To prove (2) note that if $P \in Syl_p(S_k)$, for some odd prime p, by (1) (or order considerations) $P \leq A_k$, hence $P \in Syl_p(A_k)$ as well. By Frattini's Argument (Proposition 6)

$$S_k = N_{S_k}(P)A_k$$

so, in particular, $N_{S_k}(P)$ is not contained in A_k. This forces $N_{S_k}(P) \cap A_k$ $(= N_{A_k}(P))$ to be a subgroup of index 2 in $N_{S_k}(P)$.

For example, there is no simple group of order 264. Suppose G were a simple group of order $264 = 2^3 \cdot 3 \cdot 11$. We must have $n_{11} = 12$. As usual, G would be isomorphic to a subgroup of S_{12}. Since G is simple (hence contains no subgroup of index 2), $G \leq A_{12}$. Let $P \in Syl_{11}(G)$. Since $n_{11} = 12 = |G : N_G(P)|$, we have $|N_G(P)| = 22$. As above,

$$|N_{A_{12}}(P)| = \tfrac{1}{2}|N_{S_{12}}(P)| = \tfrac{1}{2}11(11-1) = 55;$$

however, 22 does not divide 55, a contradiction to $N_G(P) \leq N_{A_{12}}(P)$.

Finally, we emphasize that we have only barely touched upon the combinatorial information available from certain permutation representations. Whenever possible in the remaining examples we shall illustrate other applications of this technique.

Playing p-Subgroups Off Against Each Other for Different Primes p

Suppose p and q are distinct primes such that every group of order pq is cyclic. This is equivalent to $p \nmid q - 1$, where $p < q$. If G has a Sylow q-subgroup Q of order q and $p \mid |N_G(Q)|$, applying Cauchy's Theorem in $N_G(Q)$ gives a group P of order p normalizing Q (note that P need not be a Sylow p-subgroup of G). Thus PQ is a group and if PQ is abelian, we obtain

$$PQ \leq N_G(P) \quad \text{and so} \quad q \mid |N_G(P)|.$$

(A symmetric argument applies if Sylow p-subgroups of G have order p and q divides the order of a Sylow p-normalizer). This numerical information alone may be sufficient to force $N_G(P) = G$ (i.e., $P \trianglelefteq G$), or at least to force $N_G(P)$ to have index smaller than the minimal index permitted by permutation representations, giving a contradiction by a preceding technique.

For example, there are no simple groups of order 1785. If there were, let G be a simple group of order $1785 = 3 \cdot 5 \cdot 7 \cdot 17$. The only possible value for n_{17} is 35, so if Q is a Sylow 17-subgroup, $|G : N_G(Q)| = 35$. Thus $|N_G(Q)| = 3 \cdot 17$. Let P be a Sylow 3-subgroup of $N_G(Q)$. The group PQ is abelian since 3 does not divide $17 - 1$, so $Q \leq N_G(P)$ and $17 \mid |N_G(P)|$. In this case $P \in Syl_3(G)$. The permissible values of n_3 are 7, 85 and 595; however, since $17 \mid |N_G(P)|$, we cannot have $17 \mid |G : N_G(P)| = n_3$. Thus $n_3 = 7$. But G has no proper subgroup of index < 17 (the minimal index of a proper subgroup is 17 for this order), a contradiction. Alternatively, if $n_3 = 7$, then $|N_G(P)| = 3 \cdot 5 \cdot 17$, and by Sylow's Theorem applied in $N_G(P)$ we have $Q \trianglelefteq N_G(P)$. This contradicts the fact that $|N_G(Q)| = 3 \cdot 17$.

We can refine this method by not requiring P and Q to be of prime order. Namely, if p and q are distinct primes dividing $|G|$ such that $Q \in Syl_q(G)$ and $p \mid |N_G(Q)|$, let $P \in Syl_p(N_G(Q))$. We can then apply Sylow's Theorems in $N_G(Q)$ to see whether

$P \trianglelefteq N_G(Q)$, and if so, force $N_G(P)$ to be of small index. If P is a Sylow p-subgroup of the whole group G, we can use the congruence part of Sylow's Theorem to put further restrictions on $|N_G(P)|$ (as we did in the preceding example). If P is not a Sylow p-subgroup of G, then by the second part of Sylow's Theorem $P \leq P^* \in Syl_p(G)$. In this case since $P < P^*$, Theorem 1(4) shows that $P < N_{P^*}(P)$. Thus $N_G(P)$ (which contains $N_{P^*}(P)$) has order divisible by a larger power of p than divides $|P|$ (as well as being divisible by $|Q|$).

For example, there are no simple groups of order 3675. If there were, let G be a simple group of order $3675 = 3 \cdot 5^2 \cdot 7^2$. The only possibility for n_7 is 15, so for $Q \in Syl_7(G)$, $|G : N_G(Q)| = 15$ and $|N_G(Q)| = 245 = 5 \cdot 7^2$. Let $N = N_G(Q)$ and let $P \in Syl_5(N)$. By the congruence conditions of Sylow's Theorem applied in N we get $P \trianglelefteq N$. Since $|P| = 5$, P is not itself a Sylow 5-subgroup of G so P is contained in some Sylow 5-subgroup P^* of G. Since P is of index 5 in the 5-group P^*, $P \trianglelefteq P^*$ by Theorem 1, that is $P^* \leq N_G(P)$. This proves

$$\langle N, P^* \rangle \leq N_G(P) \quad \text{so} \quad 7^2 \cdot 5^2 \bigm| |N_G(P)|.$$

Thus $|G : N_G(P)| \bigm| 3$, which is impossible since P is not normal and G has no subgroup of index 3.

