

Name: _____

Read Sections 6.2 and 6.3 on Lagrange's Theorem, Euler's Theorem, and Fermat's Theorem.

Reading Questions

1. Make sure you know the statements of Lagrange's Theorem, Euler's Theorem, and Fermat's Theorem and understand their proofs.
2. If a group G has order 12, what are the possible orders of subgroups of G ?
3. Let $G = D_4$ be the group of symmetries of the square, H the subgroup of rotations, and K the subgroup generated by a 180° rotation.
 - (a) What are the orders of G , H , and K ?
 - (b) What are the indices of H and K in G ? Of K in H ?
 - (c) Verify that Corollary 6.13 holds in this example.
4. (a) What is the order of $U(21)$? What are the possible orders of elements of $U(21)$, according to Corollary 6.11?
 - (b) What is $\phi(21)$? Given $a \in U(21)$, what is $a^{\phi(21)}$?

5. (a) Use Euler's Theorem to compute $25^4 \bmod 12$.

(b) Use Fermat's Theorem to compute $38^{36} \bmod 37$.

6. What struck you in this reading? What is still unclear? What remaining questions do you have?