L'anneau $\mathbb{Z}/n\mathbb{Z}$

→ Théorème chinois : $m \wedge n = 1$

$$\mathbb{Z}/mn\mathbb{Z} \overset{\sim}{\underset{j}{\rightleftharpoons}} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

$j : \overline{x} \longmapsto (\overline{x_m}, \overline{x_n})$ (Ker j = ... + coordonnées)

→ Indicatrice d'Euler $\varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$

- $m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\,\varphi(n)$
- $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$
- $\varphi(n) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$

→ Théorème d'Euler :

$$a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \,[n]$$ ($U(\mathbb{Z}/n\mathbb{Z}) = \varphi(n)$ (=> format)

Comp → Résidus quadratiques [Stica]

$H = \{ b^2 \mid b \in (\mathbb{Z}/p\mathbb{Z})^* \}$:

- $|H| = \frac{p-1}{2}$
- $a \in H \iff a^{\frac{p-1}{2}} = \overline{1}$
- $-\overline{1}$ carré $\iff p \equiv 1 \,[4]$

Complément pour dossier