Recasages possibles : 104, 108, 120, 121.
Référence : Cours d'algèbre, Perrin (p. 25-26) - Carnet de voyage en Algébrie, Caldero (p. 207-208).

Développement On admet que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. On cherche à déterminer les $n \in \mathbb{N}_{\geqslant 2}$ tels que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Lemme 1 Si $m \mid n$, le morphisme de groupes naturel $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ est surjectif.

Lemme 2 Pour $p \geqslant 3$ premier et $\alpha \in \mathbb{N}_{\geqslant 2}$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

Théorème 3 $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n \in \{2, 4\}$ ou $n \in \{p^\alpha, 2p^\alpha\}$ avec p premier impair et $\alpha \geqslant 1$.

- *Preuve du Lemme 1* : Montrons tout d'abord que ce morphisme "naturel" existe. On considère la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, qui est un morphisme d'anneaux surjectif (comme son nom l'indique). Comme $m \mid n$, on a $n\mathbb{Z} \subset m\mathbb{Z} = \mathrm{Ker}(\pi)$ donc π induit un morphisme d'anneaux $\overline{\pi} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Par restriction aux inversibles, on obtient notre morphisme de groupes naturel

$$\psi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$$

  Pour montrer la surjectivité de ψ, prenons $b \in \mathbb{Z}$ premier avec m, de sorte que $\pi(b) \in (\mathbb{Z}/m\mathbb{Z})^\times$. On cherche $k \in \mathbb{Z}$ tel que $b + km$ soit premier avec n. En effet, alors l'image β de $b + km$ dans $\mathbb{Z}/n\mathbb{Z}$ est en fait dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et vérifie $\psi(\beta) = b$. Notons $p_1, \ldots, p_r$ l'ensemble des nombres premiers divisant n mais ne divisant par b et posons $k = p_1 \cdots p_r$. Alors, on vérifie que $b + km$ est premier avec n : si p est un nombre premier qui divise n, alors on distingue selon si p divise b ou non. Si $p \mid b$, alors comme $b \wedge m = 1$, $p \nmid m$, et $p \nmid k$ par construction, donc $p \nmid km$ par le lemme d'Euclide. Ainsi, $p \nmid b + km$. Si $p \nmid b$, alors $p \mid k$ par construction, donc $p \mid km$ et $p \nmid b + km$. Dans tous les cas, $p \nmid b + km$, donc n et $b + km$ sont premiers entre eux. Comme vu précédemment, si β est la classe de $b + km$ dans $\mathbb{Z}/n\mathbb{Z}$, alors $\psi(\beta) = b$, d'où la surjectivité de ψ. Ceci conclut la preuve du **Lemme 1**.

- *Preuve du Lemme 2* : Soit p premier impair et $\alpha \geqslant 2$. Montrons tout d'abord par récurrence sur k que pour tout $k \in \mathbb{N}_{\geqslant 1}$, il existe $\lambda \in \mathbb{N}_{\geqslant 1}$ premier à p tel que

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

  · Pour $k = 1$, on a d'après le binôme de Newton $(1+p)^p = 1 + \binom{p}{1}p + \sum_{i=2}^{p} \binom{p}{i} p^i$. Or, $\binom{p}{1} = p$ et pour tout $i \in [\![2, p]\!]$, $p^3 \mid \binom{p}{i} p^i$. En effet, pour $i = 2$, $p \mid \binom{p}{2}$, d'où $p^3 \mid \binom{p}{2} p^2$, et pour $i \in [\![3, p]\!]$, $p^3 \mid p^i$. Ainsi,

$$(1+p)^p = 1 + p^2 + up^3 = 1 + p^2(1 + up), \text{ avec } u \in \mathbb{N}.$$

  En posant $\lambda = 1 + up$, qui est bien premier à p, on obtient le résultat.
  · Soit $k \in \mathbb{N}_{\geqslant 1}$. Supposons qu'il existe λ premier à p tel que

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

  Alors, toujours d'après le binôme de Newton, on a

$$(1+p)^{p^{k+1}} = (1 + \lambda p^{k+1})^p = 1 + \lambda p^{k+2} + \sum_{i=2}^{p} \binom{p}{i} \lambda^i p^{(k+1)i}$$

  Or, pour tout $i \in [\![2, p]\!]$, $(k+1)i \geqslant 2k + 2 \geqslant k + 3$ car $k \geqslant 1$. Ainsi, il existe $u \in \mathbb{N}$ tel que

$$(1+p)^{p^{k+1}} = 1 + \lambda p^{k+2} + up^{k+3} = 1 + p^{k+2}(\lambda + up).$$

  Or, λ premiers à p, donc $\lambda + up$ est premier à p, et ainsi la propriété est vraie au rang $k+1$, ce qui achève la récurrence.

