Calculer modulo n

$n \in \mathbb{N} \quad n > 1$

$$\mathbb{Z} = \{\dots; -1; 0; 1; \dots\}$$

$$\mathbb{Z}_{13} = \mathbb{Z}/13\mathbb{Z} = \{0; 1; 2; 3; 4; \dots; 12\}$$

$1+2 = 3$

$6+7 = 13 \equiv 0 \mod 13$ ← reste de la division par 13

$$a \equiv 6 \mod n \iff n \mid (a-6)$$

$a \equiv 6 \mod n$: congru

$\{0; 1; 2; 3; 4; 5; 6; 7; \boxed{8}; 9; 10; 11; 12\} = \mathbb{Z}_{13}$

$8 + k \cdot 13$: $\dots; -5; 8; 21; 34; \dots$

$3 + k \cdot 13$: $\dots; -10; -23; 3; 16; 29; \dots$

$11 + 12 = 23 \equiv 10 \mod 13$

« $11+12 = 10$ »

$a \equiv b \pmod{n}$

a est congru à b modulo n

$a \bmod b = r$

a modulo b

opérateur

$a \,\%\, b$

$b > 0$

si $a = q \cdot b + r$

$30 \equiv 25 \pmod{5}$

$5 \mid (30 - 25)$

$30 \bmod 25 = 5$

$30 \bmod 5 = 25 \bmod 5$

$a \equiv b \pmod{n} \iff n \mid (a - b)$

$100 \not\equiv 17 \pmod{4} \iff 4 \mid (100 - 17)$

$0 \quad 1$

$4 \mid 83$

$n = 15$

Trouver 2 couples de nombres congrus mod 15

et 2 couples de nombres qui ne le sont pas.

$3 \equiv 5 \mod 2$

$2 \mid (3-5)$ ✓ car $3-5 = -2 = 2 \cdot (-1)$

$a \equiv b \pmod n \Rightarrow a \bmod n = b \bmod n$

a et b ont même reste après division par n.

$117 \equiv 122 \pmod 5 \Leftrightarrow 5 \mid (117-122)$

$117 \bmod 5 = 2 = 122 \bmod 5$

$n \in \mathbb{N} \quad n > 1$

Preuve : $a \equiv b \pmod n$

$\Rightarrow n \mid (a-b) \Rightarrow \exists z \in \mathbb{Z}$ tq. $a - b = n \cdot z$

$\Rightarrow a = b + n \cdot z$

$\exists\, q, q', r, r'$ uniques avec $\begin{cases} a = q \cdot n + r \\ b = q' \cdot n + r' \end{cases}$ Thm

$0 \leq r, r' < n$

$a = q' \cdot n + r' + n \cdot z$

$a = (q' + z) \cdot n + r' \qquad 0 \leq r' < n$

$\Rightarrow r' = r$ car q et r sont uniques

dans $a = q \cdot n + r$ si $0 \leq r < n$.

$$a \bmod n = b \bmod n \Rightarrow a \equiv b \pmod n$$

$a \bmod n = b \bmod n \Rightarrow$ a et b ont même reste après division par n

$$\Rightarrow a = q \cdot n + r \qquad 0 \leq r < n$$
$$b = q' \cdot n + r$$

$$\Rightarrow a - b = q \cdot n - q' \cdot n + r - r$$

$$\Rightarrow a - b = \underbrace{(q - q')}_{\in \mathbb{Z}} \cdot n$$

$$\Rightarrow n \mid (a - b)$$

$$\Rightarrow a \equiv b \pmod n \quad \square$$