Condition de cyclicité des $(\mathbf{Z}/n\mathbf{Z})^\times$

Émile Séguret

Pour les leçons : 104, 108, 110, 120, 121

Références : en partie le Cours d'Algèbre de Perrin

Prérequis. On admet le fait suivant : si p est premier, alors le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique.

Théorème. Pour $n \geq 1$,

$$(\mathbf{Z}/n\mathbf{Z})^\times \text{ est cyclique } \iff n = 1, 2, 4, p^\alpha \text{ ou } 2p^\alpha, \text{ avec } p \geq 3 \text{ premier et } \alpha \geq 1.$$

Démonstration. On commence par décomposer n en produits de nombres premiers $n = 2^k p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $k, r \geq 0$, $\alpha_i \geq 1$, $p_i \geq 3$ premiers. On fait une preuve en deux étapes. La première permet de se restreindre à des valeurs particulières de n, que l'on traite ensuite dans la seconde étape.

Étape 1. Discuter suivant les valeurs de k et r. Pour cela on établit d'abord un lemme.

Lemme 1. Si $n = n_1 n_2$ avec $\mathrm{pgcd}(n_1, n_2) = 1$ et $\mathrm{pgcd}(\varphi(n_1), \varphi(n_2)) \geq 2$, alors $(\mathbf{Z}/n\mathbf{Z})^\times$ n'est pas cyclique.
Preuve. Par le théorème Chinois, on a l'isomorphisme d'anneaux $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z}$ qui induit l'isomorphisme de groupes $(\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/n_1\mathbf{Z})^\times \times (\mathbf{Z}/n_2\mathbf{Z})^\times = \mathrm{G}_1 \times \mathrm{G}_2$. Soit $m = \mathrm{ppcm}(\varphi(n_1), \varphi(n_2)) < \varphi(n_1)\varphi(n_2)$ (via l'hypothèse sur le pgcd). Pour $x = (x_1, x_2) \in \mathrm{G}_1 \times \mathrm{G}_2$, on a :

$$x^m = (x_1^m, x_2^m) = (1, 1), \text{ car } m \text{ divise } \varphi(n_1) = \mathrm{Card}(\mathrm{G}_1) \text{ et } \varphi(n_2) = \mathrm{Card}(\mathrm{G}_2).$$

Donc $\mathrm{ord}(x) \leq m < \varphi(n_1)\varphi(n_2) = \varphi(n)$. Via l'isomorphisme $(\mathbf{Z}/n\mathbf{Z})^\times \simeq \mathrm{G}_1 \times \mathrm{G}_2$, aucun élément de $(\mathbf{Z}/n\mathbf{Z})^\times$ n'est d'ordre $\varphi(n) = \mathrm{Card}\left((\mathbf{Z}/n\mathbf{Z})^\times\right)$. Conclusion : ce groupe n'est pas cyclique.

Applications.

1. Si $r \geq 2$, alors $(\mathbf{Z}/n\mathbf{Z})^\times$ n'est pas cyclique,
2. Si $k \geq 2$ et $r \geq 1$, alors $(\mathbf{Z}/n\mathbf{Z})^\times$ n'est pas cyclique.

Preuve. Pour le premier point on écrit $n = p_1^{\alpha_1} p_2^{\alpha_2} m$ avec p_1 et p_2 premiers avec m. On note $n_1 = p_1^{\alpha_1}$ et $n_2 = p_2^{\alpha_2} m$ de sorte que $n = n_1 n_2$ vérifie les conditions du lemme 1. En effet n_1 et n_2 sont premiers entre eux et $\varphi(n_1) = p_1^{\alpha_1 - 1}(p_1 - 1)$ et $\varphi(n_2) = p_2^{\alpha_2 - 1}(p_2 - 1)\varphi(m)$ sont tous les deux pairs. Le résultats du lemme 1 conclut.
On fait de même pour le second point en écrivant $n = 2^k p_1^{\alpha_1} m$, avec m impair non divisible par p_1. Si $n_1 = 2^k$ et $n_2 = p_1^{\alpha_1} m$ alors $\varphi(n_1) = 2^{k-1}$ et $\varphi(n_2) = p_1^{\alpha_1 - 1}(p_1 - 1)\varphi(m)$ sont pairs.

Conséquence : Il nous reste les cas $n = 2^k$ $(k \geq 0)$, $n = p^\alpha$ et $n = 2p^\alpha$ $(\alpha \geq 1$, $p \geq 3$ premier$)$.

Étape 2. Traiter ces cas.

