Last name _____

First name _____

LARSON—MATH 353–CLASSROOM WORKSHEET 25
Primitive Roots Exist.

Review

1. What is a *multiplicative function*? **Question**: Is Euler's ϕ function multiplicative?
2. Argue: if an integer p is prime then $\phi(p^n) = p^n(1 - \frac{1}{p})$
3. Argue: if an integer $n = p_1^{n_1} \dots p_k^{n_k}$ (for primes $p_1 < \dots p_n$) then

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}).$$

4. What is a *primitive root* in $\mathbb{Z}/n\mathbb{Z}$ (for integer $n > 1$)?
5. (**Prop. 2.5.3), Root Bound**). If $f \in k[x]$ is a non-zero polynomial over a field k with degree $deg(f)$ then f has at most $deg(f)$ roots (elements α of the field k where $f(\alpha) = 0$).

Chp. 2 of Stein's text.

(**Prop. 2.5.5)**) If p is prime and $d|(p-1)$ then $f = x^d - 1$ has exactly d roots.

1. Why is this true?

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

2. Why is this true?

Chp. 4 of Stein's text.

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

4. What are examples?

5. What is the *Legendre symbol*?

6. What are examples?