# Outline

① Order of element

② Lagrange theorem

③ cyclic group, generator

$(\mathbb{Z}_4, +)$ is a cyclic group generated 1.

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ is not a cyclic group.

$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ iff $\gcd(m,n) = 1$

Chinese Remainder Theorem

integer multiplication

④ Observation:

$(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is a group

$(\mathbb{Z}_6 \setminus \{0\}, \cdot)$ is not a group

$\mathbb{Z}_6^* = \{1, 5\}$

$(\mathbb{Z}_6^*, \cdot)$ is a group.

$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \underline{\gcd(a,n) = 1}\}$

$(\mathbb{Z}_n^*, \cdot)$ is a group

In $\mathbb{Z}_6$

$0 = 0$

$1+1+1+1+1+1 = 0$

How many times g operate on itself to reach identity?

$2+2+2 = 0$

$3+3 = 0$

$4+4+4 = 0$

$5+5+5+5+5 = 0$

---

In $\mathbb{Z}_2 \times \mathbb{Z}_3$

$(0,0) = (0,0)$

$(0,1)+(0,1)+(0,1) = (0,0)$

$(1,0)+(1,0) = (0,0)$

$(0,2)+(0,2)+(0,2) = (0,0)$

$(1,1)+(1,1)+(1,1)+(1,1)+(1,1)+(1,1) = (0,0)$

$(1,2)+(1,2)+(1,2)+(1,2)+(1,2)+(1,2) = (0,0)$

$\mathbb{Z}_6$

| $g$ | order / minimum # of times $g$ operates on itself to get to $e$ |
|---|---|
| 0 | x |
| 1 | 6 |
| 2 | 3 |
| 3 | 2 |
| 4 | 3 |
| 5 | 6 |

$\mathbb{Z}_2 \times \mathbb{Z}_3$

| $g$ | order / minimum # of times $g$ operates on itself to get to $e$ |
|---|---|
| $(0,0)$ | x |
| $(0,1)$ | 3 |
| $(1,0)$ | 2 |
| $(0,2)$ | 3 |
| $(1,1)$ | 6 |
| $(1,2)$ | 6 |

If $f$ is an isomorphism map between $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$, then $f$ should preserve the minimum # of times $g$ operates on itself to get to $e$ / order of $g$

$f$ must map 3 to $(1,0)$ since 3 and $(1,0)$ are the only elements with order 3.

Write $(a,b) = a(1,0) + b(0,1)$

$$f((a,b)) = af((1,0)) + bf((0,1))$$

$$= 3a + 2b \quad \text{or} \quad 3a + 4b$$

since $(0,1)$ is of order 3 and the only elements of order 2 in $\mathbb{Z}_6$ is 2 and 4.

# Order of group element

Given a finite group $G$.

For all element $g \in G$, there exists integer $d$

such that $g^d = e$.

The smallest such $d$ is called order of $g$.

## Notations

$(G, \cdot)$ multiplicatively

$$g^d = \underbrace{g \cdot g \cdot g \cdot g \cdots g}_{d \text{ times}}$$

$(G, +)$ additively

$$d \cdot g = \underbrace{g + g + g + \cdots + g}_{d \text{ times}}$$

$(\mathbb{Z}, +)$ is a group.

$1 \in \mathbb{Z}$. $1+1+\ldots\ldots\ldots \neq 0$

1 has no finite order

---

Existence of finite order for all $g \in G$ when $G$ is finite:

---

Let $g \in G$, we list down all elements of $g^i$

$$g, g^2, g^3, \ldots g^i \ldots$$

Since $G$ is finite, there exits $i$ and $j$ such that

$$g^i = g^j$$

Let $g^{-1}$ be the inverse of $g$.

$$g^{-j} = g^{-1} \cdot g^{-1} \cdot g^{-1} \ldots g^{-1} \quad (j \text{ times})$$

$$g^i \cdot g^{-j} = g^j \cdot g^{-j}$$

$$g^{i-j} = e$$

Hence, when $G$ is finite, $\exists$ integer $d = i-j$ such that $g^d = e$.

# Properties of group elements

Let $G$ be a finite abelian group.

① Let $d$ be the order of $g \in G$,

$$g^f = e \text{ iff } d \text{ divides } f.$$

Lagrange
② $d$ divides $|G|$.

