Arithmetic Polynomial

Dr. E.SURESH BABU

Assistant Professor

Computer Science and Engineering Department

National Institute of Technology, Warangal

Warangal

Arithmetic Polynomial

Why Study Polynomial Arithmetic

- ❖ Defining finite fields over sets of polynomials will allow us to create a **finite set of numbers** that are particularly appropriate for digital computation.
- ❖ Finite set of numbers will constitute a finite field
  - ✓ Specifically, We will perform all arithmetic operations on sets of polynomials

What do meant by Polynomial

❖ A Polynomial **f(x)** is a mathematical expression of the form

$$a^n x_n + a^{n-1} x_{n-1} + \ldots\ldots + a^1 x + a^0$$

- ✓ The highest exponent of **x** is the degree of the polynomial.
- ✓ Some non-negative integer **n**
- ✓ $a_n, a_{n-1}, \ldots, a_0$ are called **coefficients.**
- ✓ where x_i is called the **i^{th} term**

Polynomial Arithmetic Operation

- We can add, subtract polynomials by **combine the terms** in the polynomials with the **same powers.**

- **Polynomial Addition:** $(x^5 + 3x^3 + 4) + (6x^6 + 4x^3)$

$$\begin{array}{r} x^5 + 3x^3 + 4 \\ +\ 6x^6 + + 4x^3 \\ \hline 6x^6 + x^5 + 7x^3 + 4 \end{array}$$

$$(x^5 + 3x^3 + 4) + (6x^6 + 4x^3) = 6x^6 + x^5 + 7x^3 + 4$$

Polynomial Arithmetic Operation

❖ **Polynomial Subtraction :** $(x^5 + 3x^3 + 4) - (6x^6 + 4x^3)$

$$\begin{array}{rrrrr} & & x^5 & +3x^3 & +4 \\ - & 6x^6 + & & +4x^3 & \\ \hline & -6x^6 & +x^5 & -1x^3 & +4 \end{array}$$

$(x^5 + 3x^3 + 4) - (6x^6 + 4x^3) = -6x^6 + x^5 - x^3 + 4$

Polynomial Arithmetic Operation

- We can also multiply two polynomials. The general rule is that each **term** in the first polynomial has to **multiply each term** in the second polynomial, then **sum the resulted** polynomials up.

Polynomial Arithmetic Operation

❖ **Polynomial Multiplication :** $(x^5 + 3x^3 + 4)$ X $(6x^6 + 4x^3)$

$$
\begin{array}{rrrrrr}
 & & & x^5 & +\,3x^3 & +\;4 \\
\times & & & & 6x^6 & +\;4x^3 \\
\hline
 & & 4x^8 & +\,12x^6 & & +\;16x^3 \\
6x^{11} & +\,18x^9 & & +\,24x^6 & & \\
\hline
6x^{11} & +\,18x^9 & +\,4x^8 & +\,36x^6 & & +\,16x^3
\end{array}
$$

$(x^5 + 3x^3 + 4)$ X $(6x^6 + 4x^3)$ = $6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3$

Polynomial Division with Quotient

❖ **Polynomial Division :** $(6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3) \div (x^5 + 3x^3 + 4)$

$$
\begin{array}{r l}
 & 6x^6 + \qquad\quad 4x^3 \\
x^5 + 3x^3 + 4 & \overline{)\,6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3} \\
 & \underline{6x^{11} + 18x^9 + \qquad\quad 24x^6 \qquad\qquad} \\
 & \qquad\qquad\qquad 4x^8 + 12x^6 + 16x^3 \\
 & \qquad\qquad\qquad \underline{4x^8 + 12x^6 + 16x^3} \\
 & \qquad\qquad\qquad\qquad\qquad\qquad 0
\end{array}
$$

$(6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3) \div (x^5 + 3x^3 + 4) = 6x^6 + 4x^3$

Polynomial Division with Remainder

- But in many cases the divisors **cannot divide** the dividends, which means you will have **remainders.**

