Preuve cours 1.4

- Si $a \equiv b\,[n]$ alors $b \equiv a\,[n]$.

$a \equiv b\,[n] \Rightarrow a = Kn + b$

Donc $b = a - Kn$

$a = K_1 n + b$

$b = K_2 n + a \Rightarrow a = b - K_2 n$

Donc $\begin{cases} a = K_1 a + b \\ a = b - K_2 n \end{cases} \Rightarrow K_1 n + b - b + K_2 n$

$\boxed{a = n(K_1 + K_2)}$

Donc $\begin{cases} b = K_2 n + a \\ b = a - K_2 n \end{cases} \Rightarrow b = K_1 n - a + a + K_2 n$

$\boxed{b = n(K_1 + K_2)}$

Donc $n(K_1 + K_2) \equiv n(K_1 + K_2)\,[n]$

CQFD

an iota

- Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$.

$a \equiv b\,[n] \Rightarrow \exists k_1 \in \mathbb{Z} \mid a = k_1 n + b$

$b \equiv c\,[n] \Rightarrow \exists k_2 \in \mathbb{Z} \mid b = k_2 n + c$

Donc $a = k_1 n + \underbrace{(k_2 n + c)}_{}$

$a = n(k_1 + k_2) + c$

Soit $K = k_1 + k_2 \mid a = Kn + c$

Donc $a \equiv c\,[n]$ CQFD

Si $a \equiv c\,[n]$ et $b \equiv d\,[n]$ alors $a + b \equiv c + d\,[n]$.

Si $a \equiv c\,[n] \Rightarrow \exists k_1 \in \mathbb{Z} \mid a = k_1 n + c$ ①

Si $b \equiv d\,[n] \Rightarrow \exists k_2 \in \mathbb{Z} \mid b = k_2 n + d$ ②

① $\Leftrightarrow a - k_1 n - c = 0$

② $\Leftrightarrow b - k_2 n - d = 0$

⋮

Définition

Soient $a, b \in \mathbb{Z}$ non tous deux nuls (c.a.d. $a \neq 0$ ou $b \neq 0$).
Le plus grand entier qui divise a et b s'appelle le **plus grand diviseur commun** de a et b et se note $\mathrm{pgcd}(a, b)$.

$$PGCD = \max(\mathrm{div}(a) \cap \mathrm{div}(b))$$

avec $a, b \in \mathbb{Z}$ & $a \neq 0$ ou $b \neq 0$

Propriété fondamentale pour l'algorithme d'Euclide

Soient a et b des entiers **positifs** avec b **non nul**.
Si r est le reste de la division euclidienne de a par b alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.

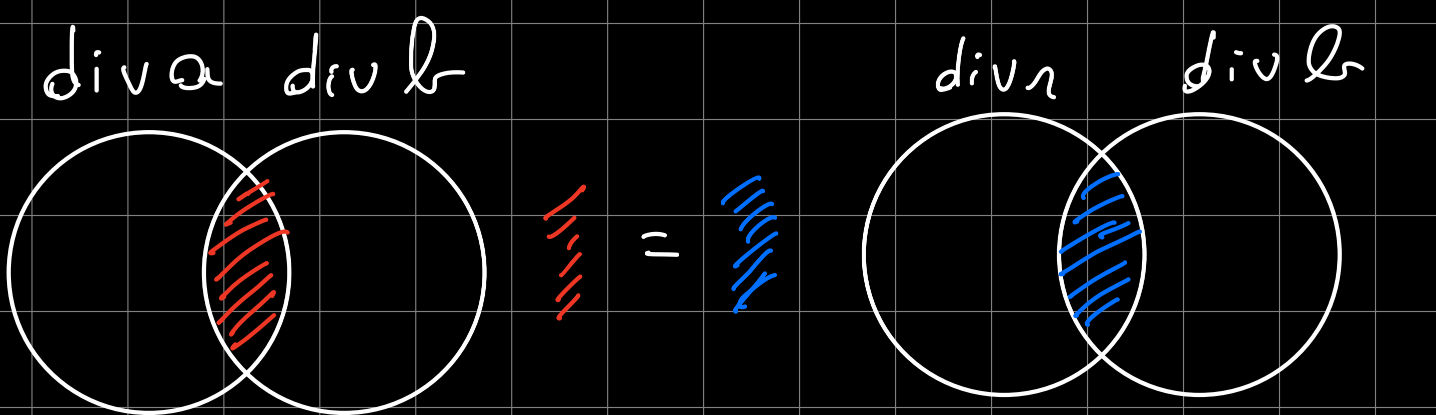
Preuve de l'algo de PGCD d'Euclid

Nous allons procédé par double inclusion :

Nous allons montré que

$$\mathrm{div}(a) \cap \mathrm{div}(b) \subset \mathrm{div}(b) \cap \mathrm{div}(r)$$

& $$\mathrm{div}(b) \cap \mathrm{div}(r) \subset \mathrm{div}(a) \cap \mathrm{div}(b)$$



On peut faire cela grace à la propriété qui dit : Si $a|b$ et $a|c$, $a|\alpha b+\beta c$.

On sait que $div(b) \cap div(r) = div(a) \cap div(b)$
et par conséquent $\max(div(b) \cap div(r))$
$= \max(div(a) \cap div(b))$.

https://youtu.be/8YUSAI4BzsY?si=PQa0Isrg1MNMUarf ← preuve

$A = div(a) \cap div(b)$, $B = div(b) \cap div(r)$

Tout d'abord, on va montrer que $\forall x \in A$, $x \in B$ et vice-versa

Soit $d \in A$, $d|a$ & $d|b$, donc
$d | \alpha a + \beta b$, α et $\beta \in \mathbb{Z}$.

$a = bn + r \qquad 0 \leq r < n$
$\Leftrightarrow r = a - bn \qquad 0 \leq r < n$

On $d|b$, donc $d|bn$, et $d|a$
Donc $d | a - bn$ ← (combi linéaire)

alor d | r.

Propriété

Soient a et b des entiers **non nuls**, les quotients de a et b par pgcd(a, b) sont des nombres premiers entre eux.

Théorème de Bezout

Soient a et b des entiers **positifs non nuls**, alors il existe des entiers u et v tels que pgcd$(a, b) = a\,u + b\,v$.

a et b sont ~~parement~~ premier entre eux ssi PGCD(a, b) = 1

$a/\text{pgcd}(a, b)$ et $b/\text{pgcd}(a, b)$ sont 1^er^ entre eux

12, 15, $\text{pgcd}(12, 15) = 3$

$\Rightarrow 12/3 = 4,\ 15/3 = 5$ 4 et 5 sont 1^er^ entre eux !

afin de prouvé cela, il faut prouvé que :

$\text{div}(a/\text{PGCD}(a, b)) \cap \text{div}(b/\text{PGCD}(a, b)) = \{1\}$

Determinons Tout d'abord $\text{div}(a/\text{PGCD}(a, b))$:

$66, 30, 6$

$66/6 = 11, \quad 30/6 = 5$

$\operatorname{div}(11) \cap \operatorname{div}(5) = \{1\}$