Math 311 - Introduction to Proof and Abstract Mathematics
Group Assignment # 19 **Name:**______________________________
Due: At the end of class on Thursday, April 11th

Congruence Classes:

Recall: Definition 6.4.1: Let $a, b \in \mathbb{Z}$, and let $m \in \mathbb{Z}^+$. The integers a and b are **congruent modulo** m, written $a \equiv b \bmod m$ if $m \mid (a - b)$.

1. The following activity is designed to introduce you to the concept of **congruence classes modulo** m in a natural way using the example of $mod\, 5$ equivalence. For every integer a, let $[a]_5$ be 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 $[1]_5 \cap [2]_5$?

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

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

Definition 6.5.2: Let $a \in \mathbb{Z}$ and let $m \in \mathbb{Z}^+$. The **congruence class of** a **modulo** m, denoted $[a]_m$, is the set of all integers congruent to a modulo m. In other words, $[a]_m = \{x \in \mathbb{Z} : x \equiv a \bmod m\}$.

2. Notice that $31 \equiv 7 \bmod 12$. Which of the following statements are true? Justify your answers.

   (a) $7 \equiv 12 \bmod 31$.

   (b) $7 \equiv 31 \bmod 12$.

   (c) $12 \equiv 31 \bmod 7$.

Definition 6.5.4 The set of **integers modulo** m, denoted $\mathbb{Z}_m$, is the set $\mathbb{Z}_m = \{[0]_m, [1]_m, \cdots, [m-1]_m\}$.

Note that in the activity you completed above, you found the elements of $\mathbb{Z}_5$. While there are many similarities between $\mathbb{Z}_5$ and the set $\{0, 1, 2, 3, 4\}$, they are not equal as sets, as they contain different types of elements (integers vs. sets of integers). The previous activity also illustrates the properties summarized in the following theorem.

Theorem 6.5.5 Congruence classes modulo m form a "partition" of $\mathbb{Z}$. That is:

- For all $a \in \mathbb{Z}$, $a \in [a]_m$.
- For all $a, b \in \mathbb{Z}$, $a \equiv b \text{mod}\, m$ if and only if $[a]_m = [b]_m$.
- For any pair a, b, we must have either $[a]_m = [b]_m$ or $[a]_m \cap [b]_m = \emptyset$.
- For any positive integer m, $\mathbb{Z}$ is the disjoint union of the set of equivalence classes modulo m.

Note: A single equivalence class can be represented infinitely many ways using as expression of the form $[a]_m$. For example, $[2]_5 = [7]_5 = [112, 682]_5 = [-1, 125, 673]_5$. However, we usually consider $[a]_m$ with $a \in \{0, 1, \cdots m-1\}$ as, in some sense, a "canonical" representative for the equivalence class.

Theorem 6.5.6 Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and assume that $[a_1]_m = [a_2]_m$ and $[b_1]_m = [b_2]_m$. Then:

- $[a_1 + b_1]_m = [a_2 + b_2]_m$.
- $[a_1 - b_1]_m = [a_2 - b_2]_m$.
- $[a_1 b_1]_m = [a_2 b_2]_m$.

3. Let $m = 7$ and suppose $a_1 = 12$, $a_2 = -2$, $b_1 = 10$, $b_2 = 24$.

   (a) Verify that $[a_1]_m = [a_2]_m$ and $[b_1]_m = [b_2]_m$.

   (b) Verify that all three parts of the previous theorem hold for this particular example.

Note: The proofs of each part of Theorem 6.5.6 are presentation eligible problems.

Definition 6.5.7: Given $[a]_m, [b]_m \in \mathbb{Z}_m$, we define the following "arithmetic" operations (mod m):

- $[a]_m +_m [b]_m = [a+b]_m$
- $[a]_m -_m [b]_m = [a-b]_m$
- $[a]_m \cdot_m [b]_m = [ab]_m$

4. Create an "addition" table and a multiplication table for $\mathbb{Z}_5$ (simplify to use "canonical" representatives for each table entry).

5. Create an "addition" table and a multiplication table for $\mathbb{Z}_6$ (simplify to use "canonical" representatives for each table entry).

6. Which properties of standard arithmetic operations seem to hold for these operations (e.g. commutativity, associativity, additive and/or multiplicative identities, additive and/or multiplicative inverses)?