CYCLICITE DES $\mathbb{Z}_n^*$

Dans tout le développement, P désigne l'ensemble des nombres premiers

Enoncé : Soit $n \geq 2$.Le groupe $\mathbb{Z}_n{}^*$ des éléments inversibles modulo n est cyclique si, et seulement si n est l'un des cas suivants :

- $n \in \{2,4\}$
- $n=p^k, p \in P\backslash\{2\}, k \in \mathbb{N}^*$.
- $n=2p^k, p \in P\backslash\{2\}, k \in \mathbb{N}^*$.

Preuve :

1. Montrons le résultat pour p premier impair.
2. Montrons le résultat pour $n=p^k, p \in P\backslash\{2\}, k \in \mathbb{N}^*$.
3. Etudions le cas $n=2^k, k \in \mathbb{N}^*$.
4. Montrons qu'un groupe fini produit de groupes cycliques est cyclique si, et seulement si leurs cardinaux sont deux à deux premiers entre eux.
5. Concluons.

1. On admet la formule d'Euler ($\forall n \in \mathbb{N}^*, n = \sum_{d|n} \Phi(d)$ où Φ est l'indicatrice d'Euler.) Soit d un diviseur de p-1 tel que $\exists x \in \mathbb{Z}_p{}^*, o(x) = d$. D'une part, dans $\mathbb{Z}_p[X]$, $X^d - 1$ admet au plus d racines ($\mathbb{Z}_p$ est intègre donc $\mathbb{Z}_p[X]$ l'est). D'autre part tout élément de $<x>$ (groupe de cardinal d) est racine de ce polynôme, ainsi $\{x \in \mathbb{Z}_p{}^*, x^d = 1\} =< x >$. Rappelons que l'ensemble des éléments de $\mathbb{Z}_p{}^*$ d'ordre d est l'ensemble des générateurs de $<x>$, donc leur cardinal est $\Phi(d)$et par suite
   $|\mathbb{Z}_p{}^*| = |\coprod_{d|p-1}\{x, o(x) = d\}| = \sum_{\substack{d|n \\ \exists x \in \mathbb{Z}_p{}^*, o(x)}} \Phi(d) = \sum_{d|n} \Phi(d)$.
   En découle l'existence d'un élément d'ordre p-1, c'est-à-dire la cyclicité de $\mathbb{Z}_p{}^*$.
2. Supposons que $k \geq 2$. Montrons que $(1+p)^{p^{k-2}} \equiv 1 + p^{k-1}[p^k]$.
   en effet, $(1+p)^{p^{k-2}} = 1 + p^{k-1} + \sum_{i=2}^{p^{k-2}} \binom{p^{k-2}}{i} p^i$.
   Or, pour $i \in [\![2, p^{k-2}]\!]$, $v_p\left(\binom{p^{k-2}}{i} p^i\right) = v_p(p^{i+k-2} \prod_{j=1}^{i-1} \frac{p^{k-2}-i}{i+1}) \geq k - 2 + i - v_p(i) \geq k$ ce qu'il fallait démontrer. Il est clair que $(1+p)^{p^{k-1}} \equiv 1[p^k]$.
   Donc $o(\overline{1+p}) = p^{k-1}$.
   Soit $q \in \mathbb{Z}\backslash p\mathbb{Z}$, soit $\bar{q}$ sa classe modulo p^k. Alors $\bar{q} \in \left(\mathbb{Z}_{p^k}\right)^*$. De plus l'ordre de q dans $\mathbb{Z}_p{}^*$ est $p-1$, d'où son ordre dans $\left(\mathbb{Z}_{p^k}\right)^*$ est $r(p-1)$pour un certain $r \in \mathbb{N}^*$ et par suite $o(q^r) = p - 1$.
   Du fait que $p - 1 \wedge p^k = 1$, il découle que $o\big((1+p)q^r\big) = p^k(p-1)$ d'où la cyclicité de $\left(\mathbb{Z}_{p^k}\right)^*$.
3. Les cardinaux de $\mathbb{Z}_2{}^*$ et $\mathbb{Z}_4{}^*$ sont premiers, d'où ils sont cycliques. Regardons $\mathbb{Z}_8{}^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. On a $\bar{3}^2 = \bar{5}^2 = \bar{7}^2 = 1$, d'où $\mathbb{Z}_8{}^*$ n'est pas cyclique. Supposons pour $n \geq 3$, $(\mathbb{Z}_{2^n})^*$ non cyclique. Soit $k = \max\{o(\bar{x}), \bar{x} \text{ dans } \mathbb{Z}_{2^n}{}^*\}$ $(k < n)$et $\bar{y} \in \mathbb{Z}_{2^n}{}^*$ tel que $o(\bar{y}) = k$.
   Regardons les classes $\bar{y}$ et $\overline{y + 2^n}$ dans $\mathbb{Z}_{2^{n+1}}{}^*$. On a : $\bar{y}^k, \overline{y+2^n}^k \in \{\bar{1}, \overline{1+2^n}\}$.

