Last name _____

First name _____

LARSON—MATH 353–CLASSROOM WORKSHEET 27
Quadratic Congruences.

Review

1. (**Prop. 2.5.8), Primitive Roots**). There is a primitive root modulo any prime.

1. What is the significance of the existence of a primitive root in $\mathbb{Z}/p\mathbb{Z}$, for a prime p? What can be said about the powers of a primitive root?

2. Why, in $\mathbb{Z}/p\mathbb{Z}$ with primitive root q, does $1 \leq i \leq j \leq p-1$ imply $q^i \neq q^j$?

Chp. 4 of Stein's text.

3. What is a *quadratic residue* in the ring of integers modulo n?

4. What are examples?

5. Why, in $\mathbb{Z}/p\mathbb{Z}$ with primitive root q, are the even powers of q all quadratic residues?

6. Why, in $\mathbb{Z}/p\mathbb{Z}$ with primitive root q, can't the odd powers of q be quadratic residues?

(**Theorem. Euler's Criterion**). The number a is a quadratic residue modulo a prime p if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

7. What are examples?

8. Why is Euler's Criterion true?

9. What is the *Legendre symbol*?