Last name ______________________

First name ______________________

LARSON—MATH 353–CLASSROOM WORKSHEET 16
$\mathbb{Z}/n\mathbb{Z}$—Integers mod n.

Review

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

New

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

1. What are examples?

2. Why is Wilson's Theorem true?

3. Why does Wilson's theorem give a "bad" algorithm for primality testing?

Algorithm 2.3.7 (Extended Euclidean Algorithm) Suppose a and b are integers and let $g = gcd(a, b)$. This algorithm finds g, x and y such that $ax + by = g$.

4. Apply the Extended Euclidean Algorithm to find $\gcd(12, 47)$ as a linear combination of 12 and 47.

Algorithm 2.3.8 (Inverse Modulo n). Suppose a and n are integers and $\gcd(a, n) = 1$. This algorithm finds an x such that $ax \equiv 1 \mod n$.

5. Apply this algorithm to find the multiplicative inverse of $12 \mod 47$.

Open Conjectures

6. **Claim:** For an integer $x \geq 2$, the number of distinct prime factors of x is no more than $\frac{1}{2}$ the number of divisors of x.

Chinese Remainder Theorem

7. Does this system have a solution?

$$x \equiv 2 \mod 3$$

$$x \equiv 3 \mod 5$$