conditions allow many more possibilities). Many of our numerical examples arise from these lists of numbers and we often use odd numbers because the Sylow congruence conditions allow fewer values for $n_p$. The purpose of these examples is to illustrate the use of the results we have proved. Many of these examples can be dealt with by more advanced techniques (for example, the Feit–Thompson Theorem proves that there are *no* simple groups of odd composite order).

As we saw in the case $n = 30$ in Section 4.5, even though Sylow's Theorem permitted $n_5 = 6$ and $n_3 = 10$, further examination showed that any group of order 30 must have both $n_5 = 1$ and $n_3 = 1$. Thus the congruence part of Sylow's Theorem is a sufficient but by no means necessary condition for normality of a Sylow subgroup. For many $n$ (e.g., $n = 120$) we can prove that there are no simple groups of order $n$, so there is a nontrivial normal subgroup but this subgroup may not be a Sylow subgroup. For example, $S_5$ and $SL_2(\mathbb{F}_5)$ both have order 120. The group $S_5$ has a unique nontrivial proper normal subgroup of order 60 ($A_5$) and $SL_2(\mathbb{F}_5)$ has a unique nontrivial proper normal subgroup of order 2 ($Z(SL_2(\mathbb{F}_5)) \cong Z_2$), neither of which is a Sylow subgroup. Our techniques for producing normal subgroups must be flexible enough to cover such diverse possibilities. In this section we shall examine Sylow subgroups for different primes dividing $n$, intersections of Sylow subgroups, normalizers of $p$-subgroups and many other less obvious subgroups. The elementary methods we outline are by no means exhaustive, even for groups of "medium" order.

## Some Techniques

Before listing some techniques for producing normal subgroups in groups of a given ("medium") order we note that in all the problems where one deals with groups of order $n$, for some specific $n$, it is first necessary to factor $n$ into prime powers and then to compute the permissible values of $n_p$, for all primes $p$ dividing $n$. We emphasize the need to be comfortable computing mod $p$ when carrying out the last step. The techniques we describe may be listed as follows:

(1) Counting elements.
(2) Exploiting subgroups of small index.
(3) Permutation representations.
(4) Playing $p$-subgroups off against each other for different primes $p$.
(5) Studying normalizers of intersections of Sylow $p$-subgroups.

## Counting Elements

Let $G$ be a group of order $n$, let $p$ be a prime dividing $n$ and let $P \in Syl_p(G)$. If $|P| = p$, then every nonidentity element of $P$ has order $p$ and every element of $G$ of order $p$ lies in some conjugate of $P$. By Lagrange's Theorem distinct conjugates of $P$ intersect in the identity, hence in this case the number of elements of $G$ of order $p$ is $n_p(p-1)$.

If Sylow $p$-subgroups for different primes $p$ have prime order and we assume none of these is normal, we can sometimes show that the number of elements of prime order is $> |G|$. This contradiction would show that at least one of the $n_p$'s must be 1 (i.e., some Sylow subgroup is normal in $G$).

This is the argument we used (in Section 4.5) to prove that there are no simple groups of order 30. For another example, suppose $|G| = 105 = 3 \cdot 5 \cdot 7$. If $G$ were simple, we must have $n_3 = 7$, $n_5 = 21$ and $n_7 = 15$. Thus

$$\begin{array}{lcl} \text{the number of elements of order 3 is } 7 \cdot 2 & = & 14 \\ \text{the number of elements of order 5 is } 21 \cdot 4 & = & 84 \\ \text{the number of elements of order 7 is } 15 \cdot 6 & = & 90 \\ \hline \text{the number of elements of prime order is } 188 & > & |G|. \end{array}$$

Sometimes counting elements of prime order does not lead to too many elements. However, there may be so few elements remaining that there must be a normal subgroup involving these elements. This was (in essence) the technique used in Section 4.5 to show that in a group of order 12 either $n_2 = 1$ or $n_3 = 1$. This technique works particularly well when $G$ has a Sylow $p$-subgroup $P$ of order $p$ such that $N_G(P) = P$. For example, let $|G| = 56$. If $G$ were simple, the only possibility for the number of Sylow 7-subgroups is 8, so

$$\text{the number of elements of order 7 is } 8 \cdot 6 = 48.$$

Thus there are $56 - 48 = 8$ elements remaining in $G$. Since a Sylow 2-subgroup contains 8 elements (none of which have order 7), there can be at most one Sylow 2-subgroup, hence $G$ has a normal Sylow 2-subgroup.

