

Entiers, modulaires

$m \geq 1$

anneau $\rightarrow$

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \dots, \overline{m-1}\}$$

← groupe
additif
cyclique

$(\mathbb{Z}/m\mathbb{Z})^*$ unités de $\mathbb{Z}/m\mathbb{Z}$ R anneau

$u \in R$ est une unité si il existe $v \in R$

$uv = 1$. R^* groupe multiplicatif

Soit $\bar{u} \in \mathbb{Z}/m\mathbb{Z}$, $\bar{u}$ est une unité si

$$\text{PGCD}(n, m) = 1 \quad (n \text{ et } m \text{ premiers entre eux})$$

$$(\mathbb{Z}/m\mathbb{Z})^* = \{ \bar{a} \in \mathbb{Z}/m\mathbb{Z} \text{ tel que } \text{PGCD}(a, m) = 1 \}$$

Fonction d'Euler

$$\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$$

$$= \text{card} \{ 0 \leq n \leq m-1 \mid \text{PGCD}(n, m) = 1 \}$$

$m \geq 2$

Proposition : $\Rightarrow \varphi(m) \leq m-1$

$$(2) \quad \varphi(p) = p-1 \quad (p \text{ premier})$$

$$(3) \quad e \geq 1, \quad \varphi(p^e) = p^{e-1}(p-1)$$

(4) Théorème des restes chinois :

Si n et m sont premiers entre eux

$$\text{alors} \quad \varphi(nm) = \varphi(n) \varphi(m)$$

