Développement : Condition de cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$

Algèbre & Géométrie

Référence : [PER] Perrin D., *Cours d'algèbre*, ellipses, 1996, p25
Pour les leçons :
- 104 : Groupes finis. Exemples et applications.
- 108 : Exemples de parties génératrices d'un groupe. Applications.
- 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 121 : Nombres premiers. Applications.

Soit $n \in \mathbb{N}^*$ ($n \geqslant 2$). $\mathbb{P}$ désigne l'ensemble des nombres premiers.
Si $m \in \mathbb{Z}$, on note $\bar{m}^{[n]}$ sa réduction modulo n (i.e. sa classe dans $\mathbb{Z}/n\mathbb{Z}$).
On admet que pour tout $p \in \mathbb{P}$, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Lemme 1.

Soient $n_1, n_2 \in \mathbb{N}$. Si $n_1 \wedge n_2 = 1$ et si $\varphi(n_1) \wedge \varphi(n_2) > 1$, alors $(\mathbb{Z}/n_1n_2\mathbb{Z})^\times$ n'est pas cyclique.

Preuve : On suppose que $n_1 \wedge n_2 = 1$ et que $\varphi(n_1) \wedge \varphi(n_2) > 1$. Comme $n_1 \wedge n_2 = 1$, d'après le théorème des restes chinois, on a un isomorphisme de groupes :

$$(\mathbb{Z}/n_1n_2\mathbb{Z})^\times \simeq (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times.$$

Soit $(a,b) \in (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$. On a $(a,b)^{\varphi(n_1)\vee\varphi(n_2)} = 1$, mais :

$$\varphi(n_1) \vee \varphi(n_2) = \frac{\varphi(n_1)\varphi(n_2)}{\varphi(n_1) \wedge \varphi(n_2)} < \varphi(n_1)\varphi(n_2) = \varphi(n_1n_2).$$

Donc, pour tout $(a,b) \in (\mathbb{Z}/n_1n_2\mathbb{Z})^\times$, l'ordre de (a,b) n'est pas $\varphi(n_1n_2) = |(\mathbb{Z}/n_1n_2\mathbb{Z})^\times|$. $(\mathbb{Z}/n_1n_2\mathbb{Z})^\times$ n'est donc pas cyclique (sinon, il serait engendré par un élément, à fortiori d'ordre $\varphi(n_1n_2)$, mais il n'existe pas ici). □

Lemme 2.

Soit $p \in \mathbb{P}$. Alors :

[1] Pour tout $\ell \in [\![1; p-1]\!]$, $p \mid \binom{p}{\ell}$.

[2] On a :

$$\forall k \in \mathbb{N} \quad \exists \lambda_k \in \mathbb{N} \quad \lambda_k \wedge p = 1, \quad (1+p)^{p^k} = 1 + \lambda_k p^{k+1}.$$

Preuve : **[1]** Soit $\ell \in [\![1; p-1]\!]$. D'après le lemme d'absorption, $\ell\binom{p}{\ell} = p\binom{p-1}{\ell-1}$.

Ainsi, p divise $\ell\binom{p}{\ell}$. Mais comme $1 \leqslant \ell \leqslant p-1$ avec p premier, $p \wedge \ell = 1$, donc par le lemme de Gauss, $p \mid \binom{p}{\ell}$.

[2] Montrons la propriété $\mathcal{P}(k)$ suivante par récurrence sur $k \in \mathbb{N}^*$: "$\exists \lambda_k \in \mathbb{N} \quad \lambda_k \wedge p = 1, \quad (1+p)^{p^k} = 1 + \lambda_k p^{k+1}$ ".
Initialisation : Si $k = 0$, alors $(1+p)^{p^0} = 1 + p = 1 + \lambda_0 p$, avec $\lambda_0 = 1$ qui vérifie bien $\lambda_0 \wedge p = 1$. Donc $\mathcal{P}(0)$ est vraie.
Hérédité : Soit $k \in \mathbb{N}$. Supposons la propriété vraie au rang k, et montrons-la au rang $k+1$.
On a :

$$\begin{aligned}(1+p)^{p^{k+1}} &= ((1+p)^{p^k})^p \\ &\overset{\mathcal{P}(k)}{=} (1+\lambda_k p^{k+1})^p \\ &= 1 + \sum_{\ell=1}^{p} \binom{p}{\ell} \lambda_k^\ell p^{\ell(k+1)}.\end{aligned}$$

