**THEOREM (Lagrange):**

Let \( H \subseteq G \) be a subgroup of a finite group \( G \). Write \( \text{ord}(H), \text{ord}(G) \) for the sizes of \( H \) and \( G \). Then

\[
\text{ord}(H) \mid \text{ord}(G).
\]

**Application:** Let \( m \) be a positive integer and \( G = \mathbb{Z}/m\mathbb{Z} \), the congruences which are prime to \( m \). Then \( G \) is a finite group of size \( \varphi(m) \), the Euler totient function.

Let \( a \in G \) be a congruence. Then

\[
H = \{ a, a^2, \ldots, a^d \} = 1 \text{ in a subgroup}
\]

\( d \) is the order of \( a \). The size of \( H \) is \( d \).

Legendre's theorem says \( d \mid \varphi(m) \)

So \( \varphi(m) = k \cdot d \), and

\[
\varphi(m) = k \cdot d \quad a^{k-1} = 1 \quad \text{(Euler's Theorem)}
\]

**Special Case (Fermat):** \( m = p \) is prime. \( \varphi(m) = p-1 \)

\[
(a, p) = 1 \quad a^{p-1} = 1
\]
Proof of Legendre's Theorem:

\( H = \{ h_1, \ldots, h_d \} \). For \( g \in G \) write

\[ C(g) = \{ gh_1, \ldots, gh_d \} \]

(1) \( C(g) \) has \( d \) elements.

If \( ghi = ghj \) multiply by \( g^{-1} \Rightarrow hi = hj \)

(2) \( g_1, g_2 \in G \) then either \( C(g_1) = C(g_2) \)

or \( C(g_1) \cap C(g_2) = \emptyset \)

If \( C(g_1) \cap C(g_2) \neq \emptyset \) then \( g_1hi = g_2hj \) so

\[ g_2g_1 = hj \cdot h_i^{-1} = h \in H. \ So \ g_1 = g_2h \]

Then \( C(g_1) = \{ g_2hh_1, \ldots, g_2hh_d \} \)

\[ C(g_2) = \{ g_2h_1, \ldots, g_2h_d \} \]

are the same set except for order.

(3) (1) & (2) imply that \( G \) is a disjoint union of sets of size \( d \), say \( k \) of them.

Thus \( k \cdot d = \text{order}(G) \Rightarrow d = \frac{\text{order}(H)}{\text{order}(G)} \)