

Coef. de Bézout: Si $a, b \in \mathbb{Z}^*$ alors il existe x et $y \in \mathbb{Z}$
tels que $a \cdot x + b \cdot y = \text{PGCD}(a, b)$

⚠ x et y sont ENTIERES !

Si a et b sont PREMIERS entre eux alors $\text{PGCD}(a, b) = 1$
et il y a au moins une solution entière à
 $ax + by = 1$!

⚠ On dit que a divise b si: $b = n \cdot a$ où a, b et $n \in \mathbb{Z}$
autrement dit si $b \bmod a = 0$!

3 ne divise pas 10 car $\frac{10}{3} \notin \mathbb{Z}$!

2 divise 10 car $\frac{10}{2} = 5 \in \mathbb{Z}$!

$$\begin{array}{r|l} b & a \\ \hline 0 & n \\ \uparrow & \\ \text{rest } 0 & \end{array}$$

Arithmétique Modulaire: (Gauss, 1801)

Modulo:

on dit que $a \bmod N = b$ si

← reste de la division entière

$$\begin{array}{r|l} a & N \\ b & k \end{array}$$

$$a = k \cdot N + b \quad \text{où } a, b, n, k \in \mathbb{Z}$$

$$\text{et } b \in [0, N-1]$$

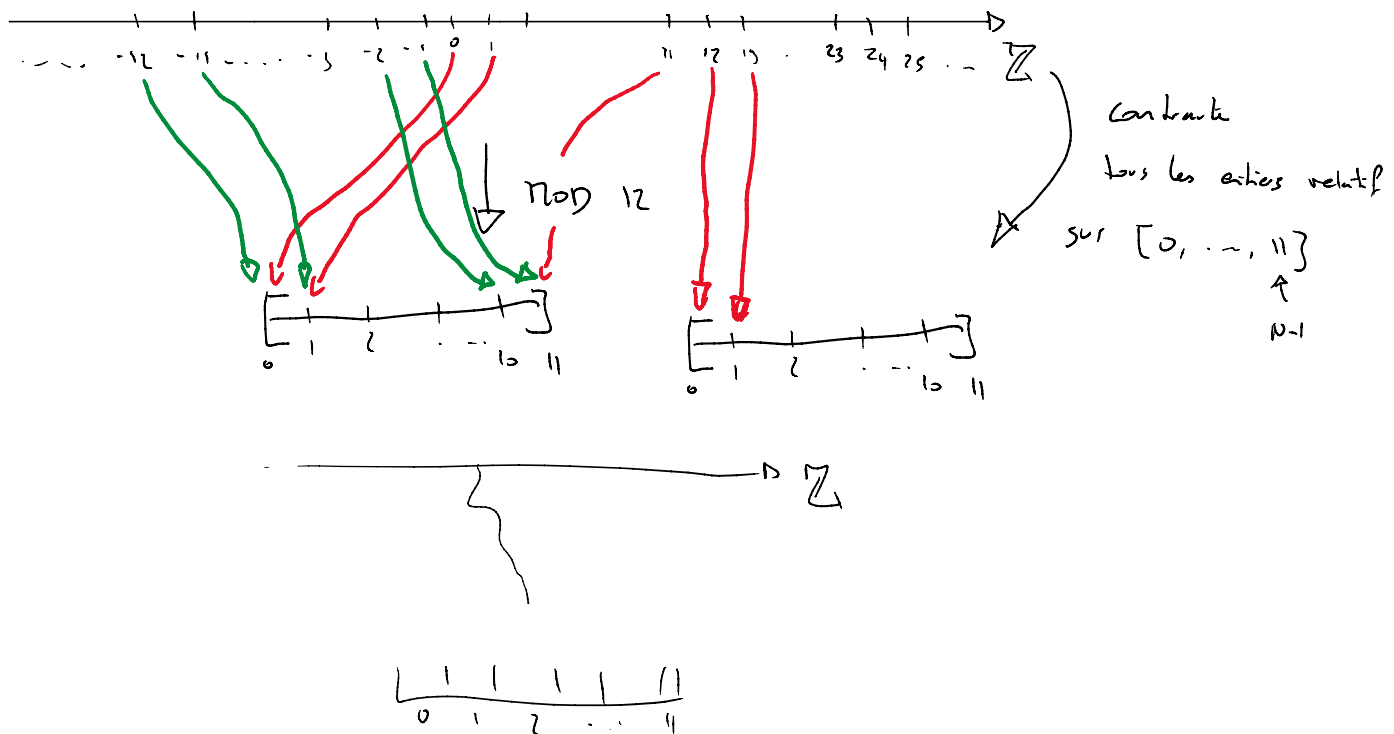
Exemple:

