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

[PERRIN, p 25]

ÉNONCÉ :

Théorème :

1. Si p est un nombre premier impair, et α un entier supérieur à 2, on a :
$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)$$
2. Pour $\alpha \geq 3$, on a
$$(\mathbb{Z}/2^\alpha)^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

DÉVELOPPEMENT :

LEMMES :

1. Soient $k \in \mathbb{N}^*$ et p un nombre premier impair, alors :
$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$
avec λ premier avec p.
2. Soit $k \in \mathbb{N}^*$, on a
$$5^{2^k} = 1 + \mu 2^{k+2}$$
avec μ impair.

Démonstration. 1. Pour $k = 1$, on a :
$$(1+p)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} p^i + p^p$$
Pour $i \in \{1, \dots, p-1\}$, $p^2 \mid \binom{p}{k} p^i$ et comme $p \geq 3$, on a $p^3 \mid p^p$. Ainsi, $(1+p)^p = 1 + up^2 + kp^3 = 1 + p^2(\underbrace{u + kp}_{:=\lambda})$.
Supposons la propriété vraie à un rang $k \geq 1$. Alors on a :
$$\begin{aligned}(1+p)^{p^{k+1}} &= \left((1+p)^{p^k}\right)^p \\ &= (1+\lambda p^{k+1})^p \\ &= 1 + \sum_{i=1}^{p-1} \binom{p}{i} \lambda^i p^{i(k+1)} + \lambda^p p^{p(k+1)}\end{aligned}$$
Pour $i = 1$, on a λp^{k+2} et pour $i \geq 2$, p^{k+3} est un facteur, d'où $(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda + up)$.

2. Pour $k = 1$, on a $5^2 = (1+4)^2 = 1 + 3 \times 8$. Supposons la propriété vraie au rang $k \geq 1$, alors on a :
$$5^{2^{k+1}} = (5^{2^k})^2 = (1 + \mu 2^{k+2})^2 = 1 + 2^{k+3}(\mu + 2^{k+1}\mu^2)$$

□

Démonstration. (*théorème*) :

1. En vertu du premier lemme, $1+p$ est un élément d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. En effet, $(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1 \pmod{p^\alpha}$ et $(1+p)^{p^{\alpha-2}} = 1 + \lambda p^{\alpha-1}$ avec p et λ premiers entre eux donc $(1+p)^{p^{\alpha-2}} \neq 1$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. Considérons désormais l'homomorphisme surjectif de groupes naturel induit par l'identité de $\mathbb{Z}$ $\Psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Soit $x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$

un élément tel que $\Psi(x)$ engendre $\mathbb{Z}/(p-1)\mathbb{Z}$. L'ordre de x est un multiple de $p-1$ et donc $\langle x \rangle$ admet un élément d'ordre $p-1$. Notons le y. Or $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est abélien et $p-1$ et $p^{\alpha-1}$ sont premiers entre eux, $(\mathbb{Z}/p^\alpha\mathbb{Z})^* = \langle xy \rangle \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

2. Pour $\alpha \geq 3$, on considère l'homomorphisme surjectif :

$$\Phi : (\mathbb{Z}/2^\alpha\mathbb{Z})^* \longrightarrow (\mathbb{Z}/4\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z}$$

En notant $N := Ker(\Phi)$, on a $|N| = 2^{\alpha-2}$ et ce dernier est cyclique car $5 \in N$ et le 2ème point du lemme nous dit que l'ordre de 5 est égal à $2^{\alpha-2}$. On a donc la suite exacte :

$$1 \longrightarrow \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \longrightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^* \xrightarrow{\Phi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

D'autre part, 1 et -1 ne sont pas égaux modulo 4 donc le sous-groupe $\{-1, 1\}$ de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ fournit un relèvement de $\mathbb{Z}/2\mathbb{Z}$, de sorte que l'extension est scindée. Comme $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est abélien, on a un produit direct :

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

□

Remarques :

- Ce résultat couplé à l'isomorphisme entre $Aut\,(\mathbb{Z}/n\mathbb{Z})$ et $(\mathbb{Z}/n\mathbb{Z})^*$ fournit la description complète du groupe $Aut\,(\mathbb{Z}/n\mathbb{Z})$, $n \in \mathbb{N}^*$.
- Il faut être en mesure de montrer le résultat suivant : *Si a et $b \in G$ commutent et sont d'ordre respectivement p et q premiers entre eux, alors $o(ab) = pq$.*
- Il faut savoir justifier l'existence des morphismes Ψ et Φ.
- On a affirmé que $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, qu'il faut savoir montrer.