CS 4450

Coding and Information Theory

This is the first lecture on
Mathematical Fundamentals (A)

Dr. Xuejun Liang

Mathematical Fundamentals

1. Modular Arithmetic
2. Group and Examples
3. Euclidean Theorem
4. Field and Examples
5. Extension Field
6. Linear (Vector) Space
7. Matrix and Groups of Linear Equations

Modular Arithmetic

Definition 1: Suppose a and b are integers, and m is positive integer. Then we write $a \equiv b \pmod{m}$ if m divides b-a.

- $a \equiv b \bmod m$ if and only if $(a-b) = k \times m$ for some k
- Z_m the equivalence class under mod m
- Canonical form $Z_m = \{0,1,2,\ldots,m-1\}$, we use the positive remainder as the standard representation.
- -a mod m = m - (a mod m)

Modulo-7 Addition in Z_7

[+]	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$5 + 13 \equiv 5 + 1 \equiv 6 \bmod 12$

$5 \times 13 \equiv 5 \times 1 \equiv 5 \bmod 12$

Group

Definition 2: A set G on which a binary operation * is defined is called a *group* if the following conditions are satisfied:

1. The binary operation * is associative.
2. G contains an element e, called an *identity element* on G, such that, for any a in G

$$a * e = e * a = a$$

3. For any element a in G, there exists another element a', called an inverse of a in G, such that

$$a * a' = a' * a = e$$

A group G is said to be *commutative* if its binary operation * satisfies the following condition: For any a and b in G,

$$a * b = b * a$$

Two important properties of groups:

1. The inverse of a group element is unique.
2. The identity element in a group G is unique.

Group examples

- $(Z_7, +, 0)$ is a group

[+]	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

- $(Z_2, +, 0)$ is a group

Order of Group: The number of elements in a group is known as the order of the group

- $(Z_m, +, 0)$ is a group
  - + is closed
  - Associative: (a + b) + c = a + (b + c)
  - Commutative: a + b = b + a (abelian group)
  - 0 is the identity for +: a + 0 = a + 0 = a
  - Additive inverse: (-a) + a = a + (-a) = 0

Group examples

Let p be a prime (e.g., p = 2, 3, 5, 7, 11, 13, 17, ...). Then (Zp-{0}, ×, 1) = ({1, 2, ..., p-1}, ×, 1) is a multiplicative (modulo-p) group.

Proof: Let $a \in Z_p$-{0}, Since $a < p$ and p is a prime, a and p must be relatively prime. By Euclidean theorem, there exist two integers i and j such that

$i \cdot a + j \cdot p = 1$ ⇒ $i \cdot a = -j \cdot p + 1 = 1 \pmod{p}$ ⇒ $a^{-1} = i \pmod{p}$

- (Z_7-{0}, ×, 1) is a group

[·]	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Euclidean Theorem

The Euclidean Algorithm (to compute $\gcd(r_0, r_1)$)

$$r_0 = q_1 r_1 + r_2, \quad 0 \le r_2 < r_1$$
$$r_1 = q_2 r_2 + r_3, \quad 0 \le r_3 < r_2$$
$$\dots$$
$$r_{m-2} = q_{m-1} r_{m-1} + r_m, \quad 0 \le r_m < r_{m-1}$$
$$r_{m-1} = q_m r_m + 0$$

$\rightarrow \gcd(r_0, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_{m-2}, r_{m-1}) = \gcd(r_{m-1}, r_m) = r_m$

$\rightarrow \gcd(r_0, r_1) = r_m$

The Extended Euclidean Algorithm (to find the inverse of $r_1 \in Z_n$, $(n=r_0)$)

1. Perform the Euclidean Algorithm for r_0 and r_1. Record the quotients $q_1, q_2, \dots, q_m$.
2. Compute $t_0, t_1, \dots, t_m$ recursively as follows

   $t_0 = 0, \qquad s_0 = 1$

   $t_1 = 1, \qquad s_1 = 0$

   $t_j = t_{j-2} - q_{j-1} t_{j-1},\ 2 \le j \le m, \qquad s_j = s_{j-2} - q_{j-1} s_{j-1},\ 2 \le j \le m,$
3. $r_1^{-1} = t_m$.

Theorem 1 $r_j = s_j r_0 + t_j r_1$, for $0 \le j \le m$.

Corollary 2 If $\gcd(r_0, r_1) = 1$, then $r_1^{-1} = t_m \bmod r_0$

Example: Compute 3^{-1} in Z_7

$r_0 = 7, r_1 = 3$

$7 = 2 \times 3 + 1$
$3 = 3 \times 1 + 0$

$q_1 = 2, q_2 = 3$

$t_0 = 0$
$t_1 = 1$
$t_2 = 0 - 2 \times 1 = -2 = 5$

$3^{-1} = 5$ in Z_7

1. Perform the Euclidean Algorithm for r_0 and r_1
   $q_1, q_2, \ldots, q_m$.
2. Compute $t_0, t_1, \ldots, t_m$ recursively as follows
   $t_0 = 0$,
   $t_1 = 1$,
   $t_j = t_{j-2} - q_{j-1} t_{j-1}$, $2 \le j \le m$,
3. $r_1^{-1} = t_m$.

[·]	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Example: Compute 28^{-1} in Z_{75}

1. Perform the Euclidean Algorithm for r_0 and r_1
   $q_1, q_2, \ldots, q_m$.
2. Compute $t_0, t_1, \ldots, t_m$ recursively as follows
   $t_0 = 0$,
   $t_1 = 1$,
   $t_j = t_{j-2} - q_{j-1}t_{j-1}$, $2 \leq j \leq m$,
3. $r_1^{-1} = t_m$.

$r_0 = 75, r_1 = 28$

$75 = 2\times 28 + 19$
$28 = 1\times 19 + 9$
$19 = 2\times 18 + 1$
$9 = 9\times 1 + 0$

$q_1 = 2, q_2 = 1, q_3 = 2, q_4 = 9$

$t_0 = 0$
$t_1 = 1$
$t_2 = 0 - 2 \times 1 = -2$
$t_3 = 1 - 1 \times (-2) = 3$
$t_4 = -2 - 2 \times 3 = -8 = 67$

$28^{-1} = 67$ in Z_{75}

Field

- A set F is a Field
  - At least two elements $0, 1 \in F$
  - Two operations $+$ and $\times$ on F
  - Associative and commutative
  - Operation $\times$ distributes over $+$
  - 0 is the identity for $+$ and 1 for $\times$
  - Additive inverse and multiplicative inverse

Order of Field: The number of elements in a field is known as the *order* of the field. A field having finite number of elements is called a *finite field.*

Property 1: For every element a in a field, $a \times 0 = 0 \times a = 0$.

Property 2: For any two nonzero elements a and b in a field, $a \times b \neq 0$.

Property 3: For $a \neq 0$, $a \times b = a \times c$ implies that $b = c$.

Finite Field Examples

(Z_7, +, ×, 0, 1) is a Field

Example:
Evaluate $((2 - 4) \times 4)/3$ in the field Z_7

[+]	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

[·]	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- (Z_p, +, ×, 0, 1) is a Field (when p is a prime number.)
  - +, × are closed
  - +, × are associative and commutative
  - Operation × distributes over +
  - 0 is the identity for + and 1 for ×
  - Additive inverse and multiplicative inverse