$$10 \bmod 3 \Rightarrow 3 \times 3 + 1 \Rightarrow 1$$

$$12 \bmod 3 \Rightarrow 3 \times 4 + 0 \Rightarrow 0$$

$$3 \bmod 12 \Rightarrow 0 \cdot 12 + 3 \Rightarrow 3$$

$$-3 \bmod 12 \Rightarrow \underbrace{0 \cdot 12 - 3}_{[0, 11]} \Rightarrow -1 \cdot 12 + 9 \Rightarrow \underline{9}$$



Notes:

1) $a \bmod N \geq N$ est-ce possible? Non
 (X 12 = 13 $\downarrow$ > 12)

Absurde:

Supposons que $a \bmod N = x > N$

Par déf. du modulo $a = k \cdot N + x$ si $x > N$

$$a = (k+1) \cdot N + \underbrace{(x-N)}$$

≥ 0 car $x > N$ (par l'absurde)!

$x \in [0, N-1]$ par déf. du module } $\swarrow$ contradiction!

$$\Rightarrow a \bmod N \leq N-1 \quad (\text{et } \geq 0 !)$$

7) $a \bmod N = a$ ist möglich? ($N \geq 1$ und $N \in \mathbb{N}$)

VRAI si et seulement si:



$$0 \leq a < N$$

⑤

Prove:

$k \in \mathbb{Z}$

$(A) \Rightarrow (B) \quad a \bmod N = a \Rightarrow a = k \cdot N + a \Rightarrow a = 0 \cdot N + a$

$\Rightarrow a \in [0, \dots, N-1] \Rightarrow a < N!$
 p.w. def.
 der Modulus Pro

Prove $(A) \Rightarrow (B)$

① $\Rightarrow$ ④

S: $a \in [0, N-1] \Rightarrow a = 0 \cdot N + a = a \bmod N$

$\uparrow$
VRAS cu $a \in [0, N-1]$

$\Rightarrow a = a \bmod N$ prove ② $\Rightarrow$ ④

CQFD!

Noter Si $a \text{ mod } N \in [-v-1, \dots, v+1]$

p.ex. sur la calculatrice $-3 \bmod 10 = -3$

$$\begin{array}{r} \in [-9, 0] \\ + \quad 10 \\ \hline \in [1, 10] \end{array}$$

Si $a \bmod N \in [0, \dots, -1]$ (PAS 0)

$$+N \in [0, \dots, N-1] \text{ ou}$$

$$-3 \bmod 10$$

$$+10 \Rightarrow \begin{array}{r} -3 \\ -(-1) \times 10 \\ \hline 7 \end{array} \quad \begin{array}{r} 10 \\ -1 \\ \hline \end{array}$$

$$\left(\begin{array}{r} -3 \\ - \\ \hline -3 \\ 0 \end{array} \right)$$

Notation: $a \bmod N = b$

$a \% N = b$ (écrit. alternative)

$$a \equiv_N b$$

"congruence modulo de N près"
CONGRUENCE

a est "congruent" à b modulo N si

$$a \bmod N = b \bmod N.$$

Quelle différence ? :

Si $a \bmod N = b$ $\rightarrow \in [0, N-1]$ alors $a \equiv_N b$ ou

l'inverse n'est PAS vrai, car si $a = 1$

l'inverse n'est PAS vrai, car si $a \equiv_n b$ alors il se peut que a et b soient en dehors de $[0, n-1]$

