Cyclicité des $(\mathbb{Z}/n\mathbb{Z})^\times$: 104, 108, 120, 121 (Perrin, cours d'algèbre)

But : On sait que si p est premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, on veut établir une sorte de réciproque.

Théorème : On a l'équivalence suivante :

$(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique $\iff n = 1, 2, 4, p^\alpha, 2p^\alpha$ où $\begin{cases} p \text{ premier impair} \\ \alpha \in \mathbb{N}^* \end{cases}$

Idée de la preuve : On décompose n en facteurs premiers : $n = 2^k \prod_{i=1}^{r} p_i^{\alpha_i}$ et on fait la preuve en 2 étapes :
- On peut se restreindre à des valeurs particulières de n
- on montre le résultat pour ces valeurs.

• Lemme 1 : si $n = n_1 n_2$ avec $n_1 \wedge n_2 = 1$ et $\varphi(n_1) \wedge \varphi(n_2) \geq 2$, alors $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.

_preuve : $\mathbb{Z}/n\mathbb{Z} \underset{\text{anneaux}}{\simeq} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ (th. chinois) induit l'isomorphisme de groupes

$$(\mathbb{Z}/n\mathbb{Z})^\times \underset{\text{groupes}}{\simeq} (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times =: G_1 \times G_2 .$$

Notons $m = \varphi(n_1) \vee \varphi(n_2)$, on a $m < \varphi(n_1)\varphi(n_2)$ par hypothèse sur le pgcd.

Si $x = (x_1, x_2) \in G_1 \times G_2$, $x^m = (x_1^m, x_2^m) = (1,1)$ car $m \mid \underbrace{\varphi(n_1)}_{=|G_1|}$ et $m \mid \underbrace{\varphi(n_2)}_{=|G_2|}$

donc $o(x) \leq m < \varphi(n)$ → aucun élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est d'ordre $\varphi(n)$

→ $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique

Conséquences :
- si $r \geq 2$, $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique
- si $k \geq 2$ et $r \geq 1$, $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.

_preuve :
- si $n = p_1^{\alpha_1} p_2^{\alpha_2} m$ avec $p_1 \wedge m = p_2 \wedge m = 1$, on note $n_1 = p_1^{\alpha_1}$ et $n_2 = p_2^{\alpha_2} m$, alors $n = n_1 n_2$ vérifie les conditions du lemme 1 : $n_1 \wedge n_2 = 1$ et $\varphi(n_1) = p_1^{\alpha_1 - 1}\underbrace{(p_1 - 1)}_{\in 2\mathbb{Z}}$ et $\varphi(n_2) = p_2^{\alpha_2 - 1}\underbrace{(p_2 - 1)}_{\in 2\mathbb{Z}}\varphi(m)$ sont pairs.
- si $n = 2^k p_1^{\alpha_1} m$ avec m impair, $p_1 \wedge m = 1$, on note $n_1 = 2^k$ et $n_2 = p_1^{\alpha_1} m$ alors $\varphi(n_1) = 2^{k-1}$ et $\varphi(n_2) = p_1^{\alpha_1 - 1}(p_1 - 1)\varphi(m)$: pairs tous les deux.

→ il reste à traiter les cas $\begin{cases} n = 2^k, & k \geq 0 \\ n = p^\alpha, & \alpha \geq 1 \\ n = 2p^\alpha, & \alpha \geq 1 \end{cases}$ $p \geq 3$ premier.

