Math 476 - Abstract Algebra 1
Day 5 Group Assignment **Name:**______________________________

The Fundamental Theorem of Arithmetic & Equivalence Relations in $\mathbb{Z}_n$

Recall:

Definition 4.2: A **prime number** is an integer $p > 1$ whose only positive divisors are 1 and p. A positive integer greater than one that is not prime is said to be **composite**.

The Fundamental Theorem of Arithmetic: Every integer greater than 1 is either a prime or can be expressed as a product of primes. Furthermore, this factorization is unique up to the order of the factors.

1. The following exercises are designed to help you understand the Fundamental Theorem of Arithmetic.

   (a) What does it mean for a positive integer n to **not** be prime? Negate Definition 4.2 to give a precise answer.

   (b) Is 6360 prime? Justify your answer.

   (c) Find positive integers x and y such that $6360 = xy$. Can this be done in more than one way? Try to find several.

   (d) Find a complete prime factorization for 6360.

2. To prove the Fundamental Theorem of Arithmetic, we would need to give an "existence/uniqueness" proof. The "existence" part requires demonstrating that each integer greater than one is prime or can be expressed as a product of primes. Here is an outline of the "existence" portion of the proof.

   (a) Let $P(n)$ be the statement: n is either prime or a product of primes. Briefly explain why $P(2)$, $P(3)$, and $P(4)$ are true.

   (b) Proceeding using proof by induction, we take $P(2)$ as our base case and suppose that $P(2), P(3), \cdots, P(n)$ are all true. Explain why $P(n + 1)$ must also be true (Hint: there are two cases).

   Note: Proving uniqueness is a bit more complicated. We will not do that part in detail – you can read more about this in your book on pages 37-38. The prof makes use of the strong form of Euclid's Lemma:

   Euclid's Lemma (Strong Form) Let $a_1, a_2, \cdots, a_n$ be integers and let p be prime. If $p|a_1a_2\cdots a_n$, then $p|a_i$ for some i with $1 \leq i \leq n$.

   Definition 4.8: Let $\mathbb{E}$ the set of even integers. A **prime number in** $\mathbb{E}$ is a positive even integer p that cannot be written as a product of two other even integers. That is, $p \in \mathbb{E}$ is prime provided there do not exist even integers x and y such that $p = xy$.

3. In this exercise, we will explore prime factorizations in $\mathbb{E}$.

   (a) List the first 8 primes in $\mathbb{E}$.

   (b) Find a way to write 60 as a product of primes in $\mathbb{E}$.

   (c) Find a second (distinct) way to write 60 as a product of primes in $\mathbb{E}$ or explain why it is impossible to do so.

   (d) Does the Fundamental Theorem of Arithmetic hold in $\mathbb{E}$?

4. In this activity, we will review equivalence relations and equivalence classes using the example of $mod5$ equivalence. For every integer a, let $[a]_5$ denote the set of all integers that are congruent to a modulo 5.

   (a) Use set notation to express $[0]_5$ in roster form. Do the same for $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$, and $[5]_5$.

   (b) What is the remainder when 4567 is divided by 5? Which, if any, of the sets you found in part (a) contains 4567?

   (c) What is $[1]_5 \cap [2]_5$? What is $[0]_5 \cup [1]_5 \cup [2]_5 \cup [3]_5 \cup [4]_5$?

   (d) If $[a]_5 = [b]_5$, what can we say about a and b?

Definition 5.2: Let n be a natural number, and let a be in integer. The **congruence class of** a **modulo** n, denoted $[a]_n$, is the set of all integers congruent to a modulo n. In other words, $[a]_n = \{x \in \mathbb{Z} : x \equiv a((mod n)\}$.

- For $0 \leq a \leq n-1$, $[a]_n$ contains all integers x for which x divided by n yields a remainder of a.
- Note that it is possible for $[a]_n = [b]_n$ even when $a \neq b$. However, $[a]_n = [b]_n$ if and only if $a \equiv b \text{mod} n)$.
- For any pair a, b, we must have either $[a]_n = [b]_n$ or $[a]_n \cap [b]_n = \emptyset$.
- For any positive integer n, $\mathbb{Z}$ is the disjoint union of the set of equivalence classes modulo n.

Definition 5.3: Let S be a set, and let $\sim$ be a binary relation on S. Then $\sim$ is called an **equivalence relation** on S provided that $\sim$ satisfies the following properties:

- **Reflexivity:** For all $a \in S$, $a \sim a$.
- **Symmetry:** For all $a, b \in S$, if $a \sim b$ then $b \sim a$.
- **Transitivity:** For all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

Theorem 5.4: Let n be any natural number. Then congruence modulo n is an equivalence relation on $\mathbb{Z}$. In other words, the relation $\sim$ defined by $a \sim b$ if and only if $a \equiv b(\text{mod} n)$ is an equivalence relation.