Modular Arithmetic

In this lecture we assume that R is one of the rings $\mathbb{Z}$ or $\mathbb{F}_2[x]$, m is an element of R, and we denote by (m) or mR the set $\{mx : x \in R\}$, which is called an *ideal* of R. The principle goal is to introduce the *quotient* or *residue class rings* R/mR and to understand how to work with its elements. We refer to m as the *modulus* of R/mR.

Quotient rings

The residue class ring R/mR is a commutative ring, whose elements are sets, called *cosets* of mR, of the form

$$\overline{a} = a + mR = \{a + mx : xinR\},$$

and multiplication and addition laws are derived from that on R:

$$\overline{a} + \overline{b} = (a + mR) + (b + mR) = (a + b) + mR = \overline{(a + b)},$$

$$\overline{a} * \overline{b} = (a + mR) * (b + mR) = (a * b) + mR = \overline{(a * b)}.$$

The fact that R/mR is a ring means that the addition $(+)$ and multiplication $(*)$ are well-defined on cosets, and satisfy the usual associative and distributive laws.

Example. Consider the ring $R/mR = \mathbb{Z}/m\mathbb{Z}$ with modulus $m = 21$. We consider the addition and muliplication of $\overline{2} = \overline{23}$ and $\overline{-2} = \overline{19}$, and show that in each pair of equal elements, we can use either the first or the second representative to define the sum and product. First, for addition, we find:

$$\overline{2} + \overline{-2} = \overline{2 + (-2)} = \overline{0},$$

but on the other hand:

$$\overline{23} + \overline{19} = \overline{23 + 19} = \overline{42},$$

which equals $\overline{0}$ since 42 is in $21\mathbb{Z}$. Multiplication is similarly independent of the representatives we chose:

$$\overline{2} * \overline{-2} = \overline{2 * (-2)} = \overline{-4} = \overline{17},$$

which holds since $-4 = 17 + (-1) * 21$, or

$$\overline{23} + \overline{19} = \overline{437} = \overline{17},$$

where the latter identity is determined by $437 = 17 + 420 = 17 + 20 * 21$.

The mod operator

In both rings $R = \mathbb{Z}$ and $R = \mathbb{F}_2[x]$, we have an operator mod$m$ for producing a canonical smallest representative for elements of the quotient rings R/mR. This means

that we can work with this smallest or reduced representative in computations in R/mR. In particular, we note that working with this representative is well-defined:

$$((a \bmod m) + (b \bmod m)) \bmod m = (a + b) \bmod m$$
$$((a \bmod m) * (b \bmod m)) \bmod m = (a * b) \bmod m$$

since, $a \bmod m = b \bmod m$ if and only if $\overline{a} = \overline{b}$.

The value $a \bmod m$ can be computed by long division — successively subtracting off multiples until the result is smaller, until the final result is smaller than m. The definition of x smaller than y is $x < y$ for positive x, y in $\mathbb{Z}$, and $\deg(x) < \deg(y)$ for polynomials x, y in $\mathbb{F}_2[x]$.

N.B. Occasionally we will use the similar binary boolean-valued operator $\_ \equiv \_ \bmod m$. The value $a \equiv b \bmod m$ is `true` if and only if $\overline{a} = \overline{b}$, or equivalently if $(a - b) \bmod m$ is zero.

Example. We use the operator mod to determine a canonical representative for x^7 in $\mathbb{F}_2[x]/(x^2 + x + 1)$. First we write $x^7 = (x^3)^2 * x$, and compute:

$$\begin{aligned} x^3 \bmod (x^2 + x + 1) &= (x^3 + x * (x^2 + x + 1)) \bmod (x^2 + x + 1) \\ &= (x^2 + x) \bmod (x^2 + x + 1) \\ &= ((x^2 + x) + (x^2 + x + 1)) \bmod (x^2 + x + 1) = 1. \end{aligned}$$

It follows that $x^7 \bmod x^2+x+1 = (1^2 * x) \bmod (x^2+x+1) = x$. By explicit long division:

$$\begin{array}{r|l} & x^5+x^4+\qquad x^2+x \\ \cline{2-2} x^2+x+1 & x^7 \\ & \underline{x^7+x^6+x^5} \\ & \quad x^6+x^5 \\ & \quad \underline{x^6+x^5+x^4} \\ & \qquad\quad x^4 \\ & \qquad\quad \underline{x^4+x^3+x^2} \\ & \qquad\qquad x^3+x^2 \\ & \qquad\qquad \underline{x^3+x^2+x} \\ & \qquad\qquad\qquad x \end{array}$$

we find similarly that $x^7 = (x^5 + x^4 + x^2 + x) * (x^2 + x + 1) + x$, verifying the equality $x^7 \bmod (x^2 + x + 1) = x$.

