Chapter 2 - Finite fields and Quadratic residues

Field

Field = set F with two binary operations called addition and multiplication. Properties to be satisfy: commutative, associative, additive identity, multiplicative identity, distributive, additive and multiplicative inverse

Examples:

1) $\mathbb{Q}$ is a field, $\mathbb{Q}$ = rational numbers

$\frac{a}{b} \times \frac{b}{a} = 1$, $\frac{b}{a}$ = multiplicative inverse

$\frac{a}{b} + \frac{0}{1} = \frac{a}{b}$, $0/1$ = additive identity

$\frac{a}{b} + \left(-\frac{a}{b}\right) = 0$, $-\frac{a}{b}$ = additive inverse

2) Z_5 is a field

$Z_5 = 0, 1, 2, 3, 4$

$2 + (3 + 4) = 2 + 2 = 4$

$(2 + 3) + 4 = 0 + 4 = 4$

$2^{-1} = 3$ since $2 \times 3 = 6 \% 5 = 1$ (inverse also exists)

$4^{-1} = 4$

3) $\mathbb{Z}_6$ is not a field

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$3 \times 4 = 12 \% 6$

$3 \times 5 = 15 \% 6$

$8 \% 6 = 2$

$16 \% 6 = 4$

$20 \% 6 = 2$

not every element has multiplicative inverse.

Vector Space

set of objects called vectors, can be added together and multiplied by scalars.

Example: $\mathbb{R}^2$ is a vector space with usual addition and multiplication.

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \end{pmatrix} \in \mathbb{R}^2$$

$$a \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} ax_1 \\ ax_2 \end{pmatrix} \in \mathbb{R}^2$$

* ~~$\mathbb{R}^3$ is also a vector space~~

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \text{additive identity exists}$$

$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ = additive inverse exists

each R^n is a vector space.

basis of vector space = let R^2 be vector space

let $v_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $v_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

v_1, v_2 = basis since: take any vector ~~element~~; let's say

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix} = 2\begin{bmatrix} 1 \\ 0 \end{bmatrix} + 1\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 2v_1 + v_2$$

$$\begin{bmatrix} 1 \\ 3 \end{bmatrix} = 1\begin{bmatrix} 1 \\ 0 \end{bmatrix} + 3\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1v_1 + 3v_2$$

- **extension field** = A bigger field containing F is also a vector space over F.

Ex: $K = F(\alpha)$ => contains rational expressions formed by using α and elements of F.

Polynomial ring = defined over field F. denoted by F[x]. It consists of finite sums of powers of x with coefficients in F.

Example: $Z_5 = \{0, 1, 2, 3, 4\}$

$Z_5[x]$ = polynomial ring with coefficients in integers modulo 5 (Z_5)

$Z_5[x] = \{2x^3 + 2x^2 + 1,\ 3x^2 + 4x + 1,\ \dots\}$

degree of polynomial = largest power of x with non-zero coefficient

$5x^3 + x^2 + x + 1 \Rightarrow$ **degree = 3**

monic polynomial = coefficient of $x^d = 1$

* $x^3 + 5x^2 + x + 1$ = monic

$d = 3$

$\text{coeff}(x^d) = 1$

* $5x^3 + x^2 + x + 1$ = not monic

$d = 3$

$\text{coeff}(x^d) \neq 1$

- f is divisible by g if $\exists\ h \in F[x]$ such that $f = gh$

- irreducible polynomials = cannot be divided by lower degree polynomials except for constant. These are "primes among polynomials"

Ex: $x^2 - 2$ = irreducible

$x^2 + 4x + 4$ = reducible

$$
\begin{array}{r|l}
x+2 & x^2+4x+4 \\
 & \underline{x^2+2x} \\
 & \quad 2x+4 \\
 & \quad \underline{2x+4} \\
 & \quad\quad 0
\end{array}
$$

→ fully divisible.

Properties of Polynomial ring

→ unique factorization

→ element α in some extension field K containing F is algebric over F if it satisfies polynomials with coeff. in F

→ degree of extension obtained by adjoining α is same as degree of monic irreducible polynomial of α.

→ derivative of polynomial $= nx^{n-1}$

$f = 5x^3 + 3x^2$

$f^1 = 15x^2 + 6x$

- Polynomial f of degree d may or may not have a root r which gives 0 on substituting with X.

If it does gives 0, then $(x-r)$ ~~is root of f~~ divides f. $(x-r)^m$ is the highest power of $(x-r)$ which divides f.

$(x-r)^m$, m = multiplicity

Ex: $x^2+4x+4 = (x+2)^{(2)}$ → multiplicity

$r = -2$ ↗ gives 0, so $(x+2)$ is a polynomial which divides it.

