Week 9

Lecture 1

Extended Topic: Polynomial Rings

Udaya Parampalli

School of Computing and Information Systems
University of Melbourne

Week 9

Lecture 1
Polynomial Rings

Lecture 2
ElGamal Signatures

Workshop 9: Workshops based on Lectures in Week 8

Quizz 3

Lecture 1

2.1 Euler's and Related Theorems

2.2 Groups, Rings and Fields

2.3 Functions and Chinese Remainder Theorem

Recap

- Numbers, Divisibility, Mod Operation, GCD, Extended GCD
- Inverse Mod n
- Properties Euler's Phi (ϕ)Function
- $\phi(p) = p - 1$, for any prime p.
- $\phi(p^a) = p^{a-1}(p-1)$, for any prime p and any integer $a \geq 1$.
- $\phi(pq) = (p-1)(q-1)$, for any two primes p and q.
- In fact, $\phi(mn) = \phi(m)\phi(n)$, for any two numbers which are relatively prime.

let $\mathbf{Z}_n^\star$ be set of numbers from 1 to $n-1$ but are relatively prime.

Theorem

If $a \in \mathbf{Z}_n^\star$, then $a^{\phi(n)} = 1 \pmod{n}$.

Inverse Mod n

Using Extended GCD Algorithm

```
$Function(a, n)$
g,x,y:=XGCD(a,n);
If g eq 1 then Return(x)
 else Return("The Inverse Does not Exist"), end if;
$end\ function$;
```

Using Eulerś Phi Function Result

```
$Function(a, n)$
$inva := a^{\phi(n)-1} \pmod{n}$.
$Return(inva)$;
$end\ function$;
```

The later function works only if a is relatively prime to n.

Lecture 2

2.1 Euler's and Related Theorems

Euler's Theorem

Definition

Remainders mod n: For $n \geq 1$, the set of remainders obtained by dividing integers by n, precisely these are elements of $\mathbf{Z}_n = \{0, 1, \cdots, n-1\}$.

However, not all elements of $\mathbf{Z}_n$ can be inverted. We define further the set of invertible numbers in $\mathbf{Z}_n$.

Definition

Reduced set of residues mod n: For $n \geq 1$, the reduced set of residues, $R(n)$ is defined as set of residues modulo n which are relatively prime to n.

Sometimes, $R(n)$ is also represented as $\mathbf{Z}^\star(n)$. In fact $\phi(n) = \#R(n)$, the cardinality(size) of the set $R(n)$.
Example: $\phi(15) = 8$, because $\phi(15) = \phi(5 \times 3) = (4 \times 2) = 8$.
$\phi(37) = 36$, as 37 is a prime number.
Next we consider Euler's theorem.

Euler's Theorem

Theorem

If $a \in \mathbf{Z}_n^\star$, then $a^{\phi(n)} = 1 \pmod{n}$.

Proof: Let $R(n) = \{r_1, r_2, \ldots, r_{\phi(n)}\}$,, be reduced set of residues modulo n. Now consider the set $a\ R(n) = \{a\ r_1, a\ r_2, \ldots, a\ r_{\phi(n)}\}$. Since a is relatively prime to n, the set $aR(n)$ is identically equal to $R(n)$. Note that the process of multiplying a only rearranges the residues in $R(n)$. Hence we can multiply all the elements in $R(n)$ and equate with the multiplication of all the elements of $a\ R(n)$. Hence we can write:

$$r_1 \times r_2 \cdots \times r_{\phi(n)} = (ar_1) \times (ar_2) \cdots \times (ar_{\phi(n)}).$$

Note that r_is are relatively prime to n and hence we can cancel r_i in the above equation by multiplying r_i^{-1}, $i = 1 \cdots \phi(n)$, to both the side of the equation. Then the above equation simplifies to

$$1 = a^{\phi(n)}. \text{ Hence the result.}$$

Fermat's Theorem

Theorem

Let p be a prime number, then if $gcd(a,p)=1$, then

$$a^{p-1} = 1 \ (mod \ p).$$

This is the particular case of Euler's Theorem when n is prime.
Fermat‘s Little Theorem

Theorem

Let p be a prime number,

$$a^p = a \ (mod \ p), \ \textit{for any integer } a.$$

When a is relatively prime, the theorem follows from the Fermatss theorem. When a is multiple of p, the result is trivially true.

Fermat's Theorem and Implications

- When p is a prime number, we learn that all nonzero numbers less than p are relatively prime and hence they are closed modulo p.
- In otherwords, all nonzero elements are invertible in $\mathbf{Z}_p$.
- They are closed under addition modulo p.
- Hence $\mathbf{Z}_p$ is closed under addition and multipliaction mod p .
- In fact, $\mathbf{Z}_p$ is a finite field, a structure extensively used in Cryptography.

