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

↳ Refs : Perrin p 25-27 + Rombaldi p 300-302

Lemme 1 : 1) Soit p un nombre premier impair et $k \in \mathbb{N}^*$, alors $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$ avec λ_k premier avec p.

2) Soit $k \in \mathbb{N}^*$, alors $(5)^{2^k} = 1 + \mu_k 2^{k+2}$ avec μ_k impair

Proposition : 1) Soit p un nombre premier impair et α un entier ≥ 2, alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

2) Soit $\alpha \geq 3$, alors $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$

Lemme 2 : Soient $n_1, n_2 \in \mathbb{N}$. Si $n_1 \wedge n_2 = 1$ et $\varphi(n_1) \wedge \varphi(n_2) > 1$, alors $(\mathbb{Z}/n_1 n_2\mathbb{Z})^\times$ n'est pas cyclique.

Théorème : Soit $n \geq 2$. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2, 4, p^\alpha$ ou $2p^\alpha$ pour $p \geq 3$ premier et $\alpha \geq 1$.

Preuve du lemme 1 : Nous allons montrer les résultats par récurrence.

1) Initialisation : Pour $k=1$, on a $(1+p)^p = \sum_{i=0}^{p} \binom{p}{i} p^i = 1 + p^2 + \underbrace{\sum_{i=2}^{p-1} \binom{p}{i} p^i + p^p}_{= up^3}$

Pour $i \in [\![2, p-1]\!]$, $p^3 \mid \binom{p}{k} p^i$ et comme $p \geq 3$, $p^3 \mid p^p$. donc $(1+p)^p = 1 + p^2 + up^3 = 1 + p^2 \underbrace{(1+up)}_{=:\lambda_1 \text{ premier avec } p}$ avec $u \in \mathbb{N}$.

à l'oral juste noter :

Hérédité : Supposons que le résultat soit vrai au rang $k \geq 1$. Ainsi

$(1+p)^{p^{k+1}} = (1+\lambda_k p^{k+1})^p = \sum_{i=0}^{p} \binom{p}{i} \lambda_k^i p^{(k+1)i} = 1 + \lambda_k p^{k+2} + \underbrace{\sum_{i=0}^{p-2} \binom{p}{i} \lambda_k^i p^{(k+1)i} + \lambda_k^p p^{p(k+1)}}_{= up^{k+3}}$

Pour $i \in [\![2, p-1]\!]$, $p^{k+3} \mid \binom{p}{i} \lambda_k^i p^{(k+1)i}$, et $p^{k+3} \mid \lambda_k^p p^{k(k+1)}$,

à l'oral juste noter :

d'où $(1+p)^{p^{k+1}} = 1 + p^{k+2} (\underbrace{\lambda + up}_{=:\lambda_{k+1} \text{ premier avec } p})$

Ce qui conclut la récurrence.

2) Initialisation : Pour $k=1$, $5^2 = (1+4)^2 = 1 + \underbrace{3}_{=\mu_1} \times 8$.

Hérédité : Supposons que le résultat soit vrai au rang $k \geq 1$. Alors

$5^{2^{k+1}} = (1 + \mu_k 2^{k+2})^2 = 1 + \mu_k 2^{k+3} + \mu_k^2 2^{2k+4} = 1 + 2^{k+3} \underbrace{(\mu_k + \mu_k^2 2^{k+1})}_{=: \mu_{k+1} \text{ impair}}$

Ce qui conclut la récurrence.

Preuve de la proposition : 1) Le lemme qui précède nous permet d'affirmer que $1+p$ est un élément d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ (en effet $(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha = 1 [p^\alpha]$ et $(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1}$, avec $p \nmid \lambda_{\alpha-2}$ donc $(1+p)^{p^{\alpha-2}} \neq 1$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$)

On note $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la projection canonique (surjective), et puisque $p^\alpha\mathbb{Z} \subset \ker(\pi)$, on peut passer au quotient et on obtient un morphisme d'anneaux surjectif $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})$]. On possède ainsi un morphisme de groupe surjectif $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p$
Soit $x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tel que $\psi(x)$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.
L'ordre de x est donc un multiple de $p-1$. On peut alors trouver un élément y d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ (il suffit de prendre $x^{\frac{o(x)}{p-1}}$)
Ainsi, puisque $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est abélien, et que $p^{\alpha-1} \wedge p-1 = 1$, l'ordre de $y(1+p)$ est $p^{\alpha-1}(p-1)$, ce qui nous permet de conclure que le groupe est effectivement cyclique.