Primes and Irreducibles

A nonzero ideal (p) in R ($= \mathbb{Z}$ or $\mathbb{F}_2[x]$) is said to be a prime ideal if p is a prime number or an irreducible polynomial. The following theorem is a generalization of Fermat's Little Theorem.

Theorem 5 *Let (p) be a prime ideal of R and let N equal $\#R/(p)-1$. Then $\overline{a}^N = 1$ for every nonzero $\overline{a}$ in $R/(p)$. Conversely if there exists an element $\overline{a}$ in $R/(p)$ of exact order N, then (p) is prime.*

N.B. Recall that we define the polynomial $g(x)$ to be primitive if and only if the element $\overline{x}$ has exact order N in $R/(g(x))$.

Irreducible polynomials

We now want to enumerate the the irreducible polynomials in $\mathbb{F}_2[x]$ of low degree, and in the process explain some of the steps for more efficiently determining [ir]reducibility of polynomials.

Degree 1: The linear polynomials x, $x+1$ are necessarily irreducible.

Degree 2: The polynomial x^2+x+1 is irreducible by the previous theorem and the fact that $\overline{x}$, $\overline{x}^2 = \overline{x}+1$, and $\overline{x}^3 = 1$. Conversely, it is clear to see that the only other candidates: x^2, x^2+x, and $x^2+1 = (x+1)^2$ are reducible.

Lemma 6 *If $f(x)$ is a polynomial, then $f(x) \bmod (x-a) = f(a)$, and in particular $f(x) = (x-a)g(x)$ if and only if $f(a) = 0$*

For polynomials over $\mathbb{F}_2$, the value $f(0)$ is the constant term, and $f(1)$ is the number of nonzero coefficients $\bmod 2$, which gives an easy test for divisibility by linear polynomials.

Degree 3: By the previous test, it is clear that the only nontrivial candidates to consider are

$$x^3+x+1, \quad x^3+x^2+1,$$

and that these are automatically irreducible, since they have no linear factor.

Degree 4: We first exclude $(x^2+x+1)^2 = x^4+x^2+1$, the only degree four polynomial which is divisible by an irreducible polynomial of degree 2. Every other reducible polynomial must therefore have a divisor of degree 1, and we apply the lemma to reduce to the list of irreducible polynomials:

$$x^4+x^3+1, \quad x^4+x+1, \quad x^4+x^3+x^2+x+1.$$

Degree 5: As in degree 4, we exclude those polynomials which have a divisor of degree 2:

$$(x^2+x+1)(x^3+x+1) = x^5+x^4+1$$
$$(x^2+x+1)(x^3+x^3+1) = x^5+x+1,$$

after which we conclude that all other polynomials of degree 5 with constant term 1 and an odd number of coefficients are irreducible:

$$\begin{array}{cc} x^5+x^3+1, & x^5+x^2+1, \\ x^5+x^4+x^3+x^2+1, & x^5+x^4+x^3+x+1, \\ x^5+x^4+x^2+x+1, & x^5+x^3+x^2+x+1. \end{array}$$

Exercise. Determine which of the above polynomials are primitive.

Cyclotomic polynomials

In the previous lecture we found that there are six irreducible polynomials of degree five. In order to understand and to count the numbers of irreducible and primitive polynomials, we first introduce cyclotomic polynomials.

Definition. The cyclotomic polynomials $\Phi_N(x)$ are defined recursively by the identity:

$$x^N - 1 = \prod_{m|N} \Phi_m(x).$$

Example. To demonstrate how this serves to define the cyclotomic polynomials, we compute the first few examples:

$$\begin{array}{ll} \Phi_1(x) = x - 1 & \Phi_4(x) = x^2 + 1 \\ \Phi_2(x) = x + 1 & \Phi_5(x) = x^4 + x^3 + x^3 + x^2 + x + 1 \\ \Phi_3(x) = x^2 + x + 1 & \Phi_6(x) = x^2 - x + 1 \end{array}$$

Moreover, if p is a prime, then

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

So far, the definition of cyclotomic polynomials does not make use of polynomials being defined over $\mathbb{F}_2$, and if we instead let the coefficient ring be $\mathbb{Z}$, then we have the following classical result.

