Fix a prime p (which divides $|G|$) and write $|G| = p^e m$, $p \nmid m$.

Def. A subgroup $H \subset G$ of order $|H| = p^e$ is called a <u>Sylow p-subgroup</u> of G.

Theorems (Sylow, 1872)

1) For every prime p, a Sylow p-subgroup of G exists.
2) All Sylow p-subgroups are conjugates of each other:
   $H, H' \subset G$ p-Sylow $\Rightarrow \exists\, g \in G$ st. $H' = gHg^{-1}$
   Moreover, any subgroup $K \subset G$ with $|K|$ a power of p is contained in a Sylow p-subgroup.
3) Let s_p be the number of Sylow p-subgroups of G.
   Then $s_p \equiv 1 \mod p$, and $s_p \mid |G|$. (or equivalently, $s \mid m = \frac{|G|}{p^e}$)

- We saw last time: if $s_p = 1$ then the unique p-Sylow is a normal subgroup.

  Ex: $|G| = 15 \Rightarrow G$ contains exactly one subgroup of order 3 and one of order 5, both are normal, and $G \simeq H \times K \simeq \mathbb{Z}/15$.

  $|G| = 21 \Rightarrow \exists!$ subgroup of order 7 (normal) and either $G \simeq \mathbb{Z}/21$ or a semidirect product of $\mathbb{Z}/7$ and $\mathbb{Z}/3$.

- For a p-group ($|G| = p^n$), Sylow tells us exactly nothing!
  Namely, a Sylow p-subgroup has p^n elements, and the only such is G itself.
  Thus, in the Sylow approach to classification, p-groups are the hardest to classify.
  In fact, the number of different p-groups grows dramatically with the exponent n!

  Eg. for $p = 2$:
  $\exists$ 1 group of order $2^1 = 2$ (cyclic)
  2 —"— $2^2 = 4$ ($\mathbb{Z}/4$, $\mathbb{Z}/2 \times \mathbb{Z}/2$)
  5 $2^3 = 8$
  14 $2^4 = 16$
  51 $2^5 = 32$ ... (and already 56092 for $2^8 = 256$)

- A corollary of Sylow's first theorem (existence of Sylow p-subgroups)

  Corollary: if $p \mid |G|$ and p is prime then G contains an element of order p.

  Pf: Let $H \subset G$ be a Sylow p-subgroup, and let $g \in H$ st. $g \neq e$. Since the order of g divides $|H| = p^e$, it is p^k for some $1 \leq k \leq e$. Now $g^{p^{k-1}}$ has order p. $\square$

- The first two theorems are proved by studying the action of G on its subsets by left multiplication.

* The proof of Sylow's first theorem uses two lemmas:

Lemma 1: Given $n = p^e m$ with $p \nmid m$, $p \nmid \binom{n}{p^e}$

Proof: $\binom{n}{p^e} = \dfrac{n(n-1)\dots(n-p^e+1)}{p^e(p^e-1)\dots\dots 1} = \prod_{k=0}^{p^e-1} \dfrac{p^e m - k}{p^e - k}$

The highest power of p dividing $p^e m - k$ or $p^e - k$ is exactly the highest power of p dividing k (look mod p^e!), hence the numerator and denominator have same powers of p in their prime factorization, and the end result has no powers of p. □

Lemma 2: Let $U \subset G$ be any subset, and consider the action of G on $\mathcal{P}(G) =$ {all subsets of G} by left multiplication. Then the stabilizer of $[U] \in \mathcal{P}(G)$, $\mathrm{Stab}([U]) = \{g \in G \,/\, gU = U\}$, has $|\mathrm{Stab}(U)|$ divides $|U|$.

Proof: Let $H = \mathrm{Stab}(U)$, then H acts on U by left multiplication ($hU = U\ \forall h \in H$) and so U is a union of orbits $\mathcal{O}_u = \{hu \,/\, h \in H\} = Hu$ for various $u \in U$. But each orbit is a (right) coset of H, and has $|\mathcal{O}_u| = |H|$. Since U is a union of such orbits, $|H|$ divides $|U|$. □

Now we can give the <u>proof of Sylow's 1st thm</u> (existence of Sylow subgroups).

Proof: Let $S = \{U \in \mathcal{P}(G) \,/\, |U| = p^e\}$: all subsets of G with p^e elements. Consider the action of G on S by left multiplication, $U \mapsto gU$, and partition S into orbits for this action. By Lemma 1, $p \nmid |S|$, so there exists an orbit $\mathcal{O}_U \subset S$ st. $p \nmid |\mathcal{O}_U|$.
Since p^e divides $|G| = |\mathcal{O}_U|\,|\mathrm{Stab}(U)|$, we find that $p^e \mid |\mathrm{Stab}(U)|$.
But by lemma 2, $|\mathrm{Stab}(U)|$ divides $|U| = p^e$. So $|\mathrm{Stab}\, U| = p^e$. We're done: $\mathrm{Stab}(U)$ is a Sylow p-subgroup! (and in fact U was a right coset of $\mathrm{Stab}(U)$). □

Next we prove <u>Sylow's 2nd theorem</u>, formulated as:

If $H \subset G$ is a Sylow p-subgroup and $K \subset G$ is any p-subgroup, then there exists a conjugate $H' = gHg^{-1}$ with $K \subset H'$. (for $|K| = p^e$ this says all Sylow p-subgps are conjugate).