• Cas $n=2^k$, $k\geq 0$:

$(\mathbb{Z}/1\mathbb{Z})^\times$, $(\mathbb{Z}/2\mathbb{Z})^\times$: ok, $(\mathbb{Z}/4\mathbb{Z})^\times=\{1,3\}\simeq\mathbb{Z}/2\mathbb{Z}$: ok

mais

$(\mathbb{Z}/8\mathbb{Z})^\times\simeq(\mathbb{Z}/2\mathbb{Z})^2$: non cyclique

Si $k\geq 3$, $f: x\in(\mathbb{Z}/2^k\mathbb{Z})^\times\longmapsto\bar{x}\in(\mathbb{Z}/8\mathbb{Z})^\times$ est un morphisme de groupes surjectif et si $(\mathbb{Z}/2^k\mathbb{Z})^\times$ était cyclique de générateur g, alors $(\mathbb{Z}/8\mathbb{Z})^\times$ serait cyclique de générateur $f(g)$: absurde

• Cas $n=p^\alpha$, $\alpha\geq 1$, p premier $p\geq 3$.

Comme $|(\mathbb{Z}/n\mathbb{Z})^\times|=\varphi(n)=p^{\alpha-1}(p-1)$, on va trouver un élément d'ordre $p^{\alpha-1}$, un d'ordre $p-1$ et considérer le produit.

Lemme 2 : $\forall k\in\mathbb{N}$, $\exists\lambda_k\in\mathbb{N}$, $\lambda_k\wedge p=1$ t.q. $(1+p)^{p^k}=1+\lambda_k p^{k+1}$

preuve : . ok pour $k=0$

. si le résultat est vrai au rang $k\geq 0$,

$$(1+p)^{p^{k+1}}=(1+\lambda_k p^{k+1})^p=1+\lambda_k p^{k+2}+\underbrace{\sum_{i=2}^{p-1}\binom{p}{i}\lambda_k^i p^{i(k+1)}+\lambda_k^p p^{p(k+1)}}.$$

Or comme $i\in[\![2,p-1]\!]$, on a $p\mid\binom{p}{i}$, $i(k+1)\geq k+2$ et $p(k+1)\geq k+3$ car $p\geq 3$

donc $\exists v\in\mathbb{N}$ tq $(1+p)^{p^{k+1}}=1+\lambda_k p^{k+2}+v\cdot p^{k+3}$

$=1+\lambda_{k+1}p^{k+2}$ où $\lambda_{k+1}=\lambda_k+pv$: premier avec p.

→ Conséquence : $a=1+p\,[p^\alpha]$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. En effet.

. $(1+p)^{p^{\alpha-1}}=1+\lambda_{\alpha-1}p^\alpha\equiv 1\,[p^\alpha]$ donc $o(a)=p^\beta$ avec $\beta\leq\alpha-1$

. $(1+p)^{p^{\alpha-2}}=1+\lambda_{\alpha-2}p^{\alpha-1}\not\equiv 1\,[p^\alpha]$ (car $p\nmid\lambda_{\alpha-2}$) → $\beta=\alpha-1$

Reste à trouver un élément d'ordre $p-1$: on considère encore la surjection

$f: x\in(\mathbb{Z}/p^\alpha\mathbb{Z})^\times\longmapsto\bar{x}\in(\mathbb{Z}/p\mathbb{Z})^\times=\langle g\rangle$. Soit $h\in(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tq $f(h)=g$ et soit $d=o(h)$, alors $(\mathbb{Z}/p\mathbb{Z})^\times\ni 1=f(\underset{\in(\mathbb{Z}/p^\alpha\mathbb{Z})^\times}{1})=f(h^d)=g^d$ → $p-1=o(g)\mid d$

→ $\exists b\in\langle h\rangle\subset(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tq $o(b)=p-1$.

Comme $p^{\alpha-1}\wedge(p-1)=1$ et que a et b commutent, $ab\in(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre $p^{\alpha-1}(p-1)=\varphi(p^\alpha)$

→ $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique

• Cas $n=2p^\alpha$ ($\alpha\geq 1$, $p\geq 3$ premier)

Thm chinois : $(\mathbb{Z}/n\mathbb{Z})^\times\underset{\text{groupes}}{\simeq}(\mathbb{Z}/2\mathbb{Z})^\times\times(\mathbb{Z}/p^\alpha\mathbb{Z})^\times\simeq(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$: cyclique par ce qui précède

→ $(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$ est cyclique