2.2 Groups, Rings and Fields

Recap of Group, Ring, and Field

Let us visit a few concepts that we have learnt already. A *Group* is a set G together with a binary operation $\cdot$ on G such that the following three properties hold:

- $\cdot$ is *associative*; that is, for any $a, b, c \in G$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
- There is an *identity* element e in G such that for all $a \in G$,
$$a \cdot e = e \cdot a = a$$
- For each $a \in G$, there exists an *inverse* element $a^{(-1)} \in G$ such that
$$a \cdot a^{-1} = a^{-1} \cdot a = e$$
- If the group also satisfies
  For all $a, b \in G$,
$$a \cdot b = b \cdot a$$
  then the group is called *abelian* (or *commutative*).

Ring

A *Ring* $(R, +, \cdot)$ is a set R,together with two binary operations, denoted by $+$ and $\cdot$, such that:

- R is an abelian group with respect to $+$.
- $\cdot$ is associative; that is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
- The *distributive laws* hold; that is , for all $a, b, c \in R$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$

Prime Fields

We note that the set $\mathbf{Z}_p = \{0, 1, \cdots, p-1\}$, where p is a prime number, satisfies axioms of a field.

- The set is closed under addition.
- Since p is prime number, any nonzero element in $\mathbf{Z}_p$ has an inverse (Use Extended Euclidean algorithm).
- you can verify that additions and multiplications are distributive.

In $\mathbf{Z}_p$, unlike in Integers, p times any element in the field is zero in the field. This leads to a concept called "characteristic" of a field. We also denote $\mathbf{Z}_p^\star$ as a set of non-zero elements of $\mathbf{Z}_p$.

Characteristic of F

Definition

Let F be a field with the multiplicative identity 1 and the additive identity 0. The characteristic of F, sometimes written as $char(F)$, is the smallest integer $n \geq 0$ such that addition of the 1 with itself n times results in 0. i.e $n(1) = 0$.

Note that for real and complex fields you cannot find a positive integer n satisfying the above criteria. Hence, the characteristic of real and complex fields is 0.

In contrast for residue class rings $\mathbf{Z}_n$, the characteristic is n.

When n is prime, $\mathbf{Z}_p$ is a field and accordingly the characteristic of $\mathbf{Z}_p$ is p. One of the consequences of the above property is that $p = 0$ in the field for any α in the field.

$\mathbf{Z}_p$ is the main source of prime fields. Another class of finite fields are those whose size is a power of prime, we will consider this class later.

Polynomial Rings

A polynomial over a field F is an expression

$$f(x) = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0 = \sum_{i=0}^{n} f_i x^i,$$

where the symbol x is an indeterminate and the coefficients $f_i, 0 \leq i \neq n$ are elements of the field. Facts:

- the zero polynomial is $f(x) = 0$.
- The degree of a polynomial $f(x)$, denoted $degf(x)$, is the largest index of a nonzero coefficient. For example, $deg(1 + x + 2x^3)$ is 3, and $deg(1) = deg(1\ x^0) = 0$.
- the degree of a nonzero polynomial is always finite.
- By convention, the degree of the zero polynomial is $(-\infty)$.

Characteristic of a Polynomial Ring

Let p be a prime and $\mathbf{Z}_p$ is a prime field. Consider polynomials over $\mathbf{Z}_p$.
Another property is an analogous to Fermat's little theorem we consider before. But before we introduce it, we consider..

Some more definitions

- A polynomial of degree n is monic if its leading coefficient f_n (the coefficient of the largest index) is equal to 1. For example, $(1 + x + 2x^3)$ is not monic, however the polynomial $(1 + x + x^3)$ is monic.
- Two polynomials $f(x)$ and $g(x)$ are equal if the coefficients $f_i = g_i$ for all i.
- Set of all polynomials over a field F is denoted $F[x]$.

Analogous to integer addition and multiplication, we can define polynomial addition and multiplication.

Polynomial Rings

Sum: The sum of two polynomials in $F[x]$ is another polynomial in $F[x]$ defined by

$$f(x) + g(x) = \sum_{i=0}^{\infty} (f_i + g_i)x^i,$$

Example: $(1 + x + 2x^3) + (1 + 2x + 2x^3) = 2 + 3x + 4x^3 = 2 + x^3$ in $F_3[x]$

Product: The product of two polynomials in $F[x]$ is another polynomial in $F[x]$ defined by

$$f(x)g(x) = \sum_{i} \big(\sum_{j=0}^{i} (f_j g_{i-j}) x^i.$$

Example: $(1 + x + 2x^3)(1 + x) = (1 + 2x + x^2 + 2x^3 + 2x^4)$ in $F_3[x]$

The set $F[x]$ together with the above two operations forms a ring.

