Inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$

Lemme 1. *Soient $k \in \mathbb{N}^\star$ et p premier, alors $(1+p)^{p^k} = 1 + \lambda p^{k+1}$, avec $\lambda \in \mathbb{N}^\star$ premier avec p.*

Démonstration.

On va raisonner par récurrence sur n.

On suppose que $k = 1$. Alors :

$$(1+p)^p = \sum_{j=0}^{p} \binom{p}{j} p^j = 1 + \sum_{j=1}^{p-1} \binom{p}{j} p^j + p^p$$

Or, pour tout $j \in [\![1, p-1]\!]$, $j\binom{p}{j} = p\binom{p-1}{j-1}$, donc $p \mid j\binom{p}{j}$. Comme $j \wedge p = 1$, donc $p \mid \binom{p}{j}$ par le lemme de Gauss. Ainsi, pour tout $j \in [\![1, p-1]\!]$, il existe $a_j \in \mathbb{N}^\star$ tel que $\binom{p}{j} = pa_j$, donc :

$$(1+p)^p = 1 + \sum_{j=1}^{p-1} \binom{p}{j} p^j + p^p = 1 + p^2 \sum_{j=1}^{p-1} a_j p^{j-1} + p^p = 1 + p^2 \left(\sum_{j=1}^{p-1} a_j p^{j-1} + p^{p-2} \right)$$

On pose $\lambda = \sum_{j=1}^{p-1} a_j p^{j-1} + p^{p-2} = a_1 + \sum_{j=2}^{p-1} a_j p^{j-1} + p^{p-2}$. Comme $\binom{p}{1} = p = pa_1$, on a $a_1 = 1$, d'où $\lambda \wedge p = 1$.

On suppose le résultat vrai au rang $k \geqslant 1$. Alors :

$$(1+p)^{p^{k+1}} = ((1+p)^{p^k})^p = (1 + \lambda p^{k+1})^p = \sum_{j=0}^{p} \binom{p}{j} \lambda^j p^{j(k+1)} = 1 + \sum_{j=1}^{p} \binom{p}{j} \lambda^j p^{j(k+1)}$$

Le terme en $j = 1$ est λp^{k+2}, et p^{k+3} divise tous les termes en $j \geqslant 2$. Alors :

$$(1+p)^{p^{k+1}} = 1 + \lambda p^{k+2} + up^{k+3} = 1 + p^{k+2}(\lambda + up)$$

Or, $(\lambda + up) \wedge p = 1$ car $\lambda \wedge p = 1$, d'où le résultat.

□

Lemme 2. *Soient $a, b \in G$ d'ordre p et q. Si a et b commutent, et si $p \wedge q = 1$, alors ab est d'ordre pq.*

Démonstration.

On a $\mathrm{ord}(ab) \mid pq$. En effet, on a : $(ab)^{pq} = a^{pq}b^{pq} = (a^p)^q(b^q)^p = e$.
De plus, si $(ab)^n = a^n b^n = 1$, alors, en élevant à la puissance q, on obtient $a^{nq}b^{nq} = a^{pq}(b^q)^n = a^{nq} = 1$. Donc $p \mid nq$, puis $p \mid n$ par le lemme de Gauss. De même, on a $q \mid n$. Ainsi, $pq \mid n$.
En prenant $n = \mathrm{ord}(ab)$, on conclut que $pq = \mathrm{ord}(ab)$.

□

Proposition 3. *Soient $p \geqslant 3$ premier et $\alpha \in \mathbb{N} \setminus \{0,1\}$, alors :*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$$

Démonstration.

Par le Lemme 1, $(1+p)$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. En effet, $(1+p) \wedge p^\alpha = 1$, donc $1+p \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
De plus :

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1\ [p^\alpha] \quad \text{et} \quad (1+p)^{p^{\alpha-2}} = 1 + \lambda' p^{\alpha-1} \quad \text{avec} \quad \lambda \nmid p \quad \text{et} \quad \lambda' \nmid p$$

Ainsi, $(1+p)^{p^{\alpha-2}} \neq 1$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.

On considère le morphisme de groupes :

$$\psi : \left| \begin{array}{ccc} (\mathbb{Z}/p^\alpha\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ \overline{k}^{p^\alpha} & \longmapsto & \overline{k}^p \end{array} \right.$$

ψ est bien définie, puisque si $\overline{k}^{p^\alpha} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, alors $k \wedge p^\alpha = 1$, et $k \wedge p = 1$, donc $\overline{k}^p \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Soit $\overline{k}^p \in (\mathbb{Z}/p\mathbb{Z})^\times$, donc $k \wedge p = 1$. Soit $d = k \wedge p^\alpha$, alors $d \mid p^\alpha$, donc $d = p^j$ avec $j \in [\![0, \alpha]\!]$.
Or, si $j \neq 0$, alors $p \mid p^j \mid k$, ce qui est contradictoire. Ainsi, $k \wedge p^\alpha = 1$, donc $\overline{k}^p = \psi\left(\overline{k}^{p^\alpha}\right)$.

Soit y un antécédent d'un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ qui est cyclique, et soit $m = \mathrm{ord}(y)$.
On a $1 = \psi(y^m) = \psi(y)^m$, donc $(p-1) \mid m$, et il existe $k \in \mathbb{N}^\star$ tel que $m = (p-1)k$.
En posant $x = y^k$, on a $x^{p-1} = y^{k(p-1)} = e$, et pour $\ell < p-1$ on a $x^\ell = y^{k\ell} \neq e$, car $k\ell < m$. Alors $\mathrm{ord}(x) = p-1$.
Posons $u = x(1+p)$. Par le Lemme 2, comme$(p-1) \wedge p^{\alpha-1} = 1$, u est d'ordre $p^{\alpha-1}(p-1)$.
Or, $\left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p^{\alpha-1}(p-1)$, donc $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p^{\alpha-1}(p-1)$, donc :

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$$

□

Références

[Per] Daniel Perrin. *Cours d'Algèbre*. Ellipses