Rombaldi p292

CYCLICITÉ DE $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$

108, 120, 121

Pour tous $p \geqslant 3$ premier et $\alpha \in \mathbb{N}^*$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

- $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique car c'est le groupe multiplicatif d'un corps fini. (Annexe)
- Montrons qu'il existe $(\lambda_k)_{k\in\mathbb{N}} \in (\mathbb{N}^*)^{\mathbb{N}}$ telle que $\forall k \in \mathbb{N}$, $\lambda_k \wedge p = 1$ et $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$:
  - $(1+p)^{p^0} = 1+p$: on pose $\lambda_0 = 1$. On a bien $\lambda_0 \wedge p = 1$.
  - $(1+p)^{p^1} = \sum_{k=0}^{p} \binom{p}{k} p^k = 1 + \binom{p}{1}p + \sum_{k=2}^{p} \binom{p}{k} p^k = 1 + \lambda_1 p^2$ où $\lambda_1 = 1 + \sum_{k=2}^{p} \binom{p}{k} p^{k-2}$. En remarquant que $\forall k \in [\![1,p-1]\!]$, $p \mid \binom{p}{k}$, et $p \geqslant 3$ donc $p \mid \binom{p}{p} p^{p-2}$, on a bien $\lambda_1 \equiv 1\ [p]$ donc $\lambda_1 \wedge p = 1$.
  - Soit $k \geqslant 1$, supposons construit λ_k satisfaisant l'hypothèse. Alors :
$$(1+p)^{p^{k+1}} = \left[(1+p)^{p^k}\right]^p = (1+\lambda_k p^{k+1})^p = \sum_{i=0}^{p} \binom{p}{i} \lambda_k^i p^{i(k+1)} = 1 + \binom{p}{1}\lambda_k p^{k+1} + \sum_{i=2}^{p} \binom{p}{i} \lambda_k^i p^{i(k+1)}$$
$$= 1 + \lambda_k p^{k+2} + \sum_{i=2}^{p} \binom{p}{i} \lambda_k^i p^{i(k+1)}.$$

Or $\forall i \in [\![2,p]\!]$, $p^{k+3} \mid \binom{p}{i} \lambda_k^i p^{i(k+1)}$, donc il existe $m \in \mathbb{Z}$ tel que $\sum_{i=2}^{p} \binom{p}{i} \lambda_k^i p^{i(k+1)} = p^{k+3} m$, puis $(1+p)^{p^{k+1}} = 1 + \lambda_{k+1} p^{k+2}$ où $\lambda_{k+1} = \lambda_k + pm$. Comme $\lambda_{k+1} \equiv \lambda_k \not\equiv 0\ [p]$ et p est premier, on a bien $\lambda_{k+1} \wedge p = 1$. □

- Justifions que $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$: déjà, $(1+p)\wedge p = (1+p)\wedge p^\alpha = 1$ donc $\overline{1+p} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
Ensuite :
  - $(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1\ [p^\alpha]$ donc $\overline{1+p}^{\,p^{\alpha-1}} = \overline{1}$, et $\mathrm{ord}(\overline{1+p}) \mid p^{\alpha-1}$. En particulier, il existe $k \in [\![0,\alpha-1]\!]$ tel que $\mathrm{ord}(\overline{1+p}) = p^k$.
  - $(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1}$ et $v_p(\lambda_{\alpha-2} p^{\alpha-1}) = v_p(\lambda_{\alpha-2}) + (\alpha-1)v_p(p) = 0 + (\alpha-1)\cdot 1 = \alpha - 1 < \alpha$ (car $\lambda_{\alpha-2} \wedge p = 1$). En particulier, $\lambda_{\alpha-2} p^{\alpha-1} \not\equiv 0\ [p^\alpha]$, donc $(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1} \not\equiv 1\ [p^\alpha]$, i.e. $\overline{1+p}^{\,p^{\alpha-2}} \neq \overline{1}$. De là, $\mathrm{ord}(\overline{1+p}) > p^{\alpha-2}$, donc $\mathrm{ord}(\overline{1+p}) = p^{\alpha-1}$. □

