Th. Fermat via Burnside

$p \in \mathbb{P}$

$\mathbb{Z}/p\mathbb{Z}$ agit sur $(u_1, u_2, \dots, u_p) \in [\![1; k]\!]$ de façon naturelle :

$\bar{i} \in \mathbb{Z}/p\mathbb{Z}$, $u \in [\![1; k]\!]^p$: $\bar{i} \cdot u = (u_{\bar{i}}, u_{\overline{2i}}, \dots, u_{\overline{pi}})$

NON, juste sur $(\mathbb{Z}/p\mathbb{Z})^*$.

(ou $i \cdot u = (u_{\overline{i+i}}, u_{\overline{2+i}}, \dots, u_{\overline{p+i}})$ ~~NON CAR $p \in \mathbb{P}$ inutile ici !~~)

Or on a ... — Gardé !

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

$= \sum_{\bar{i} \in \mathbb{Z}/p\mathbb{Z}} |\mathrm{Fix}(\bar{i})|$ → dans $p \cdot \mathbb{Z}$ gardé

$\mathrm{Fix}(\bar{0}) = [\![1; k]\!]^p$ → $|\mathrm{Fix}(\bar{0})| = k^p$

$\bar{i} \in (\mathbb{Z}/p\mathbb{Z})^*$ → $\mathrm{Fix}(\bar{i}) = \{$ mot tel que $u_{\overline{i+i}} = u_{\bar{i}}$ pour $i \in [\![1, p]\!]\}$

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

→ $|\mathrm{Fix}(\bar{i})| = k$

Besoin ici pour parcourir tous les indices !

D'où,

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

$\Rightarrow k^p \equiv (1-p)k \ [p]$

$\Rightarrow k^p \equiv k \ [p]$ Joli !

Faux

$p \in \mathbb{P}$ non utilisé !

$\not\Rightarrow$ Th. Lagrange !

$\not\Rightarrow |\{k^a\}| \mid |\mathbb{Z}/p\mathbb{Z}|$?

$\not\Rightarrow$ "ord k" $\mid p$

plein $k \mid 0$