Maintenant, le terme $\ell = 1$ de la somme est $p\lambda_k p^{k+1} = \lambda_k p^{k+2}$. Pour $\ell \in [\![2; p-1]\!]$, le terme ℓ de la somme est divisible par $\binom{p}{\ell} p^{k+2}$, et comme $p \mid \binom{p}{\ell}$ par le point **[1]**, ce même terme est divisible par p^{k+3}. Le terme $\ell = p$ est également divisible par p^{k+3} (car $p(k+1) \geqslant 2(k+1) = 2k+2 \geqslant k+3$) On peut donc écrire cette somme sous la forme $(\lambda_k + up)p^{k+2}$, avec $u \in \mathbb{Z}$.
Finalement, $\lambda_{k+1} := \lambda_k + up$ est premier à p. En effet, si d est un diviseur commun positif à λ_{k+1} et p, alors $d \mid up$ et $d \mid (\lambda_k + up)$, donc $d \mid \lambda_k$. Mais comme d divise aussi p, et que $\lambda_k \wedge p = 1$ (d'après $\mathcal{P}(k)$), $d = 1$.

Cela prouve $\mathcal{P}(k+1)$ et achève la preuve. □

Théorème 3.

$(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si $n = 2$, $n = 4$, $n = p^\alpha$ ou $n = 2p^\alpha$ avec $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$.

PREUVE : Raisonnons par analyse-synthèse.

⋆ Analyse : Soit $n \geqslant 2$ tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. On écrit $n = 2^k p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, où les p_i sont premiers impairs, les $\alpha_i \in \mathbb{N}$ et $k \in \mathbb{N}$.
Distinguons 3 cas :
$\longrightarrow$ $s = 0$: Alors, $n = 2^k$. On va traiter ce cas dans la synthèse quand on va vérifier quels sont les $(\mathbb{Z}/2^k\mathbb{Z})^\times$ cycliques.

$\longrightarrow$ $s > 1$: Dans ce cas, on écrit $n = p_1^{\alpha_1} p_2^{\alpha_2} m$, avec $m \in \mathbb{N}^*$ tel que $m \wedge p_1 = m \wedge p_2 = 1$. On pose également $n_1 = p_1^{\alpha_1}$ et $n_2 = p_2^{\alpha_2} m$, de sorte que $n = n_1 n_2$.
On a $n_1 \wedge n_2 = 1$ et $\begin{cases} \varphi(n_1) = p_1^{\alpha_1 - 1}(p_1 - 1) \\ \varphi(n_2) = \varphi(m) p_2^{\alpha_2 - 1}(p_2 - 1) \end{cases}$.
Comme p_1 et p_2 sont impairs, $2|\varphi(n_1)$ et $2|\varphi(n_2)$, donc $\varphi(n_1) \wedge \varphi(n_2) > 1$. D'après le lemme 1, $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique ; ce cas ne peut donc pas se produire.

$\longrightarrow$ $s = 1$: En posant $n_1 = p_1^{\alpha_1}$ et $n_2 = 2^k$, on a $\varphi(n_1) = p_1^{\alpha_1 - 1}(p_1 - 1)$ et $\varphi(n_2) = 2^{k-1}$.
Si $k > 1$, alors comme précédemment, comme 2 divise $\varphi(n_1)$ et $\varphi(n_2)$, $\varphi(n_1) \wedge \varphi(n_2) > 1$. Par le lemme 1, ce cas ne peut donc encore une fois pas se produire.
Si $k \leqslant 1$, par contre, le lemme 1 n'est pas applicable : $\varphi(n_1) \wedge \varphi(n_2) = 1$.