This ring resembles Integer ring in many ways.

How polynomial rings are different to Integer rings?

Firstly, if even though a polynomial ring over $\mathbf{Z}_p$ is ofinfinite size, it has a finite characteristic equal to the characteristic of its underlying field, namely $\mathbf{Z}_p$.
In fact for polynomial rings, characteristic of the ring is same as that of its underlying field used to generate the polynomials.
Prove the following result:

$$(a+b)^p = (a^p + b^p),$$

where a and b are any two polynomials over $\mathbf{F}_p$.
The above result is true even if a and b above are polynomials.

Facts:

- In any $F[x]$ subtraction is always possible but division is not always possible.
- If a polynomial $r(x)$ divides another polynomial $s(x)$, we say $r(x)|s(x)$, or $s(x)$ is divisible by $r(x)$ or $r(x)$ is a factor of $s(x)$, when $r(x)a(x) = s(x)$.
- A nonzero polynomial $p(x)$ that is divisible by $p(x)$ or by α, where α is an arbitrary field element, is called an irreducible polynomial.
- A monic irreducible polynomial is called a prime polynomial.
- $GCD[r(x), s(x)]$: Greatest common divisor of two polynomials $r(x)$ and $s(x)$, is the monic polynomial of the greatest degree that divides both of them.

- If the $GCD[r(x), s(x)]$ is 1 then the polynomials $r(x)$ and $s(x)$ are relatively prime.
- $LCM[r(x), s(x)]$: Least common multiple of two polynomials $r(x)$ and $s(x)$, is the monic polynomial of the smallest degree that is divisible by both of them.

The Division and Euclidean algorithms defined for integers analogously extend to Polynomial rings also. Construct the analogous theorems for polynomial rings.

1. Division Algorithm

2. Extended GCD Algorithm

Example. Consider $f(x) = 2x^5 + x^4 + 3 \in F_5[x]$, $g(x) = 3x^2 + 1 \in F_5[x]$. We compute the polynomials $q, r \in F_5[x]$ with $f = qg + r$ by using long division:

$$
\begin{array}{rrrrrrrrrrrrr}
 & & 4x^3 & + & 2x^2 & + & 2x & + & 1 & & & & \\
\cline{2-13}
3x^2 + 1) & & 2x^5 & + & x^4 & & & & & + & 4x & + & 3 \\
 & - & 2x^5 & & & - & 4x^3 & & & & & & \\
\cline{2-7}
 & & & & x^4 & + & x^3 & & & & & & \\
 & & & - & x^4 & & & - & 2x^2 & & & & \\
\cline{4-9}
 & & & & & & x^3 & + & 3x^2 & + & 4x & & \\
 & & & & & - & x^3 & & & - & 2x & & \\
\cline{6-11}
 & & & & & & & & 3x^2 & + & 2x & + & 3 \\
 & & & & & & & - & 3x^2 & & & - & 1 \\
\cline{8-13}
 & & & & & & & & & & 2x & + & 2
\end{array}
$$

Table: Example of Long Division

How polynomial rings are different to Integer rings?

Another difference is in the nature of the factorization problem over the ring.
The problem of factorizing a polynomial over $\mathbf{Z}_p$ is not hard, unlike the problem over Integers, where the problem is believed to be hard. There exists an efficient factorization algorithm for polynomials over a finite field due to Berlekamp, a renowned coding theorist.
After all, these rings are so called "man made" whereas some believe Integers are "God made". How can man compete with God!?

Construction of Finite Fields of size p^k

It is formally represented as the set of all residues of polynomials in $\mathbf{GF}(p)[x]$ obtained when divided by a prime polynomial $m(x)$ of order k:

$$\mathbf{GF}(p^k) = \mathbf{GF}(p)[x] \ mod \ m(x),$$

where $m(x)$ is an irreducible polynomial of degree k. Sometimes, we denore $\mathbf{GF}^\star(p^k)$ to denote all non-zero elements of $\mathbf{GF}(p^k)$. We will work through a few examples in the class.

$\mathbf{GF}(2^3)$: Finite field of 8 elements

Convince yourselves that $1 + x + x^3$ is an irreducible polynomial over F_2 (Try dividing with polynomials of degree less than or equal to 3, then you will find the polynomial is dvided by itself or by a scalar $\alpha \in \mathbf{Z}_p$) .
$\mathbf{GF}(2^3) = \mathbf{GF}(2)[x]$ *mod* $(1 + x + x^3)$. The table of elements of $GF(8)$ is given in the next slide. Note that the elements are computed as x^i *mod* $(1 + x + x^3)$ (remainder obtained when dividing x^i by $(1 + x + x^3)$. For $i > 1$, the computation x^i can be obtained recursively by multiplying x to x^{i-1}, its previous entry. Also note that multiplying x is equivalent to shifting the vector representation of x^i to the right by one place and replacing x^3 by $1 + x$. This is because $1 + x$ is the remainder when you divide x^3 by $(1 + x + x^3)$. This can be obtained by equating $1 + x + x^3$ to 0. Thus, $1 + x + x^3 = 0$ implies $x^3 = 1 + x$. You can use this relation to simplify the remainder computation. Here, $1 + x + x^3$ plays the role of a prime number and by definition this should be 0 in the field.

