Math 476 - Abstract Algebra 1
Day 6 Group Assignment **Name:**_____

Equivalence Relations in $\mathbb{Z}_n$

Recall:

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 $a \sim c$.

Definition 5.5: Let $\sim$ be an equivalence relation on a nonempty set S, and let $a \in S$. The **equivalence class of** a 9with respect to $\sim$), denoted $a_\sim$, is the set of all elements of S that are related to a by $\sim$. More precisely, $a_\sim = \{x \in S : x \sim a\}$.

As in the special example of congruence modulo n, the set of equivalence classes of an equivalence relation $\sim$ satisfy the following properties:

Theorem 5.6 Let $\sim$ be an equivalence relation on a nonempty set S. Then we have the following:

- For all $a, b \in S$, if $[a] \neq [b]$, then $[a \ \cap [b] = \emptyset$.
- For all $a \in S$, $a \in [a]$.
- For all $a \in S$, if $a \in [b]$ for some $b \in S$, then $[a] = [b]$.

Definition 5.10 For every integer $n \geq 2$, the **integers modulo** n, denoted $\mathbb{Z}_z$, is the set of the n distinct congruence classes of $\mathbb{Z}$ modulo n. That is, $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}$.

Note: We can make $\mathbb{Z}_n$ into a number system by defining addition and multiplication as follows:

$[a] + [b] = [a + b]$, and $[a] \cdot [b] = [a \cdot b]$.

These operations are a bit weird, since we are actually "adding" and "multiplying". Later in the course, we will say more about how we know that these operations are well defined. For now, we will just compute naively and hope that everything works out OK. We do want to get into the habit of simplifying the results of our "internal" computations modulo n so that we have an appropriate result form our list of "representatives".

For example, if we take $n = 5$, the complete set of congruence classes is: $\{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$ (Why don't we need any more?)

Doing some computing, we have $[2]_5 + [4]_5 = [2 + 4]_5 = [6]_5 = [1]_5$, and $[2]_5 \cdot [4]_5 = [2 \cdot 4]_5 = [8]_5 = [3]_5$.

1. The addition and multiplication tables for $\mathbb{Z}_3$ can be found in your book on page 51.
   (a) In the space provided, make addition and multiplication tables for $\mathbb{Z}_4$.

(b) In the space provided, make addition and multiplication tables for $\mathbb{Z}_5$.

(c) Do you notice any patterns or symmetries in the tables for $\mathbb{Z}_3$, $\mathbb{Z}_4$, and $\mathbb{Z}_5$?

(d) Do you notice any significant differences?

(e) Which of the axioms from I-1 seem to hold for $\mathbb{Z}_n$?

Definition 5.19 A nonzero element $[a] \in \mathbb{Z}_n$ is a **zero divisor** in $\mathbb{Z}_n$ if there is a nonzero element $[b] \in \mathbb{Z}_n$ so that $[a][b] = 0$.

Definition 5.21 A element $[x] \in \mathbb{Z}_n$ is a **unit** in $\mathbb{Z}_n$ if there is a nonzero element $[y] \in \mathbb{Z}_n$ so that $[x][y] = 1$. In this case, the element $[y]$ is called a **multiplicative inverse** of $[x]$.

2. Find all zero divisors in $\mathbb{Z}_4$.

3. Find all units in $\mathbb{Z}_4$.