CS 201: DISCRETE STRUCTURES
SECTION G
November 06, 2018
Quiz 4 Solution

Problem
Prove that addition modulo m ($+_m$ operator) is associative.

Solution
We have to prove
$(a +_m b) +_m c = a +_m (b +_m c)$

Proof:

$((a+b)+c) \bmod m$	(1)
$= ((a+b) \bmod m + c \bmod m) \bmod m$	(using $(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$
$= ((a +_m b) + c \bmod m) \bmod m$	(using definition of $+_m$, i.e., $a+_m b = (a+b) \bmod m$)
$= (a +_m b) +_m c$	

also consider:

$((a+b)+c) \bmod m$	
$= (a + (b+c)) \bmod m$	associate property of addition
$= (a \bmod m + (b+c) \bmod m) \bmod m$	(using $(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$
$= (a \bmod m + (b +_m c)) \bmod m$	(using definition of $+_m$, i.e., $a+_m b = (a+b) \bmod m$)
$= a +_m (b+_m c)$	

This shows that

$((a+b)+c) \bmod m = (a +_m b) +_m c = a +_m (b+_m c)$ hence proved