Lagrange's theorem:

If G is a finite group and $H \leq G$, then $|H| \mid |G|$.

Proof:

Step 1: Define a relation $\sim$ on G by the rule that,

$\forall g, g' \in G$, $g \sim g'$ if and only if $\exists h \in H$ s.t. $g = g'h$.

This relation is:

- reflexive: ✓

  $e \in H$ and $\forall g \in G$, $g = ge \Rightarrow g \sim g$

- symmetric: ✓

  Suppose $g \sim g'$. Then $\exists h \in H$ s.t. $g = g'h$.

  But $h^{-1} \in H$ and $g' = gh^{-1} \Rightarrow g' \sim g$.

- transitive: ✓

  Suppose $g_1 \sim g_2$ and $g_2 \sim g_3$. Then $\exists\, h_1, h_2 \in H$

  s.t. $g_1 = g_2 h_1$ and $g_2 = g_3 h_2$.

  Then $g_1 = (g_3 h_2) h_1 = g_3 (h_2 h_1)$, and $h_2 h_1 \in H$

  $\Rightarrow g_1 \sim g_3$.

Therefore, the relation $\sim$ is an equivalence relation on G.

Step 2: Let $A_1, \ldots, A_k$ be the equivalence classes of $\sim$.

Note that there are only finitely many, and that

$|A_i| < \infty$, $\forall\, 1 \le i \le k$, because $|G| < \infty$.

Since $\{A_i\}_{i=1}^{k}$ is a partition of G, we have that

$$|G| = \sum_{i=1}^{k} |A_i|.$$

Now suppose $1 \le i \le k$, choose $g \in A_i$, and define

a map $\tau : H \to A_i$ by $\tau(h) = gh$, $\forall h \in H$.

The map τ is:

- surjective: ✓

  $\forall g' \in A_i$, $g' \sim g \Rightarrow \exists\, h \in H$ s.t. $g' = gh = \tau(h)$.

- injective: ✓

  (cancellation law)

  If $\tau(h) = \tau(h')$ then $gh = gh' \Rightarrow h = h'$.

Therefore τ is a bijection, so $|H| = |A_i|$. $(\forall\, 1 \le i \le k)$

Finally,

$$|G| = \sum_{i=1}^{k} |A_i| = k\,|H| \Rightarrow |H| \,\big|\, |G|. \quad \blacksquare$$

Consequences of Lagrange's theorem

Thm: If G is a finite group and $g \in G$ then $|g| \mid |G|$.

(smallest $k \in \mathbb{N}$ with $g^k = e$)

Pf: $|g| = |\langle g \rangle| \mid |G|$. ∎

previous video

Cor: If G is a finite group and $g \in G$ then $g^{|G|} = e$.

Pf: $|g| \mid |G| \Rightarrow \exists\, k \in \mathbb{N}$ s.t. $|G| = k \cdot |g|$.

Then $g^{|G|} = (\underbrace{g^{|g|}}_{=e})^k = e$. ∎

Euler's theorem: If $n \in \mathbb{N}$, $a \in \mathbb{Z}$, and $(a,n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Pf: Let $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Then $|G| = \varphi(n)$, and

$(a,n) = 1 \Rightarrow a \in G$. By the above Cor., $a^{\varphi(n)} = 1 \bmod n$. ∎

Ex: Show that 5 is a primitive root mod 103.

$G = (\mathbb{Z}/103\mathbb{Z})^\times$, $|G| = \varphi(103) = 102 = 2 \cdot 3 \cdot 17$

divisors of 102: $(2^a 3^b 17^c,\ a, b, c \in \{0,1\})$

$1, 2, 3, 6, 17, 34, 51, 102$

Compute:

$5^1 = 5 \mod 103$

$5^2 = 25 \mod 103$

$5^3 = 22 \mod 103$

$5^6 = (5^3)^2 = 22^2 = 72 \mod 103$

$5^{17} = 5^{16} \cdot 5^1 = 32 \cdot 5 = 57 \mod 103$

$5^{34} = (5^{17})^2 = 57^2 = 56 \mod 103$

$5^{51} = 5^{34} \cdot 5^{17} = 56 \cdot 57 = -1 \mod 103$

$5^{102} = (5^{51})^2 = (-1)^2 = 1 \mod 103$

Scratch work:

n	$5^n \mod 103$
1	5
2	25
4	7
8	49
16	32

By the theorem, $|5| = 102$, so 5 is a primitive root mod 103.