# Lecture One

# Mathematical Basic Concepts

## 8. Polynomials over Fields

Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \ldots + a_1 \cdot x + a_0$

be a polynomial of degree n in one variable x over a field F (namely $a_n$, $a_{n-1}, \ldots, a_1, a_0 \in F$).

**Theorem (8.1)**: The equation f(x)=0 has at most n solutions in F.

### 8.1 Irreducible Polynomials

**Definition (8.1)**: A polynomial is irreducible in GF(p) if it does not factor over GF(p). Otherwise it is reducible.

**Examples (8.1)**:

The polynomial $x^5+x^4+x^3+x+1$ is ***reducible*** in $Z_5$ but ***irreducible*** in $Z_2$.

### 8.2 Implementing GF($p^k$) Arithmetic

**Theorem (8.1)**: Let f(x) be an irreducible polynomial of degree k over $Z_p$. The finite field GF($p^k$) can be realized as the set of degree k-1 polynomials over $Z_p$, with addition and multiplication done modulo f(x).

**Example (8.2)**: **(Implementing GF($2^k$))**

By the theorem the finite field GF($2^5$) can be realized as the set of degree 4 polynomials over $Z_2$, with addition and multiplication done modulo the irreducible polynomial: $f(x)=x^5+x^4+x^3+x+1$.

The coefficients of polynomials over $Z_2$ are 0 or 1.

So a degree k polynomial can be written down by k+1 bits.

For example, with k=4:

$x^3+x+1$ (0,1,0,1,1)

$x^4+x^3+x+1$ (1,1,0,1,1).

## 8.3 Implementing GF($2^k$)

**Addition**: bit-wise XOR (since 1+1=0)

$x^3+x+1$ (0,1,0,1,1)

+

$x^4+x^3+x+1$ (1,1,0,1,1)

------------------------------

$x^4$ (1,0,0,0,0)

**Multiplication**: $(x^2+x+1)\cdot(x^3+x+1)$ in GF($2^5$).

(1,1,1)·(1,0,1,1)

```
1 0 1 1
  1 0 1 1
    1 0 1 1
----------------
1 1 0 0 0 1
```

1 1 0 0 0 1 = $x^5+x^4+1$

## 8.4 The Number of Primitive Polynomials

The function $\mu : Z^+ \rightarrow Z^+$ defined by:

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1; \\ (-1)^r \text{ if } n = p_1p_2...p_r, \text{ where the } p_i \text{ are distinct primes;} \\ 0 \text{ if } n \text{ has a squared factor} \end{cases}$$

is called the ***Möbius Function***.

The number of monic irreducible polynomials of degree k over $F_q$ is given by:

$$\psi_q(k) = \frac{1}{k}\sum_{d|k}\mu\left(\frac{k}{d}\right)q^d$$

where this sum is over all positive divisors d of k.

Clearly, not every monic irreducible polynomial in $F_q[x]$ is necessarily a primitive polynomial over $F_q$. In fact, the number of primitive polynomials of degree k over $F_q$ is:

$$\lambda_q(k) = \frac{\phi(q^k - 1)}{k}$$

**<u>Example (8.3)</u>**: Consider (monic) irreducible polynomials of degree 8 over $F_2=Z_2$. The positive divisors of 8 are d = 1, 2, 4, 8 so that 8/d = 8, 4, 2, 1 and $\mu(8/d)$= 0, 0,−1, 1.

Therefore, the number of monic irreducible polynomials of degree 8 in $F_2[x]$ is:

$$\psi_2(8) = \frac{1}{8}\sum_{d|8}\mu\left(\frac{8}{d}\right)2^d = (0 + 0 - 16 + 256)/8 = 30.$$

Furthermore, the number of primitive polynomials of degree 8 in $F_2[x]$ is:

$$\lambda_2(8) = \frac{\phi(2^8 - 1)}{8} = \frac{\phi(255)}{8} = \frac{\phi(3.5.17)}{8} = \frac{2.4.16}{8} = 16.$$

Hence, just over half the irreducible polynomials of degree 8 in $Z_2[x]$ are primitive.

However, if $2^k - 1$ is prime then $\psi_2(k) = \lambda_2(k) = (2^k - 2)/k$ so that every irreducible polynomial of degree k is in fact a primitive polynomial in $Z_2[x]$. It is therefore beneficial, in the practical sense, to choose a reasonably large value of k such that $2^k - 1$ is prime.

Of course, if we have a prime p>2 then $p^k - 1$ is always even, and hence not a prime (excluding the trivial case: $3^1 - 1$ is prime). Thus, for prime's $p>2$, the number of primitive polynomial of degree k in $F_p[x]$ will always be less than the number of irreducible polynomials of degree k over $F_p$, with the exception of the above trivial case.

Consequently, determining a maximal period length shift register generator presents no special problem in comparison to a linear recurrence generator modulo p. We simply choose k such that $M_k$ is prime so that every irreducible polynomial over $Z_2$ is a primitive polynomial. Then taking any such polynomial as the characteristic polynomial for the shift register generator will yield maximal period length sequences.