Sylow and Simple Groups: Tricks of the Trade

Ben Marlin

April 2025

Asking one to prove that there are no simple groups of a given order is a common group theory exam question. These are fun questions that illustrate how the structure of groups is in part governed by the prime factorization of their order. Sylow's theorems frequently are the crucial tool in such proofs. In this note, I'll outline three common strategies that you can used when faced with this sort of exam question. I'll also mention some powerful results that are useful but beyond the scope of this course.

1 Review of Sylow's Theorems

We begin by reviewing Sylow's theorems. Let G be a finite group and let $p \mid |G|$ for some prime p.

Sylow's First Theorem: Sylow's first theorem tells us that if $p^k \mid |G|$ then the number of subgroups of G of size p^k is congruent to 1 modulo p. In particular, for any prime power divisor p^k of G, there exists a subgroup $H \leq G$ of order p^k. An elegant proof of this result can be found here. Note that this argument works for any $k \in \mathbb{N}$ such that $p^k \mid |G|$, not just the maximal such power.

However, it turns out that we can say more when we require k to be the maximal power such that $p^k \mid |G|$. We will see this momentarily but first let us fix some terminology and notation. Let $n \in \mathbb{N}$ be the largest number such that $p^n \mid |G|$. We call any subgroup $H \leq G$ of order p^n a p-Sylow subgroup of G. Let $\text{Syl}_p(G)$ denote the collection of p-Sylow subgroups and $n_p := |\text{Syl}_p(G)|$. Note that $\text{Syl}_p(G)$ must be nonempty by Sylow's first theorem.

Sylow's Second Theorem: Sylow's second theorem tells us if H is any subgroup of G of order p^k, $0 \leq k \leq n$, then for any $P \in \text{Syl}_p(G)$ there exists $g \in G$ such that $H \subseteq gPg^{-1}$. This theorem follows from Sylow's first theorem by a counting argument involving the action of H on the cosets G/P by left multiplication.

By considering $H \in \text{Syl}_p(G)$, it easily follows that G acts transitively on $\text{Syl}_p(G)$ by conjugation, i.e., all p-Sylow subgroups of G are conjugate to one another.

This corollary is also often called Sylow's second theorem.

Sylow's Third Theorem: Sylow's third theorem tells us that $n_p = [G : N_G(P)]$ for any $P \in \mathrm{Syl}_p(G)$. It is a consequence of Sylow's second theorem. Indeed, Sylow's second theorem says that $\mathrm{Syl}_p(G)$ consists of the orbit under conjugation of a given $P \in \mathrm{Syl}_p(G)$. By the orbit-stablizer lemma, the size of this orbit is the index of the stabilizer in G. However, the stabilizer of the action on subgroups by conjugation is precisely the normalizer, so $n_p = [G : N_G(P)]$ for any $P \in \mathrm{Syl}_p(G)$. Further, by Lagrange's theorem, it follows that $n_p \mid [G : P]$, which is often called Sylow's third theorem.

2 Contradiction by counting

Since conjugation is an automorphism, it preserves the order of subgroups. Therefore, the conjugate of any p-Sylow subgroup is also a p-Sylow subgroup. Thus, if $n_p = 1$ then the unique p-Sylow subgroup P is normal in G (each of the conjugates of P must be equal to P).

This presents our first strategy for showing that there are no simple groups of a given order: we can attempt to show that there is a unique p-Sylow subgroup for some prime p dividing the given order. However, if we are given an arbitrary group G we generally cannot directly compute $n_p = [G : N_G(P)]$, $P \in \mathrm{Syl}_p(G)$. Usually, the best we can do is try to find n_p by using $n_p \equiv 1 \mod p$ and $n_p \mid [G : P]$. Unfortunately, this is often not enough information to determine n_p exactly, so we need to do some more work. One strategy will be to show that not having any unique Sylow subgroups for some prime implies that the size of our group is too large. We will illustrate this with the following example.

Example: There are no simple groups of order 520.

Observe that $520 = 2^3 \cdot 5 \cdot 13$. Let G be a group of order 520. By Sylow's theorems, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 104$ and $n_{13} \equiv 1 \mod 13$ and $n_{13} \mid 40$. It follows that $n_5 = 1$ or $n_5 = 26$ and $n_{13} = 1$ or $n_{13} = 40$. If either of these numbers is equal to 1, then we have a unique Sylow subgroup, which must be normal, implying G is not simple. Therefore, suppose that $n_5 = 26$ and $n_{13} = 40$. We make use of the following lemma, whose proof is a good exercise:

Lemma 1 *Let G be a group with subgroups $H_1, H_2 \leq G$ with $|H_1| = |H_2| = p$ for a prime p. Then, $H_1 \cap H_2 = \{e\}$ or $H_1 = H_2$.*

By the lemma, each distinct p-Sylow subgroup of prime order contributes $p - 1$ distinct elements to the size of G. In our particular case, we see that G must have at least $26(5 - 1) + 40(13 - 1) = 584 > 520$ elements, which is a contradiction.

■

A similar argument shows that there are no simple groups of order pqr for distinct primes p, q, r.

3 Embedding Simple Groups in the Alternating Group

Lemma 2 *If G is a finite simple group with a subgroup H of index $n \geq 3$, then $|G|$ divides $\frac{n!}{2}$.*

Proof. Recall that the action of G on the cosets G/H by left multiplication induces a group homomorphism $\varphi : G \to \mathrm{Sym}(G/H) \cong S_n$ with $\ker(\varphi) = \bigcap_{g \in G} gHg^{-1} =: \mathrm{core}(H)$. Since the kernel of any homomorphism is normal and G is simple, we must have either $\ker(\varphi) = \{e\}$ or $\ker(\varphi) = G$. However, $\ker(\varphi) \leq H < G$, so we must have $\ker(\varphi) = \{e\}$. It follows that φ is injective, hence by the first isomorphism theorem $|G|$ divides $n!$ (using Lagrange's theorem).

