Lecture 6: Finite Fields (PART 3)

PART 3: Polynomial Arithmetic

Theoretical Underpinnings of Modern Cryptography

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

February 5, 2016

12:49 Noon

Goals:

- To review polynomial arithmetic
- Polynomial arithmetic when the coefficients are drawn from a finite field
- The concept of an irreducible polynomial
- Polynomials over the $GF(2)$ finite field

CONTENTS

6.1: POLYNOMIAL ARITHMETIC

- Why study polynomial arithmetic? As you will see in the next lecture, defining finite fields over sets of polynomials will allow us to create a finite set of numbers that are particularly appropriate for digital computation. Since these numbers will constitute a finite field, we will be able to carry out all arithmetic operations on them — in particular the operation of division — without error.

- A polynomial is an expression of the form

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

for some non-negative integer n and where the **coefficients** a_0, a_1, ..., 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.

6.2: ARITHMETIC OPERATIONS ON POLYNOMIALS

- 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:

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

- 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):

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

6.3: DIVIDING ONE POLYNOMIAL BY ANOTHER USING LONG DIVISION

- 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:

  – Arrange both the dividend and the divisor in the descending powers of the variable.

  – 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 $4x$.

  – 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 $-x + 2$.

– 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 $8x^2 + 3x + 2$ by $2x + 1$ yields a **quotient** of $4x - 0.5$ and a *remainder* of 2.5.

- Therefore, we can write

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

6.4: ARITHMETIC OPERATIONS ON POLYNOMIALS WHOSE COEFFICIENTS BELONG TO 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 $GF(7)$). (See Section 5.5 of Lecture 5 for the $GF(p)$ notation.)

- Here is an example of adding two such polynomials:

$$\begin{aligned} f(x) &= 5x^2 + 4x + 6 \\ g(x) &= 2x + 1 \\ f(x) + g(x) &= 5x^2 + 6x \end{aligned}$$

- Here is an example of subtracting two such polynomials:

$$\begin{aligned} f(x) &= 5x^2 + 4x + 6 \\ g(x) &= 2x + 1 \\ f(x) - g(x) &= 5x^2 + 2x + 5 \end{aligned}$$

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

- Here is an example of multiplying two such polynomials:

$$\begin{aligned} f(x) &= 5x^2 + 4x + 6 \\ g(x) &= 2x + 1 \\ f(x) \times g(x) &= 3x^3 + 6x^2 + 2x + 6 \end{aligned}$$

- Here is an example of dividing two such polynomials:

$$\begin{aligned} f(x) &= 5x^2 + 4x + 6 \\ g(x) &= 2x + 1 \\ f(x) \ / \ g(x) &= 6x + 6 \end{aligned}$$

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

6.5: DIVIDING POLYNOMIALS DEFINED OVER A FINITE FIELD

- 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 $2x \ + \ 1$.

- 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 $2 \times 4 \ mod \ 7$ is 1. So we have

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

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 $5x + 6$.

- 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

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

6.6: LET'S NOW CONSIDER POLYNOMIALS DEFINED OVER $GF(2)$

- Recall from Section 5.5 of Lecture 5 that the notation $GF(2)$ means the same thing as Z_2. We are obviously talking about arithmetic modulo 2.

- First of all, $GF(2)$ is a sweet little finite field. Recall that the number 2 is the **first** prime. [For a number to be prime, it must have exactly two **distinct** divisors, 1 and itself.]

- $GF(2)$ consists of the set $\{0, 1\}$. The two elements of this set obey the following addition and multiplication rules:

```
0 + 0 = 0                          0 X 0 = 0
0 + 1 = 1                          0 X 1 = 0
1 + 0 = 1                          1 X 0 = 0
1 + 1 = 0                          1 X 1 = 1

0 - 0 = 0
1 - 0 = 1
0 - 1 = 0 + 1 = 1
1 - 1 = 1 + 1 = 0
```

- So the addition over $GF(2)$ is equivalent to the logical XOR operation, and multiplication to the logical AND operation.

- Examples of polynomials defined over $GF(2)$:

  $x^3 \ + \ x^2 \ - \ 1$

  $-x^5 \ + \ x^4 \ - \ x^2 \ + \ 1$

  $x \ + \ 1$

6.7: ARITHMETIC OPERATIONS ON POLYNOMIALS OVER $GF(2)$

- Here is an example of adding two such polynomials:

$$\begin{aligned} f(x) &= x^2 + x + 1 \\ g(x) &= x + 1 \\ f(x) + g(x) &= x^2 \end{aligned}$$

- Here is an example of subtracting two such polynomials:

$$\begin{aligned} f(x) &= x^2 + x + 1 \\ g(x) &= x + 1 \\ f(x) - g(x) &= x^2 \end{aligned}$$

- Here is an example of multiplying two such polynomials:

$$\begin{aligned} f(x) &= x^2 + x + 1 \\ g(x) &= x + 1 \\ f(x) \times g(x) &= x^3 + 1 \end{aligned}$$

- Here is an example of dividing two such polynomials:

$$\begin{aligned} f(x) &= x^2 + x + 1 \\ g(x) &= x + 1 \\ f(x) \;/\; g(x) &= x + \frac{1}{x + 1} \end{aligned}$$

  If you multiply the divisor $x + 1$ with the quotient x, you get $x^2 + x$ that when added to the remainder 1 gives us back the dividend $x^2 + x + 1$.