Proof: Let C be the set of left cosets of H; then G acts on C (by left-multiplication), transitively (ie. there is only one orbit); $p \nmid |C| = \dfrac{|G|}{p^e} = m$; and there exists $c_0 \in C$, namely $c_0 = [H]$ itself, s.t. $\mathrm{Stab}(c_0) = H$. (Any G-action on a set with these properties would work just as well). Now restrict the action of G on C to a p-subgroup K.
The K-action on C has orbits of size dividing $|K|$, hence a power of p.

Since $p \nmid |C|$, there is at least one fixed point (ie. $\exists\, c \in C$ with $k \cdot c = c\ \forall k \in K$).
Thus $K \subset \mathrm{Stab}(c) = H'$ which is conjugate to $\mathrm{Stab}(c_0) = H$ since $c, c_0 \in$ same orbit of G.
(Concretely: assume the coset gH is fixed by K, ie. $kgH = gH\ \forall k \in K$, then $\forall k \in K$, $g^{-1}kgH = g^{-1}gH = H$, so $g^{-1}kg \in H$, hence $k \in gHg^{-1}$. Thus $K \subset gHg^{-1}$.) □

Before we can prove the 3rd theorem, we need to discuss <u>normalizers & conjugate subgroups</u>:

<u>Q</u>: given a group G and a subgroup H, what is the largest subgroup $K \subset G$ such that H is normal inside K?

Observe: the issue is whether $gHg^{-1} = H$ - might not hold $\forall g \in G$, but needs to hold $\forall g \in K$.

<u>Def</u>: The <u>normalizer</u> of a subgroup $H \subset G$ is $N(H) = \{ g \in G \,/\, gHg^{-1} = H \}$.
This is a subgroup of G, and for $H \subset K \subset G$ subgroups, H is normal in K iff $K \subset N(H)$.

<u>Ex</u>: $G = S_3$, $H = \{ id, \sigma = (123), \sigma^2 \} = A_3 \subset S_3 \Rightarrow N(H) = G$ (H is normal in G!)
(even though, for g = transposition, $g\sigma g^{-1} = \sigma^2 \neq \sigma$, $gHg^{-1} = H$ ✓)
$H = \{ id, \tau \} \simeq \mathbb{Z}/2 \subset S_3$ for τ a transposition $\Rightarrow N(H) = H$
(Note: $gHg^{-1} = H \Leftrightarrow g\tau g^{-1} = \tau \Leftrightarrow g \in \{id, \tau\}$)

The normalizer measures how close H is to being normal in G: if it is then $N(H) = G$.

* G acts by conjugation on the set of all of its subgroups. The orbit of H is the set of its conjugate subgroups $gHg^{-1} \subset G$. (If H is normal then $O_H = \{H\}$)
The stabilizer of H is $\{ g \in G \,/\, gHg^{-1} = H \} = N(H)$. So by orbit-stabilizer,
$|O_H| = |G/N(H)|$ (and $\{$subgroups conjugate to $H\} \longleftrightarrow \{$cosets of $N(H)\}$)

The number of subgroups conjugate to H in G is $|G/N(H)|$.

* Now the proof of <u>Sylow's third theorem</u> (#p-Sylows $= s_p \mid m$ and $s_p \equiv 1 \bmod p$).

<u>Pf</u>: Consider the action of G on the set of Sylow p-subgroups by conjugation.
By the 2nd theorem, this action is transitive (all p-Sylows are conjugate), and if $H \subset G$ is any Sylow p-subgroup, the stabilizer is $\{ g \in G \,/\, gHg^{-1} = H \} = N(H)$ (the normalizer), and so $s_p = |\text{orbit}| = \dfrac{|G|}{|N(H)|}$.
Since $H \subset N(H) \subset G$ subgroups and $|H| = p^e$, $p^e \mid |N(H)|$ and hence
$s_p = \dfrac{|G|}{|N(H)|} \;\Big|\; \dfrac{|G|}{p^e} = m$.

Next, we restrict to H the conjugation action on the set of all p-Sylows, and observe that H itself is fixed ($hHh^{-1} = H \ \forall h \in H$) so this gives an orbit of size 1. We claim it's the only one.

Indeed, let H' be a p-Sylow of G s.t. $hH'h^{-1} = H' \ \forall h \in H$ (orbit $= \{H'\}$).

This means $H \subset N(H')$. But $|N(H')|$ is a $\begin{cases} \text{multiple of } |H'| = p^e \\ \text{divisor of } |G| = p^e m \end{cases}$

so H and H' are Sylow p-subgroups of $N(H')$! By Sylow's 2nd they're conjugate subgroups of $N(H')$. However H' is normal in $N(H')$ (by definition!)