2) De même que précédemment, on a un morphisme de groupes surjectif $\psi : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$.
Ce morphisme induit par passage au quotient un isomorphisme
$\frac{(\mathbb{Z}/2^\alpha\mathbb{Z})^\times}{\ker(\psi)} \simeq (\mathbb{Z}/4\mathbb{Z})^\times$, ainsi par étude des cardinaux on obtient :
$\# \ker(\psi) = 2^{\alpha-2}$.
Or 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ (car $5^{2^{\alpha-2}} = 1 + \mu_{\alpha-2} 2^\alpha = 1\ [2^\alpha]$ et $5^{2^{\alpha-3}} = 1 + \underbrace{\mu_{\alpha-3}}_{\text{impair}} 2^{\alpha-1} \neq 1\ [2^\alpha]$), et $5 \in \ker(\psi)$ $(5 \equiv 1\ [4])$
donc $\ker(\psi)$ est cyclique d'ordre $2^{\alpha-2}$ engendré par 5.
On peut maintenir définir
$$\varphi : \left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times \to \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^\times \times \ker(\psi),$$
$$x \mapsto (\psi(x), \psi(x)x)$$
qui est bien définie car pour tout $x \in (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, $\psi(x) \in \{\pm \bar{1}\}$, donc $\psi(x)x = \pm x$, ainsi $\psi(\psi(x)x) = \bar{1}$ dans tous les cas.
De plus φ est un morphisme, et φ est injectif car si $x \in \ker(\varphi)$, $\psi(x) = \bar{1}$ et $\psi(x)x = \bar{1}$, donc $x = \bar{1}$. Les deux groupes ayant le même cardinal, on en déduit que φ est un isomorphisme. Ainsi
$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times \ker(\psi) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$
On en déduit que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ n'est pas cyclique (pas d'élément d'ordre $2^{\alpha-1}$ dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

<u>Preuve du lemme 2</u> : Soient n_1, n_2 tels que $n_1 \wedge n_2 = 1$ et $\varphi(n_1) \wedge \varphi(n_2) > 1$.
D'après le théorème 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 $(a,b) \in (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$. Alors $(a,b)^{ppcm(\varphi(n_1),\varphi(n_2))} = 1$
mais $ppcm(\varphi(n_1), \varphi(n_2)) = \frac{\varphi(n_1)\varphi(n_2)}{pgcd(\varphi(n_1),\varphi(n_2))} < \varphi(n_1)\varphi(n_2) = \varphi(n_1n_2)$.
Donc il n'existe pas d'élément de $(\mathbb{Z}/n_1n_2\mathbb{Z})^\times$ d'ordre $\varphi(n_1n_2)$, donc ce groupe n'est pas cyclique.

Preuve du théorème : Soit $n = 2^k p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (où $\forall i, p_i \geq 3$) tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique. Alors d'après le lemme précédent, nécessairement $r \leq 1$. En effet on aurait sinon $n = p_1^{\alpha_1} p_2^{\alpha_2} m$ avec m premier avec p_1 et p_2 et alors en posant $n_1 = p_1^{\alpha_1}$ et $n_2 = p_2^{\alpha_2} m$, on a $n_1 \wedge n_2 = 1$ et $\varphi(n_1) = p_1^{\alpha_1 - 1}(p_1 - 1)$ et $\varphi(n_2) = p_2^{\alpha_2}(p_2 - 1)\varphi(m)$ sont tous les deux pairs, et $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique ↯. De plus, le lemme nous permet d'affirmer que si $r = 1$, alors $k \leq 1$. En effet, de même, on aurait sinon $n = 2^k p_1^{\alpha_1}$, et alors avec $n_1 = 2^k$ et $n_2 = p_1^{\alpha_1}$, on a $n_1 \wedge n_2 = 1$ et $\varphi(n_1) = 2^{k-1}$ et $\varphi(n_2) = p_1^{\alpha_1 - 1}(p-1)$ sont tous les deux pairs, et $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique ↯. Enfin la proposition nous permet d'affirmer que si $r = 0$, alors $k \leq 2$.

