Sia p un primo. Dimostriamo che un gruppo di ordine p^2 è isomorfo al gruppo ciclico $\mathbf{Z}_{p^2}$ oppure al prodotto $\mathbf{Z}_p \times \mathbf{Z}_p$.

Lemma 1. *Sia G un gruppo e siano H, N due sottogruppi normali di G. Allora*

(a) $HN = \{hn : h \in H \text{ e } n \in N\}$ è un sottogruppo di G.

(b) Se $H \cap N = \{e\}$, allora HN è isomorfo a $H \times N$.

Dimostrazione. Lasciamo la dimostrazione della parte (a) al lettore. In realtà basta già che solo uno dei sottogruppi H, N sia normale. Per (b) si osserva che per ogni $h \in H$ e $n \in N$ il commutatore $nhn^{-1}h^{-1}$ appartiene a $H \cap N = \{e\}$ ed è quindi banale. In altre parole, n e h commutano.

Si considera la mappa suriettiva $\phi : H \times N \longrightarrow HN$ data da $(h, n) \mapsto hn$. La condizione $H \cap N = \{e\}$ implica che ϕ è una iniezione. Il fatto che gli elementi di H e N commutano implica che ϕ è un omomorfismo. Si conclude che ϕ è un isomorfismo come richiesto.

Proposizione 2. *Sia G un gruppo finito e sia $H \subset G$ un sottogruppo di indice $[G : H] = p$, dove p è il più piccolo divisore primo di $\#G$. Allora H è un sottogruppo normale.*

Dimostrazione. Consideriamo l'insieme X delle classi laterali sinistre di H. Allora X è un insieme di p elementi. Identifichiamo il gruppo $S(X)$ delle permutazioni di X con il gruppo simmetrico S_p.

Per ogni $g \in G$, sia $\pi_g : X \longrightarrow X$ la permutazione data da $\pi_g(xH) = gxH$ per ogni classe laterale sinistra xH di H. Allora la mappa

$$\phi : G \longrightarrow S_p$$

data da $\phi(g) = \pi_g$ è un omomorfismo di gruppi. L'ordine dell'immagine di ϕ divide sia $\#G$ che $\#S_p = p!$. L'ipotesi sul primo p implica quindi che $\#\phi(G)$ divide p. Poichè ϕ è certamente non banale, l'ordine di $\phi(G)$ è uguale a p. Poiché p è primo, gli elementi di S_p di ordine p sono p-cicli. Questo implica che per ogni $g \in G$ la permutazione π_g o è un p-ciclo o è l'identità.

Adesso facciamo vedere che $H = \ker(\phi)$ e quindi che H è normale: per ogni $h \in H$, si ha che $hH = H$. Questo implica che la permutazione π_h fissa la classe laterale H. La permutazione π_h ha quindi un punto fisso e non può essere un p-ciclo. Si ha quindi che π_h è l'identità, ossia $h \in \ker(\phi)$. Questo dimostra che $H \subset \ker(\phi)$. L'uguaglianza segue dal fatto che $[G : H] = p = \#\phi(G) = [G : \ker(\phi)]$.

Questo dimostra la proposizione.

Proposizione 3. *Sia p un primo e sia G un gruppo di ordine p^2. Allora si ha che $G \cong \mathbf{Z}_{p^2}$ oppure $G \cong \mathbf{Z}_p \times \mathbf{Z}_p$.*

Dimostrazione. Se G contiene un elemento di ordine p^2, allora $G \cong \mathbf{Z}_{p^2}$. Nel caso contrario, ogni elemento non banale di G ha ordine p. Sia $e \neq g \in G$ e sia $h \in G - \langle g \rangle$. Gli indici dei sottogruppi $N = \langle g \rangle$ e $H = \langle h \rangle$ sono uguali a p. Per la Proposizione 2 sono quindi normali. La scelta di h non solo implica che $H \cap N = \{e\}$ ma anche che HN è strettamente più grande di N e quindi $HN = G$. Il Lemma 1 implica adesso che $G = HN \cong H \times N \cong \mathbf{Z}_p \times \mathbf{Z}_p$ come richiesto.