Sia G un gruppo finito di ordine n e sia p un divisore primo di n. Scriviamo $n = p^a m$ con m non divisibile per p. Un *p-sottogruppo di Sylow* di G è un sottogruppo di ordine p^a.

Teorema. *(L. Sylow 1872) Sia G un gruppo finito come sopra.*
(a) Ogni p-gruppo $H \subset G$ è contenuto in un p-sottogruppo di Sylow di G;
(b) I p-sottogruppi di Sylow di G sono coniugati fra loro;
(c) Il numero di p-sottogruppi di Sylow divide m ed è congruo ad 1 (mod p).

Qua un *p-gruppo* è un gruppo finito di ordine una potenza di un numero primo p. Se applichiamo la parte (a) del Teorema di Sylow al gruppo banale H, vediamo che per ogni divisore primo p di $\#G$, un gruppo finito G possiede p-sottogruppi di Sylow.

Lemma 1. *Sia H un p-gruppo che agisce su un insieme finito X. Allora si ha che*

$$\#X \equiv X^H \pmod{p}.$$

Dimostrazione. L'insieme X è unione disgiunta delle orbite di H e quindi $\#X$ è la somma delle cardinalità delle orbite di H. La cardinalità di ogni orbita divide $\#H$ ed è quindi potenza di p. In particolare, un'orbita consiste in un punto fisso oppure la sua cardinalità è divisibile per p. Concludiamo che $\#X \equiv \#X^H \pmod{p}$ dove X^H indica l'insieme dei punti di X fissati da H.

Corollario 2. *Sia $H \subset G$ un p-gruppo. Allora si ha che*

$$[N_G H : H] \equiv [G : H] \pmod{p}.$$

Dimostrazione. Il gruppo H agisce sull'insieme X delle classi laterali sinistre di H. Abbiamo che $\#X = [G : H]$. Una classe gH in X è fissata da H quando $hgH = gH$ per ogni $h \in H$ ovvero quando $g^{-1}hg \in H$ per ogni $h \in H$. In altre parole, gH è fissata quando g è contenuto nel normalizzante $N_G H$ di H. I punti fissi di X sono quindi le classi laterali gH con $g \in N_G H$. Poiché ce ne sono $[N_G H : H]$, il corollaio segue dal Lemma 1.

Lemma 3. *Sia G un gruppo finito e siano P e P' due p-sottogruppi di Sylow di G. Se P normalizza P', allora $P = P'$.*

Dimostrazione. Se P normalizza P', allora si ha che $P \subset N_G P'$. Poiché P' è un sottogruppo normale di G, abbiamo l'isomorfismo naturale

$$P/(P' \cap P) \quad \cong \quad PP'/P'.$$

Il gruppo a sinistra è quoziente di P ed è quindi un p-gruppo. Invece, poiché P' è un p-sottogruppo di Sylow, l'ordine del gruppo a destra non è divisibile per p. Concludiamo che i due gruppi sono banali e quindi $P = P'$, come richiesto.

Dimostrazione del teorema di Sylow. (a) Sia $H \subset G$ un p-gruppo. Procediamo per induzione (però, nel senso inverso!) rispetto a $\#H$.

Se $\#H = p^a$, allora H stesso è un p-sottogruppo di Sylow e non c'è niente da dimostrare. Supponiamo che $\#H = p^b$ con $b < a$. Sotto quest'ipotesi p divide $[G : H]$. Per il Corollario 2, anche $[N_G H : H]$ è divisibile per p. Per il Teorema di Cauchy, il gruppo quoziente $N_G H/H$ possiede quindi un elemento x di ordine p.

Consideriamo la proiezione canonica $\pi : N_G H \longrightarrow N_G H/H$. Sia $H' = \pi^{-1}(\langle x \rangle)$. In altre parole, H' è la controimmagine del gruppo generato da x. Allora $H \subset H'$ e l'ordine di H' è p^{b+1}. Per induzione, sappiamo che H' è contenuto in un p-sottogruppo di Sylow e quindi anche H lo è, come richiesto.

(b) e (c) Consideriamo l'azione di G per coniugio sull'insieme X dei p-gruppi di Sylow di G. Sia P un p-sottogruppo di Sylow di G. Lo stabilizzatore di P è il normalizzante $N_G P$. La cardinalità dell'orbita $Y \subset X$ di un p-sottogruppo di Sylow P è quindi uguale a $[G : N_G P]$. Poichè $[G : N_G P]$ divide $[G : P] = m$, abbiamo che $\#Y$ divide m.

Consideriamo l'azione di P su Y per coniugio. Poiché $\#Y = m$ non è divisibile per p, il Lemma 1 implica che P fissa qualche elemento di Y. Gli elementi di Y sono i p-gruppi di Sylow P' coniugati a P. Un elemento P' di Y è fissato da P se e solo se P normalizza P'. Per il Lemma 3, l'unico p-sottogruppo di Sylow normalizzato da P, è P stesso. Concludiamo che l'unico punto in Y fissato da P è P stesso. Per il Lemma 1 abbiamo quindi che $\#Y \equiv 1 \pmod{p}$.

Infine consideriamo l'azione su Y per coniugio di un p-sottogruppo di Sylow qualsiasi P'. Poichè $\#Y \equiv 1 \pmod{p}$, il Lemma 1 implica che P' fissa un punto di Y. In altre parole, P' normalizza un p-sottogruppo di Sylow Q coniugato a P. Per il Lemma 3, abbiamo che $P' = Q$ e quindi P' è coniugato a P. Poichè P' era arbitrario, concludiamo che i p-sottogruppi di Sylow sono coniugati fra loro. Questo è (b).

Da (b) segue che $X = Y$, implicando (c).