Condition pour que $\mathbb{Z}/n\mathbb{Z}$ soit cyclique

Théorème : Soit $n \geq 2$. Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique si et seulement si $n = 2, 4, 2p^\alpha, p^\alpha$ où p est un nombre premier impair.

Lemme 0 : (admis) Si p est un nombre premier impair le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

Lemme 1 : Soit p premier impair et $k \in \mathbb{N}$. Il existe $\lambda \in \mathbb{N}^*$, premier avec p, tel que $(1+p)^{p^k} = 1 + \lambda p^{k+1}$.

Corollaire 1 : Si p premier impair et $\alpha \geq 1$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

Lemme 2 : Si $k \in \mathbb{N}$, il existe λ impair tel que $5^{2^k} = 1 + \lambda 2^{k+2}$.

Corollaire 2 : Si $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-1}\mathbb{Z}$.

Preuve lemme 1 : On raisonne par récurrence sur k. Pour $k = 0$ on prend $\lambda = 1$. On suppose maintenant le résultat vrai pour $k = 0, ..., n-1$. On a alors

$$\begin{aligned}(1+p)^{p^n} &= \left((1+p)^{p^{n-1}}\right)^p \\ &= (1+\lambda p^n)^p \\ &= 1 + \binom{p}{1}\lambda p^n + \sum_{k=2}^{p}\binom{p}{k}\lambda^k p^{kn} \\ &= 1 + \lambda' p^{n+1}, \text{ avec } \lambda' = \lambda + Cp\end{aligned}$$

où $C = \displaystyle\sum_{k=2}^{p}\binom{p}{k}\lambda^k p^{(k-1)n-1}$. On a ainsi la forme voulu et on remarque λ' est bien premier avec p car λ l'est. Ceci achève la récurrence. □

Preuve du corollaire 1 : En notant $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la projection canonique on peut voir que $p^\alpha\mathbb{Z} \subset \ker(\pi)$ donc on peut passer au quotient pour avoir une projection surjective $\tilde{\pi} = \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Si $x \in \mathbb{Z}$ on peut voir que $\pi(x) = \tilde{\pi}(x)$ donc le morphisme induit $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ est toujours surjectif. Par le lemme 0 on peut se donner un élément x de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ tel que son image engendre $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. On sait alors que l'ordre de x est un multiple de $p-1$ donc on peut trouver un élément y d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ (il suffit de prendre $x^{\frac{\text{ordre}(x)}{p-1}}$).

Le lemme précédent nous dit que $p+1$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. En effet, on sait que son ordre est de la forme p^β mais si $\beta \leq \alpha - 2$ le lemme affirme que

$$(p+1)^{p^\beta} = 1 + \lambda p^{\beta+1}$$

mais λ est premier avec p donc on ne peut pas avoir $p^\alpha | \lambda p^{\beta+1}$.

On conclut en disant que $\mathbb{Z}/p^\alpha\mathbb{Z}$ est abélien $\text{ord}(y) \wedge \text{ord}(p+1) = 1$ donc l'ordre du produit est le produit des ordres, à savoir $\text{ord}(y(p+1)) = (p-1)p^{\alpha-1}$. Comme $\#(\mathbb{Z}/p^\alpha\mathbb{Z})^* = (p-1)p^{\alpha-1}$, notre groupe est bien cyclique.□

Preuve du lemme 2 : C'est la même idée que le lemme 1, en plus facile.□

Preuve du corollaire 2 : Soit $\tilde{\pi} : (\mathbb{Z}/2^\alpha\mathbb{Z})^* \to \mathbb{Z}/2\mathbb{Z}$ le morphisme définit dans le corollaire 1. On note $N = \ker(\tilde{\pi})$ et $H = \{-1, 1\} \subset (\mathbb{Z}/2^\alpha\mathbb{Z}))^*$. Comme $N \cap H = \{1\}$ on a l'isomorphisme suivant

$$\begin{array}{ccc} N \times H & \to & NH := \{nh \ : \ n \in N, \ h \in H\} \\ (n,h) & \mapsto & nh \end{array}.$$

On a ainsi $\#NH = \#N\#H = \#(\mathbb{Z}/2^\alpha\mathbb{Z}))^*$ (car on sait que $\#\ker(\tilde{\pi})\#\text{Im}(\tilde{\pi}) = \#(\mathbb{Z}/2^\alpha\mathbb{Z}))^*$). On a alors

$$N \times H \simeq NH = (\mathbb{Z}/2^\alpha\mathbb{Z}))^*,$$

d'où le résultat voulu. □

Preuve du théorème : On écrit la décomposition en facteurs premiers de $n = p_1^{\alpha_1}...p_l^{\alpha_l}$. Par le théorème d'isomorphisme chinois on a alors

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times ... \times (\mathbb{Z}/p_l^{\alpha_l}\mathbb{Z})^*.$$

Si n est de la forme donnée dans l'énoncé, il est clair que $\mathbb{Z}/n\mathbb{Z}$ est cyclique avec les lemme précédents. Dans les autres cas on va pouvoir trouver un sous-groupe isomorphe à un produit non trivial de $\mathbb{Z}/m\mathbb{Z}$ et notre groupe ne pourra alors pas être cyclique. Par exemple, supposons que $n = 2^\beta p^\alpha$ avec $\beta \geq 2$. On a alors

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

et donc $\mathbb{Z}/n\mathbb{Z}$ contient le sous-groupe non-cyclique $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ et ne peut donc être cyclique. □

Remarques importantes :

- Il faut savoir démontrer le lemme 0 ainsi que ce qui a été supposé connu sur le groupe des inversible de $\mathbb{Z}n\mathbb{Z}$ (le cardinal notamment) je pense.
- L'isomorphisme donné dans la preuve du corollaire 2 n'est pas compliqué mais il faut l'avoir regardé avant le jour j quand même.