Last name ______________________

First name ______________________

LARSON—MATH 353–CLASSROOM WORKSHEET 21
Multiplicative Functions & Primitive Roots.

Review

1. (**Theorem 2.2.2, Chinese Remainder Theorem**). Let $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{N}$ such that $\gcd(n, m) = 1$. Then there exists $x \in \mathbb{Z}$ such that

$$x \equiv a \mod m,$$

$$x \equiv b \mod n.$$

Moreover x is unique modulo mn.

Multiplicative functions

1. What is a *multiplicative function*?

2. Is Euler's ϕ function multiplicative?

Primitive Roots

3. We proved that, if an integer p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. If an integer $n > 1$ is not prime, can $\mathbb{Z}/n\mathbb{Z}$ be a field?

4. What is a *primitive root* in $\mathbb{Z}/n\mathbb{Z}$ (for integer $n > 1$)?

5. What are examples of primitive roots?

6. What are the polynomials $k[x]$ over a field k?

7. What are the polynomials $k[x]$ where k is the field $\mathbb{Z}/3\mathbb{Z}$?

8. (**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 $f(\alpha) = 0$).

9. Check that $f = x^3 - 1$ has exactly 3 roots where $f \in (\mathbb{Z})/3\mathbb{Z})[x]$.

10. Check that $f = x^7 - 1$ has exactly 7 roots where $f \in (\mathbb{Z})/7\mathbb{Z})[x]$.

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