But this was not the claim of the lemma. How do we see the stronger claim that $|G|$ divides $\frac{n!}{2}$? We will embed G in A_n. Observe that we have the following morphism:

$$G \xrightarrow{\varphi} \mathrm{Sym}(G/H) \xrightarrow{\sim} S_n \xrightarrow{\sigma} \{-1, 1\}$$

which is surjective if $\mathrm{im}(\varphi)$ is not contained in A_n. By the first isomorphism theorem, $\ker(\varphi)$ has size $\frac{|G|}{2}$, which contradicts the simplicity of G. Therefore, the image of our morphism lands in A_n and the result follows because $|A_n| = \frac{n!}{2}$.

■

This is a powerful result that allows us to easily prove that many groups of small order are not simple. Conceptually (at least when dealing with very small numbers), it tells us that simple groups do have have any unreasonably large Sylow subgroups because the index of such a subgroup would be very small and would violate the condition that $|G|$ must divide the factorial of the index over 2. However, it breaks down when dealing with larger numbers because the factorial grows so fast.

Example: There are no simple groups of order 36.

A proof of this result is possible by counting as in the previous section, but it requires some thinking and care. However, it is trivial to prove with our lemma. Suppose that G is simple of order 36. Any $P \in \mathrm{Syl}_3(G)$ has order 9 and index 4 in G. By the lemma, $|G| = 36$ must divide $12 = \frac{4!}{2}$, which is absurd. Thus, G cannot be simple. Note in this case the embedding into S_n sufficed and we did not even need the full strength of the lemma.

■

By nearly a nearly identical argument, one can prove that, for example, there are no simple groups of orders 88 or 96 or 1000 or $1,500$ or $25,000$. This is a surprisingly useful technique for common exam questions.

Example: There are no simple groups of order 112.

Suppose that $|G| = 112 = 7 \cdot 2^4$ is simple. Then, any $P \in \mathrm{Syl}_2(G)$ has index 7. Thus, $|G|$ must divide $\frac{7!}{2}$, which is a contradiction. Observe, however, that $|G|$ does divide 7!, so this is an example of a case where understanding that we can embed into A_n instead of just S_n is useful.

■

We can often find subgroups with a given index by considering normalizers. Indeed, we know that $n_p = [G : N_G(P)]$, $P \in \mathrm{Syl}_p(G)$, so we always have a subgroup of index equal to the number of Sylow subgroups of a given prime.

4 Index of Minimal Prime Divisor

Recall from your homework that if G is a finite group, p is the smallest prime dividing $|G|$, and $H \leq G$ is a subgroup of index p, then H is normal in G. We can often use this result to find nontrivial normal subgroups.

Example: There are no simple groups of order pq for p and q distinct primes.

Using the minimal index condition, this is obvious. Indeed, if $q > p$ then any subgroup of order q has index p and must be normal.

■

5 Some Results of Burnside

In this section, we will note some powerful results that go beyond the scope of this course. Group-theoretic proofs are known for all results in this section other than the Feit-Thompson theorem. That said, the representation-theoretic proofs are far easier for Burnside's $p^a q^b$ theorem.

Theorem 1 *If G is a finite group and $P \in Syl_p(G)$ satisfies $P \subseteq Z(N_G(P))$ then there exists a normal subgroup $N \triangleleft G$ of order $|N| = [G : P]$.*

This theorem is called Burnside's transfer theorem. The proof relies on a special map called the transfer homomorphism. The condition about the normalizer comes from the idea that "the normalizer controls the fusion." The condition that $P \subseteq Z(N_G(P))$ may seem unreasonable but the following proposition shows that this is not the case.

Proposition 1 *If p is the smallest prime dividing $|G|$ and $P \in Syl_p(G)$ is cyclic, then $P \subseteq Z(N_G(P))$.*

Thus, any group that has a cyclic p-Sylow subgroup for the smallest prime divisor p must have a nontrivial normal subgroup $N \triangleleft G$ with $|N| = [G : P]$. We call such an N a normal p-complement of P. In fancy language, we can say that G is an internal semidirect product of P and N.

We have the following useful corollary.

Corollary 1 *If p is the smallest prime dividing $|G|$ and the order of G factors as $|G| = pq_1^{n_1} \cdots q_r^{n_r}$, then G is not simple. In particular, groups of square-free order are not simple.*

In section, I tried to prove that groups of order 525 are not simple (when I meant to do the proof for order 520). Well, the fact that there are no simple groups of order 525 is immediate from the above result.

By induction and Burnside's transfer theorem, the following powerful statement also results.

Corollary 2 *Groups of square-free order are solvable.*

A related result, also due to Burnside is the p^aq^b theorem. The standard proof is a wonderful application of the representation theory of finite groups and rudimentary algebraic number theory.

Theorem 2 *Any group of order p^aq^b is solvable for primes p and q.*

In particular, we have the following corollary.

Corollary 3 *There are no simple groups of order p^aq^b for distinct primes p and q.*

Recall that A_5 is the smallest non-abelian cyclic group. We can understand why there are no smaller non-abelian simple group just by looking at how all numbers up to 60 factor. Indeed, by consulting this table, we see that all of the numbers less than 60 are of the form p^a or p^aq^b or are square-free. However, $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$, so the alternating group manages to avoid all of our attempts to show it is not simple!

I will also mention an extremely deep and difficult result due to Feit and Thompson for the sake of completeness.

Theorem 3 *Every group of odd order is solvable. Equivalently, there are no non-abelian finite simple groups of odd order.*