

Soit G cyclique d'ordre n

① Soit $d \geq 1$. Nombre d'éléments d'ordre d dans G ? $N(d)$

• Si $d \nmid n$ alors, $N(d) = 0$
(Th. de Lagrange)

• Si $d \mid n$. On sait que $G \cong \mathbb{Z}/n\mathbb{Z}$
donc $N(d) = \text{card} \left\{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{a} \text{ d'ordre } d \right\}$

Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Alors

$\bar{a} = a \cdot \bar{1}$ et $\bar{1}$ est d'ordre n

$$\text{donc } \text{ordre}(\bar{a}) = \frac{n}{\text{PGCD}(n, a)}$$

Ecrivons $n = de$ ($e \geq 1$)

$$\text{On veut } \text{ordre}(\bar{a}) = d = \frac{de}{\text{PGCD}(de, a)}$$

$$\Leftrightarrow \text{PGCD}(de, a) = e$$

$$\Leftrightarrow e|a \text{ or } (\frac{a}{e}, d) = 1$$

$$\left[e|a : \text{donc } a = be \right.$$

$$\text{alors } \text{PGCD}(de, a) = \text{PGCD}(de, be) \\ = e \text{ PGCD}(d, b) \stackrel{\text{on var}}{=} e$$

$$\text{donc } \text{PGCD}(d, b) = 1 \quad \left. \right]$$

$$N(d) = \text{card} \left\{ 0 \leq a < n \mid e|a \right. \\ \left. \text{or } \text{PGCD}(a/e, d) = 1 \right\}$$

"dire $e|a$, c'est pareil que $a = eb$ "

$$N(d) = \text{card} \left\{ 0 \leq b < \underset{\substack{n \\ \text{vd}}}{n} \mid (b, d) = 1 \right\}$$

$$= \text{card} \{ 0 \leq b < d \mid (b, d) = 1 \}$$

$$= \varphi(d)$$

le nombre d'éléments d'ordre d dans G
 (quand $d \mid n$) est $\varphi(d)$

2. On peut partitionner G

Suivant l'ordre des éléments.

C'en-à-dire

$$G = \bigcup_{d|n} S(d)$$

disjoints

$$S(d) = \{ g \in G \mid \text{ordre } g = d \}$$

$$\text{d'où } |G| = \sum_{d|n} \text{card}(S(d))$$

$$n = \sum_{d|n} \varphi(d)$$

Application: Si p premier: $(\mathbb{Z}/p\mathbb{Z})^*$
groupe cyclique