$GF(p^m)$

Important

If the modulus $g(x)$ is an irreducible polynomial of degree m over $GF(p)$, then the finite field $GF(p^m)$ can be constructed by the set of polynomials over $GF(p)$ whose degree is at most m-1, where addition and multiplication are done modulo $g(x)$.

For example, the finite field GF(3^2) can be constructed as the set of polynomials whose degrees are at most 1, with addition and multiplication done modulo the irreducible polynomial x^2+1 (you can also choose another modulus, as long as it is irreducible and has degree 2).

Table 4.1. Addition modulo x^2+1

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x	x+2	x+2
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

Table 4.2. Multiplication modulo x^2+1

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2x+2	x	1

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

Prev
Galois' Theorem and Polynomial Arithmetic

Up
Home

Next
$GF(2^m)$