Cas $n = 2^k$ $(k \geq 0)$.
D'abord $(\mathbf{Z}/1\mathbf{Z})^\times$ et $(\mathbf{Z}/2\mathbf{Z})^\times$ sont triviaux et $(\mathbf{Z}/4\mathbf{Z})^\times = \{1 \bmod 4,\ 3 \bmod 4\} \simeq \mathbf{Z}/2\mathbf{Z}$. Ensuite $(\mathbf{Z}/8\mathbf{Z})^\times = \{1 \bmod 8,\ 3 \bmod 8,\ 5 \bmod 8,\ 7 \bmod 8\} \simeq (\mathbf{Z}/2\mathbf{Z})^2$ est non cyclique.
Soient maintenant $k \geq 3$ et $f : x \bmod 2^k \in \left(\mathbf{Z}/2^k\mathbf{Z}\right)^\times \mapsto x \bmod 8 \in (\mathbf{Z}/8\mathbf{Z})^\times$ morphisme de groupe surjectif. Si, par l'absurde, $\left(\mathbf{Z}/2^k\mathbf{Z}\right)^\times$ était cyclique engendré par g alors $(\mathbf{Z}/8\mathbf{Z})^\times$ serait cyclique engendré par $f(g)$. Impossible.

Cas $n = p^\alpha$ $(\alpha \geq 1,\ p \geq 3$ premier$)$.
Rappelons que $\mathrm{Card}((\mathbf{Z}/p^\alpha\mathbf{Z})^\times) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Notre but est de trouver un élément d'ordre $p^{\alpha-1}$ et un d'ordre $p-1$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$, pour ensuite considérer le produit.

Lemme 2. $\forall k \in \mathbf{N},\ \exists \lambda_k \in \mathbf{N}$ premier avec p, $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$.
Preuve. Par récurrence sur k.
Pour $k = 0$: $(1+p)^{p^0} = 1 + \lambda_0 p$, avec $\lambda_0 = 1$.
Supposons le résultat vrai au rang $k \geq 0$ et montrons le au rang $k+1$. On a

$$(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p = \left(1 + \lambda_k p^{k+1}\right)^p = 1 + \lambda_k p^{k+2} + \sum_{j=2}^{p-1} \binom{p}{j} \lambda_k^j p^{j(k+1)} + \lambda_k^p p^{p(k+1)}.$$

Dans la somme précédente, p divise $\binom{p}{j}$ et $j(k+1) \geq k+2$. Enfin $p(k+1) \geq k+3$, puisque $p \geq 3$ (cela est faux si $k = 0$ et $p = 2$). On peut donc trouver un entier u tel que $(1+p)^{p^{k+1}} = 1 + \lambda_k p^{k+2} + u p^{k+3} = 1 + \lambda_{k+1} p^{k+2}$ avec $\lambda_{k+1} = \lambda_k + up$ premier à p.

Conséquence : l'élément $a = 1 + p \bmod p^\alpha$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. En effet :
- $(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1 \bmod p^\alpha$, donc l'ordre s'écrit p^β avec $\beta \leq \alpha - 1$,
- $(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1} \not\equiv 1 \bmod p^\alpha$ (car p ne divise pas $\lambda_{\alpha-2}$), donc $\beta = \alpha - 1$.

Il nous reste à trouver un élément d'ordre $p-1$. Pour cela on considère (encore) $f : x \bmod p^\alpha \in (\mathbf{Z}/p^\alpha\mathbf{Z})^\times \mapsto x \bmod p \in (\mathbf{Z}/p\mathbf{Z})^\times = <g>$ morphisme de groupe surjectif. Soit $h \in (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ tel que $g = f(h)$ et $d = \mathrm{ord}(h)$, alors :

$$1 \bmod p = f(1 \bmod p^\alpha) = f(h^d) = f(h)^d = g^d.$$

Donc $p - 1 = \mathrm{ord}(g)$ divise d. Il existe donc $b \in <h> \subset (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ tel que $\mathrm{ord}(b) = p - 1$.
Comme $p^{\alpha-1}$ est premier avec $p-1$ et que a et b commutent, alors le produit ab est d'ordre le produit des ordres $p^{\alpha-1}(p-1) = \varphi(p^\alpha)$. Conclusion : $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ est cyclique engendré par ab.

Cas $n = 2p^\alpha$ $(\alpha \geq 1,\ p \geq 3$ premier$)$.
On utilise simplement le théorème Chinois et le cas précédent : $(\mathbf{Z}/2p^\alpha\mathbf{Z})^\times \simeq (\mathbf{Z}/2\mathbf{Z})^\times \times (\mathbf{Z}/p^\alpha\mathbf{Z})^\times \simeq (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ cyclique.

Remarques :
- pour une preuve du fait que $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique, voir le Cours d'Algèbre de Perrin page 74,
- pour $k \geq 3$, on a montré que $\left(\mathbf{Z}/2^k\mathbf{Z}\right)^\times$ n'est pas cyclique, plus précisément, on a l'isomorphisme $\left(\mathbf{Z}/2^k\mathbf{Z}\right)^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{k-2}\mathbf{Z}$.