Il facile de déduire que $\max\{o(\bar{x}), \bar{x} \text{ dans } \mathbb{Z}_{2^{n+1}}{}^*\} \leq k+1 < n+1$, d'où $(\mathbb{Z}_{2^{n+1}})^*$ n'est pas cyclique. Finalement $(\mathbb{Z}_{2^n})^*$ est cyclique si et seulement si $n \leq 2$.

4. Soit $G=\prod_{i=1}^{r} G_i$ avec les $(G_i)_{i\in[\![1,r]\!]}$ cycliques. Soit $(N, n_1,\cdots, n_r) = (|G|, |G_1|,\cdots, |G_r|)$.
   Soit $M=PPCM(n_1,\cdots, n_r)$.Il est clair que $M|N$.
   Supposons que G est cyclique, soit $g=(g_1,\cdots, g_r) \in G, o(g) = N$. Du fait que $N=PPCM(o(g_1),\cdots, o(g_r))$, et que $o(g_i)|n_i$, il découle que $N|M$, donc $N = M$ c'est à dire que les $(n_i)_{i\in[\![1,r]\!]}$ sont premiers entre eux.
   Supposons les $(n_i)_{i\in[\![1,r]\!]}$ sont premiers entre eux. Naturellement $N=M$.
   Soit $g=(g_1,\cdots, g_r) \in G$ tel que $\forall i, o(g_i) = n_i$. Il est clair que $o(g)=N$ donc G est cyclique.
5. Soit $n=\prod_{i=1}^{r} {p_i}^{\alpha_i}$ (avec $r \geq 2$) un entier décomposé en puissances de facteurs premiers (supposés ordonnés par ordre croissant).
   Du théorème chinois, les anneaux $\mathbb{Z}_n$ et $\prod_{i=1}^{r} \mathbb{Z}_{{p_i}^{\alpha_i}}$ sont isomorphes,
   donc $\mathbb{Z}_n{}^* \cong \prod_{i=1}^{r} \left(\mathbb{Z}_{{p_i}^{\alpha_i}}\right)^*$
   Si n admet deux facteurs premiers impairs distincts p et q, alors 2 est un commun diviseur de $|(\mathbb{Z}_p)^*|$ et $|(\mathbb{Z}_q)^*|$ d'où $\mathbb{Z}_n{}^*$ n'est pas cyclique. Donc une condition nécessaire pour que $\mathbb{Z}_{\prod_{i=1}^{r} {p_i}^{\alpha_i}}$ soit cyclique est que $r \leq 2$ et que $p_1 = 2$. De 3. et 4. il découle que cette condition est suffisante. Ainsi on a déterminé tous les entiers $n\in \mathbb{N}^*\backslash\backslash\{2\}$ tels que $\mathbb{Z}_n^*$ soit cyclique.