③ In particular, $\forall g \in G$, $g^{|G|} = e$

① $\Rightarrow$ If $d$ divides $f$, $f = dq$, $q \in \mathbb{Z}$

$$g^f = g^{dq} = (g^d)^q = e^q = e$$

$\Leftarrow$ Prove by contradiction. If $g^f = e$.

If $d \nmid f$, $f = dq + r$, $1 \le r \le d-1$

$$g^f = g^{dq+r} = g^{dq} \cdot g^r = g^r = e$$

But $g^r \neq e$ because $d$ by def should be the smallest such integer. Contradiction.

(2) $G = \{g_1, g_2, \ldots, g_n\}$ $|G| = n$

Let $a \in G$

$aG = \{ag_1, ag_2, \ldots, ag_n\}$

Note that $aG = G$.

E.g. $3(\mathbb{Z}_6, +) = \{3+0, 3+1, 3+2, 3+3, 3+4, 3+5\}$

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

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

Take the product of all element in $aG$ and $G$ respectively.

$g_1 g_2 \ldots g_n = ag_1 . ag_2 . \ldots . ag_n$ abelian

$g_1 g_2 \ldots g_n = a^n \underline{g_1 \ldots g_n}$

$a^n = e$ (multiplying both sides by $(g_1 \ldots g_n)^{-1}$)

By property (1), order of $a$ must divides $n$

(3) $\forall g \in G, g^{|G|} = e$.

Let $d = ord(g)$, the order of $g$

By definition, $g^d = e$

By property (2), $d \mid |G|$. Hence, $|G| = dd'$ for $d' \in \mathbb{Z}$. $g^{|G|} = g^{d.d'} = (e)^{d'} = e$.

# Cyclic group

Given a finite group $G$. If there exists an element $g \in G$ such that order of $g$ is $|G|$, then $G$ is a cyclic group.

$g$ is called the generator of $G$.

In particular, $ord(g)$ must be $|G|$.

---

In $(\mathbb{Z}_6, +)$, order of $1$ is $6$.

$1$ is a generator of $\mathbb{Z}_6$

$\mathbb{Z}_6$ is a cyclic group.

In $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ is not a cyclic group.

| | order |
|---|---|
| $(1,0)$ | $2$ |
| $(0,1)$ | $2$ |
| $(1,1)$ | $2$ |
| $(0,0)$ | $\times$ |

All non-identity elements have order $2$.

# Chinese Remainder Theorem (Simple case)

Let $m_1, m_2$ such that $m_1$ and $m_2$ are coprime.
(no common divisors)

then there exist unique solution $x$ to the following:

$$x \equiv x_1 \mod m_1$$
$$x \equiv x_2 \mod m_2$$

Equivalently,

If $N = m_1 m_2$ where $m_1$ and $m_2$ are coprime
then $f : \mathbb{Z}_N \longleftrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$

$$x \longleftrightarrow (x \mod m_1, x \mod m_2)$$

$f$ is bijective.

---

(E.g) $f: \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$

$$1 \to (1, 1)$$
$$2 \to (0, 2)$$
$$3 \to (1, 0)$$
$$4 \to (0, 1)$$
$$5 \to (1, 2)$$
$$0 \to (0, 0)$$

# General statement for Chinese Remainder Theorem

Let $N = m_1 m_2 \ldots m_k$ where $\gcd(m_i, m_j) = 1, i \neq j$

(i.e., all of the $m_i$'s pairwise coprime)

The map

$$f : \mathbb{Z}_N \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$$

$$x \longmapsto (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k)$$

is a bijective map.

---

Equivalently:

Let $m_1, m_2, \ldots, m_k$ be pairwise coprime integers.

There exists a unique solution $x$ to the following:

$$x \equiv x_1 \bmod m_1$$

$$x \equiv x_2 \bmod m_2$$

$$\vdots$$

$$x \equiv x_k \bmod m_k$$

for any given integers $x_1, x_2, \ldots, x_k$

# Consequence of Chinese Remainder Theorem

① $$\mathbb{Z}_N \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$$

when $N = m_1 m_2 \cdots m_k$

where $\gcd(m_i, m_j) = 1$ if $i \neq j$

② $$\mathbb{Z}_N^* = \{ a \in \mathbb{Z}_N \mid \gcd(a, N) = 1 \}$$

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*$$

$$|\mathbb{Z}_N^*| = |\mathbb{Z}_{m_1}^*| \times |\mathbb{Z}_{m_2}^*| \cdots \times |\mathbb{Z}_{m_k}^*|$$

$$\varphi(N) = \varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_k)$$

# Proof Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k$ be pairwise coprime integers.
There exists a unique solution $x$ to the following:

$$x \equiv x_1 \bmod m_1$$

$$x \equiv x_2 \bmod m_2$$

$$\vdots$$

$$x \equiv x_k \bmod m_k$$

for any given integers $x_1, x_2, \ldots, x_k$

---

We need to show existence and uniqueness

① Unique (special case where $k=2$)

