Supplemental Lecture Notes

CSE 20

August 26, 2021

This document contains (semi) formally written versions of some proofs done in lecture on August 26. It should serve as one example of how to write a proof.

Claim: For any m, congruence mod m is an equivalence relation.

Proof. Let $m \in \mathbb{Z}$ be arbitrary. We will show that congruence mod m is reflexive, symmetric, and transitive, thus making it an equivalence relation.

First, we show the relation is reflexive. We claim that for all $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$. Let a be an arbitrary integer. Then $a - a = 0$, and $m \mid 0$, as every integer divides 0. Thus, $a \equiv a \pmod{m}$.

Second, we show the relation is symmetric. We claim that for all integers a, b, $a \equiv b \pmod{m} \to b \equiv a \pmod{m}$. Let a, b be arbitrary integers. Suppose $a \equiv b \pmod{m}$. Then there exists some $k \in \mathbb{Z}$ with $a - b = km$. Negate both sides to see that $b - a = -km$. Since $-k$ is still an integer, $m \mid b - a$ and we see that $b \equiv a \pmod{m}$.

Finally, we show that the relation is transitive. We claim that for all integers a, b, c, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$. Let a, b, c be arbitrary integers, and assume $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then there exist integers k, l with $a - b = km$ and $b - c = lm$. We can add the two equations together to get $(a - b) + (b - c) = km + lm$. By further simplifying we get $a - c = m(k + l)$. Since $k + l$ is an integer, we see that $m \mid a - c$, indicating that $a \equiv c \pmod{m}$. Thus, congruence mod m is an equivalence relation.

□