i	Elements:x^i	As Polynomials	As Vectors
$-\infty$	0	0	$[0, 0, 0]$
0	1	1	$[1, 0, 0]$
1	x	x	$[0, 1, 0]$
2	x^2	x^2	$[0, 0, 1]$
3	x^3	$1 + x$	$[1, 1, 0]$
4	x^4	$x + x^2$	$[0, 1, 1]$
5	x^5	$1 + x + x^2$	$[1, 1, 1]$
6	x^6	$1 + x^2$	$[1, 0, 1]$
7	x^7	1	$[1, 0, 0]$

Table: Elements of $\mathbf{GF}(2^3)$ as powers of x

$\mathbf{GF}(3^2)$: Finite field of 9 elements

Convince that $2 + 2x + x^2$ is an irreducible polynomial over F_3, ternary field.

$$\mathbf{GF}(3^2) = \mathbf{GF}(3)[x] \ \mathit{mod} \ (2 + 2x + x^2).$$

The computations run on similar lines.
In this case, x^2 is $1 + x$ (Remainder when dividing x^2 by $(2 + 2x + x^2)$). This can be obtained by equating $2 + 2x + x^2$ to 0. Here $2 + 2x + x^2$ is zero in the field. The table is provided in the next slide.
Construct by hand the following fields:
$\mathbf{GF}(2^4) = \mathbf{GF}(2)[x] \ \mathit{mod} \ (1 + x + x^4)$
$\mathbf{GF}(2^4) = \mathbf{GF}(2)[x] \ \mathit{mod} \ (1 + x + x^2 + x^3 + x^4)$
Do you see any problem? In the second case, x cannot generate all the elements, you may have to try generating with some other elements of the field like $1 + x$.

i	Elements:x^i	As Polynomials	As Vectors
$-\infty$	0	0	$[0, 0]$
0	1	1	$[1, 0]$
1	x	x	$[0, 1]$
2	x^2	$1 + x$	$[1, 1]$
3	x^3	$1 + 2x$	$[1, 2]$
4	x^4	2	$[2, 0]$
5	x^5	$2x$	$[0, 2]$
6	x^6	$2 + 2x$	$[2, 2]$
7	x^7	$2 + x$	$[2, 1]$
8	x^8	1	$[1, 0]$

Table: Elements of $\mathbf{GF}(3^2)$ as powers of x

Primitive Irreducible Polynomials

An irreducible polynomial $m(x)$ of degree k over $\mathbf{GF}(p)$, p a prime, is a primitive irreducible polynomial, if the element x in $\mathbf{GF}(p)[x]$ *mod* $m(x)$ generates all nonzero elements of $\mathbf{GF}(p^k)$. This is another way of saying that the the multiplicative order of x modulo $m(x)$ is $p^k - 1$.
When you construct $\mathbf{GF}(p^k)$ using a primitive irreducible polynomial of degree k, $m(x)$, as a polynomial ring:

$$\mathbf{GF}(p^k) = \mathbf{GF}(p)[x] \ mod \ m(x),$$

then the multiplicative order of the indeterminate x is exactly equal to $p^k - 1$. We shall discuss fast algorithm later.

Multiplicative groups of Finite Fields

Structure	Size	Multiplicative Group	Size of the Multiplicative Group
$\mathbf{Z}(2)$	2	$\mathbf{Z}_2^\star$	1
$\mathbf{Z}(3)$	3	$\mathbf{Z}_3^\star$	2
$\mathbf{Z}(5)$	5	$\mathbf{Z}_5^\star$	4
$\mathbf{Z}(p)$	p	$\mathbf{Z}_p^\star$	$p-1$
$\mathbf{GF}(2^4)$	16	$\mathbf{GF}^\star(16)$	15
$\mathbf{GF}(3^2)$	9	$\mathbf{GF}^\star(9)$	8
$\mathbf{GF}(p^k)$	p^k	$\mathbf{GF}^\star(p^k)$	p^k-1

Primitive Elements

We discussed primitive elements of simple finite fields in this lecture. In general, determining primitive elements of finite fields is a challenging subject.

Week 9

Lecture 1
Polynomial Rings

Lecture 2
ElGamal Signatures

Workshop 9: Workshops based on Lectures in Week 8

Quizz 3