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

CN / Soit $n \geq 2$ tq $\mathbb{Z}/n\mathbb{Z}^\times$ est cyclique et soit r un générateur. On pose $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ la déc de n. On a d'après le théorème d'Euler :

$$r^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}} \quad \text{pour tout } i \in [\![1, t]\!]$$

donc $$r^{\operatorname{ppcm}(\phi(p_1^{\alpha_1}), \dots, \phi(p_t^{\alpha_t}))} \equiv 1 \pmod{n}$$

donc $o_n(r)$ divise le ppcm, càd $\phi(n) \mid \operatorname{ppcm}(\phi(p_i^{\alpha_i}))_{i=1}^t$

D'autre part $\operatorname{ppcm}(\phi(p_i^{\alpha_i}))_{i=1}^t \mid \phi(p_1^{\alpha_1}) \dots \phi(p_t^{\alpha_t}) = \phi(n)$.

Il vient que $\phi(p_1^{\alpha_1}), \dots, \phi(p_t^{\alpha_t})$ sont deux à deux premiers entre eux, ce qui impose (argument de parité) que $n \in \{2^\alpha, p^\alpha, 2p^\alpha\}$

Cas $n = p$ p premier impair

Soit $G = \mathbb{Z}/p\mathbb{Z}^\times$ et soit $e = \operatorname{ppcm}\{o(x) \mid x \in G\}$. D'après Lagrange, tous les ordres divisent $|G|$, ainsi $e \mid p-1$.

D'autre part, chaque $x \in G$ est racine du polynôme $X^e - 1$. Or ce polynome admet au plus e racines, donc $p - 1 \leq e$.

Ainsi $e = p-1$, et comme G est abélien, on sait qu'il possède un élément d'ordre e, cqfd.

Pour les autres cas, nous utiliserons le lemme suivant :

Lemme. (LTE)

Soit p un nombre premier impair, et soient a, b deux entiers tels que $p \mid a - b$ mais p ne divise ni a ni b. Alors

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n)$$

Cas $n = p^2$ p premier impair

Soit g un générateur modulo p, on va montrer qu'au moins un parmi g et $g+p$ est générateur modulo p^2 :

On a $p-1 = o_p(g) \mid o_{p^2}(g) \mid p(p-1)$

et de même pour $g+p$, puisque $g+p \equiv g \pmod p$.

Ainsi, $o_{p^2}(g), o_{p^2}(g+p) \in \{p-1, p(p-1)\}$. Il suffit alors de montrer qu'il est impossible que ces deux ordres soient égaux à $p-1$. En effet, si c'était le cas, on aurait $p^2 \mid (g+p)^{p-1} - g^{p-1}$. Or, d'après notre lemme, on a

$$v_p\left((g+p)^{p-1} - g^{p-1}\right) = v_p(p) + v_p(p-1) = 1$$

Contradiction. D'où le résultat.

Cas $n = p^k$ p premier impair $k \geq 2$

Soit g un générateur mod p^2, on va montrer par récurrence que g est un générateur modulo p^k pour tout $k \geq 2$:

Le cas $k=2$ est immédiat. Supposons le résultat vrai au rang k et montrons qu'il l'est au rang $k+1$:

On a $p^{k-1}(p-1) = o_{p^k}(g) \mid o_{p^{k+1}}(g) \mid p^k(p-1)$

Donc $o_{p^{k+1}}(g) \in \{p^{k-1}(p-1), p^k(p-1)\}$. Il suffit de montrer que $o_{p^{k+1}}(g) = p^{k-1}(p-1)$ est impossible. En effet, on aurait dans ce cas que $p^{k+1} \mid g^{p^{k-1}(p-1)} - 1$,

Or, d'après le lemme, on a

$$v_p\left(g^{p^{k-1}(p-1)} - 1\right) = v_p\left(g^{p-1} - 1\right) + v_p\left(p^{k-1}\right) = 1 + k - 1 = k$$

Contradiction. D'où le résultat.

