Modern Cryptography

Mathematical Prerequisites (For the students with no mathematics background)

Aug 20, 2025

Shashank Singh

Integer Arithmetic

Integer Arithmetic

Integer Arithmetics: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Addition ($+$), For all $a, b, c \in \mathbb{Z}$	Multiplication ($\cdot$), $\forall a, b, c \in \mathbb{Z}$
• $a + b = c \in \mathbb{Z}$. • $(a + b) + c = a + (b + c)$ • $\exists 0 \in \mathbb{Z}, a + 0 = 0 + a = a$ • $\exists(-a) \in \mathbb{Z}, a + (-a) = 0$	• $a \cdot b = c \in \mathbb{Z}$. • $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ • $\exists 1 \in \mathbb{Z}, a \cdot 1 = 1 \cdot a = a$
• $a + b = b + a$	• $a \cdot b = b \cdot a$

☛ $(\mathbb{Z}, +)$ is an Abelian group.

☛ $(\mathbb{Z}, \cdot)$ is a semi-group with (multiplicative) identity 1.

Group

Consider a set G and an operation $\star : G \times G \to G$ defined on G. Then $(G, \star)$ is called a group if the following hold:

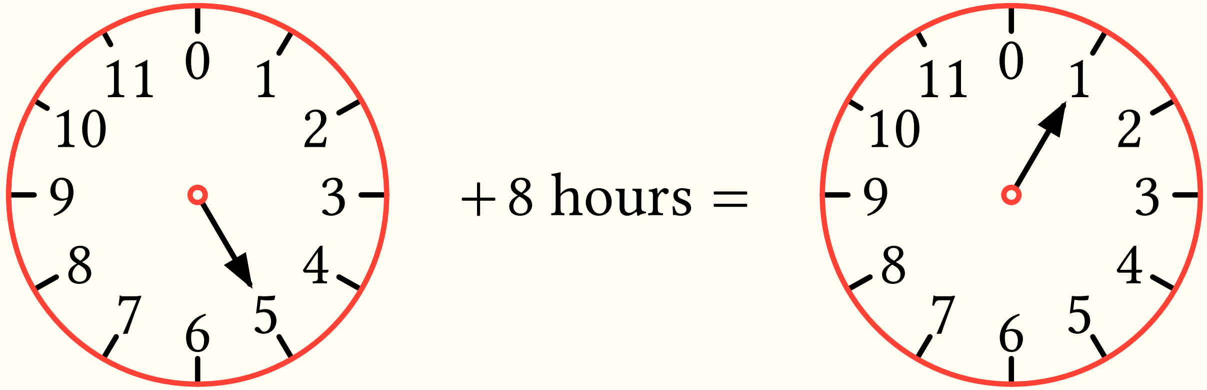
1. **Closure of G under $\star$**: $\forall x, y \in G,\ x \star y \in G$.
2. **Associativity**: $\forall x, y, z \in G,\ (x \star y) \star z = x \star (y \star z)$
3. **Identity element**: $\exists e \in G : x \star e = e \star x = x \forall x \in G$.
4. **Inverse element**: $\forall x \in G, \exists y \in G : x \star y = y \star x = e$, where e is the identity element.

If additionally $\forall x, y \in G, x \star y = y \star x$, then $(G, \star)$ is called an Abelian group (or a commutative group).

Examples: $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$ are groups. $(\mathbb{Z}, \cdot)$ is not a group (why?).

Clock Arithmetics

Clock Arithmetics



Consider the set $\mathbb{Z}_{12} = \{1, 2, 3, ..., 11, 0(= 12)\}$.

- Define a binary operation $\oplus : \mathbb{Z}_{12} \times \mathbb{Z}_{12} \to \mathbb{Z}_{12}$, such that

$$a \oplus b = b \text{ hours after } a \text{ o'clock}$$

- Is $(\mathbb{Z}_{12}, \oplus)$ a group?

Clock Arithmetics..