Therefore $H = H'$. This shows the only orbit of size 1 for the action of H by conjugation on the set of Sylow p-subgroups of G is $\{H\}$ itself.

Since the size of an orbit of an H-action divides $|H| = p^e$, all other orbits have size divisible by p. We conclude that $s_p = \#\{p\text{-Sylows}\} \equiv 1 \bmod p$. $\square$

One more example, to show that things can get more complicated quickly.

Let's try to classify groups of order 12. If $|G| = 12$ then Sylow gives

- a subgroup $H \subset G$, $|H| = 4$; the number of these is $s_2 \in \{1, 3\}$ ($s_2 | 3$, $s_2 \equiv 1 \bmod 2$)
- a subgroup $K \subset G$, $|K| = 3$; the number is $s_3 \in \{1, 4\}$ ($s_3 | 4$, $s_3 \equiv 1 \bmod 3$)

* At least one of these is normal: indeed, if $s_3 = 4$ then the nontrivial elements of $K_1, \dots, K_4$ all have order 3, and $K_i \cap K_j = \{e\}$ (order divides 3, < 3), so we have 8 elements of order 3. So there are at most 4 elements of order $\in \{1, 2, 4\}$, hence $s_2 = 1$ and H is normal.

* If both H and K are normal then $G \simeq H \times K$ (using $|G| = |H| \cdot |K|$, $H \cap K = \{e\}$ see last time) and so G is abelian, one of $\mathbb{Z}/4 \times \mathbb{Z}/3 \simeq \mathbb{Z}/12$

$$(\mathbb{Z}/2 \times \mathbb{Z}/2) \times \mathbb{Z}/3 \simeq \mathbb{Z}/2 \times \mathbb{Z}/6.$$

* If H is normal but K isn't, consider the action of G on $\{K_1, K_2, K_3, K_4\}$ by conjugation. Conjugation by a nontrivial element of K_1 maps K_1 to itself, but doesn't fix any of the 3 others: indeed recall the stabilizer of K_i is $\{g \in G \,/\, gK_ig^{-1} = K_i\} = N(K_i)$, and by orbit-stabilizer, $|N(K_i)| = \frac{|G|}{s_3} = \frac{12}{4} = 3$, so $N(K_i) = K_i$. So: a nontrivial element of K_1 acts on $\{K_1, K_2, K_3, K_4\}$ by a 3-cycle permuting $\{K_2, K_3, K_4\}$, and similarly for others.

Hence the action of G on $\{K_1 .. K_4\}$ gives a homom. $\varphi : G \longrightarrow S_4$, $y_i \longmapsto$ 3-cycles

This implies $\mathrm{Im}(\varphi) \supset A_4$, hence $= A_4$, and $G \simeq A_4$.

* If K is normal but H isn't, then there are 2 subcases – $H \simeq \mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$!

→ if $H \simeq \mathbb{Z}/4$, let $x \in H$ generator, let $K = \{e, y, y^2\}$, then $G \simeq K \rtimes H$ is determined by the conjugation action of H on K, ie. need to know $xyx^{-1} \in K$.
Can't have $xyx^{-1} = e$ ($\Rightarrow y = e$) or $xyx^{-1} = y$ ($\Rightarrow x$ and y commute, $G \simeq H \times K$ abelian).
So instead $xyx^{-1} = y^2 (= y^{-1})$.
Then G is generated by x, y, with $x^4 = y^3 = e$ and $xy = y^2 x$.
This group is unfamiliar to us – semidirect product $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$, where $\mathbb{Z}/4$ acts on the normal subgroup $\mathbb{Z}/3$ by

$$\begin{aligned} \mathbb{Z}/4 &\longrightarrow \mathrm{Aut}(\mathbb{Z}/3) = \{\pm id\} \\ k &\longmapsto (-1)^k \end{aligned}$$

→ if $H \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$, then look at conjugation action $H \xrightarrow{\varphi} \mathrm{Aut}(K) \simeq \mathbb{Z}/2$, necess. $\ker(\varphi) \simeq \mathbb{Z}/2$, denote by z its generator, $x \in H$ st. x, z generate H, y generator of K, then G is gen. by x, y, z with

$$\begin{cases} x^2 = z^2 = y^3 = e \\ xz = zx \quad (\mathbb{Z}/2 \times \mathbb{Z}/2) \\ zy = yz \quad (z \in \ker\varphi) \\ xy = y^2 x \quad (xyx^{-1} = y^2) \end{cases}$$

Can check this is actually $G \simeq D_6$
(the subgroup gen^d by y and z is $\simeq \mathbb{Z}/6$ and normal in G, take y = rotation by $2\pi/3$
z = rotation by π
x = any reflection).

Thus there are 5 isom. classes of groups of order 12:
$(\mathbb{Z}/12, \mathbb{Z}/2 \times \mathbb{Z}/6, A_4, \mathbb{Z}/3 \rtimes \mathbb{Z}/4, D_6)$.