MATH 113: DISCRETE STRUCTURES
MONDAY WEEK 13 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 $m \mid a - b$.

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

Congruence is an *equivalence relation* on $\mathbb{Z}$, meaning that it is reflexive ($a \equiv a$), symmetric (if $a \equiv b$ then $b \equiv a$), and transitive (if $a \equiv b$ and $b \equiv c$, then $a \equiv c$). An equivalence relation $\sim$ on a set S is a relation between elements of S which satisfies the same three properties. Whenever we have an equivalence relation, we may consider *equivalence classes*, subsets of S consisting of all elements equivalent ($\sim$) to each other. For instance, if $s \in S$, then

$$\widetilde{s} = \{r \in S \mid r \sim s\}$$

is the equivalence class of s.

Problem 2. Prove that $\widetilde{s} = \widetilde{t}$ if and only if $s = t$. Conclude that the equivalence classes of $\sim$ partition S into disjoint subsets whose union is all of S.

We write $S/\sim$ for the set of equivalence classes of $\sim$, *i.e.*, $S/\sim = \{\tilde{s} \mid s \in S\}$. Note that $S/\sim$ is a set of subsets of S.

Problem 3. Suppose that $P = \{A_1, A_2, \ldots, A_n\}$ is a set of subsets $A_i \subseteq S$ which partition S. Define $s \approx t$ if and only if $s, t \in A_i$ for some i. Prove that $\approx$ is an equivalence relation on S and that $P = S/\approx$. Does anything go wrong if P is a partition of S into infinitely many subsets?

When considering the congruence modulo m equivalence relation 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 $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\equiv$ for the set of congruence classes modulo m.

Problem 4. What is $|\overline{a}|$? $|\mathbb{Z}/m\mathbb{Z}|$?

Question 5. How did you use equivalence relations in combinatorics? What about the Knights of the Round Table problem?

Problem 6. (a) Suppose that $f : X \to Y$ is a surjective function. For $y \in Y$, let $f^{-1}y = \{x \in X \mid f(x) = y\}$; this is the set of solutions to the equation $f(x) = y$ and is called the *fiber* of f over y. Prove that $\{f^{-1}y \mid y \in Y\}$ is a partition of X and thus defines an equivalence relation $\sim_f$ on X where $x \sim_f x'$ if and only if $f(x) = f(x')$.

(b) Find a function with domain $\mathbb{Z}$ such that the construction from part (a) produces congruence modulo m.

Problem 7. For the following two functions, say as much as you can about the construction from 5(a).

(a) Let $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ denote the unit circle. Consider the function $f : \mathbb{R} \to S^1$ such that

$$f(x) = (\cos(2\pi x), \sin(2\pi x)).$$

(b) Consider the function $g : \mathbb{R}^2 \to S^1 \times S^1$ such that

$$g(x, y) = ((\cos(2\pi x), \sin(2\pi x)), (\cos(2\pi y), \sin(2\pi y))).$$