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, \ldots, 11\}.$$

For $a, b \in \mathbb{Z}_{12}$, define

$$\begin{aligned} a \oplus b &= \text{remainder when } (a+b) \text{ is divided by } 12 \\ &\equiv (a+b) \bmod 12. \text{ (Notation)} \end{aligned}$$

Similarly,

$$\begin{aligned} a \odot b &= \text{remainder when } (a \cdot b) \text{ is divided by } 12 \\ &\equiv (a \cdot b) \bmod 12. \text{ (Recall the Notation)} \end{aligned}$$

Question: Does $(\mathbb{Z}_{12}, \oplus)$ form a group?

What about $(\mathbb{Z}_{12}, \odot)$?

Modular Arithmetics

Modular Arithmetic

Let $n \in \mathbb{N}$. Define,

$$\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n - 1\}.$$

For $a, b \in \mathbb{Z}_n$, define

$$a \oplus b := (a + b) \bmod n$$
$$a \odot b := (a \cdot b) \bmod n.$$

Exercise:
1. Show that $(\mathbb{Z}_n, \oplus)$ is an Abelian group.
2. Show that $(\mathbb{Z}_n, \odot)$ is a semi-group. Note that a set together with a binary operation is called a semi group if the binary operation is associative.

Exercise: If $p \in \mathbb{N}$ is a prime, then $\left(\left(\mathbb{Z}_p\right)^*, \odot\right)$ is an Abelian group.

Proof:

$$\left(\mathbb{Z}_p\right)^* = \{1, 2, ..., p - 1\}$$

For $a, b \in \left(\mathbb{Z}_p\right)^*$, we have

1. $a \odot b = a \cdot b \pmod p \in \left(\mathbb{Z}_p\right)^*$.
2. $$\begin{aligned}(a \odot b) \odot c &= a \cdot b \,(\text{mod } p) \odot c \\ &= (ab + pt) \odot c = (ab + pt)c \,(\text{mod } p) \\ &= abc \,(\text{mod } p) = a \odot (b \odot c)\end{aligned}$$
3. 1 is the identity element.
4. For $a \in \left(\mathbb{Z}_p\right)^*$, $\gcd(a, p) = 1 \Rightarrow ax + py \equiv 1 \bmod p$, hence $a^{-1} = x \bmod p$.

□

Exercise: Find $\frac{1}{5}$ in $(\mathbb{Z}_{17}^{*}, \odot)$.

Solution:

As 17 is a prime, $\gcd(5, 17) = 1$. In fact, we compute the GCD as follows:

$$\begin{aligned} 17 &= 5 \times 3 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 1 \times 2 + 0. \end{aligned} \tag{1}$$

Thus,

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - (17 - 5 \times 3) \times 2 \\ &= 5 \times 7 + 17 \times (-2) \end{aligned}$$

Hence $1 = 5 \times 7 \bmod 17$, i.e., $5 \odot 7 = 1$ and so $\frac{1}{7} = 5$ in $\mathbb{Z}_{17}$.

Order of an element in Finite Groups

We have now seen some examples of finite groups. Let $(G, \cdot)$ be a group with $|G| = n$ and $1 \in G$ is the identity element.

- The number of elements in the finite set G is called the order of the group $(G, \cdot)$. We represent it using $o(G)$.
- For $g \in G$, we can define the order $o(g)$ of the element g in the group $(G, \cdot)$ as the smallest positive integer ℓ such that

$$g^{\ell} := \underbrace{g \cdot g \cdot g......g \cdot g}_{\ell \text{ times}} = 1.$$

and we write $o(g) = \ell$. (*Why does it even exit?*)

Consider the set $G' = \{g^i : 1 \le i \le o(G)\}$

- Note that $G' \subset G$.
- If all the elements in G' are distinct, $G' = G$ and $1 \in G'$ and hence there is a t such that $g^t = 1$.
- If the elements in G' are not distinct, there exists $s > t \in \mathbb{N}$ such that $g^s = g^t$ implying $g^{s-t} = 1$.
- The smallest exponent ℓ such that $g^\ell = 1$ is called the order of g.

