Last name _____

First name _____

LARSON—MATH 305—CLASSROOM WORKSHEET 24
Computing Powers & 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. (**Euler's ϕ is Multiplicative**). Show: If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m) \cdot \phi(n)$.

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?

Solving Quadratic Congruences (Note)

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

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

Calculating Powers of a Unit

3. Write 147 in binary.

4. Find $3^{147} \pmod 5$ by writing 147 in binary, and finding successive powers of 3 $\pmod 5$.

Primitive Roots! (Section 2.5)

5. Is there a number $a \pmod 5$ so that the *order* of a is $\phi(5)$?

6. Is there a number $a \pmod 6$ so that the *order* of a is $\phi(6)$?

Major Theory 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.