Lagranges Theorem $[G:H] = \frac{|G|}{|H|}$

Note that the converse of Lagranges Theorem is false just because $c \mid |G|$ does NOT mean that a subgroup of order c exists.

Consider A_4, $|A_4| = 12$ by Lagranges theorem we could have subgroups of orders $1, 2, 3, 4, 6$.

Prop A_4 has no subgroups of order 6.

Proof: Suppose H is a subgroup of A_4 of order 6

$[A_4 : H] = 2$

$\Rightarrow$ H has two cosets, 1 of these must be $eH = H = He$

So $A_4 = H \amalg gH = H \amalg Hg \quad \forall g \notin H$

Take $g \notin H$ consider

$g^2 H$, either $g^2 H = H$ or $g^2 H = gH$

If $g^2 H = gH$, then by cancellation law, $gH = H \Rightarrow g \in H$

which is a contradiction

$\therefore \quad gH = H \Rightarrow g^2 \in H \quad \forall g \in A_4$

Suppose $g^3 = e \Rightarrow g^2 = g^{-1} \Rightarrow g^2 \in H$ then $g^{-1} \in H$

(These exist since all 3-cycles in A_4 have the property)

$\Rightarrow g \in H$

for all $g \in A_3$ s.t. $g^3 = e$

$\therefore$ Subgroup contains at least 8 elements (8 3-cycles + identity). This is a contradiction

$\therefore$ $\exists$ no subgroup of A_4 of order 6. ∎

Euler ϕ-function is a map $\phi : \mathbb{N} \to \mathbb{N}$ defined by

$$\phi(n) = \begin{cases} 1 & \text{if } n = 1 \\ \#\text{ of } m \text{ s.t. } 1 \leq m < n \text{ and } \gcd(m,n) = 1 \end{cases}$$

Note that, from Prop 3.4, we know that $|U(n)|$ is exactly # of m s.t. $\gcd(m,n) = 1$, $1 \leq m < n$ (↑ group of units in $\mathbb{Z}_n$)

Theorem 1 $\phi(n) = |U(n)|$ where $U(n)$ is the group of units modulo n.

Ex] $U(12) = \{1, 5, 7, 11\}$

$\phi(12) = |U(12)| = 4$

If p is prime $\phi(p) = p-1$

Theorem (Euler's Theorem): Let a and n be integers s.t. $n > 0$ and $\gcd(a,n) = 1$

Then $a^{\phi(n)} = 1 \pmod{n}$

Proof:

Since $|U(n)| = \phi(n) \Rightarrow a^{\phi(n)} = 1 \quad \forall a \in U(n)$

and since all a with $\gcd(a,n) = 1$ are in $U(n)$

$$a^{\phi(n)} = 1 \mod n$$ ∎

Theorem (Fermats Little Theorem). Let p be a prime number and suppose $p \nmid a$. Then

$$a^{p-1} = 1 \pmod{p}$$

Furthermore for any $b \in \mathbb{Z}$ $b^p = b \pmod{p}$