CS 13: Mathematical Foundations of Computing

Number Theory Practice

Congruences

Let a and b be integers, and let c and m be positive integers. Prove that if $ac \equiv_{cm} bc$, then $a \equiv_m b$.

Proof	Commentary & Scratch Work
____________________	*We're proving an implication. So, we start by assuming the left side.*
____________________	*Apply a definition to remove the* $\equiv_{cm}$ *notation.*
____________________	*Apply a definition to remove the divides notation.*
____________________	*Arithmetic.*
____________________	*Conclude why we're done.*

Divisibility

Prove that if $d \mid n$ and $n \mid m$, that $d \mid m$.

Evens and Odds

(a) Let $a \in \mathbb{Z}$. Prove $a(a+1)$ is even.

We go by cases.

Suppose a is even. Then, by def. $a = 2k$ for some $k \in \mathbb{Z}$

So, $a(a+1) = 2k(2k+1) = 2(k(2k+1))$. Since we found an $\ell \in \mathbb{Z}$ (namely, $k(2k+1)$) such that $a(a+1) = 2\ell$, $a(a+1)$ is even.

[Do odd case]

(b) Let k be an odd integer. Prove that $8 \mid k^2 - 1$.

Proof	**Commentary & Scratch Work**
$k = 2\ell + 1$	*Use the definition of odd.*
$k^2 - 1 = (2\ell+1)^2 - 1$	*Substitute into the definition of odd.*
$= 4\ell^2 + 4\ell + \cancel{1 - 1}$ $= 4(\ell^2 + \ell)$ $= 4\ell(\ell+1)$	*Arithmetic*
	Apply part (a)
	Combine results.
	Apply a definition.
	Conclude why we're done

Subset Proof

Prove that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof	Commentary & Scratch Work
	Define variables and assume something to start proving an implication.
	The definition of subset is an implication. So, create a variable to work with.
	Apply the definition of subset.
	Apply the definition of subset again.
	Conclude why we're done.