Last name _____

First name _____

LARSON—MATH 305—CLASSROOM WORKSHEET 15
Fields, Congruences, & Cancellation

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. Suppose $a \equiv b \pmod{n}$. Let $a = nq + r$ ($0 \leq r \leq |b|$, from the Division Algorithm). Explain why $a \equiv r \pmod{n}$.

2. What is an example of a field?

3. What is a *unit* in $\mathbb{Z}/n\mathbb{Z}$?

Chapter 2—Fields

1. **Claim**: if p is prime then $\mathbb{Z}/p\mathbb{Z}$ is a field.

2. **Claim**: if n is composite then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Working with Congruences

3. (Adding) If $a \equiv b \pmod{n}$ and $a' \equiv b' \pmod{n}$ then $a + a' \equiv b + b' \pmod{n}$.

4. (Multiplication) If $a \equiv b \pmod{n}$ then $a * c \equiv b * c \pmod{n}$ for any $c \in \mathbb{Z}$.

5. (**Cancellation**) If $a * c \equiv b * c \pmod{n}$ AND $\gcd(c, n) = 1$ then $a \equiv b \pmod{n}$.

6. What are the units in $\mathbb{Z}/n\mathbb{Z}$?

7. When does the (linear) congruence $a * x \equiv b \pmod{n}$ have a solution?