Infinite Systems to Finite Systems

Modular Arithmetic

Text – Chapter 10 – Sections 2, 3

Modular Addition

- The algorithm is the same as in the set of whole numbers.
- The sum must be expressed as the remainder when the sum is divided by the mod of the system.
- 5+4=9=3 (mod 6)

+	0	1	2	3	4.	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Is Mod 6 Under Addition A Group?

- Closed? – Yes, no strangers.
- Associative?

  (2+3)+4 =5+4 =9=3(mod6)

  2+(3+4)=2+7=
  2+1(mod 6)=3(mod 6)

+	0	1	2	3	4.	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- Identity? – Yes, the 0 row and column have the elements in order.
- Inverses? 0 in each row and column once and only once. 2 and 4 are inverses. All elements have inverses.
- Commutative? Yes, symmetry about diagonal.

In-class Assignment 24 - 1

Modular Multiplication

- The algorithm for multiplication in a mod system is the same as in multiplication with whole numbers.
- The product must be expressed as the remainder when the product is divided by the mod.
- 4 x 3 = 12 = 2 (mod 5)

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

In-class Assignment 24 – 2, 3, 4

Is Mod 5 Under Multiplication a Group (Abelian)?

- Close? –Yes, no strangers.
- Associative?
  - 2x(3x4)=4(mod 5)
    (2x3)x4=4(mod 5) maybe

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- Identity? – Yes, the row and column head 1 have the elements in order.
- Inverses? Yes, the identity 1 is in each row and column once and only once. 3 and 2 are inverses of each other.
- Mod 5 under multiplication forms a group.
- Commutative? – Yes, symmetry about diagonal.

In-class Assignment 24 – 2, 3, 4

The Adjusted Set, A

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Mod 5 with multiplication and the base set is not a group because 0 does not have an inverse.

If 0 is deleted from the base set the resulting set is the adjusted set, A. A = {1, 2, 3, 4}

A = {1, 2, 3, …, m−1}

Then, the adjusted set, A, with mod 5 multiplication forms an Abelian group.

In-class Assignment 24 – 5

Recognizing Groups Without Tables

- A modular system with addition using the base set, B forms a group.
  B ={0, 1, 2, ..., $m-1$}
  - (B, +) forms a group.

- A modular system with a prime mod, the adjusted set, and multiplication forms a group.
  - (A, x, prime mod) forms a group.

In-class Assignment 24 – 6