonstration:

$\Rightarrow$ ) Soit  $d$  un diviseur commun de  $a$  et de  $b$

$$\begin{cases} d|a \\ d|b \end{cases} \Rightarrow d|a-b \Rightarrow d|a-kb \quad \begin{array}{l} \text{propriété de combinaison} \\ \text{linéaire (voir divisibilité)} \end{array}$$

$\Leftarrow$ ) Soit  $d$  un diviseur commun à  $(a-kb)$  et  $b$

$$\begin{cases} d|a-kb \\ d|b \end{cases} \Rightarrow \begin{cases} d|a-kb \\ d|kb \end{cases} \Rightarrow d|(a-kb)+kb \Rightarrow d|a$$

Rq:  $D(0, a) = D(a)$

### Corollaire:

1) [SI]  $0 < b \leq a$  [Alors]  $D(a, b) = D(r, b)$

où  $r$  est le reste de la division euclidienne de  $a$  par  $b$

2) [SI]  $b$  divise  $a$  [Alors]  $D(a, b) = D(b)$

Démonstration:

1. trivial avec  $a = bq + r$ .

2.  $b|a \Rightarrow r = 0 \Rightarrow D(a, b) = D(0, b) = D(b)$

## 2°) PGCD de 2 entiers

### Définition:

Si  $a$  et  $b$  sont deux entiers relatifs non simultanément nuls, le Plus Grand Commun Diviseur de  $a$  et  $b$ , noté  $\text{PGCD}(a, b)$  est le plus grand élément de  $D(a, b)$

### Conséquences immédiates

- le PGCD est un entier strictement positif
- $\text{PGCD}(a, b) = \text{PGCD}(b, a) = \text{PGCD}(|a|, |b|)$
- [Si]  $0 < b \leq a$  [Alors]  $\text{PGCD}(a, b) \leq b$
- $a$  et  $b$  sont premiers entre eux [ssi]  $\text{PGCD}(a, b) = 1$
- $\text{PGCD}(-1; b) = 1$
- $\forall b \neq 0 \quad \text{PGCD}(0, b) = |b|$

### Propriétés: Réduction du PGCD

- $\text{PGCD}(a, b) = \text{PGCD}(a - b, b) = \text{PGCD}(a - kb, b) \quad \forall k \in \mathbb{Z}$
- [Si]  $0 < b \leq a$  [Alors]  $\text{PGCD}(a, b) = \text{PGCD}(r, b)$   
où  $r$  est le reste dans la division euclidienne de  $a$  par  $b$
- [Si]  $b$  est un diviseur positif de  $a$  [Alors]  $\text{PGCD}(a, b) = b$