Shift ciphers using modular arithmetic

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1.7: Assigning numbers to letters

Encryption : plaintext + k mod 26

Decryption : ciphertext − k mod 26

ciphertext + (−k) mod 26

$-k \equiv 26-k \mod 26$

$-1 \equiv 25 \mod 26$

$-2 \equiv 24 \mod 26$

$\mathbb{Z}/26\mathbb{Z} = \{0, 1, 2, \ldots, 25\} = \mathbb{Z}_{26}$

Set of reminders modulo 26

operation + that add two integer, reduce modulo 26

closure

$\forall a, b \in \mathbb{Z}_{26}$

$a+b \in \mathbb{Z}_{26}$

$e_k(m) = m + k \mod 26, \ m \in \mathbb{Z}_{26}$

$d_k(c) = c + (-k) \mod 26, \ c \in \mathbb{Z}_{26}$

$a = 1$

$b = 25$

$a+b = 26 \equiv 0 \mod 26$

To prove that d_k is inverse of e_k:

w.t.s : $d_k(c) = m$ if $c = e_k(m)$

Proof: Let $c = e_k(m) = m+k \mod 26$

$$
\begin{aligned}
d_k(c) &= d_k(m+k) \\
&= (m+k) + (-k) \mod 26 \\
&= m + (k + (-k)) \mod 26 && \text{associative} \\
&= m + 0 \mod 26 && \text{inverse} \\
&= m \mod 26 && \text{identity}
\end{aligned}
$$

Definition of Group

G be a set of elements with operation $\cdot$

and satisfy:

closure : $a \cdot b \in G \quad \forall a, b \in G$

identity : $e \in G$ such that $e \cdot a = a \cdot e = a$, $\forall a \in G$

inverse : b is inverse of a if $a \cdot b = b \cdot a = e$, $\forall a \in G$
$b \in G$

associative : $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$,

$(G, \cdot)$ is a group.

Outline

1) Definition of group
   - closure
   - identity
   - inverse
   - associative

2) Finite vs infinite, order of a group

3) Abelian vs non-abelian

4) Operation table

5) Direct product

6) Isomorphism

Examples

① $(\mathbb{Z}_{26}, +)$ is a group of size 26

② $(\mathbb{Z}_n, +)$ is a group of size n.

$\mathbb{Z}_n$ = set of remainders modulo n $= \{0, 1, 2, \ldots, n-1\}$

③ $(\mathbb{Z}, +)$ is a group of infinite size:

closure : $\forall a, b \in \mathbb{Z}$, $a+b \in \mathbb{Z}$
identity : $0 \in \mathbb{Z}$ and $0+a = a+0 = a$ $\forall a \in \mathbb{Z}$
inverse : $\forall a \in \mathbb{Z}$, $-a \in \mathbb{Z}$ and $a+(-a) = 0$
associative : $\forall a, b, c \in \mathbb{Z}$: $(a+b)+c$ is equal to $a+(b+c)$

④ $(\mathbb{Z}, *)$ is not a group.
↖ integer multiplication
identity = 1, $1 * a = a * 1 = a$ $\forall a \in \mathbb{Z}$
$2 \in \mathbb{Z}$ $2 * b = 1$ if $b = \frac{1}{2} \notin \mathbb{Z}$

There is no inverse for 2.

Finite group vs Infinite group

Definition: If $(G, \cdot)$ is a group of size n, then the order of G is n.

Abelian vs non-abelian

In $(\mathbb{Z}_{26}, +)$: $a+b = b+a \quad \forall\, a, b \in \mathbb{Z}_{26}$ commutative

A group that satisfy commutativity is a abelian group.

Homework

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$$

With operation $* =$ matrix multiplication is a non-abelian group.

(matrix multiplication is not commutative: $A * B \neq B * A$ for some matrices A, B)

Operation table

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

0 is identity

each row has identity 0

Observation:

1. unique identity
2. unique inverse

Lemma

Given a group $(G, \cdot)$, show that

(a) the identity of $(G, \cdot)$ is unique

If there are two identities e, f

$e \cdot a = a \cdot e = a$

$f \cdot a = a f = a$

show that e is equal to f

(b) $\forall a \in G$, the inverse of a is unique.

Direct product

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +) = \{(a, b) \mid a \in \mathbb{Z}_2, b \in \mathbb{Z}_3\}$

$= \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$ of order 6

$(a,b), (c,d) \in (\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$

$(a,b) \times (c,d) = (a+c, b+d)$

Two groups $(G, \cdot)$, $(H, *)$, we can create a group $(G, \cdot) \times (H, *)$

$= \{(g,h) \mid g \in G, h \in H\}$

with ~~operation~~ $\times$ such that

$(g,h) \times (g',h') = (g \cdot g', h * h')$

---

order of $(G, \cdot) \times (H, *)$ = order of $(G, \cdot)$ $\times$ order of $(H, *)$

Proof that $(G, .) \times (H, *)$ is a group

closure : $(g, h), (g', h') \in (G, .) \times (H, *)$

$$(g, h) \times (g', h') = (g.g', h * h') \in G \times H$$

$$g.g' \in G$$
$$h * h' \in H$$

identity: $(e_G, e_H) \times (g, h) = (e_G . g, e_H * h) \quad \forall g \in G, h \in H$

$$= (g, h)$$

$$(g, h) \times (e_G, e_H) = (g.e_G, h * e_H)$$
$$= (g, h)$$

inverse : $\forall g \in G, h \in H,$

$\exists$ inverse for g denoted as g^{-1}

inverse for h denoted as h^{-1}

$$(g, h) \times (g^{-1}, h^{-1}) = (g \cdot g^{-1}, h * h^{-1})$$
$$= (e_G, e_H)$$

$$(g^{-1}, h^{-1}) \times (g, h) = (e_G, e_H)$$

associative : operation is element-wise

Isomorphism

Two groups G, H are isomorphic if

there exists a bijective map from elements in G to

elements in H that preserve the operations of

the group elements.

$$f : (G, \cdot) \longrightarrow (H, *)$$

$\forall\, g, g' \in G$

$$f(g \cdot g') = f(g) * f(g')$$

If $g \cdot g' = \bar{g}$

then

$$f(g) * f(g') = f(\bar{g})$$

Examples

1) $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$ is isomorphic to $(\mathbb{Z}_3, +) \times (\mathbb{Z}_2, +)$

2) $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$ is isomorphic to $(\mathbb{Z}_6, +)$

3) $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ is not isomorphic to $(\mathbb{Z}_4, +)$

1) $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$ is isomorphic with $(\mathbb{Z}_3, +) \times (\mathbb{Z}_2, +)$

$(0,0) \xrightarrow{f} (0,0)$

$(0,1) \longrightarrow (1,0)$

$(0,2) \longrightarrow (2,0)$

$(1,0) \longrightarrow (0,1)$

$(1,1) \longrightarrow (1,1)$

$(1,2) \longrightarrow (2,1)$

Let $f((a,b)) = (b,a)$

show that f preserves the operations.

$(\mathbb{Z}_6, +)$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$

•	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(2,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)