GF(2^m)

Finite fields of order 2^m are called binary fields or characteristic-two finite fields. They are of special interest because they are particularly efficient for implementation in hardware, or on a binary computer.

The elements of GF(2^m) are binary polynomials, i.e. polynomials whose coefficients are either 0 or 1. There are 2^m such polynomials in the field and the degree of each polynomial is no more than *m*-1. Therefore the elements can be represented as *m*-bit strings. Each bit in the bit string corresponding to the coefficient in the polynomial at the same position. For example, *GF*(2^3) contains 8 element {0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1}. x+1 is actually $0x^2$+1x+1, so it can be represented as a bit string 011. Similarly, x^2+x = $1x^2$+1x+0, so it can be represented as 110.

In modulo 2 arithmetics, 1+1 ≡ 0 mod 2, 1+0 ≡ 1 mod 2 and 0+0 ≡ 0 mod 2, which coincide with bit-XOR, i.e. 1⊕1=0, 1⊕0=1 0⊕0=0. Therefore for binary polynomials, addition is simply bit-by-bit XOR. Also, in modulo 2 arithmetics, -1 ≡ 1 mod 2, so the result of subtraction of elements is the same as addition. For example:

- (x^2+x+1) +(x+1) =x^2+2x+2, since 2 ≡ 0 mod 2 the final result is x^2. It can also be computed as 111⊕011=100. 100 is the bit string representation of x^2.
- (x^2+x+1) -(x+1) =x^2

Multiplication of binary polynomials can be implemented as simple bit-shift and XOR. For example:

- (x^2+x+1)*(x^2+1) = x^4+x^3+$2x^2$+x+1. The final result is x^4+x^3+x+1 after reduction modulo 2. It can also be computed as 111*101=11100⊕111=11011, which is exactly the bit string representation of x^4+x^3+x+1.

$$\begin{array}{r} 111 \\ \times\ \ 101 \\ \hline 111 \\ 0000 \\ 11100 \\ \hline 11011 \end{array}$$

In GF(2^m), when the degree of the result is more than m-1, it needs to be reduced modulo a irreducible polynomial. This can be implemented as bit-shift and XOR. For example, x^3+x+1 is an irreducible polynomial and $x^4+x^3+x+1 \equiv x^2+x \bmod (x^3+x+1)$. The bit-string representation of x^4+x^3+x+1 is 11011 and the bit-string representation of x^3+x+1 is 1011. The degree of 11011 is 4 and the degree of the irreducible polynomial is 3, so the reduction starts by shifting the irreducible polynomial 1011 one bit left, you get 10110, then $11011 \oplus 10110 = 1101$. The degree of 1101 is 3 which is still greater than m-1=2, so you need another XOR. But you don't need to shift the irreducible polynomial this time. $1101 \oplus 1011 = 0110$, which is the bit-string representation of x^2+x.

Useful Links

- Binary Polynomial Calculator

Prev	Up	Next
GF(p^m)	Home	Chapter 5. Elementary Number Theory