Dans la suite $p \in \mathbb{N}$ est un nombre premier.

Lemme 1 : Soit G un p-groupe non trivial, alors $Z(G) \neq \{e\}$.

preuve : On fait agir G sur lui même par conjugaison.
On note N le nombre d'orbites différentes et $orb(x_1), \dots orb(x_N)$ ces orbites.
On note $J := \{ i \in [\![1;N]\!],\ |orb(x_i)| = 1 \}$
Par la formule des classes :

$|G| = \sum_{i=1}^{N} card(orb(x_i)) = \sum_{i \in J^c} card(orb(x_i)) + card(J)$. On a $g \in Z(G) \iff |orb(g)| = 1 \iff orb(g) = \{g\}$.

donc si $g \in Z(G)$, $\exists ! i \in J$; $g = x_i$ on a une bijection $J \longrightarrow Z(G)$, $i \longmapsto x_i$

l'équation devient $|G| = \sum_{i \in J^c} card(orb(x_i)) + |Z(G)|$. Puisque $\forall g \in G$, $\underbrace{card(orb(g))}_{= [G : stab(g)]\ \text{car}\ orb(g) \mapsto \frac{G}{stab(g)},\ hgh^{-1} \mapsto \overline{h}\ \text{bijection}} . |stab(g)| = |G|$

$\forall i \in J^c$, $\underbrace{|orb(x_i)|}_{>1} \mid |G|$

donc $card(orb(x_i)) \equiv 0 [p]$ et en réduisant modulo p on a $0 \equiv 0 + |Z(G)| [p]$ et donc $p \mid \underbrace{|Z(G)|}_{\geq 1}$
donc $|Z(G)| > 1$.

Lemme 2 : Si G est un groupe fini tel que $\frac{G}{Z(G)}$ est cyclique alors G est abélien. □

preuve : on écrit $\frac{G}{Z(G)} = \langle \bar{a} \rangle$.

Soient $x, y \in G$. On a $\bar{x} = \bar{a}^m$ et $\bar{y} = \bar{a}^m$. Donc $\exists h_1, h_2 \in Z(G)$, $x = a^m h_1$, $y = a^m h_2$
on a $xy = a^m h_1 a^m h_2 = a^m h_2 a^m h_1 = yx$ puisque tous les éléments commutent entre eux.
Donc G est abélien.

proposition : Soit G un groupe d'ordre p^2. Alors $G \simeq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ ou $\frac{\mathbb{Z}}{p^2\mathbb{Z}}$.

preuve : Par Lagrange et par le lemme 1 $|Z(G)| = p$ ou p^2

2ème cas : Dans ce cas on a $Z(G) = G$ abélien.
1er cas : On a $\left|\frac{G}{Z(G)}\right| = p$ et $\frac{G}{Z(G)} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ cyclique et par le lemme 2 G est abélien (en fait ce cas était impossible car dans ce cas, $Z(G) = G$ d'ordre p^2 et pas p)
Donc :
G est abélien. Si il existe $g \in G$ d'ordre p^2 alors G est cyclique $\simeq \frac{\mathbb{Z}}{p^2\mathbb{Z}}$.
Sinon, on prend g_1 d'ordre p et $g_2 \notin \langle g_1 \rangle$ (d'ordre aussi p du coup) ← car tous d'ordre p (sauf e)
Alors si $\begin{cases} H = \langle g_1 \rangle \\ N = \langle g_2 \rangle \end{cases}$ on a :

- $H \cap N = \{e\}$ (neutre de G) car si $x \in H \cap N \setminus \{e\}$, x est d'ordre p par Lagrange (p premier) et donc $\langle x \rangle = H = N$ → Absurde
- $N.H$ est de cardinal $p \times p = p^2$ (car $N \times H \longmapsto N.H$, $(x;y) \longmapsto xy$ est alors une bijection)

donc $G = N.H$

De plus G étant abélien $\varphi : N \times H \longmapsto G$, $(x;y) \longmapsto xy$ est un morphisme et bijectif.

D'où $G \simeq N \times H \simeq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$

□

Remarque : $N.H < G \Rightarrow NH = HN \Leftarrow H$ ou $N \lhd G$

Si le groupe n'était pas abélien avec H ou $N \lhd G$ on aurait un produit semi-direct.

Leçons : 101 : groupe opérant sur un ensemble.

103 : conjugaison dans un grp

104 : groupes finis