# CONDITIONS DE CYCLICITÉ DE $(\mathbb{Z}/n\mathbb{Z})^\times$

108 : On traite tous les cas sans les lemmes
120
121 : Lemmes + $p^\alpha$, $2p^\alpha$

Leçons : 104 - 108 - 120 - 121

Références Rombaldi p 300 - 302, Perrin p25-27

On admet que pour $p \in \mathbb{P}$, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

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

**Lemme 2 :** Soit $p \in \mathbb{P}$. Alors :
1) $\forall k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$
2) $\forall k \in \mathbb{N}$, $\exists d_k \in \mathbb{N}$, $p \wedge d_k = 1$ ; $(1+p)^{p^k} = 1 + d_k p^{k+1}$

**Th :** $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2, 4, p^\alpha, 2p^\alpha$ $(p \in \mathbb{P} \setminus \{2\}, \alpha \in \mathbb{N}^*)$

---

**preuve** Raisonnons par analyse - synthèse

**Analyse** Soit $n \in \mathbb{N}$, $n \geq 2$ tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclique.

On écrit $n = 2^k \prod_{i=1}^{r} p_i^{\alpha_i}$ où $p_i \in \mathbb{P} \setminus \{2\}$ pour tout $i \in [\![1, r]\!]$, $\alpha_i \in \mathbb{N}$.

Traitons 3 cas

- $s = 0$, $n = 2^k$
- $s > 1$, $n = \underbrace{p_1^{\alpha_1}}_{n_1} \underbrace{p_2^{\alpha_2} m}_{n_2}$ avec $m \in \mathbb{N}^*$ tel que $\begin{cases} p_1 \wedge m = 1 \\ p_2 \wedge m = 1 \end{cases}$

Ainsi $n_1 \wedge n_2 = 1$

Or $\varphi(n_1) = p_1^{\alpha_1 - 1}(p_1 - 1)$, $\varphi(n_2) = \varphi(m) p_2^{\alpha_2 - 1}(p_2 - 1)$.

Comme $p_1, p_2$ sont impairs, $2 \mid \varphi(n_1), \varphi(n_2)$ donc $\varphi(n_1) \wedge \varphi(n_2) > 1$.

Par le lemme 1, $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.

- $s = 1$ : $n = \underbrace{2^k}_{n_1} \underbrace{p^\alpha}_{n_2}$

Ainsi $n_1 \wedge n_2 = 1$

$\varphi(n_1) = 2^{k-1}$

$\varphi(n_2) = p^{\alpha-1}(p-1)$

Si $k > 1$ alors $\varphi(n_1) \wedge \varphi(n_2) > 1$ donc $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.

Si $k \leq 1$, on ne peut pas conclure.

**Synthèse**

- $s = 0$ alors $n = 2^k$

* $k = 1$, $(\mathbb{Z}/2\mathbb{Z})^\times$ est cyclique. * $k = 2$, $(\mathbb{Z}/4\mathbb{Z})^\times = \langle \bar{3} \rangle$, $(\mathbb{Z}/4\mathbb{Z})^\times$ est cyclique

* $\underline{K=3}$, $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1},\bar{3},\bar{5},\bar{7}\}$, aucun élément n'est d'ordre $\varphi(8)=4$.
Donc $\underline{(\mathbb{Z}/8\mathbb{Z})^\times \text{ n'est pas cyclique}}$

* $\underline{K\geq 3}$ Soit $\varphi : \begin{cases} (\mathbb{Z}/2^K\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/8\mathbb{Z})^\times \\ m[2^K] \longmapsto m[8] \end{cases}$ $8 \mid 2^K$ car $K\geq 3$ donc $\varphi$ est bien définie.

$\varphi$ est un morphisme de groupes surjectif.
Ainsi, si $(\mathbb{Z}/2^K\mathbb{Z})^\times$ cyclique alors $(\mathbb{Z}/8\mathbb{Z})^\times$ est cyclique, absurde
Donc $\underline{(\mathbb{Z}/2^K\mathbb{Z})^\times \text{ n'est pas cyclique}}$.

- $\underline{s=1,\ k=0;\ n=p^\alpha}$

On a $\varphi(n) = p^{\alpha-1}(p-1)$
Par le lemme 2, $(1+p)^{p^{\alpha-1}} \equiv 1\ [p^\alpha]$ donc $\theta_{p^\alpha}(1+p) = p^\beta$ où $\beta \leq \alpha-1$
Or $(1+p)^{p^{\alpha-2}} = 1 + d_{\alpha-2}\, p^{\alpha-1} \neq 1$ car $p \nmid d_{\alpha-2}$.

Donc $\beta = \alpha-1$
Ainsi $\underline{\theta_{p^\alpha}(1+p) = p^{\alpha-1}}$.
On cherche un élément d'ordre $p-1$.
Soit $\varphi : \begin{cases} (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \\ m[p^\alpha] \longmapsto m[p] \end{cases}$, $\varphi$ est un morphisme surjectif bien défini.

