جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني
Department of Cyber Security

Subject:

Polynomial (Equation and Arithmetic)

Class:

Second

Lecturer: 3

Asst. Raed alshmary

Lecture: (3)

Introduction

Polynomials Equation

In cryptography, stream ciphers are encryption algorithms that encrypt plaintext one bit or byte at a time, often by combining the plaintext with a pseudorandom keystream. To build efficient stream ciphers, algebraic structures like polynomials play a crucial role, especially when working over finite fields (Galois fields).
A finite field, denoted as $GF(p)$ or $GF(2^n)$, is a set with a finite number of elements where we can perform addition, subtraction, multiplication, and division. In stream ciphers, operations are often performed over $GF(2)$ (the field with two elements: 0 and 1) or extensions of it like $GF(2^n)$.

For example:

- **$GF(2)$ contains two elements: 0 and 1.**
- **Arithmetic in this field follows modulo 2 rules.**
  - **0+0=0,0+1=1,1+1=0 (mod 2).**
  - **0×0=0,0×1=0,1×1=1.**

Modulo 2 or (mod2) is a mathematical operation that finds the remainder when one number is divided by 2. Here are the basic rules:

1. **Even Numbers:**
   Any even number (e.g., 0, 2, 4, 6, ...) gives a result of 0 when taken modulo 2.
   - **$Example: 4 \ mod \ 2 = 0$**
   -
2. **Odd Numbers:**
   Any odd number (e.g., 1, 3, 5, 7, ...) gives a result of 1 when taken modulo 2.
   - **$Example: 5 \ mod \ 2 = 1$**

3. **Properties:**

$$(a+b)mod2 = ((amod2)+(bmod2))mod2$$
$$(a \cdot b)mod2 = ((amod2)\cdot(bmod2))mod2$$

$$n \bmod 2 = 0 \; if \; n \; is \; even$$

$$n \bmod 2 = 1 \; if \; n \; is \; odd$$

Polynomials in Stream Ciphers

Polynomials are used in stream ciphers to represent feedback functions, state updates, and key mixing. These polynomials are treated in finite fields, and the arithmetic performed on them is modulo a characteristic polynomial.
A polynomial in a field $GF(2^n)$ can be expressed as:

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

Where:

- **$a_n, a_{n-1}, \ldots, a_1, a_0$ are coefficients from the field (either 0 or 1 in $GF(2)$).**
- **The arithmetic of polynomials is done modulo a characteristic polynomial in stream cipher design.**

Polynomial Arithmetic in Finite Fields

In a stream cipher, we deal with polynomial arithmetic over finite fields, particularly in $GF(2)$. Let's look at the operations.

a. Addition of Polynomials in GF(2)
Addition in $GF(2)$ is done by XORing the coefficients of the polynomials. There is no carry, and the sum is computed modulo 2.

Example:

$$P(x) = x^3 + x^2 + 1, \quad Q(x) = x^2 + x + 1$$

To add:

$$P(x) + Q(x) = (x^3 + x^2 + 1) + (x^2 + x + 1)$$

Result (mod 2):

$$= x^3 + (x^2 + x^2) + x + (1 + 1) = x^3 + x$$

So:

$$P(x) + Q(x) = x^3 + x$$

b. Multiplication of Polynomials in $GF(2)$
Multiplication is done by multiplying the polynomials as usual but reducing the result modulo a characteristic polynomial and applying mod 2 rules to the coefficients.

Example: Multiply $P(x) = x + 1$ by $Q(x) = x^2 + x$.
First, perform standard polynomial multiplication:

$$P(x) \cdot Q(x) = (x + 1)(x^2 + x) = x^3 + x^2 + x^2 + x = x^3 + 2x^2 + x$$

Now reduce modulo 2:

$$= x^3 + x$$

c. Polynomial Division and Modular Reduction

In cryptographic systems like stream ciphers, we often need to divide polynomials or reduce them modulo an irreducible polynomial.

Example of Modular Reduction: Let's reduce the polynomial $P(x) = x^4 + x + 1$ modulo $g(x) = x^3 + x + 1$.

Perform polynomial long division:

1. Divide x^4 by x^3, which gives x.
2. Multiply x by $x^3 + x + 1$, and subtract:

$$x^4 + x^2 + x \quad \text{from} \quad x^4 + x + 1$$

Result:

$$x^2 + 1$$

Thus, $x^4 + x + 1 \mod (x^3 + x + 1) = x^2 + 1$.

Another exmple: reduce the polynomial $P(x) = x^5 + x^3 + x$ modulo $g(x) = x^3 + x + 1$.

Step 1:
Set up the division
We are dividing the polynomial:

$$x^5 + x^3 + x$$

by the divisor:

$$x^3 + x + 1$$

Write the dividend $x^5 + x^3 + x$ under the division symbol and the divisor $x^3 + x + 1$ outside.

