

Séance du 13/11/19.

Spe' Maths.

$$a|b \quad \boxed{\Leftrightarrow} \quad \exists k \in \mathbb{Z} \text{ t. q. } b = ak.$$

$$a|b \quad \text{et} \quad a|c \quad \boxed{\Rightarrow} \quad \exists (\alpha, \beta) \in \mathbb{Z}^2$$

t. q.  $a | (\alpha b + \beta c)$ .

✓ il existe un unique

Division euclidienne de  $a$  par  $b$ ,  $\exists! (q, r) \in \mathbb{Z}^2$

$$a = bq + r \quad \text{t. q.} \quad 0 \leq r < b.$$

$$34 \quad 21$$

$$\downarrow \quad \downarrow$$

$$1 \quad 1$$

$$2 \quad 3$$

$$17$$

$$7$$

$$34$$

$$21$$

$$\text{PGCD}(34; 21) = 1.$$

$$\text{PGCD}(ka; kb).$$

$$\text{PGCD}(ka; kb) = k \times \text{PGCD}(a; b).$$

$$\text{PGCD}(\overset{9}{3 \times 3}; \overset{6}{3 \times 2}) = 3 \times \text{PGCD}(3; 2)$$

$\begin{matrix} & a & b \\ \times & & \end{matrix}$

$$\star \text{PGCD}(9; 6) = 3$$

$$\star 3 \times \text{PGCD}(3; 2) = 3 \times 1 = 3$$

$$\frac{1}{6 \times 2} + \frac{1}{4 \times 3} \quad \text{PGCD}(a; b) = D$$

$$\Rightarrow \exists (u; v) \in \mathbb{Z}^2$$

$$t.q. \quad au + bv = D.$$

$$\text{PGCD}(32; 44) = 4.$$

$\Rightarrow$

$$\exists (u; v) \in \mathbb{Z} \quad t.q.$$

$$32x u + 44x v = 4.$$

$$32u = 4 - 44v$$

$$y \quad u = \frac{4 - 44v}{32}$$

Egalité de Bezout:

$$\exists \text{int}(a; b) \in \mathbb{Z}^2 \quad \text{PGCD}(a; b) = D \Rightarrow \exists (u; v) \in \mathbb{Z}^2 \quad t.q.$$

$$au + bv = D.$$

Soient  $a$  et  $b$  deux entiers non nuls.

$$E = \{ ma + nb \mid (m; n) \in \mathbb{Z}^2 \}. \text{ Constitués d'éléments strictement } \oplus$$

$E$  est non vide.  $|b| \in E$ .

$E$  contient donc un plus petit élément.  $\{ 4; 8; 1; 25 \dots \}$

Soit  $d$  le plus petit élément de  $E$ .

$$\text{donc } d = au + bv.$$

$$x \in ]2; 3[.$$

$$\text{On pose: } \text{PGCD}(a; b) = D \Rightarrow D/a \text{ et } D/b.$$

$$D/(au + bv).$$

$$D/d. \Rightarrow \boxed{D \leq d}.$$

$\exists q$   $d$  divise  $a$ :  $a = dq + r$ . où  $0 \leq r < d$

On suppose  $r \neq 0$ .

$$r = a - dq.$$

$$r = a - (au + bv) \times q.$$

$$r = a - auq - bvq. \quad r = b(1 - vq) + a(uq)$$

$$r = \underbrace{a(1 - uq)}_M + \underbrace{b(-vq)}_N.$$

$\Downarrow$   
 $d \mid b$ .

$$r \in E \quad \# \quad r < d.$$

$$\Rightarrow r = 0.$$

$$a = dq \Rightarrow d \mid a$$

$d \mid a$  et  $d \mid b$ .  $d$  est un diviseur commun de  $a$  et  $b$ .

$$\Rightarrow \boxed{d \leq D} \quad \Rightarrow \boxed{D = d = au + bv}.$$

Or  $\boxed{D \leq d}$ .

