Conditions de cyclicité de $(\mathbb{Z}/n\mathbb{Z})^*$

Achille Méthivier

Théorème 1. *Les propositions suivantes sont équivalentes.*

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

Lemme 2. *Soit* p *premier impair,* $k \in \mathbb{N}$*, alors il existe* $\lambda \in \mathbb{N}^*$*, premier avec* p*, tel que* $(1+p)^{p^k} = 1 + \lambda p^{k+1}$.

Démonstration. Raisonnons par récurrence sur k. Pour $k = 0$, on prends $\lambda = 1$, qui est bien premier avec p. Supposons qu'il existe λ comme voulu tel que $(1+p)^{p^k} = 1 + \lambda p^{k+1}$. Alors

$$\begin{aligned}(1+p)^{p^{k+1}} &= (1+\lambda p^{k+1})^p \\ &= 1 + \lambda p^{k+2} + \sum_{i=2}^{p} \binom{p}{i} \lambda^i p^{(k+1)i} \\ &= 1 + (\lambda + up)p^{k+2},\end{aligned}$$

ce qui achève la récurrence. □

Proposition 3. *Soit* p *premier impair, on a*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}.$$

Démonstration. La surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ passe au quotient pour donner le morphisme surjectif d'anneaux $\psi : \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ tel que, si $x \in \mathbb{Z}$ et $\bar{x}$ sa classe $\bmod p^\alpha$, $\psi(\bar{x}) = \pi(x)$. On déduit que le morphisme de groupes induit $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ est toujours surjectif. Soit $x \in \mathbb{Z}/p^\alpha\mathbb{Z}$ tel que $\psi(x)$ engendre $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. L'ordre de x est un multiple de $p-1$, il existe donc y d'ordre $p-1$ dans $\langle x \rangle$. De plus, le lemme précédent montre que $p+1$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. En effet, son ordre est de la forme p^β et si $\beta \leq \alpha - 2$,on aurait

$$(1+p)^{p^{\beta-2}} = 1 + \lambda p^{\beta-1},$$

et comme $p \not| \lambda$, $(1+p)^{p^{\beta-2}} \neq 1 \bmod p^\alpha$. Comme $\mathbb{Z}/p^\alpha\mathbb{Z}$ est abélien, et $(p-1) \wedge p^{\alpha-1} = 1$, l'élément $y(p+1)$ est d'ordre $p^{\alpha-1}(p-1)$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. Comme $\#(\mathbb{Z}/p^\alpha\mathbb{Z})^* = p^{\alpha-1}(p-1)$, il est bien cyclique. □

Lemme 4. *Pour* $k \in \mathbb{N}$*,* $5^{2^k} = 1 + \lambda 2^{k+2}$*, avec* λ *impair.*

Démonstration. On raisonne par récurrence sur k. Pour $k = 0$, on a bien $5 = 1 + 2^2$ et $\lambda = 1$. Pour $k \in \mathbb{N}$, supposons qu'il existe λ impair tel que $5^{2^k} = 1 + \lambda 2^{k+2}$. Alors

$$5^{2^{k+1}} = (1 + \lambda 2^{k+2})^2 = 1 + \lambda 2^{k+3} + \lambda^2 2^{2k+4},$$

et on conclut puisque $\lambda(1 + \lambda 2^{k+1})$ est impair. □

Proposition 5. *On a les isomorphismes suivants* $(\mathbb{Z}/2\mathbb{Z})^* \simeq \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$*. Et pour* $\alpha \geq 3$*,*

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}.$$

Démonstration. Considérons le morphisme de groupes défini comme dans la preuve de la dernière proposition

$$\psi : (\mathbb{Z}/2^\alpha\mathbb{Z})^* \to (\mathbb{Z}/4\mathbb{Z})^*.$$

Notons $N = \ker(\psi)$ et $H = \{-1, 1\} \subset (\mathbb{Z}/2^\alpha\mathbb{Z})^*$. Puisque $\mathbb{Z}/2^\alpha\mathbb{Z}$ et abélien et $N \cap H = \{1\}$ (car 1 et -1 ne sont pas congru $\bmod 4$), on a l'isomorphisme de groupes suivant

$$\begin{array}{ccc} N \times H & \to & NH = \{nh : n \in N\ h \in H\} \\ (n, h) & \to & nh. \end{array}$$

Donc $\#NH = \#N \times \#H = 2^{\alpha-1}$. Comme $NH \subset (\mathbb{Z}/2^\alpha\mathbb{Z})^*$, par cardinalité $NH = (\mathbb{Z}/2^\alpha\mathbb{Z})^*$, donc

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

Finalement, le lemme précédent montre que 5 est d'ordre $2^{\alpha-2}$ dans N, de cardinal $2^{\alpha-2}$, donc $N \simeq \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ et $H \simeq \mathbb{Z}/2\mathbb{Z}$, d'où l'isomorphisme voulu. □

Démonstration du théorème. On écrit la décomposition en facteurs premiers de n

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Le théorème des restes chinois donne

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z},$$

et donc

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*,$$

et on conclut aisément avec les lemmes précédents. □

I Références

1. Cours d'algèbre, Perrin (pages 25/26)