Polynomial Division with Remainder

❖ **Polynomial Division :** $3x^6 + 7x^4 + 4x^3 + 5) \div (x^4 + 3x^3 + 4)$

$$
\begin{array}{r|l}
 & 3x^2 - 9x + 34 \\
\hline
x^4 + 3x^3 + 4 & 3x^6 + \quad 7x^4 + 4x^3 \quad + 5 \\
 & 3x^6 + 9x^5 \quad + 12x^2 \\
\hline
 & -9x^5 + 7x^4 + 4x^3 - 12x^2 \quad + 5 \\
 & -9x^5 - 27x^4 \quad - 36x \\
\hline
 & 34x^4 + 4x^3 - 12x^2 + 36x + 5 \\
 & 34x^4 + 102x^3 + \quad 136 \\
\hline
 & -98x^3 - 12x^2 + 36x - 131
\end{array}
$$

Subtract

Subtract

Subtract

$(3x^6 + 7x^4 + 4x^3 + 5) \div (x^4 + 3x^3 + 4) =$ **$3x^2 - 9x + 34$ with remainder $-98x^3 - 12x^2 + 26x - 131$**

Arithmetic Operations On Polynomials To A Finite Field

Arithmetic Operations On Polynomials Whose Coefficients Belong To A Finite Field

- We can perform modular arithmetic with polynomials over a field.
- The operands and modulus are polynomials.
- **Let** $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ **and**

  $g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0$ be two polynomials over a field F,

Arithmetic Operations On Polynomials Over a Finite Field

❖ Let's consider the **set of all polynomials** whose coefficients belong to the finite field Z_7 (**which is the same as GF(7)**).

1. Adding Two Polynomials: $f(x) = 5x^2 + 4x + 6$; $g(x) = 2x + 1$

$$
\begin{array}{rr}
f(x) + g(x) = & 5x^2 + 4x + 6 \\
+ & 2x + 1 \\
\hline
& 5x^2 + 6x + 0 \quad (7 \bmod 7)
\end{array}
$$

Ans : $5x^2 + 6x$

Arithmetic Operations On Polynomials Over a Finite Field

❖ Let's consider the **set of all polynomials** whose coefficients belong to the finite field Z_7 (**which is the same as GF(7)**).

2. Subtract Two Polynomials: $f(x) = 5x^2 + 4x + 6$; $g(x) = 2x + 1$

$$
\begin{array}{rr}
f(x) - g(x) = & 5x^2 + 4x + 6 \\
- & 2x + 1 \\
\hline
 & 5x^2 + 2x + 5 \quad (5 \text{ Mod } 7 = 5)
\end{array}
$$

Ans : $5x^2 + 2x + 5$

Arithmetic Operations On Polynomials Over a Finite Field

3. Multiply Two Polynomials: $f(x) = 5x^2 + 4x + 6$; $g(x) = 2x + 1$

$$
\begin{array}{r}
f(x) \times g(x) = 5x^2 + 4x + 6 \\
\times \qquad\qquad 2x + 1 \\
\hline
5x^2 + 4x + 6 \\
10x^3 + 8x^2 + 12x \qquad \\
\hline
\end{array}
$$

$10x^3 + 13x^2 + 16x + 6 \mod 7 = \mathbf{3x^3 + 6x^2 + 2x + 6}$

Dividing Polynomials Defined Over A Finite Field

Dividing Polynomials Defined Over A Finite Field

- **Dividing polynomials** defined over a finite field is a little bit more frustrating than performing other arithmetic operations on such polynomials.

Dividing Polynomials Defined Over A Finite Field

- Consider again the polynomials defined over GF(7). Let's say we want to divide $5x^2 + 4x + 6$ by $2x + 1$.

Dividing Polynomials Defined Over A Finite Field

❖ **Step-1 :** In a long division, we must start by **dividing $5x^2$ by $2x$.**

- ✓ This requires that we divide **5 by 2 in GF(7).**
- ✓ Dividing **5 by 2** is the same as **multiplying 5** by the **multiplicative inverse of 2.**
- ✓ Multiplicative inverse of **2 is 4** since **$2 \times 4 \bmod 7$ is 1.** So we have $5/2 = 5 \times 2^{-1} = 5 \times 4 = 20 \bmod 7 = 6$

Dividing Polynomials Defined Over A Finite Field

- ✓ Therefore, the first term of the **quotient is 6x.**
- ✓ Since the product of **6x and 2x + 1 is $5x^2 + 6x$,**
- ✓ we need to subtract **$5x^2 + 6x$ from $5x^2 + 4x + 6$** which result is

  $(4 - 6)x + 6$ (since the additive inverse of 6 is 1) is the same as

  $(4 + 1)x + 6$, and that is the same as ***$5x + 6$.***

Dividing Polynomials Defined Over A Finite Field

❖ **Step-2 :** Our new dividend for the next round of long division is **$5x + 6$. (i.e $5x + 6 / 2x + 1$)**

- ✓ To find the next quotient term, we need to **divide $5x$ by $2x$.**
- ✓ We see that the **next quotient term** is again **6**.