En particulier, $(1+p)^{p^{\alpha-1}} \equiv 1\ [p^\alpha]$, donc l'ordre de $(1+p)$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est un diviseur de $p^{\alpha-1}$. Or, il existe $\lambda \in \mathbb{N}_{\geqslant 1}$ premier à p tel que

$$(1+p)^{p^{\alpha-2}} = 1 + \lambda p^{\alpha-1}.$$

Puisque λ est premier à p, p ne divise pas λ et donc p^α ne divise pas $\lambda p^{\alpha-1}$. Ainsi, $(1+p)^{p^{\alpha-2}} \not\equiv 1\ [p^\alpha]$, *i.e* l'ordre de $(1+p)$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ ne divise pas $p^{\alpha-2}$. C'est donc exactement $p^{\alpha-1}$.

Comme $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, on cherche désormais un élément de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ d'ordre $p-1$. D'après le **Lemme 1**, on a un morphisme de groupes surjectif

$$\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

On choisit $a \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ antécédent de $\overline{1} \in \mathbb{Z}/(p-1)\mathbb{Z}$ par ψ. Alors, si $d \in \mathbb{N}_{\geqslant 1}$ est l'ordre de a dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, on a $a^d = \dot{1}$ donc $\psi(a^d) = d\psi(a) = \psi(\dot{1}) = \overline{0}$. Ainsi, comme $\psi(a) = \overline{1}$, on a $\overline{d} = \overline{0}$, et donc $p-1 \mid d$. Si on écrit $d = (p-1)m$ avec $m \in \mathbb{N}_{\geqslant 1}$, on voit alors que a^m est d'ordre $p-1$. Finalement, comme $p^{\alpha-1}$ et $p-1$ sont premiers entre eux, l'élément $(1+p)a^m$ est d'ordre $p^{\alpha-1}(p-1)$ qui est exactement $\varphi(p^\alpha) = \#(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. On a bien trouvé un générateur de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ qui est donc un groupe cyclique, ce qui achève la preuve du **Lemme 2**.

- *Preuve du Théorème 3* : Montrons que la condition donnée dans l'énoncé est suffisante. On a $(\mathbb{Z}/2\mathbb{Z})^\times \simeq \{1\}$ et $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$ qui sont cycliques. D'après le **Lemme 2**, si p est premier impair et $\alpha \geqslant 1$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique. Enfin, d'après le théorème des restes chinoix,

$$\mathbb{Z}/2p^\alpha\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z},$$

donc en passant aux inversibles,

$$(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times \simeq \{1\} \times (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$$

qui est cyclique. Montrons désormais que la condition est nécessaire. Soit $n \in \mathbb{N}_{\geqslant 1}$ différent de $2, 4, p^\alpha, 2p^\alpha$ pour tout p premier impair et $\alpha \in \mathbb{N}_{\geqslant 1}$. Supposons que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. Alors, n est divisible soit par 8, soit par $4p$, soit par pq avec $p \neq q$ premiers impairs. Si $8 \mid n$, alors par le **Lemme 1**, on a un morphisme de groupes surjectif $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$. En particulier, $(\mathbb{Z}/8\mathbb{Z})^\times$ est cyclique, ce qui est faux puisque $(\mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Par le même raisonnement, si $4p \mid n$ ou si $pq \mid n$ avec $p \neq q$ premiers impairs, alors on obtient que $(\mathbb{Z}/4p\mathbb{Z})^\times$ ou $(\mathbb{Z}/pq\mathbb{Z})^\times$ est cyclique. Or, d'après le théorème des restes chinoix, on a

$$(\mathbb{Z}/4p\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \quad \text{et} \quad (\mathbb{Z}/pq\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z}.$$

On voit alors que comme $p-1, q-1$ et 2 sont pairs, d'après la réciproque du théorème des restes chinoix, ces groupes ne sont pas cycliques. En conclusion $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est bien cyclique que dans les cas $n = 2, 4, p^\alpha, 2p^\alpha$ avec p premier impair et $\alpha \in \mathbb{N}_{\geqslant 1}$.