Theorem 7.1 (Lagrange)

If $G$ is a finite group and $n = |G|$ and $H$ is any subgroup of $G$, then $|H|$ is a divisor of $n$ and the number of distinct cosets of $H$ in $G$ is $|G|/|H|$.

Corollary (#4) If $n = |G|$ and $a \in G$ then $a^n = e$ (the identity in $G$).

Fermat's little theorem says

If $p$ is prime and $a$ is any integer, then $a^p \equiv a \mod p$.

FLT follows from Corollary #4 — why?

Recall $U(p) = \{1, 2, 3, \ldots, p-1\}$ (operation in multiplication mod $p$)

So $|U(p)| = p-1$.

So Corollary #4 says $b^{p-1} \equiv 1 \mod p$ for any $b \in \{1, 2, 3, \ldots, p-1\}$.

Multiply both sides of $b^{p-1} \equiv 1 \mod p$ by $b$ to get $b^p \equiv b \mod p$ for $b \in \{1, 2, \ldots, p-1\}$.
Now if \( b = p \), we get \( p^p \equiv p \mod p \), which is also true. \((0^p \equiv 0 \mod p)\)

Now if \( a \) is any integer, we can write

\[
a = p \cdot q + r \quad \text{where} \quad 0 \leq r < p
\]

Now

\[
a^p = (p^q + b)^p
\]

\[
= \sum_{k=0}^{p} \binom{p}{k} (pq)^k b^{p-k}
\]

\[
= p^b + \sum_{k=1}^{p} \binom{p}{k} (pq)^k b^{p-k}
\]

\[
= b^p + p \cdot (\text{something}) \equiv b^p \mod p.
\]

\[
\equiv b \mod p
\]

\[
\equiv a \mod p.
\]

More generally, \( U(n) = \) set of numbers in \( \{1, 2, \ldots, n-1\} \) relatively prime to \( n \) with multiplication mod \( n \).

Notation: \(|U(n)|\) is denoted \( \varphi(n) \)

(\( \varphi \) is the "Euler phi function" or the "Euler totient function")

Corollary 4.4: If \( a \) is relatively prime to \( n \), then \( a^{\varphi(n)} \equiv 1 \mod n \)
Example: \( \varphi(15) = 8 \), so
\[ a^8 \equiv 1 \mod 15 \] for any \( a \) that's relatively prime to 15.

(This is the basis of RSA cryptography.)
More comments on Lagrange:

"(Order of H) divides (order of G)"

1) If G is a cyclic group of order n, then for every divisor d of n, G has one (cyclic) subgroup of order d.

Example: If $G = \langle a \rangle$ and $|a| = 12$, then
- $\langle a^3 \rangle = \{e, a^3, a^6, a^9\}$ has order 4
- $\langle a^3 \rangle = \{e, a^3, a^6, a^9\}$ has order 4
- $\langle a^4 \rangle = \{e, a^4, a^8\}$ has order 3
- $\langle a^6 \rangle = \{e, a^6\}$ has order 2

Then $\langle e \rangle$ and $\langle a \rangle$ have orders 1 and 12.

2) If G is any group of finite order n and H is a subgroup of G and d is the order of H, then d is a divisor of n.

Lagrange does not say: If d is a divisor of $n = |G|$, then G has a subgroup of order d.
Classic example: \( A_4 \) has order 12.

\[ A_4 = \{ (1), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243) \} \]

Claim: There can be no subgroup of order 6.

Suppose that \( H < A_4 \) and \( |H| = 6 \).

Then \( |A_4 : H| = 2 \).

Let \( a \) be any 3-cycle.

Consider the three "coset labels" \( H, \text{all}, a^2H \).

Since there are only two distinct cosets, we must have either (1) \( H = aH \), (2) \( H = a^2H \), or (3) \( \text{all} = a^2H \).

In case 1, \( H = aH \) implies \( a \in H \).

In case 2, \( H = a^2H \) implies \( a^2 \in H \), so \( (a^2)^2 \in H \), meaning \( a^4 \in H \). But \( a^4 = a^3 \cdot a = a \).

Again, \( a \in H \).

In case 3, \( \text{all} = a^2H \) implies \( a^2 \in aH \), so \( a^2 = ah \) for some \( h \in H \). Now \( a^3a^2 = a^3ah \) says \( a = h \). So again, \( a \in H \).

So we know every one of the 8 three-cycles in \( A_4 \) has to be in \( H \). But \( |H| = 6 \). Contradiction!

So \( A_4 \) has no subgroup of order 6.