(can be generalize to any value of $k$)

If $x, y$ satisfy the congruences

we want to show that $x \equiv y \mod m_1 m_2$

---

(1) $x \equiv x_1 \mod m_1$

(2) $x \equiv x_2 \mod m_2$

(3) $y \equiv x_1 \mod m_1$

(4) $y \equiv x_2 \mod m_2$

---

(1)-(3) $x - y \equiv 0 \mod m_1$

(2)-(4) $x - y \equiv 0 \mod m_2$

---

$m_1 \mid x - y$

$m_2 \mid x - y$

Because $\gcd(m_1, m_2) = 1$

$m_1 m_2 \mid x - y \rightarrow x \equiv y \mod m_1 m_2$

## ② Existence (non-construction proof)

Let $m_1, m_2, \ldots, m_k$ be pairwise coprime integers.
There exists a unique solution $x$ to the following:

$$x \equiv x_1 \mod m_1$$

$$x \equiv x_2 \mod m_2$$

$$\vdots$$

$$x \equiv x_k \mod m_k$$

for any given integers $x_1, x_2, \ldots, x_k$

---

Proof:

Define the map

$$f : x \longrightarrow (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k)$$

By uniqueness shown in ①, $f$ is a 1-1 map between $\mathbb{Z}_N$ and $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$

where $N = m_1 m_2 \ldots m_k$.

Since $\mathbb{Z}_N$ contains $N$ elements and

$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ contains $N$ elements, the map $f$ is also onto.

This means $\exists\ x \in \mathbb{Z}_N$ such that

$f(x) = (x_1, x_2, \ldots, x_k)$ for all integers $x_i$.

# Revision : One-to-One and Onto

Let $f$ be a function from $X$ to $Y$.

1. $f$ is one-to-one | injective if

   $f(x) = f(y)$ implies that $x = y$

2. $f$ is onto | surjective if $\forall y \in Y$,

   $\exists\, x \in X$ such that $f(x) = y$

3. If $f$ is one-to-one and $|X| = |Y|$,

   then $f$ is onto.

# Euler Totient function, $\varphi$

$\varphi(n)=$ number of integers between 1 to $n-1$ that are coprime with $n$.

From homework 2,

$\varphi(p) = p-1$

$\varphi(p^k) = p^k - p^{k-1}$

$\varphi(mn) = \varphi(m)\varphi(n)$ when $\gcd(m,n)=1$

# Homework 1

1. Prove that

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

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

2a. Make multiplication table for $\mathbb{Z}_5$.

b. Show that $(\mathbb{Z}_5, \cdot)$ is not a group.

integer multiplication

c. Show that $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is a group.

omit the 0 element

3a. Make multiplication table for $\mathbb{Z}_6$

b. Show that $(\mathbb{Z}_6 \setminus \{0\}, \cdot)$ is not a group.

4a. Make operation tables for $(\mathbb{Z}_6, +)$ and $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$.

b. Show that they are isomorphic.

5a. Make operation tables for $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$.

b. Show that they are not isomorphic.

# Homework 2

1. Compute the following values :

$\varphi$ : Euler tortient function

(a) $\varphi(2)$, $\varphi(3)$, $\varphi(5)$

(b) $\varphi(2^2)$, $\varphi(3^2)$, $\varphi(5^2)$

(c) $\varphi(2^3)$, $\varphi(3^3)$, $\varphi(5^3)$

(d) $\varphi(6)$, $\varphi(10)$, $\varphi(15)$

Can you derive a formula for $\varphi(n)$ ?

Unique prime factorization

$$n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$p_i$ are prime

Examples

$6 = 2 \cdot 3$

$8 = 2^3$

$100 = 2^2 \cdot 5^2$

---

$$\varphi(n) = \varphi(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})$$

$$= \varphi(p_1^{a_1})\,\varphi(p_2^{a_2}) \cdots \varphi(p_n^{a_n})$$

$$= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots$$

$$(p_n^{a_n} - p_n^{a_n-1})$$

(9) $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$

$\varphi(p) = p-1$ when $p$ is prime.