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”.

Review

1. (Primitive Roots). There is a primitive root in \( \mathbb{Z}/p\mathbb{Z} \), when \( p \) is prime.

2. (Corollary.) \( \psi : (\mathbb{Z}/p\mathbb{Z})^* \) is a cyclic group (with respect to multiplication).

Quadratic Reciprocity (Chapter 4)

\( d \) is a quadratic residue in \( \mathbb{Z}/p\mathbb{Z} \) if there is an \( x \in \mathbb{Z}/p\mathbb{Z} \) such that \( x^2 \equiv d \pmod{p} \).

1. Find all the quadratic residues in \( \mathbb{Z}/13\mathbb{Z} \).

The Legendre symbol \( \left( \frac{a}{p} \right) \) is defined to be 0 if \( \gcd(a,p) > 1 \), 1 if \( a \) is a quadratic residue in \( \mathbb{Z}/p\mathbb{Z} \), and \(-1\) otherwise.

2. Find \( \left( \frac{a}{13} \right) \) for each \( a \in \mathbb{Z}/13\mathbb{Z} \).
Lemma 4.14. The map $\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \{1, -1\}$ defined by $\psi(a) = \left(\frac{a}{p}\right)$ is a surjective group homomorphism.

3. What is a group homomorphism?

4. Check that this claim is true in $\mathbb{Z}/13\mathbb{Z}$.

5. Show: the map $\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \{1, -1\}$ defined by $\psi(a) = \left(\frac{a}{p}\right)$ is a surjective group homomorphism.

6. What implications does the proof of this claim have?

**Major Theory Plan:**

1. Existence of units.
2. Chinese Remainder Theorem.
3. $\phi$ is multiplicative.
5. Quadratic Residues & Legendre Symbol (Chp.4)
6. Euler’s Criterion.
7. Gauss’ Lemma
8. Quadratic Reciprocity.