Proposition : $x \equiv y \pmod{n} \iff x - y = k \cdot n \quad \text{avec } k \in \mathbb{Z}$

Preuve :
- Soit $x \in \mathbb{Z} \implies x = q \cdot n + r \quad \text{avec } 0 \leqslant r < n$
- Soit $y \in \mathbb{Z} \implies y = q' \cdot n + r' \quad \text{avec } 0 \leqslant r' < n$

($\Longrightarrow$) $\boxed{x \equiv y \pmod{n} \implies x - y = k \cdot n \quad \text{avec } k \in \mathbb{Z}}$

$$x \equiv y \pmod{n} \implies r \text{ et } r' \text{ sont égaux}$$

$$\implies x - y = (q \cdot n + r) - (q' \cdot n + r')$$

$$= (q - q') \cdot n + \underbrace{(r - r')}_{=0}$$

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

($\Longleftarrow$) $\boxed{x - y = k \cdot n \quad \text{avec } k \in \mathbb{Z} \implies x \equiv y \pmod{n}}$

$$x - y = (q \cdot n + r) - (q' \cdot n + r') = (q - q') \cdot n + \underbrace{(r - r')}_{\text{qui doit être un multiple de } n}$$

$$\left.\begin{array}{ll} \text{Or} & 0 \leqslant r < n \\ & 0 \leqslant r' < n \end{array}\right\} \implies -n < r - r' < n$$

Mais le seul multiple de n strictement compris entre $-n$ et n est zéro.

$$\implies r - r' = 0 \implies r = r' \implies x \equiv y \pmod{n}$$

□