- Total no. of roots of F cannot exceed d.

Ex: $x^2+4x+4 = (x+2)(x+2)$

$x^3+3x^2-6x = (x+3)(x^2-6)$

$= (x+3)(x+\sqrt{6})(x-\sqrt{6})$

Finite fields

- F_q = finite number of 'q' elements in it. Let p be the characteristic of F_q, then F_q contains the prime field $F_p = Z/pZ$ and F_q is a vector space over F_p.

Example:

distribution | cancellation

Z_p (p = prime) with + & * mod p is a finite field.

0 identity (+) | 1 identity (*)

Z_2, Z_3, Z_5

Z_4 is not finite field

↳ inverse of 2 does not exist

Existence of multiplicative generators of finite field

F_q => means "q-1" non-zero elements, they form an abelian group

↙

group in which result of applying the group operation to two elements does not depend on the order in which they are written

F_n^* = elements coprime to n
= $a \in F_n^*$ such that $\boxed{gcd(a, n) = 1}$

Example:

$(Z, +)$ = abelian group

$2+3 = 3+2$
$-3+1 = 1+(-3)$ } commutative

$2+(3+6) = (2+3)+6$ = Associative

$2+0 = 2$ = identity

$2 \times 0 = 0$. (0 is additive identity)

$2-2 = 0$ (additive inverse also exist)

Generator 'g' of a finite field

generator 'g' of order $q-1$. Powers of g run through all elements of F_q^*.

Example:

$gcd(2,13) = 1$
$gcd(11,13) = 1$

$Z_{13} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$
$Z_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

$g = 2$ = generator

$\{2^1, 2^2, 2^3, 2^4 \% 13, 2^5 \% 13 - - \}$

$\{2, 4, 8, 16 \% 13, 32 \% 13 - -$

$\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

Similarly $g = 6, 7, 11$ are also generators

- Every finite field has a generator g
  If g is a generator of Fq^* then g^j is also a generator iff $gcd(j, q-1) = 1$.

- There are $\varphi(q-1)$ different generators of Fq^*.

Example:

Z_{13}^* ≠ ~~13 etc~~

↙

$q = 13$

$\varphi(q-1) = \varphi(12)$ generators

1, 5, 7, 11 are coprime to 12

Hence $\varphi(12) = 4$

Hence there are 4 different generators of Fq^*.

- For every prime p, there exists an integer g such that powers of g exhaust all non-zero residue classes modulo p.

Example: We can get all non-zero residues modulo 19 from 1 to 18 by taking powers of 2.

$2^0 \% 19 = 1$

$2^1 \% 19 = 2$

$2^2 \% 19 = 4$

$2^3 \% 19 = 8$

$2^4 \% 19 = 16$

$2^5 \% 19 = 13$

⋮

- If F is a prime number, then there are $\frac{p^F - p}{f}$ distinct monic irreducible polynomials of degree f in $F_p[x]$.

- Let F_q where $q = p^f$ be a finite field and let $F[x]$ be an irreducible polynomial of degree F over Fp.
The 2 elements of F_q can be multiplied or divided in $O(\log^3 q)$ bit operations.

If k ∈ +ve integer, then an element of F_q can be raised to k^{th} power in $O(\log k \log^3 q)$ bit operations.

Ex:

$F(x) = x^4 + x^3 + x^2 + 1$

$g(x) = x^3 + 1$

Find gcd(F, g) using euclidean algorithm ?

Soln:

$a > b$

$$gcd(a, b) = gcd(b, a \% b)$$

$a \rightarrow x^4 + x^3 + x^2 + 1$, $b \rightarrow x^3 + 1$

$gcd(x^4 + x^3 + x^2 + 1, x^3 + 1)$

$gcd(x^3 + *, x^2 + x)$

$gcd(x^2 + x, x + 1)$

$\leftarrow$ remainder $r = 0$

Hence $\boxed{gcd(f, g) = x + 1}$

$$\begin{array}{r|l} & x + 1 \\ \hline x^3 + 1 & x^4 + x^3 + x^2 + 1 \\ & x^4 + x \\ \hline & x^3 + x^2 + x + 1 \\ & x^3 + 1 \\ \hline & x^2 + x \end{array}$$

$$\begin{array}{r|l} & x + 1 \\ \hline x^2 + x & x^3 + * \\ & x^3 + x^2 \\ \hline & x^2 + * \\ & x^2 + x \\ \hline & x + 1 \end{array}$$

$$\begin{array}{r|l} & x \\ \hline x + 1 & x^2 + x \\ & x^2 + x \\ \hline & 0 \end{array}$$

Quadratic residues: Suppose p is an odd prime. ($p > 2$) We are interested in knowing which of the non-zero elements $\{1, 2, \ldots p-1\}$ of F_p are squares.

