CSCI-4116
Emerg notes :(

Anas Alhadi

B00895875

March 14, 2025

Rec

<u>Recall:</u>

Let G be an abelian group, $g \in G$ written $< g >= \{g^k | 0 \leq k \leq e\}, e = ord_G g.finite$

Lagrangs Theorem

1. Euler theorm: if gcd(a,m) = 1 then $a^{\varphi(m)} \equiv 1 (\bmod\ m)$
2. if m = p, so a prime, then $\varphi(m) = p - 1$
3. So, for any base a, then $a^{p-1} \equiv 1 (\bmod\ m)$. WHich follows immediatly, and is fermat's little theorme

Theorem 5.11

Recall the group mod 13, in which we found subgroubs g=2,3,4 to be generators for cyclic groups. In that case we found that the order of the group —¡g¿— divides the order of G. Mainly order of G=12. and order $< 2 >$ was 12, 12—12. ord $< 3 > = 4$, 4—12

Corollary of this is that $g^{|G|} = 1$, Proof: notice tehorems 5.5 and 5.11
in this case $a^{\varphi(m)=1}$ is nothing but a special case if the above. in which

a