Theorem 7 *The cyclotomic polynomial $\Phi_N(x)$ is irreducible over $\mathbb{Z}$, of degree $\varphi(N)$.*

The function $\varphi(N)$ is called the Euler φ-function, and is defined by

$$\varphi(N) = \prod_{p^r||N} p^{r-1}(p-1),$$

where $p^r||N$ means that p^r divides N but that p^{r_1} does not divide N.

The analogous statement about irreducibility over $\mathbb{F}_2$ is false, but we can make a very precise statement of the form of the factorization of cyclotomic polynomials over $\mathbb{F}^2$.

Theorem 8 *An irreducible polynomial $g(x) \in \mathbb{F}_2[x]$ of degree n divides the polynomial $x^N + 1$ and no other polynomial $x^m + 1$ for $m < N$ if and only if $g(x)$ divides $\Phi_N(x)$. The integer N equals $2^n - 1$ if and only if $g(x)$ is primitive.*

Corollary 9 *The cyclotomic polynomial $\Phi_N(x) \in \mathbb{F}_2[x]$ for $N = 2^n - 1$ is the product of the distinct primitive polynomials of degree n.*

Example. Previously we found that there were 6 irreducible polynomials of degree 5 in $\mathbb{F}_2[x]$. Since $N = 2^5 - 1 = 31$ is prime, every irreducible polynomial of degree 5 is in fact primitive. Since the degree of $\Phi_{31}(x)$ is $\varphi(31) = 31 - 1 = 30$, we could have concluded in advance that there were exactly 6 primitive and irreducible polynomials of this degree.

LFSR Keystreams

Since the period $N = 2^n - 1$ of the LFSR output sequence, with primitive connection polynomial, grows exponentially in the size of n, LFSR's provide good constructions for sequences of large period. Moreover a LFSR can be made computationally efficient by choosing a sparse primitive polynomial such as

$$\begin{aligned} 14: &\quad x^{14} + x^7 + x^5 + x^3 + 1 \\ 15: &\quad x^{15} + x^5 + x^4 + x^2 + 1 \\ 16: &\quad x^{16} + x^5 + x^3 + x^2 + 1 \\ 17: &\quad x^{17} + x^3 + 1 \end{aligned}$$

A naïve stream cryptosystem can be built from a LFSR by taking the bit sum of the keystream with the message stream to produce ciphertext. Unfortunately, knowledge of just $2n$ bits of the LFSR keysteam allows the determination of the entire sequence, by an algorithm due to Berlekamp and Massey. Therefore such a LFSR cryptosystem should be considered insecure. A relatively new stream cryptosystem, called the *shrinking generator* cryptosystem, using two LFSR's in unison, has so far resisted any such algorithms.

Shrinking generator. Let L_1 and L_2 be two LFSR's with output sequences $t_0t_1t_2\ldots$ and $s_0s_1s_2\ldots$. The first sequence is called the controlling sequence and the second sequence the input sequence. At clock cycle i bits t_i and s_i are output. If t_i is 0 then the bit s_i is discarded, and otherwise s_i forms part of the output keystream. The resulting keystream $s_{i_1}s_{i_2}s_{i_3}\ldots$ is used for forming the bit sum with the message stream to form ciphertext.

Public Key Cryptography

The theory of public key cryptography was introduced by Diffie and Hellman in 1976. Public key cryptography does not displace symmetric key cryptography — they solve different problems. The recent NIST contest which resulted in the Advanced Encryption Standard did not resulted in a new symmetric key, not public key standard. Why? Symmetric key algorithms do the bulk of encryption, and are orders of magnitude faster than public key systems of comparable security. They dispense with the restrictive conditions needed to build the split of public and private keys, and focus on speed. Public key cryptography, on the other hand, solves the key exchange problem — how to establish a common key between two parties that may have never met. It also finds use in specialized algorithms for digital signatures and message authentication.

The foundational concept of public key cryptography is that of the invertible one-way function $f : X \to Y$ — a function which is efficiently computable on any value $x \in X$, but

for which the inverse is hard: given y finding an x such that $y = f(x)$ is computationally hard. Most public key systems rely on *trapdoor* one-way functions. For such a function the constructor of the function has priviledged information which allows the efficient inversion of the function.

We begin with a description of symmetric and public protocols for message exchange in order to understand the role of each in cryptography.