**Last name** ______________________

**First name** ______________________

**LARSON—MATH 353–CLASSROOM WORKSHEET 14**
**$\mathbb{Z}/n\mathbb{Z}$—Integers mod n.**

**Review**

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

**New**

(**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 $x^m \equiv 1 \mod n$.

1. What are examples?

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

2. What are examples?

3. Why is Euler's Theorem true?

(**Proposition 2.1.22, Wilson's Theorem**). An integer $p > 1$ is prime if and only if $(p-1)! \equiv -1 \mod p$.

4. What are examples?

5. Why is Wilson's Theorem true?