⋆ Synthèse : On va traiter tous les cas qu'on a gardés dans l'analyse.
$\longrightarrow$ Cas $s = 0$, i.e. $n = 2^k$: Si $k = 1$, $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ est bien entendu cyclique.
Si $k = 2$, $(\mathbb{Z}/4\mathbb{Z})^\times = \{1; 3\}$ est cyclique, engendré par 3.
Si $k = 3$, $(\mathbb{Z}/8\mathbb{Z})^\times = \{1; 3; 5; 7\}$ n'est pas cyclique (chaque élément est d'ordre 2, et donc aucun d'ordre $\varphi(8) = 4$).
Soit $k \geqslant 3$. Soit $\varphi : (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$ l'application de réduction modulo 8 définie par :

$$\forall \bar{n}^{[2^k]} \in (\mathbb{Z}/2^k\mathbb{Z})^\times \quad \varphi(\bar{n}^{[2^k]}) = \bar{n}^{[8]}.$$

Comme $k \geqslant 3$, et que donc $8|2^k$, φ est bien définie. C'est de plus un morphisme de groupes surjectif.
Si $(\mathbb{Z}/2^k\mathbb{Z})^\times$ était cyclique, en notant g un générateur de ce groupe, comme φ est surjective, $\varphi(g)$ engendrerait $(\mathbb{Z}/8\mathbb{Z})^\times$, qui n'est pourtant pas cyclique. Cela ne se peut ; donc $(\mathbb{Z}/2^k\mathbb{Z})^\times$ n'est pas cyclique.

$\longrightarrow$ Cas $s = 1$ et $k = 0$, i.e. $n = p^\alpha$, $p \in \mathbb{P}$ impair et $\alpha \geqslant 1$: Alors, $\varphi(n) = p^{\alpha-1}(p-1)$.
D'après le lemme 2 (appliqué à $k = \alpha - 1$), $(1+p)^{p^{\alpha-1}} \equiv 1[p^\alpha]$.
Soit $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ l'application de réduction modulo p. ψ est un morphisme de groupes surjectif bien défini.
On sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique (d'ordre $p-1$), engendré par un élément g. Il existe $h \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tel que $\varphi(h) = g$.
Soit β l'ordre de h. On a :

$$\begin{aligned} 1 &= \varphi(h)^\beta \\ &= g^\beta, \end{aligned}$$

et g est d'ordre $p-1$, donc $p-1|\beta$. Il existe donc $k \in \mathbb{Z}$ tel que $\beta = k(p-1)$, et h^k est d'ordre $p-1$.
Montrons que $1+p$ est d'ordre p^α dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. D'après le lemme 2, $1+p$ est d'ordre divisant p^α, donc il suffit de montrer que $(1+p)^{\alpha-1} \neq 1$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.
On a $(1+p)^{\alpha-1} = 1 + \lambda_{\alpha-1} p^{\alpha-1}$. S'il était égal à 1 modulo p^α, on aurait $\lambda_{\alpha-1} p^{\alpha-1} \equiv 0[p^\alpha]$, et donc $p^\alpha | \lambda_{\alpha-1} p^{\alpha-1}$.
Ainsi, $p|\lambda_{\alpha-1}$, mais par le lemme 2, $\lambda_{\alpha-1} \wedge p = 1$, ce qui est absurde.
Donc l'ordre de $1+p$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ est p^α.
Maintenant, $(1+p)h^k$ est d'ordre $p^\alpha \vee (p-1) = p^{\alpha-1}(p-1)$, qui est l'ordre de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Cet élément engendre donc $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, qui est finalement cyclique.

$\longrightarrow$ Cas $s = 1$ et $k = 1$, i.e. $n = 2p^\alpha$, $p \in \mathbb{P}$ impair et $\alpha \geqslant 1$: Par le théorème des restes chinois,

$$\begin{aligned} (\mathbb{Z}/2p^\alpha\mathbb{Z})^\times &\simeq (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \\ &\simeq \{1\} \times (\mathbb{Z}/p^\alpha\mathbb{Z})^\times, \end{aligned}$$

donc $(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$ est un produit de deux groupes cycliques d'ordres premiers entre eux. Il est donc cyclique.

$\longrightarrow$ En résumé : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si $n = 2^k$ avec $k \in \{0; 1\}$ (i.e. $n = 2$ ou $n = 4$), ou $n = p^\alpha$ ou $n = 2p^\alpha$, avec $p \in \mathbb{P}$ impair et $\alpha \geqslant 1$.
Cela achève la preuve. □