**Last name** _____

**First name** _____

## LARSON—MATH 353–CLASSROOM WORKSHEET 12
## $\mathbb{Z}/n\mathbb{Z}$—Integers mod n.

### Review

1. (**Proposition 2.1.10, Cancellation**). If $\gcd(c, n) = 1$ and $ac \equiv bc \mod n$, then $a \equiv b \mod n$.
2. (**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 $\mathbb{Z}/n\mathbb{Z}$.
3. What are examples of complete sets of residues?
4. (**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 $n$.

### New

(**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 $n$.

1. 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 $b$.

2. 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 $x^m \equiv 1 \mod n$.

3. What are examples?

(**Theorem 2.1.20, Euler's Theorem**). If $\gcd(x, n) = 1$, then $x^{\phi(n)} \equiv 1 \mod n$.

4. What are examples?

5. Why is Euler's Theorem true?