**Homework 05**

Question 1 (35 pts)

1. Show that x3 + x + 1 is irreducible in Z3 [x], and construct a field with 8 elements.

x3 + x + 1 === (x + 2)(x2 + x + 2) is in fact reducible!

1. Write out the addition and multiplication tables for GF(23)

Reference: http://math.stackexchange.com/questions/245621/arithmetic-operations-in-galois-field

Addition Table:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 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 Table:

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



