MATH 144, HANDOUT 6:
MODULAR ARITHMETIC

On this handout, we will consider a particular family of equivalence relations on the integers and explore the way in which arithmetic interacts with them.

Definition 1. For each $m \in \mathbb{N}$, define $m\mathbb{Z}$ to be the set of all integers that are divisible by m; in set-builder notation, we have $m\mathbb{Z} = \{n \in \mathbb{Z} \mid n = mk \text{ for some } k \in \mathbb{Z}\}$.

Example 2. $5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ (the integers divisible by 5), and $2\mathbb{Z}$ is the set of even integers. What is $3\mathbb{Z}$? What about $1\mathbb{Z}$?

Exercise 3. Consider the sets $3\mathbb{Z}$, $5\mathbb{Z}$, $15\mathbb{Z}$, and $10\mathbb{Z}$.

(a) List at least five elements in each of the above sets.
(b) Notice that $3\mathbb{Z} \cap 5\mathbb{Z} = m\mathbb{Z}$ for some m; what is m? Describe $15\mathbb{Z} \cap 10\mathbb{Z}$ a similar way.
(c) Draw a Venn diagram illustrating how the sets $3\mathbb{Z}$, $5\mathbb{Z}$, and $15\mathbb{Z}$ intersect.
(d) Draw a Venn diagram illustrating how the sets $5\mathbb{Z}$, $15\mathbb{Z}$, and $10\mathbb{Z}$ intersect.

Theorem 4. Let $m \in \mathbb{N}$. If $a, b \in m\mathbb{Z}$, then $-a$, $a + b$, and ab are also in $m\mathbb{Z}$.

Definition 5. For each $m \in \mathbb{N}$, define a relation on $\mathbb{Z}$ via $a \equiv_m b$ iff $(a - b) \in m\mathbb{Z}$. We read $a \equiv_m b$ as "a is congruent to b modulo m."

Prove the following theorem:

Theorem 6. For $m \in \mathbb{N}$, the relation $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

Definition 7. For $m \in \mathbb{N}$, let $[a]_m$ denote the equivalence class of a with respect to $\equiv_m$. The class $[a]_m$ is called the **class of** a **modulo** m. The set of all equivalence classes determined by $\equiv_m$ is denoted $\mathbb{Z}/m\mathbb{Z}$.

Exercise 8. Describe $[0]_3$, $[1]_3$, $[2]_3$, $[4]_3$, and $[-2]_3$ with lists as in Example **??**. Which of these are equal? How many (different) classes are in $\mathbb{Z}/3\mathbb{Z}$?

Theorem 9. For $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $[a]_m = [b]_m$ iff $(a - b)$ is divisible by m.