If some $a \in F_p^*$ is a square, say $b^2 = a$ then a has precisely two square roots $\pm b$.

Thus the squares in F_p^* can be found out by computing $\boxed{b^2 \bmod p}$ for $b = 1, 2 \ldots (p-1)/2$.

Example: squares in F_{11}?

$p = 11$

$b = 1, 2 \ldots (11-1)/2 = 1, 2 \ldots 5$

Squares $= b^2 \bmod p = 1^2 \% 11,\ 2^2 \% 11,\ 3^2 \% 11,$

$4^2 \% 11,\ 5^2 \% 11$

squares = 1, 4, 9, 5, 3

So now **Quadratic residues mod p** = means

the squares of F_p

The remaining non-zero elements are called **non-residues**.

Ex: in F_{11}

Quadratic residues mod p = {1, 4, 9, 5, 3}

Non-residues = {2, 6, 7, 8, 10}

- There are $\frac{(p-1)}{2}$ non-residues and $\frac{(p-1)}{2}$ quadratic residues.

- If g is generator of F_p, then any element can be written in the form g^j. The square of any element is of form g^j with j even.

Legendre Symbol: Let a be an integer and $p > 2$ be odd prime. We define the legendre symbol $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a non-residue mod } p \end{cases}$$

Legendre symbol is a way of identifying "whether or not an integer is quadratic residue modulo p."

Proposition: $\frac{a}{p} \equiv a^{(p-1)/2} \bmod p$

Properties of Legendre symbol:

1) $\left(\frac{a}{p}\right)$ depends only on the residue of a modulo p

2) $\frac{ab}{p} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3) for b prime to p, $\left(\frac{ab^2}{p}\right) = \frac{a}{p}$

4) $\left(\frac{1}{p}\right) = 1$ & $\left(\frac{-1}{p}\right) = (-1)^{p-1/2}$

Ex 1: $\left(\frac{10}{13}\right)$

Soln: $\left(\frac{10}{13}\right) = \left(\frac{2 \times 5}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right)$

For $\left(\frac{2}{13}\right)$

$$\left(\frac{2}{13}\right) = (2)^{\frac{13-1}{2}} \pmod{13} = 2^6 \bmod 13$$
$$= 64 \bmod 13$$
$$= 12 \bmod 13$$

$$\left(\frac{2}{13}\right) = 12 \bmod 13 = -1 \bmod 13$$

$$\left(\frac{2}{13}\right) = -1$$

For $\left(\frac{5}{13}\right) = 5^{\frac{13-1}{2}} \bmod 13$

$$= 5^6 \bmod 13$$
$$= 15625 \bmod 13$$
$$= 12 \bmod 13$$
$$= -1 \bmod 13$$
$$= -1$$

$$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right) \times \left(\frac{5}{13}\right) = (-1) \times (-1) = 1$$

$$\left(\frac{10}{13}\right) = 1$$

Law of Quadratic reciprocity

Let p & q be odd primes, then

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right)$$

$$= \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \bmod 4 \\ \frac{p}{q}, & \text{otherwise.} \end{cases}$$

The Jacobi symbol

Let a be an integer, and let n be any positive odd number.

Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factorization of n. Then we define the Jacobi symbol $\left(\frac{a}{n}\right)$ as the product of the Legendre symbols for the prime factors of n:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}$$

Proposition: For any positive odd n we have $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$

Proposition: For any two positive odd integers m & n, we have:

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$$

Ex 1: $\left(\frac{5}{21}\right)$

Soln: $\left(\frac{5}{21}\right) = \left(\frac{5}{3}\right) \times \left(\frac{5}{7}\right)$

$= \left(\frac{5}{3}\right) \times \left(\frac{5}{7}\right)$

For $\left(\frac{5}{3}\right) = 5^{\frac{3-1}{2}} \bmod 3 = 5 \bmod 3$

$= 2 \bmod 3$

$5 \equiv 2 \bmod 3$

$\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = 2^{\frac{3-1}{2}} \bmod 3 = 2^{} \bmod 3$

$= -1 \bmod 3$

$\left(\frac{5}{3}\right) = -1$

For $\left(\frac{5}{7}\right) = 5^{\frac{7-1}{2}} = 5^{3} \bmod 7 = 125 \bmod 7$

$= -1 \bmod 7$

$125 \bmod 7 = 6$

$-1 \bmod 7 = (7-1) = 6$

$\left(\frac{5}{7}\right) = -1$, Hence $\left(\frac{5}{21}\right) = (-1) \times (-1) = 1$

Ans.