101

Développement $\left((\mathbb{Z}/p\mathbb{Z})^*, \times\right)$ est cyclique (p premier)

3 étapes :

① lemme : si G est un groupe abélien, $x_1, \dots x_r$ éléments de G d'ordre $p_1, \dots, p_r$ premiers entre eux 2 à 2 alors $x_1 \dots x_r$ est d'ordre $p_1 \dots p_r$

② $q \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$ tel que $q^\alpha \mid (p-1)$ alors il existe des éléments de $\left((\mathbb{Z}/p\mathbb{Z})^*, \times\right)$ d'ordre q^α (montrons pour $\alpha = 1$ et α)

③ conclure.

① On le fait par récurrence sur r.

• pour $r = 2$

$(x_1, x_2) \in G^2$ tel que $o(x_1) = p_1$ et $o(x_2) = p_2$ et $p_1 \wedge p_2 = 1$

$(x_1 x_2)^{p_1 p_2} = x_1^{p_1} x_2^{p_2}$ car G est abélien

$= 1$ (car $k = o(x_1 x_2) \mid p_1 p_2$)

Soit $k \in \mathbb{Z}$ tel que $(x_1 x_2)^k = 1$. Comme G est abélien

$$1 = (x_1 x_2)^{k p_2} = x_1^{k p_2} x_2^{k p_2} = x_1^{k p_2} \quad \text{car } o(x_2) = p_2$$

d'où $p_1 \mid k p_2$

or $p_1 \wedge p_2 = 1$ donc d'après le lemme de Gauss $p_1 \mid k$

(Rem $k p_2 = p_1 q + r$ avec $0 \le r < p_1$

d'où $r = k p_2 - p_1 q$

$x^r = x^{k p_2 - p_1 q} = 1$ et d'après la minimalité $r = 0$)

Par symétrie $p_2 \mid k$ et comme $p_1 \wedge p_2 = 1 \Rightarrow p_1 p_2 \mid k$

aussi $k = p_1 p_2$

- Cas général. On suppose la propriété vraie pour r

pour $r+1$ $\quad y = x_1 \cdots x_r$ avec $o(y) = p_1 \cdots p_r$ $\quad \oplus (p_1 \cdots p_r) \wedge p_{r+1} = 1$ (1)

$o(x_{r+1}) = p_{r+1}$

(1) comme $p_{r+1} \wedge p_i = 1 \quad \forall i \in [\![1, r]\!]$

$\Rightarrow \prod_{i=1}^{r} p_i \wedge p_{r+1} = 1$ (décomp du ppcm en produit de facteurs)

on applique le résultat précédent

(2) Montrons le résultat attendu avec $\alpha = 1$.

p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et $(\mathbb{Z}/p\mathbb{Z})^*$ est son groupe multiplicatif. (ts elts non nuls sont inversibles)

q premier tel que $q \mid p-1$

$\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$, notons $y_x = x^{\frac{p-1}{q}}$

On a $(y_x)^q = \left(x^{\frac{p-1}{q}}\right)^q = x^{p-1} = 1$ d'après le petit th. de Fermat. ($x \wedge p = 1$)

Donc $o(y_x) \mid q$ et comme q est premier

Alors 2 possibilités $\begin{cases} o(y_x) = 1 \\ o(y_x) = q \end{cases}$

donc $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$

Montrons qu'il existe au moins 1 élt de $(\mathbb{Z}/p\mathbb{Z})^*$ tel que $o(y_x) = q$ par l'absurde.

Donc on suppose que $o(y_x) = 1$, d'où $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$ (x parcourt $(\mathbb{Z}/p\mathbb{Z})^*$) $\quad y_x^1 = y_x = 1$

$P(X) = X^{\frac{p-1}{q}} - 1$ a donc au moins $p-1$ racines (tous les x)

or $\deg P = \frac{p-1}{q} < p-1$ d'où la contradiction.

d'où $o(y_x) = q$

2) On applique le même raisonnement

$\forall x \in (\mathbb{Z}/p\mathbb{Z})^* \quad y_x = x^{\frac{p-1}{q^\alpha}}$

Alors $y_x^{q^\alpha} = \left(x^{\frac{p-1}{q^\alpha}}\right)^{q^\alpha} = x^{p-1} = 1$

donc $o(y_x) \mid q^\alpha$

D'où l'ordre $o(y_x)$ est de la forme q^{r_x} avec $r_x \leq \alpha$
Les car q premier.

Soit r le plus grand des r_x

$\forall x \in (\mathbb{Z}/p\mathbb{Z})^* \quad \left(x^{\frac{p-1}{q^r}}\right)^{q^r} = (y_x)^{q^r} = \left(y_x^{q^{r_x}}\right)^{q^{r-r_x}} = 1$

d'où le polynôme $Q(X) = X^{\frac{p-1}{q^{\alpha-r}}} - 1$ admet au moins $p-1$ racines
$\left(\text{les } (y_x)^{q^r}\right)$ d'où $\deg Q \geq p-1$

donc $\frac{p-1}{q^{\alpha-r}} \geq p-1$.

Le seul cas possible est $\frac{p-1}{q^{\alpha-r}} = p-1$, donc $q^{\alpha-r} = 1$

$\underline{\alpha = r}$

il existe bien un élément de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre α.