## Exploiting Subgroups of Small Index

Recall that the results of Section 4.2 show that if $G$ has a subgroup $H$ of index $k$, then there is a homomorphism from $G$ into the symmetric group $S_k$ whose kernel is contained in $H$. If $k > 1$, this kernel is a proper normal subgroup of $G$ and if we are trying to prove that $G$ is not simple, we may, by way of contradiction, assume that this kernel is the identity. Then, by the First Isomorphism Theorem, $G$ is isomorphic to a subgroup of $S_k$. In particular, the order of $G$ divides $k!$. This argument shows that if $k$ is the smallest integer with $|G|$ dividing $k!$ for a finite simple group $G$ then $G$ contains no proper subgroups of index less than $k$. This smallest permissible index $k$ should be calculated at the outset of the study of groups of a given order $n$. In the examples we consider this is usually quite easy: $n$ will often factor as

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \quad \text{with} \quad p_1 < p_2 < \dots < p_s$$

and $\alpha_s$ is usually equal to 1 or 2 in our examples. In this case the minimal index of a proper subgroup will have to be at least $p_s$ (respectively $2p_s$) and this is often its exact value.

For example, there is no simple group of order 3393, because if $n = 3393 = 3^2 \cdot 13 \cdot 29$, then the minimal index of a proper subgroup is 29 ($n$ does not divide $28!$ because 29 does not divide $28!$). However any simple group of order 3393 must have $n_3 = 13$, so for $P \in Syl_3(G)$, $N_G(P)$ has index 13, a contradiction.

## Permutation Representations

This method is a refinement of the preceding one. As above, if $G$ is a simple group of order $n$ with a proper subgroup of index $k$, then $G$ is isomorphic to a subgroup of $S_k$. We may identify $G$ with this subgroup and so assume $G \leq S_k$. Rather than relying only on Lagrange's Theorem for our contradiction (this was what we did for the preceding technique) we can sometimes show by calculating within $S_k$ that $S_k$ contains no simple subgroup of order $n$. Two restrictions which may enable one to show such a result are

(1) if $G$ contains an element or subgroup of a particular order, so must $S_k$, and
(2) if $P \in Syl_p(G)$ and if $P$ is also a Sylow $p$-subgroup of $S_k$, then $|N_G(P)|$ must divide $|N_{S_k}(P)|$.

Condition (2) arises frequently when $p$ is a prime, $k = p$ or $p + 1$ and $G$ has a subgroup of index $k$. In this case $p^2$ does not divide k!, so Sylow $p$-subgroups of $G$ are also Sylow $p$-subgroups of $S_k$. Since now Sylow $p$-subgroups of $S_k$ are precisely the groups generated by a $p$-cycle, and distinct Sylow $p$-subgroups intersect in the identity,

$$\text{the no. of Sylow } p\text{-subgroups of } S_k = \frac{\text{the no. of } p\text{-cycles}}{\text{the no. of } p\text{-cycles in a Sylow } p\text{-subgroup}}$$

$$= \frac{k \cdot (k-1) \cdots (k-p+1)}{p(p-1)}.$$

This number gives the index in $S_k$ of the normalizer of a Sylow $p$-subgroup of $S_k$. Thus for $k = p$ or $p + 1$

$$|N_{S_k}(P)| = p(p-1) \qquad (k = p \text{ or } k = p+1)$$

(cf. also the corresponding discussion for centralizers of elements in symmetric groups in Section 4.3 and the last exercises in Section 4.3). This proves, under the above hypotheses, that $|N_G(P)|$ must divide $p(p-1)$.

For example, if $G$ were a simple group of order $396 = 2^2 \cdot 3^2 \cdot 11$, we must have $n_{11} = 12$, so if $P \in Syl_{11}(G)$, $|G : N_G(P)| = 12$ and $|N_G(P)| = 33$. Since $G$ has a subgroup of index 12, $G$ is isomorphic to a subgroup of $S_{12}$. But then (considering $G$ as actually contained in $S_{12}$) $P \in Syl_{11}(S_{12})$ and $|N_{S_{12}}(P)| = 110$. Since $N_G(P) \leq N_{S_{12}}(P)$, this would imply $33 \mid 110$, clearly impossible, so we cannot have a simple group of order 396.

We can sometimes squeeze a little bit more out of this method by working in $A_k$ rather than $S_k$. This slight improvement helps only occasionally and only for groups of even order. It is based on the following observations (the first of which we have made earlier in the text).

**Proposition 12.**
(1) If $G$ has no subgroup of index 2 and $G \leq S_k$, then $G \leq A_k$.
(2) If $P \in Syl_p(S_k)$ for some odd prime $p$, then $P \in Syl_p(A_k)$ and $|N_{A_k}(P)| = \frac{1}{2}|N_{S_k}(P)|$.

*Proof:* The first assertion follows from the Second Isomorphism Theorem: if $G$ is not contained in $A_k$, then $A_k < GA_k$ so we must have $GA_k = S_k$. But now

$$2 = |S_k : A_k| = |GA_k : A_k| = |G : G \cap A_k|$$

so $G$ has a subgroup, $G \cap A_k$, of index 2.