RECALL: Let G be a finite group and p be a prime number. Write $|G| = p^e m$ with $e \geq 0$ and $p \nmid m$.

- A p-subgroup of G is a subgroup of order p^k for some $k \geq 0$.
- A Sylow p-subgroup of G is a subgroup of order p^e.
- We write $\mathrm{Syl}_p(G)$ for the set of Sylow p-subgroups of G. We often write n_p for $\#\mathrm{Syl}_p(G)$.

MAIN THEOREM OF SYLOW THEORY: Let G be a finite group and p be a prime number. Write $|G| = p^e m$ with $e \geq 0$ and $p \nmid m$.

(1) There exists a Sylow p-subgroup of G.
(2) Every Sylow subgroup is conjugate. Moreover, for any p-subgroup Q and any Sylow p-subgroup P, there is some $g \in G$ such that $Q \leq gPg^{-1}$.
(3) The number of Sylow p-subgroups of G is congruent to 1 modulo p.
(4) The number of Sylow p-subgroups of G divides m.

LEMMA: Let G be a finite group and p be a prime number. Let P be a Sylow p-subgroup of G and Q be any p-subgroup of G. Then $Q \cap N_G(P) = Q \cap P$.

(1) Let $p < q$ be distinct primes and G be a group of order pq. Use the Sylow Theorem to show that G is not simple.

By parts (3) and (4) of the Sylow Theorem, the number of q-Sylow subgroups divides p and is congruent to 1 modulo q, meaning of the form $1 + qk$. The only divisors of p are 1 and p, but $p < q$ implies p is not congruent to 1 modulo q. This means there is only one q-Sylow. This must then be a normal subgroup of order q, a proper normal subgroup.

(2) Consider $G = S_4$.

(a) Show[1] that G has a subgroup isomorphic to D_4, the symmetry group of the square.

We know from before that D_4 acts on the four vertices V of the square, and this action is faithful. The corresponding permutation representation is an injective homomorphism $\rho : D_4 \to \mathrm{Perm}(V)$; after labelling the vertices, we can identify $\mathrm{Perm}(V) \cong S_4$. The image of D_4 in S_4 is the isomorphic copy of D_4.

(b) Show that S_4 has exactly three subgroups isomorphic to D_4, that these three are conjugate, and that any subgroup of S_4 of order 8 is isomorphic to D_4.

Consider the 2-Sylows of S_4. By the Sylow Theorem, the number of these is congruent to 1 modulo 2 and divides 3, so there are either 1 or 3. We claim that no subgroup of order 8 is normal. Indeed, a normal subgroup is a disjoint union of conjugacy classes including $\{e\}$, and the nonidentity conjugacy classes of S_4 have size $3, 6, 6, 8$; one cannot express 8 as 1 plus a sum of these. This shows the claim. Therefore, there cannot be a unique 2-Sylow (which would necessarily be normal), so there are three. Since any subgroup of order 8 is a 2-Sylow, and these are all conjugate, they are all isomorphic.

(c) Describe the subgroups of order 3 of S_4.

[1]Hint: D_4 acts on the vertices of a square.

Without using the Sylow Theorem we already know that any group of order three is isomorphic to C_3, and that there are eight elements of order 3 in S_4. Each subgroup of order 3 has two elements of order 3 plus the identity. Thus there are four subgroups of order three, each isomorphic to C_3. Note that the Sylow theorem gives the two possibilities 1 or 4 for the number of 3-Sylows.

(3) Proof of part (1) of Sylow's Theorem: Fix p. We will argue by induction on n that every group of n has a Sylow p-subgroup.

(a) Write $n = p^e m$. Address the case $e = 0$. Henceforth assume $e > 0$, so $p \mid n$.

If $p \nmid n$, the identity is a p-Sylow.

(b) Case 1: Assume that p divides $|Z(G)|$. Explain why there is some $N \trianglelefteq G$ with $|N| = p$.

There is an element g of order p in the center by Cauchy. Any subgroup of the center is normal, so $N = \langle g \rangle$ works.

(c) Apply the induction hypothesis to G/N. How can you use this to find a Sylow p-subgroup in G?

The order of G/N is $p^{e-1}m < n$. By induction, there is a p-Sylow subgroup of G/N. This has order p^{e-1} and the index is m. By the Lattice Isomorphism theorem, there is a subgroup of index m in G, which has order p^e, so a p-Sylow.

(d) Case 2: Assume that p does not divide $|Z(G)|$. Show that there is some $g \in G$ such that $[G : C_G(g)]$ is *not* a multiple of p and *not* one. What does this say about $|C_G(g)|$? What do you get from the induction hypothesis?

Consider the class equation. Since the order of G is a multiple of p, and the order of the center is not, there is a nontrivial conjugacy class of size not a multiple of p. Thus there is some $g \in G$ with $[G : C_G(g)]$ not a multiple of p. This means that the order of $C_G(g)$ is $p^e u$ with $u|m$ and $u \neq m$. By the induction hypothesis, $C_G(g)$ has a p-Sylow, which is a subgroup $H \leq C_G(g)$ with $|H| = p^e$. This H is a p-Sylow subgroup of G.

(4) Proof of parts (2) and (3) of Sylow's Theorem: Fix a Sylow p-subgroup P. Let $\mathcal{S}_P$ be the set of conjugates of P, namely $\{gPg^{-1} \mid g \in G\} \subseteq \mathrm{Syl}_p(G)$. We need to show that (2) $\mathrm{Syl}_p(G) = \mathcal{S}_P$ and that (3) $\#\mathrm{Syl}_p(G) \equiv 1 \bmod p$.

(a) Let Q be any p-subgroup of G, and let Q act on $\mathcal{S}_P$ by conjugation. Use the Lemma to show that for any $P_i \in \mathcal{S}_P$, $\mathrm{Stab}_Q(P_i) = Q \cap P_i$.

(b) Show that $|\mathcal{S}_P| = \sum_{i=1}^{s} [Q : Q \cap P_i]$ where P_i ranges through a set of representatives of distinct orbits for the action of Q on $\mathcal{S}_P$.

(c) Take $Q = P$ and WLOG $P_1 = P$. Deduce that $|\mathcal{S}_P| \equiv 1 \bmod p$.

(d) To show (2) by contradiction, suppose that Q is not contained in any conjugate of P. Observe that $Q \cap P_i \subsetneqq Q$ for all i. Revisit the equation in part (b) and the conclusion of part (c) to obtain a contradiction.

(e) Deduce part (3) from part (c) and part (2).