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)

January 26, 2017

3:31pm

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:

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