- Soit $x + p\mathbb{Z}$ un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Posons $y = x^{p^{\alpha-1}}$ et $\bar{y} = y + p^\alpha\mathbb{Z}$. Déjà, $x + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$ donc $x \wedge p = 1$, donc $y \wedge p^\alpha = 1$ et $\bar{y} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Montrons que l'ordre r de $\bar{y}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est $p-1$:
  - Montrons que $r \mid p-1$: d'après le théorème d'EULER, $y^{p-1} = x^{p^{\alpha-1}(p-1)} = x^{\varphi(p^\alpha)} \equiv 1\ [p^\alpha]$, donc $r \mid p-1$.
  - Montrons que $p-1 \mid r$: remarquons que $p^{\alpha-1} - 1 = (p-1)q$ où $q = \sum_{k=0}^{\alpha-2} p^k$, donc $x^{p^{\alpha-1}-1} = (x^{p-1})^q \equiv 1^q \equiv 1\ [p]$ (car $x + p\mathbb{Z}$ génère $(\mathbb{Z}/p\mathbb{Z})^\times$: il est d'ordre $p-1$). De là, $y = x\, x^{p^{\alpha-1}-1} \equiv x\ [p]$, et $\bar{y} = \bar{x}^{p^{\alpha-1}}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Enfin, $y^r \equiv 1\ [p^\alpha]$ donc $p^\alpha \mid y^r - 1$, donc $p \mid y^r - 1$ (car p est premier), donc $y^r \equiv 1\ [p]$, donc $p-1 \mid r$ car l'ordre d'un élément est minimal pour la division.

- Comme $p^{\alpha-1} \wedge (p-1) = 1$ et $\overline{1+p}$ et $\bar{y}$ commutent, l'ordre de $(\overline{1+p})\bar{y}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est $p^{\alpha-1}(p-1) = \#(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, et donc $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique. ■

ANNEXE 1 : $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique

Soit $d \mid p-1$, montrons que $(\mathbb{Z}/p\mathbb{Z})^\times$ admet $\varphi(d)$ éléments d'ordre d : si $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre d, alors les d éléments distincts de $\langle x \rangle$ sont racines de $X^d - 1$. Or ce dernier a au plus d racines dans le corps commutatif $\mathbb{Z}/p\mathbb{Z}$, donc

$\langle x \rangle$ est exactement l'ensemble des racines de $X^d - 1$. En particulier, tous les éléments d'ordre d (s'ils existent) engendrent le même groupe, constitué des racines de $X^d - 1$. De là, s'il existe au moins 1 élément d'ordre d, alors il y en a exactement $\varphi(d)$. Or si $\psi(d)$ désigne le nombre d'éléments d'ordre d de $(\mathbb{Z}/p\mathbb{Z})^\times$, alors par partition de $(\mathbb{Z}/p\mathbb{Z})^\times$ selon l'ordre, $\sum_{d|p-1} \psi(d) = p-1 = \sum_{d|p-1} \varphi(d)$. Or d'après le raisonnement précédent, $\forall d | p-1$, $\psi(d) = 0$ ou $\psi(d) = \varphi(d)$, donc $\forall d | p-1$, $\psi(d) = \varphi(d)$. En particulier $\psi(p-1) = \varphi(p-1) > 0$: $(\mathbb{Z}/p\mathbb{Z})^\times$ admet donc au moins un élément d'ordre $p-1$, et donc est cyclique. ■

<u>Annexe 2</u> : Cas $p=2$

- $(\mathbb{Z}/2\mathbb{Z})^\times \simeq \{1\}$ et $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/3\mathbb{Z}$ sont cycliques.
- $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$ n'est pas cyclique.
- Soit $\alpha \geq 3$, par l'absurde supposons $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ cyclique engendré par $x + 2^\alpha\mathbb{Z}$. Alors son image par le morphisme surjectif $y + 2^\alpha \mathbb{Z} \longmapsto y + 8\mathbb{Z}$ engendrerait $(\mathbb{Z}/8\mathbb{Z})^\times$, ce qui est impossible.

<u>Annexe 3</u> : Liste exhaustive des cas où $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique

$$(\mathbb{Z}/n\mathbb{Z})^\times \text{ est cyclique} \iff n \in \{1, 2, 4, p^\alpha, 2p^\alpha \ : p \geq 3 \text{ premier}, \alpha \geq 1\}$$