6.8: SO WHAT SORT OF QUESTIONS DOES POLYNOMIAL ARITHMETIC ADDRESS?

- Given two polynomials whose coefficients are derived from a set S, what can we say about the coefficients of the polynomial that results from an arithmetic operation on the two polynomials?

- If we insist that the polynomial coefficients all come from a particular S, then which arithmetic operations are permitted and which prohibited?

- Let's say that the coefficient set is a **finite field** F with its own rules for addition, subtraction, multiplication, and division, and let's further say that when we carry out an arithmetic operation on two polynomials, we subject the operations on the coefficients to those that apply to the finite field F. Now what can be said about the set of such polynomials?

6.9: POLYNOMIALS OVER A FIELD CONSTITUTE A RING

- The group operator is polynomial addition, with the addition of the coefficients carried out as dictated by the field used for the coefficients.

- The polynomial 0 is obviously the identity element with respect to polynomial addition.

- Polynomial addition is associative and commutative.

- The set of all polynomials over a given field is closed under polynomial addition.

- We can show that polynomial multiplication distributes over polynomial addition.

- We can also show polynomial multiplication is associative.

- Therefore, the set of **all** polynomials over a field constitutes a ring. Such a ring is also called the **polynomial ring**.

- Since polynomial multiplication is commutative, the set of polynomials over a field is actually a **commutative ring**.

- In light of the constraints we have placed on what constitutes a polynomial, it does not make sense to talk about multiplicative inverses of polynomials in the set of **all** possible polynomials that can be defined over a finite field. (Recall that our polynomials do not contain negative powers of x.)

- Nevertheless, as you will see in the next lecture, it is possible for a finite set of polynomials, whose coefficients are drawn from a finite field, to constitute a finite field.

6.10: WHEN IS POLYNOMIAL DIVISION PERMITTED?

- Polynomial division is obviously **not** allowed for polynomials that are **not** defined over fields. For example, for polynomials defined over the set of all integers, you cannot divide $4x^2 + 5$ by the polynomial $5x$. If you tried, the first term of the quotient would be $(4/5)x$ where the coefficient of x is not an integer.

- **You can always divide polynomials defined over a field.** What that means is that the operation of division is legal when the coefficients are drawn from a finite field. Note that, in general, when you divide one such polynomial by another, you will end up with a remainder, as is the case when, in general, you divide one integer by another integer in purely integer arithmetic.

- Therefore, in general, for polynomials defined over a field, the division of a polynomial $f(x)$ of degree m by another polynomial $g(x)$ of degree $n \leq m$ can be expressed by

$$\frac{f(x)}{g(x)} \quad = \quad q(x) \quad + \quad \frac{r(x)}{g(x)}$$

where $q(x)$ is the quotient and $r(x)$ the remainder.

- So we can write for any two polynomials defined over a field

$$f(x) \quad = \quad q(x)g(x) \ + \ r(x)$$

assuming that the degree of $f(x)$ is not less than that of $g(x)$.

- When $r(x)$ is zero, we say that $g(x)$ divides $f(x)$. This fact can also be expressed by saying that $g(x)$ is a **divisor** of $f(x)$ and by the notation $g(x)|f(x)$.

6.11: IRREDUCIBLE POLYNOMIALS, PRIME POLYNOMIALS

- When $g(x)$ divides $f(x)$ without leaving a remainder, we say $g(x)$ is a **factor** of $f(x)$.

- A polynomial $f(x)$ over a field F is called **irreducible** if $f(x)$ cannot be expressed as a product of two polynomials, both over F and both of degree lower than that of $f(x)$.

- An irreducible polynomial is also referred to as a **prime polynomial**.

6.12: HOMEWORK PROBLEMS

1. Where is our main focus in studying polynomial arithmetic:

    a) in evaluating the value of a polynomial for different values of the variable x and investigating how the value of the polynomial changes as x changes;

    or

    b) in adding, subtracting, multiplying, and dividing the polynomials and figuring out how to characterize a given set of polynomials with respect to such operations.

2. Divide

$$3x^2 + 4x + 3$$

by

$$5x + 6$$

assuming that the polynomials are over the field Z_7.

3. Complete the following equalities for the numbers in $GF(2)$:

$$1 \ + \ 1 \quad = \quad ?$$

$$
\begin{aligned}
1 - 1 &= ? \\
-1 &= ? \\
1 \times 1 &= ? \\
1 \times -1 &= ?
\end{aligned}
$$

4. Calculate the result of the following if the polynomials are over $GF(2)$:

$$
\begin{array}{ccc}
(x^4 + x^2 + x + 1) & + & (x^3 + 1) \\
(x^4 + x^2 + x + 1) & - & (x^3 + 1) \\
(x^4 + x^2 + x + 1) & \times & (x^3 + 1) \\
(x^4 + x^2 + x + 1) & / & (x^3 + 1)
\end{array}
$$

5. When is polynomial division permitted in general?

6. When the coefficients of polynomials are drawn from a finite field, the set of polynomials constitutes a

   - a group
   - an Abelian group
   - a ring
   - a commutative ring

- an integral domain
- a field

7. What is an irreducible polynomial?