LARSON—MATH 305—CLASSROOM WORKSHEET 19
Euler’s, Fermat’s & Wilson’s Theorem

Organizational Notes

1. A Zoom recording link and class notes will be sent out after each Zoom class.

2. Remember to send your answers to the classroom worksheets. Title your email with enough to help me record your “participation”.

3. Homework 3 is due today (Sept. 30).

4. Test 1 is Friday, Oct. 9.

Review

1. What is a complete set of residues (mod n)?

2. (Claim): If \( a_1, a_2, \ldots, a_n \) is a complete set of residues (mod n) and \( a \) is a unit (that is, \( \gcd(a, n) = 1 \)) then \( aa_1, aa_2, \ldots, aa_n \) is a complete set of residues (mod n).

3. What is the order of a unit \( a \) in \( \mathbb{Z}/n\mathbb{Z} \)?

4. How do we know that the order of a unit \( a \) in \( \mathbb{Z}/n\mathbb{Z} \) is well-defined (always exists)?

5. What is Euler’s \( \phi \) function? How is \( \phi(n) \) defined for a positive integer \( n \)?
Chapter 2

1. (Euler’s Theorem) Claim: if $x$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ then:

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$  

Check the claim for some values of $x$ and $n$.

2. Show that Euler’s Theorem is true.

3. (Fermat’s Theorem) Claim: if $p$ is prime and $x$ is a non-zero integer then:

$$x^{p-1} \equiv 1 \pmod{p}.$$  

4. Show that Fermat’s Theorem is true.

5. (Wilson’s Theorem) Claim: $p$ is prime if and only if $(p - 1)! \equiv -1 \pmod{p}$.

Check the claim for some values of $p$.

6. Show that Wilson’s Theorem is true.