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

Référence : Risler-Boyer p47 et Perrin p.24

Théorème :
Soitp premier impair et $\alpha \geq 1$. Alors :

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

Preuve :

On sait que $\left(\mathbb{Z}/n\mathbb{Z}\right)^* \cong Aut(\mathbb{Z}/n\mathbb{Z})$. Montrons par récurrence sur k le lemme suivant :

Lemme :Soit $k \in \mathbb{N}$, il existe $\lambda_k \in \mathbb{N}^*$ premier avec p tel que :

$$(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$$

Preuve du lemme :
— Pour k=0 : $(1+p)^1 = 1 + p^{0+1} et \lambda_0 \equiv 1[p]$
— Supposons que la propriété est vraie à un rang k>1. Montrons qu'elle est vraie au rang k+1.
On a :

$$\begin{aligned}(1+p)^{p^{k+1}} &= \left((1+p)^{p^k}\right)^p = (1+\lambda_k p^{k+1})^p \\ &= \sum_{l=0}^{p} \binom{p}{l} \lambda_k^l p^{l(k+1)} \\ &= 1 + \lambda_k p^{k+2} + p^{k+2}\left(p^k \sum_{l=2}^{p} \binom{p}{l} \lambda_k^l p^{(l-2)(k+1)}\right)\end{aligned}$$

En posant $\lambda_{k+1} = \lambda_k + p^k \sum_{l=2}^{p} \binom{p}{l} \lambda_k^l p^{(l-2)(k+1)} \equiv 1[p]$ on a le résultat. □

Soit $(1+p)^{p^{\alpha-1}}$, par le lemme : $(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1[p^\alpha]$.
Posons $m = ord(1+p)$, on a $m | p^{\alpha-1}$, donc $m = p^k$ avec $k \leq \alpha - 1$.
Or, $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$ donc $(1+p)^{p^{\alpha-2}} \not\equiv 1[p]$ et on a $ord(1+p) = p^{\alpha-1}$. (*On a construit un élément d'ordre* $p^{\alpha-1}$)

Soit $\Psi : \left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^* \to \left(\mathbb{Z}/p\mathbb{Z}\right)^*, \bar{k} \mapsto \bar{k}$. Le morphisme Ψ envoie bien un inversible sur un inversible. En effet, si $\bar{k}$ est dans $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^*$ alors il est premier avec p^α donc il est premier avec p, et c'est donc un inversible de $\mathbb{Z}/p\mathbb{Z}$. Le morphisme est surjectif : si on prend un élément $\bar{k}$ de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ alors on sait que c'est un inversible de $\mathbb{Z}/p^\alpha\mathbb{Z}$, il suffit de considérer sa classe modulo p^α qui est la même que modulo p.
Soit y un antécédent d'un générrateur de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ cyclique et soit $m = ord(y)$.
On a $1 = \Psi(y^m) = \Psi(y)^m$, donc $p-1 | m$. Ainsi, il existe $k \in \mathbb{N}, m = k(p-1)$
En posant, $x = y^k$, on a $ord(x) = p-1$. (*On a construit un élément d'ordre p-1*)

Posons $u = x(1+p)$ alors comme $p^{\alpha-1}$ et $p-1$ sont premier entre eux et que $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^*$ est abélien, $ord(u) = p^{\alpha-1}(p-1)$

Le groupe $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^*$ est cyclique et donc isomorphe à $\left(\mathbb{Z}/\varphi(\alpha)\mathbb{Z}\right)^*$. Comme $\varphi(\alpha) = p^{\alpha-1}(p-1)$ alors on a le résultat voulu. □