Last name ________________________

First name ________________________

LARSON—MATH 353–CLASSROOM WORKSHEET 08
Fundamental Theorem of Arithmetic.

Review

1. Why does, for $a, b > 0$, with unique integers q, r with $a = bq + r$ $(0 \le r < b)$, $\gcd(a, b) = gcd(b, r)$?
2. How can the Division Algorithm be used to compute $\gcd(a, b)$?
3. **(Theorem 1.1.19. Euclid).** Let p be a prime and $a, b \in \mathbb{N}$. If $p|ab$ then $p|a$ or $p|b$.
4. **(Proposition 1.1.20)** Every natural number is a product of primes.

New

1. What is the Fundamental Theorem of Arithmetic?

2. How can we use Euclid's Lemma to prove the Fundamental Theorem of Arithmetic?

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 $a \equiv b \mod n$.

3. What are some examples?

4. What is $n\mathbb{Z}$?

5. What is $\mathbb{Z}/n\mathbb{Z}$?

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

6. 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 $\mathbb{Z}/n\mathbb{Z}$.

7. What are examples of complete sets of residues?