Leçons:
104, 108, 120, 121

Lemme:
Pour $k \in \mathbb{N}^*$, $p \in \mathcal{P}$, $(p \neq 2)$ alors
$(1+p)^{p^k} = 1 + \lambda p^{k+1}$ tq $\text{pgcd}(\lambda, p) = 1$

Théorème:
1) Si $p \in \mathcal{P}$ $(p \neq 2)$, $\alpha \geq 2$ alors :
$$\left(\frac{\mathbb{Z}}{p^\alpha \mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{p^{\alpha-1}(p-1)\mathbb{Z}}$$
2) Si $\alpha \geq 3$ alors $\left(\frac{\mathbb{Z}}{2^\alpha \mathbb{Z}}\right)^\times$ n'est pas cyclique

V2

Référence:
[PERI]: Perrin, Cours d'algèbre
[BERI]: Berhuy, Algèbre le grand combat.

Pour le lemme: CPERI p.25

Raisonnons par récurence, pour $k \in \mathbb{N}^*$ notons P_k: "$(1+p)^{p^k} = 1 + \lambda p^{k+1}$":

Initialisation: Pour $k = 1$

$$(1+p)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} p^i + p^p \quad \text{par binôme de Newton}$$

Pour $i \in \{1, \dots, p-1\}$ on a $p \mid \binom{p}{i}$ et $p \mid p^i$ donc $p^2 \mid \binom{p}{i} p^i$ et $p \geq 3$ donc $p^2 \mid p^p$

Donc $(1+p^p) = 1 + p^2 \underbrace{(u + p^{p-2})}_{:= \lambda}$ $\left(p^2 \times u = \sum_{i=1}^{p-1} \binom{p}{i} p^i\right)$

On a bien que $\text{pgcd}(\lambda, p) = 1$ car le 1er terme de u est 1.

Hérédité: Supposons pour $k \in \mathbb{N}^*$ que P_k est vrai, montrons P_{k+1}:

$$(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p$$
↓ par hypothèse de récurrence
$$= \left(1 + \lambda p^{k+1}\right)^p$$
↓ Binôme Newton
$$= 1 + \sum_{i=1}^{p} \binom{p}{i} \lambda^i p^{(k+1)i}$$
↓ sort 1er terme
$$= 1 + p\lambda p^{k+1} + \sum_{i=2}^{p} \binom{p}{i} \lambda^i p^{(k+1)i}$$
↓ même idée que initialisation
$$= 1 + p^{k+2} \underbrace{(\lambda + u')}_{\lambda'}$$

et $\text{pgcd}(\lambda', p) = 1$ car λ premier à p.

□

Pour le théorème [PER] + ma ref

Pour 1): [PER] p.26

On va chercher un candidat d'ordre $(p-1)p^{d-1}$ (car $\left|\left(\frac{\mathbb{Z}}{p^d\mathbb{Z}}\right)^\times\right| = (p-1)p^{d-1}$.)

On va chercher un élément d'ordre $(p-1)$ et p^{d-1} et on va espérer que le produit sera d'ordre $(p-1)p^{d-1}$. (Spoiler ça sera bien le cas)

- Cherchons un élément d'ordre p^{d-1}

On va utiliser le lemme avec $k = d-1$, on a:

$$(1+p)^{p^{d-1}} = 1 + \lambda p^d$$
$$\equiv 1 \quad [p^d]$$

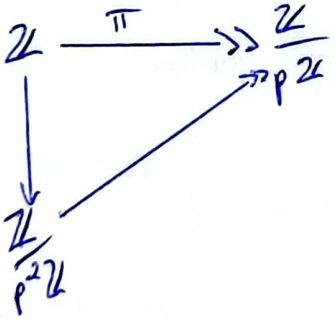
et en remarquant que:

$$(1+p)^{p^{d-2}} = 1 + \lambda p^{d-1}$$
$$\not\equiv 1 \quad [p^d] \text{ car } \text{pgcd}(\lambda, p) = 1$$

On en déduit que $\underline{o(1+p) = p^{d-1}}$ (si c'était pas le cas, on a que c'est un p^b (car $o(1+p) \mid p^{d-1}$) mais du coup $(1+p)^{p^b} = 1 \; [p^d]$ et en mettant à une bonne puissance on aurait $(1+p)^{p^{d-2}} = 1 \; [p^2]$ absurde)

- Cherchons un élément d'ordre $p-1$

Considérons le morphisme surjectif naturel $\Psi : \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^\times \twoheadrightarrow \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$



car $p \mid p^2$ donc $p^2\mathbb{Z} \subset p\mathbb{Z} = \ker(\pi)$

(à écrire si le temps, sinon passer)

On sait $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$ qui est cyclique.

Par surjectivité de Ψ, on peut prendre $x \in \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^\times$ tq $\Psi(x)$ engendre $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$. On a :

$1_{\mathbb{Z}/p\mathbb{Z}} = \psi(1_{\mathbb{Z}/p^2\mathbb{Z}})$

$= \psi(\alpha^{o(\alpha)})$

$= \psi(\alpha)^{o(\alpha)}$

Or $o(\psi(\alpha)) = p-1$ (car générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$)

Donc $p-1 \mid o(\alpha)$.

Donc dans le groupe $\langle\alpha\rangle$ il existe y tq $\underline{o(y) = p-1}$.

Conclusions

D'après un lemme (qui doit être dans le plan), puisque $\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^\times$ est abélien et $\text{pgcd}(p-1, p^{2-1}) = 1$ on a que :

$$o(y\alpha+p1) = (p-1)p^{2-1}$$

or $\left|\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^\times\right| = \varphi(p^2) = (p-1)p^{2-1}$

On a donc que $\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^\times$ est cyclique.

Pour 2) : no rej.

Remarquons $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^\times$ et $\left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^\times$ sont cycliques :

$\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^\times = \{1\}$ et $\left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^\times = \{\pm 1\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$

Remarquons que $\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^\times$ n'est pas cyclique.

$\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^\times = \{\pm 1, \pm 3\}$ or tous ces éléments sont d'ordre 2 (sauf 1 qui est 1)

or $\left|\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^\times\right| = \varphi(8) = 4 \neq 2$. Donc $\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^\times$ n'est pas cyclique.

Supposons par l'absurde que $\left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^\times$ est cyclique

considérons le morphisme surjectif naturel

$$\varphi : \left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^\times \longrightarrow \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^\times$$

Puisqu'on a supposé que $\left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^\times$ est cyclique on peut prendre g un générateur de ce groupe.

Mais alors par surjectivité de ρ, $\rho(g)$ est un générateur de $\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^\times$, ce qui est absurde.

□

Commentaire:

- Savoir mq $\left(\frac{\mathbb{Z}}{2^k\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{k-2}\mathbb{Z}}$ [BERJ p.489]

- Savoir mq " si $o(a)=p$ et $o(b)=q$, $ab=ba$ et $pgcd(p,q)=1$ Alors $o(ab)=pq$" [PERJ p.16]

- Savoir mq $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$ (cas particulier de $\mathbb{F}_q^\times \simeq \frac{\mathbb{Z}}{(q-1)\mathbb{Z}}$) [PERJ p.74]

- Savoir justifier que le passage aux inversible dans un morphisme d'anneau donne un morph. de groupe. [BERJ p.395]

- Savoir mq $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ cyclique ssi ...
  ↳ écrire avec Thm chinois, écrire l'isomorphisme obtenue