Wielandt's proof of the main Sylow theorem

This is an alternative proof of the main part of Sylow theory due to Wielandt (1959). Notably it does not use Cauchy's Theorem. However it uses a similar technique to the proof of Cauchy's Theorem in lectures, namely to look in a bigger set than the one you want, and do some counting modulo p to show that what you are looking for is in there somewhere!

The method actually proves the following result due to Frobenius (1895).

Theorem. Let G be a finite group, p a prime and $r \in \mathbb{N}$ such that p^r divides $|G|$. Then the number of subgroups of G of order p^r is congruent to 1 (mod p).

Proof. Let $|G| = p^r m$ and $X = \{A \subseteq G : |A| = p^r\}$, the set of subsets of G of order p^r. Then G acts on X by $g \cdot A = \{ga : a \in A\}$ and any orbit $\mathrm{orb}_G(B)$ of G contains an element A with $1 \in A$ (since if $b \in B$, $1 \in A = b^{-1} \cdot B$). Now $\mathrm{Stab}_G(A)$ acts on A by left multiplication $g \cdot a = ga \in A$ and so partitions A into a union of right cosets of $\mathrm{Stab}_G(A)$, including the identity coset. Thus $\exists\, s \leqslant r$ such that $|\mathrm{Stab}_G(A)| = p^s$ and $|\mathrm{orb}_G(A)| = |G|/|\mathrm{Stab}_G(A)| = p^{r-s}m$ (by the Orbit–Stabilizer Theorem) with

$$|\mathrm{orb}_G(A)| = m \quad \Leftrightarrow \quad s = r \quad \Leftrightarrow \quad \mathrm{Stab}_G(A) = A \quad \Leftrightarrow \quad A \leqslant G,$$

in which case $\mathrm{orb}_G(A)$ is the set of left cosets of A. Otherwise, $|\mathrm{orb}_G(A)|$ is divisible by pm. We conclude that the number u of subgroups of order p^r is the number of orbits of size m in X, and that $|X| \equiv um \pmod{pm}$.

Now it is possible at this point to make a combinatorial argument to compute $|X|$ modulo pm. However, there is an ultra-slick trick which avoids this.

The key is to observe that $|X|$ is independent of the group structure of G: it depends only on $|G| = p^r m$. Hence to compute $|X|$ modulo pm, we can replace G by any group H with $p^r m$ elements! Everything we have proven above applies equally to H, and so $|X| \equiv vm \pmod{pm}$, where v is the number of subgroups of order p^r in H. Now there is a choice of H for which we already know what v is: for $H = \mathbb{Z}_{p^r m}$ (or any cyclic group of order $p^r m$), $v = 1$. Hence $|X| \cong m \pmod{pm}$.

Returning now to the original group G, we thus have that $um \equiv m \pmod{pm}$, i.e., $um = m + kpm$ for some $k \in \mathbb{Z}$, i.e., $u = 1 + kp$ and $u \equiv 1 \pmod{p}$. $\square$