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

réf: Perrin, Cours d'Algèbre p25
Rombaldi, Algèbre et géométrie p347.

L'objectif est de montrer le théorème suivant:

Théorème:

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

On commence par montrer le lemme suivant.

Lemme:

Soient $n_1, n_2 \in \mathbb{N}$ tel que $n_1 \wedge n_2 = 1$ et si $\varphi(n_1) \wedge \varphi(n_2) > 1$ alors $(\mathbb{Z}/n_1 n_2\mathbb{Z})^\times$ n'est pas cyclique

Preuve: Par le théorème des restes chinois on a:

$$(\mathbb{Z}/n_1 n_2\mathbb{Z})^\times \simeq (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$$

Soit $(a,b) \in (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$ alors $(a,b)^{\varphi(n_1) \vee \varphi(n_2)} = 1$ mais

$$\varphi(n_1) \vee \varphi(n_2) = \frac{\varphi(n_1)\varphi(n_2)}{\varphi(n_1) \wedge \varphi(n_2)} < \varphi(n_1)\varphi(n_2) = \varphi(n_1 n_2)$$

Ainsi aucun élément n'est d'ordre $\varphi(n_1 n_2)$ donc le groupe n'est pas cyclique.

Preuve:

Analyse: Soit $n \in \mathbb{N}$ cyclique, on écrit $n = 2^m p_1^{\alpha_1} \dots p_s^{\alpha_s}$ avec p_s premier impairs distincts.

Si $s = 0$: Alors $n = 2^k$. On traite ce cas dans la synthèse.

Si $s \geq 1$: Alors $n = m p_1^{\alpha_1} p_2^{\alpha_2}$ avec $m \in \mathbb{N}^*$ tel que $m \wedge p_1 = 1$ et $m \wedge p_2 = 1$. On pose donc $n_1 = p_1^{\alpha_1}$ et $n_2 = m p_2^{\alpha_2}$ de sorte que $n = n_1 n_2$.

On sait que $n_1 \wedge n_2 = 1$ et $\varphi(n_1) = p_1^{\alpha_1 - 1}(p_1 - 1)$

$$\varphi(n_2) = \varphi(m)\, p_2^{\alpha_2 - 1}(p_2 - 1)$$

Comme p_1 et p_2 sont impairs, $2 | \varphi(n_1)$ donc $\varphi(n_1) \wedge \varphi(n_2) \geq 2$ d'après le lemme $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.

$$2 | \varphi(n_2)$$

Si $s = 1$: Alors $n = 2^k p^\alpha$ et $\varphi(2^k) = 2^{k-1}$

$$\varphi(p^\alpha) = p^{\alpha - 1}(p - 1)$$

Si $k>1$: Alors $\ell \mid \varphi(p^\alpha)$ et $\ell \mid \varphi(\ell^k)$ par le Lemme $(\mathbb{Z}/_{n\mathbb{Z}})^\times$ n'est pas cyclique.

Il reste le cas $(s=1, k=0)$ et $(s=1, k=1)$.

Synthèse : On a les cas suivants.

Cas 1 : $s=0$ i.e $n=\ell^k$:

Si $k=1$, $(\mathbb{Z}/_{\ell\mathbb{Z}})^\times = \{1\}$ qui est cyclique.

Si $k=2$, $(\mathbb{Z}/_{4\mathbb{Z}})^\times = \{1,3\}$ qui est cyclique engendré par 3.

Si $k=3$, $(\mathbb{Z}/_{8\mathbb{Z}})^\times = \{1,3,5,7\}$ n'est pas cyclique car tous les éléments sont d'ordre 2 et $\varphi(8)=4$

Soit $k\geq 3$, on définit l'application :

$$\varphi : (\mathbb{Z}/_{\ell^k\mathbb{Z}})^\times \longrightarrow (\mathbb{Z}/_{8\mathbb{Z}})^\times$$
$$\overline{n} \longmapsto n \bmod 8.$$

qui est bien définie car $8 \mid \ell^k$, de plus c'est un maphisme surjectif.

Si $(\mathbb{Z}/_{\ell^k\mathbb{Z}})^\times$ est cyclique, en notant g un générateur de ce groupe, comme φ est surjectif, $\varphi(g)$ engendrerait $(\mathbb{Z}/_{8\mathbb{Z}})^\times$ ce qui est absurde.

Cas 2 : $s=1$ et $k=0$ i.e $n=p^\alpha$ avec p premiers impairs.

On utilise le Lemme suivant.

Lemme : Si $k \in \mathbb{N}^\times$, on a :

$$(1+p)^{p^k} = 1 + \lambda_k p^{k+1} \quad \text{avec } \lambda_k \text{ premier avec } p.$$

On sait que $(\mathbb{Z}/_{p\mathbb{Z}})^\times$ est cyclique, on utilise le morphisme surjectif.

$$\Psi : (\mathbb{Z}/_{p^\alpha\mathbb{Z}})^\times \longrightarrow (\mathbb{Z}/_{p\mathbb{Z}})^\times$$
$$\overline{n} \longmapsto n \bmod p.$$

Qui est bien définie car $p \mid p^\alpha$.

