

Th. Fermat via Burnside

$$p \in \mathbb{P}$$

$\mathbb{Z}/p\mathbb{Z}$ agit sur $(\underbrace{m_1, m_2, \dots, m_p}_{\text{not}}) \in [1, k]^p$ de façon naturelle:

$\bar{i} \in \mathbb{Z}/p\mathbb{Z}, m \in [1, k]^p : \bar{i} \cdot m = (m_{\bar{i}}, m_{\bar{i}+1}, \dots, m_{\bar{i}+p-1})$
 Non, j'acte sur $(\mathbb{Z}/p\mathbb{Z})^*$.
 (ou $i \cdot m = (m_{i+1}, m_{i+2}, \dots, m_{i+p})$)

On a a...

Garde!

$$|\mathbb{Z}/p\mathbb{Z}| \cdot |\text{Orb}([1, k]^p, \mathbb{Z}/p\mathbb{Z})|$$

$$= \sum_{\bar{i} \in \mathbb{Z}/p\mathbb{Z}} |\text{Fix}(\bar{i})| \rightarrow \text{dans } p \cdot \mathbb{Z} \text{ force}$$

$$\text{Fix}(\bar{0}) = [1, k]^p \rightarrow |\text{Fix}(\bar{0})| = k^p$$

$$\bar{i} \in (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \text{Fix}(\bar{i}) = \{ \text{mot tel que } m_{\bar{i}+1} = m_{\bar{i}} \text{ pour } i \in [1, p-1] \}$$

$p \in \mathbb{P}$ donne
mots constants!

$$\rightarrow |\text{Fix}(\bar{i})| = k$$

D'où,

$$\sum_{\bar{i} \in \mathbb{Z}/p\mathbb{Z}} |\text{Fix}(\bar{i})| = k^p + (p-1)k$$

$$\Rightarrow k^p \equiv (1-p)k \pmod{p}$$

$$\Rightarrow k^p \equiv k \pmod{p} \quad \text{Joli!}$$