MATH 335 lecture 10

Chris Camano: ccamano@sfsu.edu

September 22, 2022

Exam discussion Midterm is two parts one in class and one out of class.
In person exam will be short questions, including definitions euler phi function for example with corresponding example. Simple computations, groups will be on test, compute arithmetic group properties over binary operators.. Small qeuestions with justification and small proofs. The test is testing your attention note taking and proficiency with the information.
The take home exam will have a similar structure to the homework should be done within 36 hours done in latex. Take home exam is open book and open notes. First part is closed book no external resources.
Hosten will poste a study guide outlining the primary ideas on the test. He posts study guides are a linear retellling of the information presented in the course each of which can function as a seed for future studying chapter 3 of the text book. All matieral up to today will be on the exam. Sounds like tuesday will be review , study guide will be up friday evening.

Take home exam will be individual.

Definition 1. Intergs mod m

$$\mathbb{Z}_n = \{[0],[1],...,[n-1]\}$$

Under a binary operation defined as follows this forms a group:

$$[a]+[b] = [a+b \mod m]$$

This realtion is well defined and independent of the choice of equivilance class.

- Associative: [a]+([b]+[c])=([a]+[b])+[c], leveraging integer addition associativity.
- identity element: [0]
- inverse element:[-1] $\forall a \in \mathbb{Z}_n$

Remark: if $0 \leq a < m-1$ then the inverse of [a] is $[n-a]$

$$|\mathbb{Z}_n|$$

Additional binary operation for $\mathbb{Z}_n$
Let the binary operation be as follows:

$$[a] \cdot [b] := [ab \mod m]$$

Proof that this binary operator is well defined.
Suppose $[a] = [a^*], [b] = [b^*]$, and show that:

$$[a][b] = [a^*][b^*]$$

$$[a] = [a^*] \to n|a - a^*$$
$$[b] = [b^*] \to n|b - b^*$$

We need to show:

$$[ab] = [a^*b^*] \sim n|ab - a^*b^*$$

$$ab - a^*b* = ab - ab^* + ab^* - a^*b^*$$
$$a(b - b^*) + b^*(a - a^*)$$
$$n|a - a^*, n|b - b^* \to n|a(b - b^*) + b^*(a - a^*) \to n|ab - a^*b^*$$

There is not an inverse so this is not a group [0] will never have an inverse. There is a way to "fix" multiplication over $\mathbb{Z}_n$ by only looking at the values who do have an inverse. :

Definition 2. Instead let

$$G = \{[a] \in \mathbb{Z}_n : [a] \text{ has a multiplicitive inverse}\}$$

This set is called the group of units modulo n, commonly denoted by U(n)

The cardinality of the group of units modulo n is equivilant to the phi function of n. This is also the reduced residue system of mod n over the integers.