$$o(g) = \inf\{\ell : g^\ell = 1, \ell \in \mathbb{N}\}$$

***Remark**: Such an ℓ always exists in finite groups. In infinite groups such an ℓ may not exist, in that case, order of g is infinite.*

Cyclic Group

Let $(G, \cdot)$ be finite group with $o(G) = n$. For $g \in G$, define

$$\langle g \rangle := \left\{ g^i \mid 1 \leq i \leq n \right\} \subset G.$$

Cyclic Group

Let $(G, \cdot)$ be finite group with $o(G) = n$. For $g \in G$, define

$$\langle g \rangle := \left\{ g^i \mid 1 \leq i \leq n \right\} \subset G.$$

Exercise: Show that $(\langle g \rangle, \cdot)$ is group. The group $(\langle g \rangle, \cdot)$ is called a **cyclic subgroup** of the group $(G, \cdot)$ generated by an element g of G.

Remark: The cyclic subgroup generated by an element $g \in G$, can be defined for infinite groups as well.

$$\langle g \rangle := \left\{ g^i \mid i \in \mathbb{Z} \right\} \subset G.$$

Example. Consider the set

$$(\mathbb{Z}_{13})^{*} = \{1, 2, \ldots, 12\}$$

and a binary operation $\odot$, which is multiplication modulo 13.

$$\langle 4 \rangle = \{4, 3, 12, 9, 10, 1\}$$
$$\langle 5 \rangle = \{5, 12, 8, 1\}$$

Cyclic Group..

Definition: A group $(G, \cdot)$ is said to be cyclic group if there exists a $g \in G$ such that $G = \langle g \rangle$.

Example. Consider the set $(\mathbb{Z}_{13})^* = \{1, 2, ..., 12\}$ and a binary operation $\odot$, which is multiplication modulo 13.

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

Thus $(\mathbb{Z}_{13})^*$ is a cyclic group generated by 2.

- ☛ In a finite cyclic group $G = \langle g \rangle$, every element of G can be written as some power of the generator g.
- ☛ $g^{o(G)} = 1$ in a finite cyclic group $G = \langle g \rangle$. **(Proof?)**

Exercise: Show that $g^{o(G)} = 1$ in a finite cyclic group $G = \langle g \rangle$..

Discrete Logarithm Problem

Definition: Let $(G, \cdot) = \langle g \rangle$ be a finite cyclic group of order n, i.e. $o(G) = n$, and $h \in G$. We can write h as

$$h = g^e = \underbrace{g \cdot g \cdot g ......g \cdot g}_{e \text{ times}},$$

for some $e \in \mathbb{Z}_n$. We call e the discrete logarithm of h to the base g and write $e = \log_g h.$

Remark: We also use the notation $\mathbb{Z}_n$ for $\mathbb{Z}_n$, use simple $\cdot$ to represent the binary op $\odot$ and often write ab to mean $a \cdot b$.

Exercise: In the group $(\mathbb{Z}_{13}^*, \cdot)$, calculate $\log_2 5$?

Example of a cyclic group

Theorem: If $p \in \mathbb{Z}^+$ is a prime, the $\left(\mathbb{Z}_p^*, \cdot\right)$ is a cyclic group of order $(p - 1)$.

Example of a cyclic group

Theorem: If $p \in \mathbb{Z}^+$ is a prime, the $\left(\mathbb{Z}_p^*, \cdot\right)$ is a cyclic group of order $(p-1)$.

