Cryptography:Mathematical Foundation
Polynomial Rings and Finite Fields

Udaya Parampalli

Department of Computing and Information Systems
University of Melbourne

August, 2016

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 is p is prime number, any nonzero element in $\mathbf{Z}_p$ has an inverse (Use 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.

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.

$\mathbf{Z}_p$ is the main source of prime fields. However from Algebra, we know that finite fields of the size of prime powers exist. How to construct them?

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 $(-\infty)$.

- 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 multiplications, we can define polynomial addition and multiplication.

Polynomial Ring

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.

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. *Euclidean Algorithm*

How polynomial rings are different to Integer rings?

Firstly, if even though polynomial ring over $\mathbf{Z}_p$ is infinite 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 $\mathbf{F}_p$.

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 $GF(p)[x]$ obtained when divided by a prime polynomial $m(x)$ of order k:

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

where $m(x)$ is an irreducible polynomial of degree k. We will work through few examples in the class.

$GF(2^3)$: 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 wil find the polynomial is dvided by itself or by a scalar $\alpha \in \mathbf{Z}_p$) .
$GF(2^3) = GF(2)[x]$ *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 a 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 $GF(2^3)$ as powers of x

$GF(3^2)$: Finite field of 9 elements

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

$$GF(3^2) = GF(3)[x] \ mod \ (2 + 2x + x^2).$$

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:
$GF(2^4) = GF(2)[x] \ mod \ (1 + x + x^4)$
$GF(2^4) = GF(2)[x] \ mod \ (1 + x + x^2 + x^3 + x^4)$
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 $GF(3^2)$ as powers of x

Primitive Irreducible Polynomials

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

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

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