Last name _____

First name _____

LARSON—MATH 305—CLASSROOM WORKSHEET 29
Existence of Primitive Roots

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".

3. Homework #5 is due today, Mon., Oct. 25.

Review

1. A *primitive root* in $\mathbb{Z}/n\mathbb{Z}$ is an element a such that the *order* of a is $\phi(n)$.

2. (**Big Question**). Does every integer ring $\mathbb{Z}/n\mathbb{Z}$ have a primitive root???

3. (**Root Bound**) Let k be a field. Show that a polynomial $f \in k[x]$ of degree d has at most d roots in k.

4. Show that if p is prime and $d|(p-1)$ then $x^d - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ has exactly d roots in $\mathbb{Z}/p\mathbb{Z}$.

Primitive Roots! (Section 2.5)

1. If a has order r, and b has order s in $\mathbb{Z}/n\mathbb{Z}$ then ab has order rs.

2. (Corollary). If $p-1 = q_1^{n_1} q_2^{n_2} \dots q^{n_r}$ then $x^{q_i^{n_i}} - 1$ has $q_i^{n_i}$ roots in $\mathbb{Z}/p\mathbb{Z}$ and $x^{q_i^{n_i - 1}} - 1$ has $q_i^{n_i - 1}$ roots.

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

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

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.