Patrick Austin

3/11/2018

CS 491 1001 Homework 2

1. The set of residue classes modulo 5, i.e. {0,1,2,3,4}, does form a group with respect to modular addition. This can be demonstrated by proving A1-A5 for addition modulo 5.

A1 holds since, as the first table in part 2 demonstrates, the set is closed under addition modulo 5.

A2, associativity, holds since (a+b)+c = a+(b+c) for all a,b,c in the set.

A3, identity, holds since there is an element e such that a + e = e + a for all a in the set. This e is 0.

A4, inverse, holds since every element a in the set has an element a’ such that a + a’ = a’ + a = e. As shown in A3, e=0. If a=0, a’=0. If a=1, a’=4. If a=2, a’=3. If a=3, a’=2. If a=4, a’=1.

A5, commutativity, holds since clearly a+b=b+a for all a and b in the set.

Since A1-A5 hold, the set of residue classes modulo 5 form a group with respect to modular addition.

2. Here are the required tables for GF(3):

Addition modulo 3:

|  |  |  |  |
| --- | --- | --- | --- |
| + | 0 | 1 | 2 |
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Multiplication modulo 3:

|  |  |  |  |
| --- | --- | --- | --- |
| \* | 0 | 1 | 2 |
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

Additive and multiplicative inverse modulo 3:

|  |  |  |
| --- | --- | --- |
| (w) | (-w) | (w-1) |
| 0 | 0 | Does Not Exist |
| 1 | 2 | 1 |
| 2 | 1 | 2 |

3. Here are the required tables for GF(23):

Addition modulo x3+x2+1:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|  | + | 0 | 1 | x | x+1 | x2 | x2+1 | x2+x | x2+x+1 |
| 000 | 0 | 0 | 1 | x | x+1 | x2 | x2+1 | x2+x | x2+x+1 |
| 001 | 1 | 1 | 0 | x+1 | x | x2+1 | x2 | x2+x+1 | x2+x |
| 010 | x | x | x+1 | 0 | 1 | x2+x | x2+x+1 | x2 | x2+1 |
| 011 | x+1 | x+1 | x | 1 | 0 | x2+x+1 | x2+x | x2+1 | x2 |
| 100 | x2 | x2 | x2+1 | x2+x | x2+x+1 | 0 | 1 | x | x+1 |
| 101 | x2+1 | x2+1 | x2 | x2+x+1 | x2+x | 1 | 0 | x+1 | x |
| 110 | x2+x | x2+x | x2+x+1 | x2 | x2+1 | x | x+1 | 0 | 1 |
| 111 | x2+x+1 | x2+x+1 | x2+x | x2+1 | x2 | x+1 | x | 1 | 0 |

Multiplication modulo x3+x2+1:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|  | \* | 0 | 1 | x | x+1 | x2 | x2+1 | x2+x | x2+x+1 |
| 000 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 001 | 1 | 0 | 1 | x | x+1 | x2 | x2+1 | x2+x | x2+x+1 |
| 010 | x | 0 | x | x2 | x2+x | x2+1 | x2+x+1 | 1 | x+1 |
| 011 | x+1 | 0 | x+1 | x2+x | x2+1 | 1 | x | x2+x+1 | x2 |
| 100 | x2 | 0 | x2 | x2+1 | 1 | x2+x+1 | x+1 | x | x2+x |
| 101 | x2+1 | 0 | x2+1 | x2+x+1 | x | x+1 | x2+x | x2 | 1 |
| 110 | x2+x | 0 | x2+x | 1 | x2+x+1 | x | x2 | x+1 | x2+1 |
| 111 | x2+x+1 | 0 | x2+x+1 | x+1 | x2 | x2+x | 1 | x2+1 | x |

4. Here is the specified table for GF(23) with m(x) = x3+x2+1:

|  |  |  |  |
| --- | --- | --- | --- |
| Power Representation | Polynomial Representation | Binary Representation | Decimal (Hex) Representation |
| 0 | 0 | 000 | 0 |
| g0 (=g7) | 1 | 001 | 1 |
| g1 | g | 010 | 2 |
| g2 | g2 | 100 | 4 |
| g3 | g2+1 | 101 | 5 |
| g4 | g2+g+1 | 111 | 7 |
| g5 | g+1 | 011 | 3 |
| g6 | g2+g | 110 | 6 |