(3) Décomposons $p-1$ en produits de facteurs premiers

$p-1 = q_1^{\alpha_1} \cdots q_r^{\alpha_r} \quad q_i \wedge q_j = 1 \ \forall i \neq j \quad \alpha_i \in \mathbb{N}^* \ \forall i$

d'après la question précédente, il existe $\forall i \in [\![1, r]\!]$
un élément $x_i \in (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $q_i^{\alpha_i}$

Or les $q_i^{\alpha_i}$ sont premiers 2 à 2, donc

$x_1 \cdots x_r \in (\mathbb{Z}/p\mathbb{Z})^*$ et d'ordre $q_1^{\alpha_1} \cdots q_r^{\alpha_r} = p-1$

Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ possède 1 élt d'ordre $p-1$, il est cyclique

1°/ $(x_1, x_2) \in G^2$ $\begin{cases} o(x_1) = p_1 \\ o(x_2) = p_2 \end{cases}$ $p_1 \wedge p_2 = 1$

a) G abélien $(x_1 x_2)^{p_1 p_2} = (x_1^{p_1})^{p_2} (x_2^{p_2})^{p_1} = 1$ donc $o(x_1 x_2) \mid p_1 p_2$

b) Soit $k \in \mathbb{Z}$ tq $(x_1 x_2)^k = 1$

G abélien $(x_1 x_2)^{k p_2} = 1$

$= x_1^{k p_2} x_2^{k p_2} = x_1^{k p_2}$

d'où $p_1 \mid k p_2$ et $p_1 \wedge p_2 = 1$ donc $p_1 \mid k$

idem $p_2 \mid k$ par symétrie

or $p_1 \wedge p_2 = 1$ donc $p_1 p_2 \mid k$

d'où $o(x_1 x_2) = p_1 p_2$.

2°/ p premier, $\mathbb{Z}/p\mathbb{Z}$ est 1 corps

→ tous les éléments non nuls sont inversibles → $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est 1 groupe

Pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, notons $y_x = x^{\frac{p-1}{q}}$

on a $y_x \in (\mathbb{Z}/p\mathbb{Z})^*$ et $(y_x)^q = x^{p-1} = 1$

d'après petit th de fermat $p \nmid x$

donc $o(y_x) \mid q$ et q premier.

2 choix. $\begin{cases} \text{soit } o(y_x) = 1 \\ \text{soit } o(y_x) = q \end{cases}$

oral $\begin{cases} \text{Montrer par l'absurde qu'il existe au moins 1 élt } x \in (\mathbb{Z}/p\mathbb{Z})^* \\ \text{d'ordre } q. \end{cases}$

Supposons que pour tout x de $(\mathbb{Z}/p\mathbb{Z})^*$ $o(y_x) = 1$

donc avec $y_x = 1$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$

le polynôme $P(X) = X^{\frac{p-1}{q}} - 1$ a donc au moins $p-1$ racines (les x)

or $\deg P = \frac{p-1}{q} < p-1$ ⇒ contradiction

∃ au moins $1 x \in (\mathbb{Z}/p\mathbb{Z})^*$ tq $o(y_x) = q$.

3) Rien raisonner. $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$

$y_x = x^{\frac{p-1}{q^\alpha}}$ et $(y_x)^{q^\alpha} = x^{p-1} = 1$

d'où $o(y_x) \mid q^\alpha$

donc l'ordre y_x est de la forme q^{r_x} avec $0 \le r_x \le \alpha$

soit r le plus grand des r_x qd x décrit $(\mathbb{Z}/p\mathbb{Z})^*$

$\forall x \in (\mathbb{Z}/p\mathbb{Z})^* \quad \left(x^{\frac{p-1}{q^\alpha}}\right)^{q^r} = (y_x)^{q^r} = \left(y_x^{q^{r_x}}\right)^{q^{r-r_x}} = 1$

on introduit le polynôme $Q(X) = X^{\frac{p-1}{q^{\alpha-r}}} - 1$

il admet au moins $p-1$ racines (les x^{q^r})

donc $\deg Q \ge p-1$ ie $\frac{p-1}{q^{\alpha-r}} \ge p-1$

q premier seul cas $q^{\alpha-r} = 1$ soit $\alpha = r$

donc dans $(\mathbb{Z}/p\mathbb{Z})^*$, il existe un élt d'ordre q^α..

4) $(p-1)$ se décomp en nbs premiers $q_1^{\alpha_1} \dots q_r^{\alpha_r}$ avec $\forall i \neq j \; q_i \wedge q_j = 1$

$\alpha_i \in \mathbb{N}^*$

d'après la q. préc., $\forall i \in [\![1, r]\!]$ on peut trouver un élément x_i de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $q_i^{\alpha_i}$.

$\forall i \neq j \; q_i^{\alpha_i} \wedge q_j^{\alpha_j} = 1$ ⇒ base (q1)

d'où $x_1 \dots x_r$ de $(\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre $q_1^{\alpha_1} \dots q_r^{\alpha_r} = p-1$

donc le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ possède 1 élément d'ordre $p-1$, il est cyclique.