CSE 311: Foundations of Computing I

Modular Arithmetic Annotated Proofs

Relevant Definitions

$a \mid b$ ("*a divides b*")
For $a, b \in \mathbb{Z}$, where $a \neq 0$: $a \mid b$ iff $\exists (k \in \mathbb{Z})\ b = ka$

$a \equiv b \pmod{m}$ ("*a is congruent to b modulo m*)
For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$: $a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Division Theorem
For $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$: There exist unique $q, r \in \mathbb{Z}$, where $0 \leq r < d$ such that $a = dq + r$

The Claim

Prove for all integers a, b and positive integers m, $a \equiv b \pmod{m} \leftrightarrow a \bmod m = b \bmod m$.

Proof	Commentary & Scratch Work
Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.	*Remove the $\forall$'s...* *We want to prove a bi-implication; so, we will have two sub-proofs. First, we'll assume the left and prove the right. Then, we'll assume the right and prove the left.*
Suppose $a \equiv b \pmod{m}$.	*Begin with assuming the left and proving the right. At this point in the proof, we will be manipulating relevant definitions until the end.*
By definition of congruence, we have $m \mid (a - b)$.	*We can't work with $\equiv$'s. So, use the definition to remove the notation.*
By definition of divides, we have $a - b = km$ for some integer k.	*Divides isn't much better; apply definitions.*
Adding b to both sides, we have $a = b + km$. Taking both sides mod m, we have $a \bmod m = (b + km) \bmod m = b \bmod m$. So, $a \bmod m = b \bmod m$.	*Now, re-arrange the equations to get it to mods. Manipulate until we have what we wanted.*
Now, suppose $a \bmod m = b \bmod m$.	*Now, we prove the other implication. It's the same "unroll the definitions" idea.*
By the division theorem, we have $a = mk_a + (a \bmod m)$ for some $k_a \in \mathbb{Z}$ and $b = mk_b + (b \bmod m)$ for some $k_b \in \mathbb{Z}$	*We need to get to equivalences, which we can do via divides, which we can get via equations. The division theorem seems like the right approach.*

Re-arranging both equations, we have: a mod $m = a - mk_a$ and b mod $m = b - mk_b$.	*We want the equations in terms of mod, because we can set them equal.*
Since these are equal, we have $a - mk_a = b - mk_b$. Re-arranging, we have $a - b = (k_a - k_b)m$. So, by definition of divides, $m \mid (a - b)$. So, by definition of mod, we have $a \equiv b \pmod{m}$.	*Re-rolling the definitions in reverse. It's worth noting that this feels a lot like the first half of the proof in reverse. The only difference is that it uses different variables.*