MATH 113: DISCRETE STRUCTURES
WEDNESDAY WEEK 12 HANDOUT

The book says that integers a and b are congruent modulo another integer m (denoted $a \equiv b \pmod{m}$) if a and b have the same remainder upon division by m. In your homework, you will prove that this is equivalent to $m \mid a - b$, and you should assume this result for the rest of today's class.

Question 1. When is $a \equiv b \pmod 2$? $a \equiv b \pmod 1$? $a \equiv b \pmod 0$?

Problem 2. Prove that $\equiv \pmod{m}$ is an equivalence relation on $\mathbb{Z}$. What are the associated equivalence classes? How many equivalence classes are there?

When considering the equivalence relation $\equiv \pmod{m}$ on $\mathbb{Z}$, we write $\overline{a}$ for the equivalence class of a. (We elide m from the notation; it should be clear from context.) We call $\overline{a}$ the congruence class of a modulo m. We write $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(\equiv \pmod{m})$ for the set of congruence classes modulo m.

Problem 3. Define addition an multiplication of equivalence classes in $\mathbb{Z}/m\mathbb{Z}$. Show that for every $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ there exists $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ such that $\overline{a} + \overline{b} = \overline{0}$.

Let's now shift gear and discuss the *dynamics* of addition in $\mathbb{Z}/m\mathbb{Z}$. Fix $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$. Make a directed graph[1] $G(\overline{a}, m)$ with vertex set $\mathbb{Z}/m\mathbb{Z}$ such that $(\overline{b}, \overline{c})$ is an edge if and only if $\overline{c} = \overline{b} + \overline{a}$.

Problem 4. Draw $G(\overline{a}, m)$ for a germane collection of $\overline{a}$ and m.

Problem 5. Make a conjecture regarding the shape of $G(\overline{a}, m)$. Prove it.

[1]The edges in a directed graph have a source and target, indicated by an arrow. Thus the edges in a directed graph are encoded by ordered pairs of vertices, with first entry the source, and second entry the target.