Cas $n = 2^\alpha$

Il est évident que $\mathbb{Z}/1\mathbb{Z}^\times$, $\mathbb{Z}/2\mathbb{Z}^\times$ et $\mathbb{Z}/4\mathbb{Z}^\times$ sont cycliques. En revanche, $\mathbb{Z}/8\mathbb{Z}^\times$ ne l'est pas (tous ses éléments sont d'ordre 2). Pour tout $\alpha \geq 4$, si $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ était cyclique, alors son générateur mod 2^α va parcourir toutes les classes mod 8, donc sa classe mod 8 engendrerait $(\mathbb{Z}/8\mathbb{Z})^\times$, absurde.

En conclusion, $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi $n \in \{1, 2, 4, p^\alpha, 2p^\alpha\}$ avec p premier impair et $\alpha \in \mathbb{N}^*$.

Bonus : Pour $n \in \{1, 2, 4, p^q, 2p^q\}$, comptons le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}^\times$:

Soit g un générateur modulo n, alors $\mathbb{Z}/n\mathbb{Z}^\times = \{\bar{g}, \bar{g}^2, \dots, \bar{g}^{\phi(n)}\}$
Pour $k \in [\![1, \phi(n)]\!]$, g^k est un générateur ssi $o_n(g^k) = p - 1$
Or, on a la formule

$$o_n(g^k) = \frac{o(g)}{k \wedge o(g)} = \frac{\phi(n)}{k \wedge \phi(n)}$$

Ainsi, $o_n(g^k) = \phi(n)$ ssi $k \wedge \phi(n) = 1$. Le nombre de tels k entre 1 et $\phi(n)$ est exactement $\phi(\phi(n))$!

Preuve du lemme admis

Etape 1 : On montre le résultat lorsque $p \nmid n$

On a $v_p(a^n - b^n) = v_p(a-b) + v_p(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$

Puisque $p \mid a - b$ on a $a \equiv b \ (p)$. Ainsi,

$$a^{n-1} + a^{n-2}b + \dots + b^{n-1} \equiv a^{n-1} + a^{n-1} + \dots + a^{n-1} \equiv n a^{n-1} \ (p)$$

Comme $p \nmid n$ alors $v_p\left(\sum_{i=0}^{n-1} a^i b^{n-1-i}\right) = 0 = v_p(n)$.

Etape 2 : On montre le résultat lorsque $n = p$

Il suffit de montrer que $v_p\left(\sum_{i=0}^{p-1} a^i b^{p-1-i}\right) = v_p(n) = 1$.

On a modulo p^2 :

$$a^i = (b + (a-b))^i \equiv b^i + i b^{i-1}(a-b) + \underbrace{\dots}_{0} \ (p^2)$$

donc

$$\begin{aligned}\sum_{i=0}^{p-1} a^i b^{p-1-i} &\equiv \sum_{i=0}^{p-1} \left(b^{p-1} + i(a-b)b^{p-2}\right) \\ &\equiv \sum_{i=0}^{p-1} b^{p-1} + (a-b)b^{p-2} \sum_{i=0}^{p-1} i \\ &\equiv p b^{p-1} + \underbrace{(a-b) b^{p-2} p \frac{(p-1)}{2}}_{\equiv 0} \ (p^2)\end{aligned}$$

Donc $\sum_{i=0}^{p-1} a^i b^{p-1-i}$ est divisible par p mais non par p^2, donc sa valuation p-adique vaut 1, comme voulu.

Par une récurrence immédiate, on obtient

$$v_p(a^{p^\alpha} - b^{p^\alpha}) = v_p(a-b) + \alpha$$

Étape 3 : Pour n quelconque.

On pose $n = p^\alpha m$ avec $p \nmid m$, alors

$$\begin{aligned} v_p(a^n - b^n) &= v_p((a^m)^{p^\alpha} - (b^m)^{p^\alpha}) \\ &= v_p(a^m - b^m) + \alpha \qquad \text{(étape 2)} \\ &= v_p(a-b) + v_p(m) + \alpha \qquad \text{(étape 1)} \\ &= v_p(a-b) + \alpha \\ &= v_p(a-b) + v_p(n) \end{aligned}$$

Cqfd.