Dividing Polynomials Defined Over A Finite Field

- **Final Result :** when the coefficients are drawn from the set GF(7), **5x2 + 4x + 6 divided by 2x + 1** yields a **quotient of 6x + 6** (Adding the Two Steps) and the remainder is zero.

Observation

- So we can say that as a polynomial defined over the field GF(7), $5x^2 + 4x + 6$ is a **product of two factors**, $2x + 1$ and $6x + 6$.
- We can therefore write $5x^2 + 4x + 6 = (2x + 1) \times (6x + 6)$

Arithmetic Operations On Polynomials Over Finite Field

Polynomials Over Finite Field

- Finite fields of order 2^n are called binary fields.
  - ✓ These **Binary fields** are of special interest
    - Efficient implementation in hardware/computer.
- The elements of $GF(2^n)$ are binary polynomials,
  - ✓ Polynomials whose **coefficients are either 0 or 1.**

Representation of Polynomials Using Bits

- Represent the **8-bit word (10011001)** using a polynomials.

n-bit word	1	0	0	1	1	0	0	1

Polynomial: $1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1x^0$

First simplification: $1x^7 + 1x^4 + 1x^3 + 1x^0$

Second simplification: $x^7 + x^4 + x^3 + 1$

Arithmetic Operations On Polynomials Over GF(2)

- Addition and subtraction operations on polynomials are the same operation.

Examples

❖ **Polynomials Addition and Subtraction** $(x^5 + x^2 + x) + (x^3 + x^2 + 1)$ in GF(2). We use the symbol ⊕ (XOR) for polynomial addition.

$$
\begin{array}{ll}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 & \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 & \\
\text{---} & \\
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 & \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

Arithmetic Operations On Polynomials Over GF(2)

❖ Polynomials Multiplication

1. The **coefficient multiplication** is done in GF(2).

2. The **multiplying x^i by x^j** results in x^{i+j}.

3. The multiplication may create terms with **degree more than $n - 1$,** which means the **result needs to be reduced** using a modulus polynomial.

Arithmetic Operations On Polynomials Over GF(2)

❖ Polynomials Multiplication

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

$$g(x) = x + 1$$

$$f(x) \times g(x) = x^2 (x + 1) + x(x + 1) + 1(x + 1)$$

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

$$= x^3 + 2x^2 + 2x + 1 \quad \text{Mod } 2 \quad = x^3 + 0x^2 + 0x + 1$$

$$= x^3 + 1$$

Irreducible Polynomial

Irreducible Polynomial

- If a polynomial is **divisible** only by **itself** and **constants**, then we call this polynomial an **irreducible polynomial.**
- An **irreducible polynomial** is also referred to as a **prime polynomial.**

Irreducible Polynomial….

- A **polynomial f(x)** over a GF(2^n) is called irreducible
  - ✓ if f(x) cannot be expressed as a **product** of two polynomials, both over GF(2^n) and both of degree **lower than** that of f(x).
- Note : When **g(x) divides f(x)** without leaving a **remainder**, we say g(x) is a **factor** of f(x).

Irreducible Polynomial Over GF(2^n)

Degree	*Irreducible Polynomials*
1	$(x + 1)$, (x)
2	$(x^2 + x + 1)$
3	$(x^3 + x^2 + 1)$, $(x^3 + x + 1)$
4	$(x^4 + x^3 + x^2 + x + 1)$, $(x^4 + x^3 + 1)$, $(x^4 + x + 1)$
5	$(x^5 + x^2 + 1)$, $(x^5 + x^3 + x^2 + x + 1)$, $(x^5 + x^4 + x^3 + x + 1)$, $(x^5 + x^4 + x^3 + x^2 + 1)$, $(x^5 + x^4 + x^2 + x + 1)$

Thank U