Last time:

Lemma $|cl(a)| = [G : C_G(a)]$ for all $a \in$ group G.

Proof: Let G act on G by conjugation, i.e.

$$g \bullet h = ghg^{-1}$$

Then the orbit of h is $G \bullet h = \{ghg^{-1} : g \in G\}$
$$= cl(h).$$

By the orbit stabilizer theorem

$$\left| G/G_h \right| = |cl(h)|$$

Observe that $G_h = \{g \in G : g \bullet h = h\}$
$$= \{g \in G : ghg^{-1} = h\} = C_G(h)$$

$$\Rightarrow \underbrace{\left| G/C_G(h) \right|}_{[G : C_G(h)]} = |cl(h)|.$$

$\square$

Sylow Theorem #1 (1872)

Suppose G is a finite group such that for some prime p, $p^k \mid o(G)$ and $p^{k+1} \nmid o(G)$ for some positive integer k. Then there exists a subgroup of G of order p^k.

Proof. We will use induction on the order of the group.

First, suppose $o(G)=1$. Then there is no prime that divides $o(G)$, so the theorem is satisfied.

Next, assume the theorem has been proved for $o(G) \leq n$, where $n \geq 1$.

Now, if $o(G) = n+1$, and $\exists$ a prime p and $k \geq 1$ such that $p^k \mid (n+1)$ and $p^{k+1} \nmid (n+1)$.

Suppose there is no subgroup of order p^k in G.

Let's use the class equation

$$|G| = |Z(G)| + \sum_j [G : C_G(x_j)]$$

$\{x_j\}$ ← one representative from each conjugacy class.

Note that $|G| = [G : C_G(x_i)] \cdot |C_G(x_i)|$

← proper subgroup of G.

↑ p^k does not divide $|C_G(x_i)|$.

[If $p^k \mid |C_G(x_i)|$ then since $|C_G(x_i)| \leq n$, by the induction hypothesis, $\exists H < C_G(x_i) < G$ s.t. $|H| = p^k$. This would contradict the assumption.].

So by the index equation, $p \mid [G : C_G(x_i)]$ for all i.

$$3^5 = (\quad)(\quad)$$

← must have factor of p. ← 3^4 but not 3^5

$\Rightarrow$ From the class equation

$$|Z(G)| = \underbrace{|G|}_{p^k} - \sum_j \underbrace{[G : C_G(x_j)]}_{p}$$

$\Rightarrow \quad p \mid |Z(G)| \quad \Rightarrow \quad |Z(G)| > 1.$

$Z(G)$ is an abelian subgroup, by the FTFGAG, $Z(G)$ must have an element y of order p. $\Rightarrow H := \langle y \rangle$ is a normal abelian subgroup of G of order p.

Consider G/H. This is a group of order $\leq n$, and

$p^{k-1} \mid |G/H|$ but $p^k \nmid |G/H|$.

By the induction hypothesis, there exists a subgroup K of order p^{k-1} $\quad K < G/H$

By the homework exercise, there exists $B < G$ s.t. $K = B/H$. $\Rightarrow \underbrace{|K|}_{p^{k-1}} = \dfrac{|B|}{|H|} = \dfrac{|B|}{p}$

$\Rightarrow |B| = p^k$.

This is a contradiction. So the assumption was wrong, so $\exists$ subgroup of G of order p^k.

By induction, this is true for any $o(G)$. $\boxtimes$

Fun Friday Quiz

1. What is your name?

2. Define the center of a group G.

3. Let $S = \{a, b, c\}$ be a subset of the group G. Define $N_G(S)$.