Studying Normalizers of Intersections of Sylow p-Subgroups

One of the reasons the counting arguments in the first method above do not immediately generalize to Sylow subgroups which are not of prime order is because if $P \in Syl_p(G)$ for some prime p and $|P| = p^a$, $a \geq 2$, then it need not be the case that distinct conjugates of P intersect in the identity subgroup. If distinct conjugates of P *do* intersect in the identity, we can again count to find that the number of elements of p-power order is $n_p(|P| - 1)$.

Suppose, however, there exists $R \in Syl_p(G)$ with $R \neq P$ and $P \cap R \neq 1$. Let $P_0 = P \cap R$. Then $P_0 < P$ and $P_0 < R$, hence by Theorem 1

$$P_0 < N_P(P_0) \quad \text{and} \quad P_0 < N_R(P_0).$$

One can try to use this to prove that the normalizer in G of P_0 is sufficiently large (i.e., of sufficiently small index) to obtain a contradiction by previous methods (note that this normalizer is a proper subgroup since $P_0 \neq 1$).

One special case where this works particularly well is when $|P_0| = p^{a-1}$ i.e., the two Sylow p-subgroups R and P have large intersection. In this case set $N = N_G(P_0)$. Then by the above reasoning (i.e., since P_0 is a maximal subgroup of the p-groups P and R), $P_0 \trianglelefteq P$ and $P_0 \trianglelefteq R$, that is,

$$N \text{ has 2 distinct Sylow } p\text{-subgroups: } P \text{ and } R.$$

In particular, $|N| = p^a k$, where (by Sylow's Theorem) $k \geq p + 1$.

Recapitulating, if Sylow p-subgroups pairwise intersect in the identity, then counting elements of p-power order is possible; otherwise there is some intersection of Sylow p-subgroups whose normalizer is "large." Since for an arbitrary group order one cannot necessarily tell which of these two phenomena occurs, it may be necessary to split the nonsimplicity argument into two (mutually exclusive) cases and derive a contradiction in each. This process is especially amenable when the order of a Sylow p-subgroup is p^2 (for example, this line of reasoning was used to count elements of 2-power order in the proof that a simple group of order 60 is isomorphic to A_5 — Proposition 23, Section 4.5).

Before proceeding with an example we state a lemma which gives a sufficient condition to force a nontrivial Sylow intersection.

Lemma 13. In a finite group G if $n_p \not\equiv 1 (\text{mod } p^2)$, then there are distinct Sylow p-subgroups P and R of G such that $P \cap R$ is of index p in both P and R (hence is normal in each).

Proof: The argument is an easy refinement of the proof of the congruence part of Sylow's Theorem (cf. the exercises at the end of Section 4.5). Let P act by conjugation on the set $Syl_p(G)$. Let $\mathcal{O}_1, \dots, \mathcal{O}_s$ be the orbits under this action with $\mathcal{O}_1 = \{P\}$. If p^2 divides $|P : P \cap R|$ for all Sylow p-subgroups R of G different from P, then each $\mathcal{O}_i$ has size divisible by p^2, $i = 2, 3, \dots, s$. In this case, since n_p is the sum of the lengths of the orbits we would have $n_p = 1 + kp^2$, contrary to assumption. Thus for some $R \in Syl_p(G)$, $|P : P \cap R| = p$.

For example, there are no simple groups of order 1053. If there were, let G be a simple group of order $1053 = 3^4 \cdot 13$ and let $P \in Syl_3(G)$. We must have $n_3 = 13$. But $13 \not\equiv 1 (\text{mod } 3^2)$ so there exist $P, R \in Syl_3(G)$ such that $|P \cap R| = 3^3$. Let $N = N_G(P \cap R)$, so by the above arguments $P, R \leq N$. Thus $3^4 \mid |N|$ and $|N| > 3^4$. The only possibility is $N = G$, i.e., $P \cap R \trianglelefteq G$, a contradiction.

Simple Groups of Order 168

We now show how many of our techniques can be used to unravel the structure of and then classify certain simple groups by classifying the simple groups of order 168. Because there are no nontrivial normal subgroups in simple groups, this process departs from the methods in Section 5.5, but the overall approach typifies methods used in the study of finite simple groups.

We begin by assuming there is a simple group G of order $168 = 2^3 \cdot 3 \cdot 7$. We first work out many of its properties: the number and structure of its Sylow subgroups, the conjugacy classes, etc. All of these calculations are based only on the order and simplicity of G. We use these results to first prove the uniqueness of G; and ultimately we prove the existence of the simple group of order 168.

Because $|G|$ does not divide $6!$ we have

(1) *G has no proper subgroup of index less than 7,*

since otherwise the action of G on the cosets of the subgroup would give a (necessarily injective since G is simple) homomorphism from G into some S_n with $n \leq 6$.

The simplicity of G and Sylow's Theorem also immediately imply that

(2) *$n_7 = 8$, so the normalizer of a Sylow 7-subgroup has order 21. In particular, no element of order 2 normalizes a Sylow 7-subgroup and G has no elements of order 14.*