Step 2:
Divide the leading term
The leading term of the dividend is x^5, and the leading term of the divisor is x^3. Divide these terms:

$$\frac{x^5}{x^3} = x^2$$

This is the first term of the quotient.

Step 3:
Multiply and subtract
Now, multiply x^2 by the divisor $x^3 + x + 1$

$$x^2 \cdot (x^3 + x + 1) = x^5 + x^3 + x^2$$

Subtract this from the original polynomial $x^5 + x^3 + x$:

$$(x^5 + x^3 + x) - (x^5 + x^3 + x^2) = -x^2 + x$$

After subtraction, we're left with:

$$-x^2 + x$$

Step 4:

Divide the new leading term

The new leading term is $-x^2$, but we ignore the negative sign for now. Divide $-x^2$ by the leading term x^3 of the divisor. Since the degree of the remainder is less than the degree of the divisor, we stop the division here.

Thus, the remainder is:

$$-x^2 + x$$

Step 5:

Express the result

The quotient we obtained is x^2 , and the remainder is $-x^2 + x$. However, the remainder can be simplified in modulo 2 (where $-x^2 = x^2$) because we are working over a field where the coefficients are reduced mod 2.

So, $-x^2 + x = x^2 + x$. But since the remainder must be less than the degree of the divisor, and the degree of $x^2 + x$ is less than 3 (degree of the divisor), we accept it.

$$x^2 + 1$$

Thus:

$$x^5 + x^3 + x \mod (x^3 + x + 1) = x^2 + 1$$

Some Examples:

Example 1: Solving a Quadratic Polynomial in $GF(2)$

Solve the following quadratic equation over $GF(2)$:

$$x^2 + x + 1 = 0$$

In $GF(2)$ the possible values of x are 0 or 1. Let's check both values:

- ***For*** $x = 0$ **:**

$$0^2 + 0 + 1 = 1$$

So, $x = 0$ is not a solution.

For $x = 1$**:**

$$1^2 + 1 + 1 = 1 + 1 + 1 = 1 \pmod 2$$

So, x=1 is not a solution either.

Thus, there are no solutions to the equation $x^2 + x + 1 = 0$ in $GF(2)$.

Example 2: Solving a Cubic Polynomial in $GF(2)$.

$$x^3 + x^2 + x = 0$$

Let's factor the equation:

$$x(x^2 + x + 1) = 0$$

Now, we solve for x:

1. **For** $x = 0$:

$$0(0^2 + 0 + 1) = 0$$

So, $x = 0$ is a solution.

2. **For** $x = 1$, we need to solve the equation:

$$1^2 + 1 + 1 = 1 + 1 + 1 = 1 \pmod 2$$

So, $x = 1$ is **not** a solution for $x^2 + x + 1 = 0$.

Thus, the only solution to $x^3 + x^2 + x = 0$ in $GF(2)$ is:

$$x = 0$$

Example 3: Addition of Polynomials in $GF(2)$.

Add the following polynomials over $GF(2)$:

$$P(x) = x^3 + x^2 + 1, \quad Q(x) = x^2 + x$$

In $GF(2)$, addition is performed by XORing the coefficients (i.e., 1 + 1 = 0, 0 + 1 = 1, 1 + 0 = 1).

$$P(x) + Q(x) = (x^3 + x^2 + 1) + (x^2 + x)$$

Group the terms:

$$= x^3 + (x^2 + x^2) + x + 1$$

Simplify:

$$= x^3 + 0 + x + 1 = x^3 + x + 1$$

So, the result is:

$$P(x) + Q(x) = x^3 + x + 1$$

Example 5: Solving a Polynomial Division in $GF(2)$:

Perform polynomial long division for:

$$\frac{x^4 + x^2 + x}{x^2 + x + 1} \text{ in } GF(2)$$

1. Divide the leading term x^4 by x^2:

$$\frac{x^4}{x^2} = x^2$$

Multiply x^2 by $x^2 + x + 1$:

$$x^2(x^2 + x + 1) = x^4 + x^3 + x^2$$

Subtract from the original polynomial:

$$(x^4 + x^2 + x) - (x^4 + x^3 + x^2) = -x^3 + x$$

In $GF(2)$, $-x^3 = x^3$, so we have:

$$x^3 + x$$

2. Divide the leading term x^3 by x^2:

$$\frac{x^3}{x^2} = x$$

Multiply x by $x^2 + x + 1$:

$$x(x^2 + x + 1) = x^3 + x^2 + x$$

Subtract:

$$(x^3 + x) - (x^3 + x^2 + x) = -x^2 = x^2$$

Thus, the remainder is x^2, and the quotient is $x^2 + x$.

The division result is:

$$\frac{x^4 + x^2 + x}{x^2 + x + 1} = x + 1 + \frac{x^2}{x^2 + x + 1}$$