

congruent to 0 mod p are closed under multiplication. It can be shown that there is a generating polynomial $g(X)$ such that every element in $GF(p^n)^*$ can be expressed as a power of $g(X)$. This also means that the smallest exponent k such that $g(X)^k \equiv 1$ is $p^n - 1$. This is the analog of a primitive root for primes. There are $\phi(p^n - 1)$ such generating polynomials, where ϕ is Euler's function. An interesting situation occurs when $p = 2$ and $2^n - 1$ is prime. In this case, every nonzero polynomial $f(X) \neq 1$ in $GF(2^n)$ is a generating polynomial. [Remark, for those who know some group theory: The set $GF(2^n)^*$ is a group of prime order in this case, so every element except the identity is a generator.]

The **discrete log problem** mod a prime, which we'll discuss in Chapter 7, has an analog for finite fields; namely, given $h(x)$, find an integer k such that $h(X) = g(X)^k$ in $GF(p^n)$. Finding such a k is believed to be very hard in most situations.

LFSR Sequences

We can now explain a phenomenon that is mentioned in Section 2.11 on LFSR sequences.

Suppose that

$$x_{n+m} \equiv c_0x_n + c_1x_{n+1} + \cdots + c_{m-1}x_{n+m-1} \pmod{2}$$

is a recurrence relation and for simplicity assume that the associated polynomial

$$P(X) = X^m + c_{m-1}X^{m-1} + c_{m-2}X^{m-2} + \cdots + c_0$$

is irreducible mod 2. Then $\mathbf{Z}_2[X] \pmod{P(X)}$ is the field $GF(2^m)$. We regard $GF(2^m)$ as a vector space over \mathbf{Z}_2 with basis $\{1, X, X^2, X^3, \dots, X^{m-1}\}$. Multiplication by X gives a linear transformation of this vector space. Since

$$\begin{aligned} X \cdot 1 &= X, & X \cdot X &= X^2, & X \cdot X^2 &= X^3, & \dots \\ X \cdot X^{m-1} &= X^m \equiv c_0 + c_1X + \cdots + c_{m-1}X^{m-1}, \end{aligned}$$

multiplication by X is represented by the matrix

$$M_X = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & c_{m-1} \end{pmatrix}.$$

Suppose we know $(x_n, x_{n+1}, x_{n+2}, \dots, x_{n+m-1})$. We compute

$$\begin{aligned} &(x_n, x_{n+1}, x_{n+2}, \dots, x_{n+m-1}) M_X \\ &= (x_{n+1}, x_{n+2}, x_{n+3}, \dots, c_0x_n + \cdots + c_{m-1}x_{n+m-1}) \\ &\equiv (x_{n+1}, x_{n+2}, x_{n+3}, \dots, x_{n+m}). \end{aligned}$$

Therefore, multiplication by M_X shifts the indices by 1. It follows easily that multiplication on the right by the matrix M_X^j sends (x_1, x_2, \dots, x_m) to $(x_{1+j}, x_{2+j}, \dots, x_{m+j})$. If $M_X^j \equiv I$, the identity matrix, this must be the original vector (x_1, x_2, \dots, x_m) . Since there are $2^m - 1$ nonzero elements in $GF(2^m)$, it follows from Lagrange's theorem in group theory that $X^{2^m-1} \equiv 1$, which implies that $M_X^{2^m-1} = I$. Therefore, we know that $x_1 \equiv x_{2^m}$, $x_2 \equiv x_{2^m+1}, \dots$

For any set of initial values (we'll assume that at least one initial value is nonzero), the sequence will repeat after k terms, where k is the smallest positive integer such that $X^k \equiv 1 \pmod{P(X)}$. It can be shown that k divides $2^m - 1$.

In fact, the period of such a sequence is exactly k . This can be proved as follows, using a few results from linear algebra: Let $v = (x_1, \dots, x_m) \neq 0$ be the row vector of initial values. The sequence repeats when $vM_X^j = v$. This means that the nonzero row vector v is in the left null space of the matrix $M_X^j - I$, so $\det(M_X^j - I) = 0$. But this means that there is a nonzero column vector $w = (a_0, \dots, a_{m-1})^T$ in the right null space of $M_X^j - I$. That is, $M_X^j w = w$. Since the matrix M_X^j represents the linear transformation given by multiplication by X^j with respect to the basis $\{1, X, \dots, X^{m-1}\}$, this can be changed back into a relation among polynomials:

$$X^j(a_0 + a_1X + \dots + a_{m-1}X^{m-1}) \equiv a_0 + a_1X + \dots + a_{m-1}X^{m-1} \pmod{P(X)}.$$

But $a_0 + a_1X + \dots + a_{m-1}X^{m-1} \pmod{P(X)}$ is a nonzero element of the field $GF(2^m)$, so we can divide by this element to get $X^j \equiv 1 \pmod{P(X)}$. Since $j = k$ is the first time this happens, the sequence first repeats after k terms, so it has period k .

As mentioned previously, when $2^m - 1$ is prime, all polynomials (except 0 and 1) are generating polynomials for $GF(2^m)$. In particular, X is a generating polynomial and therefore $k = 2^m - 1$ is the period of the recurrence.

3.11 Exercises

1. (a) Find integers x and y such that $17x + 101y = 1$.
- (b) Find $17^{-1} \pmod{101}$.

2. (a) Solve $7d \equiv 1 \pmod{30}$.
- (b) Suppose you write a message as a number $m \pmod{31}$. Encrypt m as $m^7 \pmod{31}$. How would you decrypt? (*Hint:* Decryption is done by raising the ciphertext to a power mod 31. Fermat's theorem will be useful.)