Soit g un générateur de $(\mathbb{Z}/_{p\mathbb{Z}})^\times$ et h' un antécédent de g par Ψ i.e $\Psi(h')=g$.

Donc on a $p-1 \mid o(h')$ ainsi dans le groupe cyclique $\langle h' \rangle$ d'ordre $o(h')$ il existe h d'ordre $p-1$.

Montrons que $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/_{p^\alpha\mathbb{Z}})$.

En effet $p \wedge 1+p$ et on a :

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1 \,[p^\alpha]$$
$$(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1} \not\equiv 1 \,[p^\alpha]$$

Car $\lambda_{\alpha-1} \wedge p = 1$ donc $p^\alpha \nmid \lambda_{\alpha-1} p^{\alpha-1}$.
Ainsi $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Comme $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est abélien et $p^{\alpha-1} \wedge p-1$,
$h(1+p)$ est d'ordre $p^{\alpha-1}(p-1) = \varphi(p^\alpha)$.

Ainsi $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

Cas $2=1$ et $\beta=1$ i.e $n = 2p^\alpha$ et p premier impair.

Par le théorème des restes chinois

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

Qui est clairement cyclique.
On donc bien montré l'équivalence.

Montrer le Lemme + $(\mathbb{Z}/p\mathbb{Z})$ cyclique.

Lemme: Soit p premier.

1 - Soit $\ell \in [\![1, p-1]\!]$, $p \mid \binom{p}{\ell}$.

2 - Pour tout k, $\exists \lambda_k \in \mathbb{N}$ tq :

$$\lambda_k \wedge p = 1 \text{ et } (1+p)^{p^k} = 1 + \lambda_k p^{k+1}.$$

Preuve:

1 - Pour $\ell \in [\![1, p-1]\!]$ on sait que : $\ell\binom{p}{\ell} = p\binom{p-1}{\ell-1}$.
Ainsi $p \mid \ell\binom{p}{\ell}$ or $p \wedge \ell = 1$ donc par Gauss $p \mid \binom{p}{\ell}$.

2 - On raisonne par récurrence sur $k \in \mathbb{N}$.

Initialisation : Si $k=0$ avec $\lambda_0 = 1$ on a :

$$(1+p)^{p^0} = 1 + p = 1 + \lambda_0 p^{0+1}$$

Hérédité : On suppose le résultat vraie pour $k \in \mathbb{N}$.
On obtient ainsi :

$$(1+p)^{p^{k+1}} = (1+\lambda_k p^{k+1})^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} \lambda_k^i p^{(k+1)i} + \lambda_k^p p^{(k+1)p}$$

Or pour $i=1$, on a : $p\lambda_k p^{k+1} = \lambda_k p^{k+2}$.

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

et $p^{k+3} \mid \lambda_k^p p^{(k+1)p}$ car $p(k+1) \geq 2(k+1) \geq k+3$.

Ainsi il existe $u \in \mathbb{N}$ tel que :

$$(1+p)^{p^{k+1}} = 1 + (\lambda_k + up)\, p^{k+2}$$

On pose donc $\lambda_{k+1} = \lambda_k + up$.

Soit $d = \lambda_{k+1} \wedge p$ alors $d \mid up$ donc $d \mid \lambda_k$ donc $d=1$ car $\lambda_k \wedge p = 1$

$d \mid \lambda_k + up$

$d \mid p$

D'où $\lambda_{k+1} \wedge p = 1$.

Lemme : Soit p premier et d un diviseur de $p-1$.

1. Il y a $\varphi(d)$ élément d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^\times$
2. $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Preuve : On note $\psi(d)$ le nombre d'éléments d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Dire que $\psi(d) > 0$ équivaut à dire qu'il existe dans $(\mathbb{Z}/p\mathbb{Z})^\times$ au moins un élément x d'ordre d et que le groupe $G = \{\bar{1}, x, \dots, x^{d-1}\}$ est alors formé de d solutions distinctes de l'équation $X^d - \bar{1} = \bar{0}$. Or cette équation a au plus d solutions dans le corps commutatif $\mathbb{Z}/p\mathbb{Z}$, donc G est exactement l'ensemble de toutes les solutions de cette équation.

Les éléments d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^\times$ sont donc les générateurs des groupes cycliques G et il y a $\varphi(d)$ tels générateurs, donc $\psi(d) = \varphi(d)$ si $\psi(d) > 0$.

Comme tout élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ a un ordre qui divise $p-1$, on a :

$$p-1 = \sum_{d \mid p-1} \psi(d)$$

De plus on a :

$$p = \sum_{d \mid p-1} \varphi(d) = \sum_{d \mid p-1} \psi(d) \quad \text{avec } \psi(d) = 0 \text{ ou } \psi(d) = \varphi(d).$$

Ainsi $\Psi(d) = \varphi(d)$ pour tout $d \mid p-1$.

2 - On a $\Psi(p-1) = \varphi(p-1) > 0$ donc le groupe est cyclique.