# MTH 417: Lecture # 16

Cliff Sun

October 1, 2025

Recall Lagrange's theorem.

**Corollary 0.1.** *If $p$ is prime, then $|G| = p$, then $G$ is cyclic of order of $p$. The only subgroups of $G$ is $\{e\}$ and $G$*

*Proof.* Let $H \leq G$, then $|H|/|G| = p$. So $|H| = 1$ or $p$. $\square$

More generally, any finite $G$, $g \in G$, the order of $g$ is defined as

$$o(g) = |\langle g \rangle| \Big| |G| \tag{1}$$

**Corollary 0.2.** *Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Then*

$$a^{\varphi(n)} \equiv 1 \mod n \tag{2}$$

*Recall that*

$$\varphi(n) = \left|\mathbb{Z}_n^\times\right| \tag{3}$$

*Proof.* Note that $[a]_n \in \mathbb{Z}_n^\times$, so

$$o([a]_n) \Big| \varphi(n) \tag{4}$$

Therefore,

$$\varphi(n) = o([a]_n)k \;\; k \in \mathbb{N} \tag{5}$$

However,

$$[a_n]^{o([a])} = [1] \in \mathbb{Z}_n^\times \tag{6}$$

The rest of this proof follows trivially. $\square$

Recall, $N \leq G$ is normal if $\forall g \in G$, then $gNg^{-1} = N$. We can check

$$N \text{ is normal if } G \iff gN = Ng$$