Or $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$, donc il existe $h \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tel que $\varphi(h) = g$
On note $d = o(h)$, ainsi $1 = \varphi(h)^d = g^d$, donc $p-1 \mid d$ donc $d = (p-1)k$.
Ainsi $h^k$ est d'ordre $p-1$.
Or $p^{\alpha-1} \wedge (p-1) = 1$ et $h^k$ et $p+1$ commutent alors $o(h^k(p+1)) = p^{\alpha-1}(p-1) = \varphi(p^\alpha)$
Donc $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

- $\underline{s=1,\ K=1,\ n=2p^\alpha}$

Par le théorème des restes chinois, comme $2 \wedge p^\alpha = 1$.

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

Donc $\underline{(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times \text{ est cyclique}}$. ∎

preuve lemme 1 On montre que $(\mathbb{Z}/(n_1n_2)\mathbb{Z})^\times$ n'a pas d'élément d'ordre $\varphi(n_1n_2)$.

Soient $n_1, n_2 \in \mathbb{N}$. Supposons que $n_1 \wedge n_2 = 1$ et $\varphi(n_1) \wedge \varphi(n_2) > 1$.

Comme $n_1 \wedge n_2 = 1$, par le théorème des restes chinois :

$$(\mathbb{Z}/(n_1n_2)\mathbb{Z})^\times \simeq (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times. \quad (*)$$

Soit $(a,b) \in (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$,

on note $m = \varphi(n_1) \vee \varphi(n_2)$.

On a $(a,b)^m = 1 \quad (m \mid \varphi(n_1), m \mid \varphi(n_2))$.

Or $\varphi(n_1) \vee \varphi(n_2) = \dfrac{\varphi(n_1)\varphi(n_2)}{\varphi(n_1) \wedge \varphi(n_2)} < \varphi(n_1)\varphi(n_2) = \varphi(n_1n_2) \quad (\varphi(n_1) \wedge \varphi(n_2) > 1)$

Donc pour tout $x \in (\mathbb{Z}/(n_1n_2)\mathbb{Z})^\times$ (pas iso $(*)$), on a $o(x) \neq \varphi(n_1n_2) = |(\mathbb{Z}/(n_1n_2)\mathbb{Z})^\times|$

$(\mathbb{Z}/(n_1n_2)\mathbb{Z})^\times$ n'admet aucun élément d'ordre $\varphi(n_1n_2)$, donc $(\mathbb{Z}/(n_1n_2)\mathbb{Z})^\times$ n'est pas cyclique. ▨

---

preuve lemme 2

1) Soit $l \in [\![1, p-1]\!]$, on a : $l\binom{p}{l} = p\binom{p-1}{l-1}$, ainsi $p \mid l\binom{p}{l}$

Or comme $p \in \mathbb{P}$, et $l < p$, on a : $p \wedge l = 1$.

Ainsi par le lemme de Gauss :

$$p \mid \binom{p}{l}.$$

2) Soit $K \in \mathbb{N}^*$, on montre par récurrence sur $K$ :

$(P_K)$ : " $\exists d_K \in \mathbb{N}_0, d_K \wedge p = 1, (1+p)^{p^K} = 1 + d_K p^{K+1}$ ".

Initialisation $K = 0$, $(1+p)^{p^0} = 1 + p = 1 + d_0 p^{0+1}$ avec $d_0 = 1 (\wedge p = 1)$

La propriété est initialisée.

Hérédité Soit $K \in \mathbb{N}$, supposons $(P_K)$.

On a : $(1+p)^{p^{K+1}} = \left((1+p)^{p^K}\right)^p$

$= (1+\alpha_K p^{K+1})^p$ par hypothèse de récurrence

$= \sum_{l=0}^{p} \binom{p}{l} (\alpha_K p^{K+1})^l$

$= 1 + \sum_{l=1}^{p} \binom{p}{l} (\alpha_K^l p^{l(K+1)})$

$= 1 + \alpha_K p^{K+2} + \underbrace{\sum_{l=2}^{p-1} \binom{p}{l} \alpha_K^l p^{\overbrace{l(K+1)}^{\geq K+2}}}_{\text{on montre que c'est divisible par } p^{K+3}} + \alpha_K^p p^{\overbrace{p(K+1)}^{\geq K+3}}$

~~• Pour $l \in [\![2, p-1]\!]$, $\binom{p}{l} p^{K+2} \mid \binom{p}{l} \alpha_K^l p^{l(K+1)}$~~

~~Par 1), $p \mid \binom{p}{l}$, donc $p^{K+3} \mid \binom{p}{l} \alpha_K^l p^{l(K+1)}$~~

~~• Pour $l = p$, $\alpha_K^p p^{p(K+1)} \geq \alpha_K^p p^{2(K+2)} \geq \alpha_K^p p^{K+3}$, donc $p^{K+3} \mid \alpha_K^p p^{p(K+1)}$~~

Ainsi $(1+p)^{p^{K+1}} = 1 + \alpha_K p^{K+2} + p^{K+3} u$ pour $u \in \mathbb{Z}$

$= 1 + (\alpha_K + pu) p^{K+2}$

On pose $\alpha_{K+1} = \alpha_K + pu$.

Soit $d$ un diviseur positif de $\alpha_{K+1}$ et $p$.

$$\begin{cases} d \mid \alpha_K + up \\ d \mid p \end{cases} \Rightarrow \begin{cases} d \mid \alpha_K + up \\ d \mid up \end{cases} \Rightarrow d \mid \alpha_K$$

Or $\alpha_K \wedge p = 1$, donc $d = 1$.

Ainsi $\alpha_{K+1} \wedge p = 1$. ■