Exemple:

$$3 \bmod 10 = 3 \quad \Rightarrow \quad 3 \equiv_{10} 3 \quad \text{ok}$$

$$\begin{array}{l} 13 \text{ et } 23 \\ 13 \bmod 10 = 3 \\ 23 \bmod 10 = 3 \end{array} \quad \left. \vphantom{\begin{array}{l} 13 \text{ et } 23 \\ 13 \bmod 10 = 3 \\ 23 \bmod 10 = 3 \end{array}} \right\} 13 \equiv_{10} 23 \quad \text{Mais } 13 \bmod 10 \neq 23 \\ 23 \bmod 10 \neq 13$$

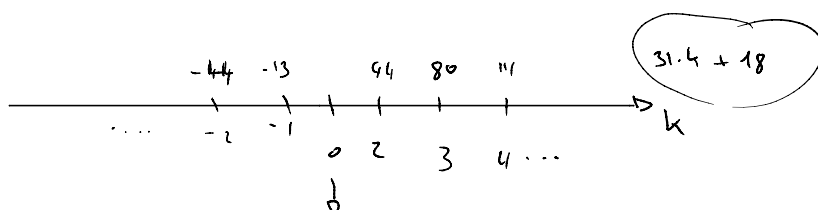
Exercice: Quels sont les éléments (entiers relatifs) congruents à 173 mod 31 ?

$$173 \bmod 31 = 18 \equiv_{31} 142 \equiv_{31} 111 \equiv_{31} 80 \equiv_{31} 49$$

$$\equiv_{31} -13 \equiv_{31} -44 \equiv_{31} \dots$$

Par def. du modulo $18 = k \cdot 31 + 18$ où $k \in \mathbb{Z}$

Tous les entiers de la forme $k \cdot 31 + 18$ avec $k \in \mathbb{Z}$ sont CONGRUENTS entre eux



$$\begin{array}{r} 0 \cdot 31 + 18 \\ 18 \end{array}$$

L'ensemble des éléments congruents à 173 mod 31

est un ensemble du type

$$E_{18} = \{x \text{ tels que } x = k \cdot 31 + 18, k \in \mathbb{Z}\}$$

$$-44 \equiv_{31} 173$$

Question: Si on définit $\equiv_N$, combien des "ensembles de congruence"

du type $E_i = \{x \text{ tels que } x = k \cdot N + i, k \in \mathbb{Z}\}$

y a-t-il ? Il y en a N ! $E_0, E_1, \dots, E_{N-1}$

Exemple avec $N=31$: $E_{18} = \{x = k \cdot 31 + 18\} = \{\dots, -44, -13, 18, 49, 80, \dots\}$

$$E_0 = \{x = k \cdot 31 + 0\} = \{\dots, -31, 0, 31, 62, 93, \dots\}$$

E_1

E_2

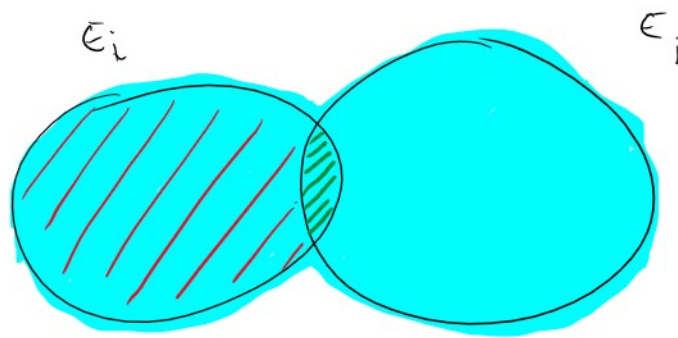
$\vdots$

E_{30}

Exercice: Prouvez que les N sous-ensembles $E_0, E_1, \dots, E_{N-1}$ couvrent tous les entiers relatifs $\mathbb{Z}$ et les ensembles sont DISJOINTS.

1) $E_0 \cup E_1 \cup E_2 \dots \cup E_{N-1} = \mathbb{Z} \Rightarrow$ tout $x \in \mathbb{Z}$ appartient à Au moins un des E_i .

2) $E_i \cap E_j = \emptyset \rightarrow$ ensemble vide si $i \neq j$ (par absurde)



$E_i \cap E_j$

$E_i \setminus E_j$

$E_i \cup E_j$