Last name ______________________

First name ______________________

LARSON—MATH 353–CLASSROOM WORKSHEET 10
$\mathbb{Z}/n\mathbb{Z}$—Integers mod n.

Review

1. What is the Fundamental Theorem of Arithmetic?
2. How can we use Euclid's Lemma to prove the Fundamental Theorem of Arithmetic?
3. **Def.** If $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, we say that a is *congruent to b modulo n* if $n|(a-b)$, and write $a \equiv b \mod n$.
4. What is $n\mathbb{Z}$?
5. What is $\mathbb{Z}/n\mathbb{Z}$?

New

(**Proposition 2.1.10, Cancellation**). If $\gcd(c, n) = 1$ and $ac \equiv bc \mod n$, then $a \equiv b \mod n$.

1. Why is Proposition 2.1.10 true?

(**Definition 2.1.11, Complete Set of Residues**). We call a subset $R \subseteq \mathbb{Z}$ of size n whose reductions modulo n are pairwise distinct a complete set of residues modulo n. In other words, a complete set of residues is a choice of representative for each equivalence class in $\mathbb{Z}/n\mathbb{Z}$.

2. What are examples of complete sets of residues?

(**Lemma 2.1.12**). If R is a complete set of residues modulo n and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then $aR = \{ax : x \in R\}$ is also a complete set of residues modulo n.

3. Why is Lemma 2.1.12 true?

(**Proposition 2.1.13, Units**). If $\gcd(a, n) = 1$, then the equation $ax \equiv b \mod n$ has a solution, and that solution is unique modulo n.

4. Why is Prop. 2.1.13 true?

(**Proposition 2.1.15, Solvability**). The equation $ax \equiv b \mod n$ has a solution if and only if $\gcd(a, n)$ divides b.

5. Why is Prop. 2.1.15 true?

(**Definition 2.1.16, Order of an Element**). Let $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ and suppose that $\gcd(x, n) = 1$. The order of x modulo n is the smallest $m \in \mathbb{N}$ such that $x^m \equiv 1 \mod n$.

6. What are examples?