Let

$$\begin{aligned} p = {} & 124620366781718784065835044608106590434820374651678805754818788883289666801188210855036039570272508747509864768438458621054865537970253930571891217684318286362846948405301614416430468066875699415246993185704183030512549594371372159029285303, \end{aligned}$$

$\left(\mathbb{Z}_p^\star, \cdot\right) = \langle 5 \rangle$

Finte Ring and Finite Field

- Recall, $(\mathbb{Z}, +)$ is an Abelian group and $(\mathbb{Z}^\star, \cdot)$ is a semi-group.
  - Multiplication can be performed in $\mathbb{Z}$, but division (inverse of multiplication) is not always possible, i.e., when we divide an integer by another, the result is not always an integer.
  - In other words $\frac{1}{a} \notin \mathbb{Z}\ \forall a \in \mathbb{Z}$, however this is true for rationals.
- The structure $(\mathbb{Q}, +, \cdot)$, where addition, inverse of addition (subtraction), multiplication and division(inverse of multiplication), all can be performed, and $\cdot$ is distributive over $+$, is termed a Field. Similarly, $(\mathbb{Z}, +, \cdot)$ is an example of a Ring.
- More precise mathematical definitions of Ring and Field are presented below.

Definition: (Ring)

A ring $(R, +, \cdot)$ is a set R, which is CLOSED under two operations $+$ and $\cdot$, and satisfying the following properties:

- $(R, +)$ is an Abelian group.
- The binary operation $\cdot$ is associative in R i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$
- The operation $\cdot$ is distributive over $+$ i.e.,

$$\begin{aligned} (a + b) \cdot c &= (a \cdot c) + (b \cdot c) \\ a \cdot (b + c) &= (a \cdot b) + (b \cdot c) \quad \forall a, b, c \in \mathbb{Z}. \end{aligned}$$

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are very common examples of a Ring.
- The set of all $n \times n$ matrices with entries from a ring (or even a field) forms a ring under matrix addition and matrix multiplication.
- $(\mathbb{Z}_n, \oplus, \odot)$ forms a ring as well. (prove it)

Field

Definition: (Field)
A field $(F, +, \cdot)$ is a ring with multiplicative identity, where every non-zero element of F has a multiplicative inverse.

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are fields.
- $(\mathbb{Z}, +, \cdot)$ is not a field and so is $(\mathbb{Z}_n, \oplus, \odot)$.

> **Question:** Is there a field with finitely many elements?

Finite Fields

- $(\mathbb{Z}_n, \oplus, \odot)$, where p is a prime, is a field.
  - Compute $\frac{1}{7}$, i.e., 7^{-1} in $(\mathbb{Z}_7, \oplus, \odot)$. What is the value of $\frac{3}{7}$ in $\mathbb{Z}_7$?

Example: Let $F_4 = \{0, 1, x, 1 + x\}$, with two binary operations $+$ and $\cdot$, defined as follows:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	c
d	a	d	c	b

Show that $(F_4, +, \cdot)$ is a field. Note that, it has 4 elements.

Question: Is there a field consisting of 6 elements? Justify your answer.

Finite Field of Order p^n

- Let F_p be a finite field $\left(\mathbb{Z}_p, +, \cdot\right)$ and $f(x) \in F_p[x]$ be a monic irreducible polynomial of degree n.
- Let $F_{p^n} = \left\{g(x) \in F_p[x] : \deg(g(x)) \leq n - 1\right\}$, define binary operations $\oplus$ and $\odot$ on F_{p^n} as follows:

$$g_1(x) \oplus g_2(x) = g_1(x) + g_2(x) \bmod f(x)$$
$$g_1(x) \odot g_2(x) = g_1(x) \cdot g_2(x) \bmod f(x)$$

- $\left(F_{p^n}, \oplus, \odot\right)$, as described above forms a finite field of order p^n.

Remarks:
- The number of elements in any finite field is equal to p^n for some prime p and positive integer n.
- Two finite fields of the same order are isomorphic, i.e., they behave in the same fashion modulo a mapping of elements.

Example: Let $F_4 := \frac{F_2[x]}{\langle x^2+x+1\rangle} = \{0, 1, x, 1+x\}$, with two binary operations $+$ and $\cdot$, defined modulo $x^2 + x + 1$ as follows:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$x+1$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	x
$1+x$	0	$1+x$	x	1