CYCLICITÉ DE $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$

Théorème : $\forall p \geq 3$ et $\forall \alpha \geq 1$, alors, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

Preuve : Soit $p \geq 3$.

→ si $\alpha = 1$, alors, $\mathbb{Z}/p\mathbb{Z}$ est un corps et donc $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

→ si $\alpha \geq 2$. On part du fait que $\#(\mathbb{Z}/p^\alpha\mathbb{Z})^\times = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. On va donc chercher un élément de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ d'ordre $p^{\alpha-1}(p-1)$. or, $p^{\alpha-1} \wedge (p-1) = 1$, donc il suffit de trouver un élément a d'ordre $p^{\alpha-1}$ et un élément b d'ordre $p-1$. Le produit ab aura alors l'ordre voulu.

Trouvons b :

On pose $f : \bar{x} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \longmapsto \dot{x} \in (\mathbb{Z}/p\mathbb{Z})^\times \doteq \langle g \rangle$. car on sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et on note g un générateur. f est un morphisme surjectif, ~~bijectif~~ par un argument de cardinalité. Soit alors $h \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tq. $f(h) = g$ et d l'ordre de h. Alors :

$$\dot{1} = f(\bar{1}) = f(h^d) = f(h)^d = g^d.$$

Donc $|g| = p-1 \mid d$ donc $\exists b \in \langle h \rangle \subseteq (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tq. $|b| = p-1$.

↑ car $\langle h \rangle$ est cyclique et $p-1$ est un diviseur de son ordre d.

Trouvons a : Pour ceci, on a besoin d'un lemme.

Lemme : $\forall k \in \mathbb{N}$, $\exists \lambda_k \in \mathbb{N}^*$ tq. $\lambda_k \wedge p = 1$ et $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$ pour $p \geq 3$.

Preuve : (par récurrence sur k) :

* si $k = 0$, alors $(1+p)^{p^0} = 1+p$ et $\lambda_0 = 1$ convient.
* si le résultat est acquis pour $k \geq 0$, alors :

$$\begin{aligned}(1+p)^{p^{k+1}} = [(1+p)^{p^k}]^p &= (1+\lambda_k p^{k+1})^p \\ &= \sum_{j=0}^{p} \binom{p}{j} \lambda_k^j p^{j(k+1)} \\ &= 1 + \lambda_k p^{k+2} + \sum_{j=2}^{p-1} \binom{p}{j} \lambda_k^j p^{j(k+1)} + \lambda_k^p p^{p(k+1)}\end{aligned}$$

Or, dans cette somme, $p \mid \binom{p}{j}$ et $j(k+1) \geq k+2$ $\forall j \geq 2$. Enfin, le dernier terme, $p(k+1) \geq k+3$ car $p \geq 3$. On a donc que $\exists u \in \mathbb{Z}$ tq.

$$(1+p)^{p^{k+1}} = 1 + \lambda_k p^{k+2} + u p^{k+3} = 1 + \lambda_{k+1} p^{k+2}$$

avec $\lambda_{k+1} := \lambda_k + up$, premier avec p car λ_k l'est. ∎

Retournons à la preuve du thm : on considère $a = p+1 \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. On va mq. $|a| = p^{\alpha-1}$.

→ $(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1 \ [p^\alpha]$ donc, $|a| = p^\beta$ où $\beta \leq \alpha-1$ car $|a|$ divise $p^{\alpha-1}$.

→ $(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1} \not\equiv 1 \ [p^\alpha]$ car p ne divise $\lambda_{\alpha-2}$ donc $\beta > \alpha-2$ donc $\beta = \alpha-1$.

Donc, $a = 1+p$ est d'ordre $p^{\alpha-1}$.

On a bien trouvé un élément d'ordre $p-1$ et un d'ordre $p^{\alpha-1}$, ce qui permet de conclure.

Remarques :

- Un super développement : il est assez riche, facile à présenter, et tient bien le temps demandé en expliquant bien les choses. Je conseille (très) vivement d'expliquer votre démarche au début : vous avez le temps de le faire, et tout paraît très limpide ensuite.
- Pour la récurrence, le Perrin montre le cas $k=1$, je ne sais pas pourquoi... Cela rajoute des calculs, et ne sert pas spécialement à grand chose.
- Remarquez que l'hypothèse $p \neq 3$ n'intervient que dans la récurrence, mais est pourtant cruciale, car pour $p=2$, ça ne marche plus... A savoir justifier d'ailleurs :)