Finalement, on obtient $n = 2, 4, p^\alpha$ ou $2p^\alpha$.

Réciproquement, la proposition et le lemme chinois permettent de conclure que dans ces cas là, $(\mathbb{Z}/n\mathbb{Z})^\times$ est effectivement cyclique.

Avant de passer aux remarques, montrons quelques lemmes que l'on a utilisés dans les différentes preuves :

Lemme 1 : Si $a, b \in G$ sont des éléments qui commutent, d'ordres respectifs p et q tels que $p \wedge q = 1$, alors ab est d'ordre pq.

Preuve : Puisque a et b commutent, $(ab)^{pq} = a^{pq} b^{pq} = 1$, donc $o(ab) \mid pq$. Réciproquement, si $(ab)^n = 1$, alors $a^n b^n = 1$, donc $a^{nq} b^{nq} = 1$, donc $a^{nq} = 1$, ainsi $p \mid nq$ donc $p \mid n$. De même avec b : $q \mid n$ donc $pq \mid n$.

⚠ Toutes les hyp sont importantes : $p \wedge q = 1$ (considérer x et x^{-1}) et $ab = ba$ (considérer $(a\ b)$ et $(a\ b\ c)$ dans S_3).

Lemme 2 : $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, iso à $\mathbb{Z}/(p-1)\mathbb{Z}$.

Preuve : On pose $n = p - 1$. Alors d'une part $n = \sum_{d \mid n} \varphi(d)$. D'autre part : soit d diviseur de n, supposons qu'il existe x d'ordre d. Alors $\langle x \rangle \simeq \mathbb{Z}/d\mathbb{Z}$. Alors $\forall y \in \langle x \rangle$, $y^d = 1$, or $Y^d - 1$ a au plus d racines dans $(\mathbb{Z}/p\mathbb{Z})^\times$, donc tous les éléments d'ordre d sont dans $\langle x \rangle$. Ainsi le nombre $N(d)$ d'éléments d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^\times$ est $\varphi(d)$ (nbr de générateurs de $\mathbb{Z}/d\mathbb{Z}$) ou 0. Or $n = \sum_{d \mid n} N(d)$. Ainsi $\sum_{d \mid n} N(d) = \sum_{d \mid n} \varphi(d)$ avec $N(d) \leq \varphi(d)$, donc $\forall d \mid n$, $N(d) = \varphi(d)$, en particulier $N(n) = \varphi(n) > 0$ donc $(\mathbb{Z}/p\mathbb{Z})^\times$ contient un élément d'ordre n, donc $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, iso à $\mathbb{Z}/n\mathbb{Z}$.

Lemme 3 : $\forall k \in [\![1, p-1]\!],\ p \mid \binom{p}{k}$

Preuve : Soit $k \in [\![1, p-1]\!]$, alors $p \mid p! = k!(p-k)!\binom{p}{k}$, or $\forall j \in [\![1, p-1]\!]$, $j \wedge p = 1$, donc $p \wedge k!(p-k)! = 1$, donc d'après le lemme de Gauss, $p \mid \binom{p}{k}$.

Remarques : * En utilisant ce qui précède et le fait que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, on obtient une description complète de $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Cela est utile pour étudier par exemples des produits semi-directs faisant intervenir des $\mathbb{Z}/n\mathbb{Z}$, ce qui peut par exemple servir à étudier les groupes d'ordre pq (cf Perrin).

* Pour le cas $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, on aurait aussi pu directement poser $N = \mathrm{Ker}(\varphi)$, $H = \{\pm 1\}$, alors $N \cap H = \{1\}$ ($-1 \neq 1 [4]$) et puisque $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est abélien, on a un iso de groupes

$N \times H \to NH$
$(n, h) \mapsto nh$

. Alors $\# NH = \# N \times \# H = 2^{\alpha-1}$, donc par cardinalité $NH = (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, d'où

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

(mais l'idée est globalement la même).