Last name _____

First name _____

LARSON—MATH 305—CLASSROOM WORKSHEET 23
Euler's ϕ, Finding Inverses & Quadratic Congruences

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. (**Chinese Remainder Theorem (Section 2.2)**). If $\gcd(m, n) = 1$ then there is an integer x such that:
$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

2. (**Euler's ϕ is Multiplicative (Section 2.2)**). Claim: If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m) \cdot \phi(n)$. Check the claim with some examples.

Section 2.2

1. (**Euler's ϕ is Multiplicative**). Show: If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m) \cdot \phi(n)$.

Finding Inverses (Section 2.3)

2. To solve the congruence $14x \equiv 1 \pmod 5$ we need to find the multiplicative inverse of $14 \pmod 5$. How can we find that?

3. Solve the congruence $14x \equiv 1 \pmod 5$.

Solving Quadratic Congruences (Note)

4. Claim: The congruence $3x^2 + 11x + 7 \equiv 0 \pmod 5$ can be rewritten in the form $y^2 \equiv d \pmod 5$ $(d \in \mathbb{Z})$.

5. Claim: Any congruence $ax^2 + bx + c \equiv 0 \pmod p$ (p is prime) can be rewritten in the form $y^2 \equiv d \pmod p$.

Up next: Finding powers $a^x \pmod n$ & then Primitive Roots! (Section 2.5)

Plan:

(a) Existence of units.
(b) Chinese Remainder Theorem.
(c) ϕ is multiplicative.
(d) Existence of primitive roots.
(e) Quadratic Residues & Legendre Symbol (Chp.4)
(f) Euler's Criterion.
(g) Gauss Lemma
(h) Quadratic Reciprocity.