Soit G un groupe fini de cardinal p, où p est un nombre premier. Alors G est cyclique et $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Proof. Soit e l'élément neutre de G. Pour tout $g \in G\backslash\{e\}$, l'ordre de $\langle g\rangle$ divise $\mathrm{Card}(G)=p$ d'après le théorème de Lagrange. Comme p est premier, l'ordre de g est soit 1 soit p. Par choix de $g \neq e$ on a $\mathrm{ord}(g) \neq 1$, donc $\mathrm{ord}(g) = p$. Ainsi $\langle g\rangle$ contient p éléments et donc $\langle g\rangle = G$: G est cyclique.
L'application

$$\varphi : \mathbb{Z} \to G, \qquad \varphi(k) = g^k$$

induit un morphisme surjectif $\bar{\varphi} : \mathbb{Z}/p\mathbb{Z} \to G$. Comme $\mathrm{Card}(\mathbb{Z}/p\mathbb{Z})= \mathrm{card}(G) = \mathrm{Card}(p)$, ce morphisme surjectif est bijectif, donc un isomorphisme. On a donc $G \simeq \mathbb{Z}/p\mathbb{Z}$. □