Let's Now Consider Polynomials Defined over GF(2)

- 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. (A prime has exactly two distinct divisors, 1 and itself.)
- *GF* (2) consists of the set {0, 1}. The two elements of this set obey the addition and multiplication below. So the addition over *GF* (2) is equivalent to the logical XOR operation, and multiplication to the logical AND operation.

Addition and Multiplication over *GF* (2)

$$0 + 0 = 0 \qquad 0 \times 0 = 0$$
$$0 + 1 = 1 \qquad 0 \times 1 = 0$$
$$1 + 0 = 1 \qquad 1 \times 0 = 0$$
$$1 + 1 = 0 \qquad 1 \times 1 = 1$$

$$0 - 0 = 0$$
$$1 - 0 = 1$$
$$0 - 1 = 0 + 1 = 1$$
$$1 - 1 = 1 + 1 = 0$$

Arithmetic Operations on Polynomials Over GF(2) (1)

- 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:

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

Arithmetic Operations on Polynomials Over GF(2) (2)

- 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 $x^2 + x + 1$.

When is Polynomial Division Permitted? (1)

- 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.
- 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

$$f(x)/g(x) = q(x) + r(x)/g(x)$$

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

When is Polynomial Division Permitted? (2)

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

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

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 $g(x) | f(x)$.

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.**

Polynomials Over a Field Constitute a Ring (1)

- 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.

Polynomials Over a Field Constitute a Ring (2)

- 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.

Finally . . .

- Acknowledgment: These lecture notes are based on the textbook by William Stallings and notes prepared by Avinash Kak, Purdue University. My sincere thanks are devoted to them and to all other people who offered the material on the web.

- Students are advised to study and solve the problems and answer the questions in **Assignment-A2**.