Lecture A2:

Polynomial Arithmetic

4th Year Course- CCSIT, UoA

Lecture goals

- To review and practice with polynomial arithmetic

Polynomial Arithmetic

- A polynomial is an expression of the form

$$a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0$$

for some non-negative integer *n* and where the coefficients $a_0, a_1, \ldots, a_n$ are drawn from some designated set *S*. *S* is called the coefficient set.

- When $a_n \neq 0$, we have a polynomial of degree *n*.
- A zeroth-degree polynomial is called a constant polynomial.
- Polynomial arithmetic deals with the addition, subtraction, multiplication, and division of polynomials.
- Note that we have no interest in evaluating the value of a polynomial for a specific value of the variable *x*.

Arithmetic Operations on Polynomials (1)

- We can add two polynomials:

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 \\ g(x) &= b_1x + b_0 \\ f(x) + g(x) &= a_2x^2 + (a_1+b_1)x + (a_0+b_0) \end{aligned}$$

- We can subtract two polynomials:

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 \\ g(x) &= b_3x^3 + b_0 \\ f(x) - g(x) &= -b_3x^3 + a_2x^2 + a_1x + (a_0-b_0) \end{aligned}$$

Arithmetic Operations on Polynomials (2)

- We can multiply two polynomials:

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 \\ g(x) &= b_1x + b_0 \\ f(x) \times g(x) &= a_2b_1x^3 + (a_2b_0 + a_1b_1)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0 \end{aligned}$$

- We can divide two polynomials (result obtained by long division):

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 \\ g(x) &= b_1x + b_0 \\ f(x) \,/\, g(x) &= ? \end{aligned}$$

Dividing Polynomials Using Long Division (1)

- Let's say we want to divide the polynomial $8x^2 + 3x + 2$ by the polynomial $2x + 1$
- In this example, our dividend is $8x^2 + 3x + 2$ and the divisor is $2x + 1$. We now need to find the quotient.
- Long division for polynomials consists of the following steps:
  1. Arrange both the dividend and the divisor in the descending powers of the variable.
  2. Divide the first term of the dividend by the first term of the divisor and write the result as the first term of the quotient. In our example, the first term of the dividend is $8x^2$ and the first term of the divisor is $2x$. So the first term of the quotient is $4x$.

Dividing Polynomials Using Long Division (2)

3. Multiply the divisor with the quotient term just obtained and arrange the result under the dividend so that the same powers of *x* match up. Subtract the expression just laid out from the dividend. In our example, $4x$ times $2x + 1$ is $8x^2 + 4x$. Subtracting this from the dividend yields $-x + 2$.
4. Consider the result of the above subtraction as the new dividend and go back to the first step. (The new dividend in our case is $-x + 2$).

- In our example, dividing $8x2 + 3x + 2$ by $2x + 1$ yields a quotient of $4x - 0.5$ and a remainder of 2.5.
- Therefore, we can write

$$8x^2 + 3x + 2 = 4x - 0.5 + \frac{2.5}{2x + 1}$$

Arithmetic Operations on Polynomials Whose Coefficients Belong to a Finite Field (1)

- Let's consider the set of all polynomials whose coefficients belong to the finite field Z_7 (which is the same as $GF(7)$).
- Here is an example of adding two such polynomials:
  - $f(x) = 5x^2 + 4x + 6$
  - $g(x) = 5x + 6$
  - $f(x) + g(x) = 5x^2 + 2x + 5$
- Here is an example of subtracting two such polynomials:
  - $f(x) = 5x^2 + 4x + 6$
  - $g(x) = 5x + 6$
  - $f(x) - g(x) = 5x^2 + 6x$

since the additive inverse of 5 in Z_7 is 2 and that of 6 is 1. So $4x - 5x$ is the same as $4x + 2x$ and $6 - 6$ is the same as $6 + 1$, with both additions modulo 7.

Arithmetic Operations on Polynomials Whose Coefficients Belong to a Finite Field (2)

- Here is an example of multiplying two such polynomials:
  - $f(x) = 5x^2 + 4x + 6$
  - $g(x) = 5x + 6$
  - $f(x) \times g(x) = 4x^3 + x^2 + 5x+1$

- Here is an example of dividing two such polynomials:
  - $f(x) = 5x^2 + 4x + 6$
  - $g(x) = 2x + 1$
  - $f(x) / g(x) = 6x + 6$

  If you multiply the divisor $2x + 1$ with the quotient $6x + 6$, you get the dividend $5x^2 + 4x + 6$.

Dividing Polynomials Defined over a Finite Field (1)

- First note that we say that a polynomial is defined over a field if all its coefficients are drawn from the field. It is also common to use the phrase polynomial over a field to convey the same meaning.
- Dividing polynomials defined over a finite field is a little bit more frustrating than performing other arithmetic operations on such polynomials. Now your mental gymnastics must include both additive inverses and multiplicative inverses.
- 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 (2)

- 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 2×4 *mod* 7 is 1. So we have

$$5/2 = 5 \times 2^{-1} = 5 \times 4 = 20 \ mod \ 7 = 6$$

- 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 the dividend $5x^2 + 4x + 6$. The result is $(4 - 6)x + 6$, which (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 (3)

- Our new dividend for the next round of long division is therefore $5x + 6$. To find the next quotient term, we need to divide $5x$ by the first term of the divisor, that is by $2x$. Reasoning as before, we see that the next quotient term is again 6.
- The final result is that when the coefficients are drawn from the set *GF* (7), $5x^2 + 4x + 6$ divided by $2x + 1$ yields a quotient of $6x + 6$ and the remainder is zero.
- 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

$$5x^2 + 4x + 6 = (2x + 1) \times (6x + 6)$$