CSE 311: Foundations of Computing I

Modular Arithmetic Annotated Proofs

Relevant Definitions

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

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

Division Theorem	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 $a = dq + r$	

A Modular Arithmetic Property

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 $m \in \mathbb{Z}^+$.	*Prove 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: $a \bmod m = a - mk_a$ and $b \bmod m = b - mk_b$.	*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.*

Another Modular Arithmetic Property

Prove for all integers $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Proof	Commentary & Scratch Work
Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.	*Prove the $\forall$'s...*
Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.	*Prove the implication...*
Then, by definition of modular equivalences, we have $m \mid (a - b)$ and $m \mid (c - d)$.	*Apply a definition*
Furthermore, by definition of divides, we have $k, l \in \mathbb{Z}$ such that $a - b = km$ and $c - d = lm$.	*Apply a definition*
	Now, we actually have to think about what to do. In particular, we're going to "re-roll" definitions. But how? Working backwards, we want $a + c \equiv b + d \pmod{m} \leftrightarrow m \mid ((a + c) - (b + d))$ *So, we put our pieces together to get there.*
Adding the equations together and re-arranging, we have $\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= km + lm \\ &= (k + l)m\end{aligned}$	
By definition of divides, we have $m \mid (a + c) - (b + d)$.	*Apply a definition*
By definition of congruences, we have $a + c \equiv b + d \pmod{m}$.	*Apply a definition*

Another-nother Modular Arithmetic Property

Prove for all integers $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof	Commentary & Scratch Work
Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.	*Prove the $\forall$'s...*
Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.	

Then, by definition of modular equivalences, we have $m \mid (a - b)$ and $m \mid (c - d)$.	*Apply a definition*
Furthermore, by definition of divides, we have $k, l \in \mathbb{Z}$ such that $a - b = km$ and $c - d = lm$.	*Apply a definition*
Solving for a and c, and multiplying the results, we get $$\begin{aligned} ac &= (km + b)(lm + d) \\ &= (klm)m + (dk)m + (bl)m + bd \end{aligned}$$	*We want equations in terms of ac and bd; so, we solve for a and c.*
Taking both sides mod m, we get $$ac \text{ mod } m = bd \text{ mod } m$$	
By the first theorem we proved, it follows that $$ac \equiv bd \pmod{m}$$	*Always use theorems that have already been proven whenever possible!*

A Modular Arithmetic Proof

Prove for all integers $n \in \mathbb{Z}$, $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Proof	Commentary & Scratch Work
Let $n \in \mathbb{Z}$ be arbitrary. We go by cases.	*After trying small examples, it looks like mod 2 is a good way to go! We split up our efforts into the two cases mod 2.*
Case 1 (n is even):	
Suppose n is even. Then, there is some $k \in \mathbb{Z}$ such that $n = 2k$.	
Multiplying both sides by n, we have $n^2 = (2k)^2 = 4k^2$. So, by definition of divides and congruences, we have $n^2 \equiv 0 \pmod{4}$.	*We want to prove something about n^2; so, we get an equation for n^2 and start manipulating and applying theorems...*
Case 2 (n is odd):	
Suppose n is odd. Then, there is some $k \in \mathbb{Z}$ such that $n = 2k + 1$.	
Multiplying both sides by n, we have $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. Taking both sides mod 4, we get $n^2 \text{ mod } 4 = 1 \text{ mod } 4$. By the first theorem we proved, it follows that $n^2 \equiv 1 \pmod{4}$.	*We want to prove something about n^2; so, we get an equation for n^2 and start manipulating and applying theorems...*
Since the claim is true for both cases, it's true in general.	