Cyclic Group & DLP

Prof. Ashok K Bhateja

IIT Delhi

Group

Definition: A group $(G, *)$ consists of a set G with a binary operation $*$ on G satisfying the following

- Closure property: $a * b \in G \ \forall\ a, b \in G$
- Associativity: operation $*$ is associative. i.e. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
- Existence of Identity element: $\exists\ e \in G$ s.t. $e * a = a = a * e \ \forall\ a \in G$
- Existence of Inverse: For each $a \in G$ there exists an element $a^{-1} \in G$, s.t. $a * a^{-1} = e = a^{-1} * a$

- A group G is abelian (or commutative) if,

  $a * b = b * a \ \forall\ a, b \in G.$

Order of Group

- Definition: The number of elements in a finite group is called its order. A group G is finite if $|G|$ is finite.

  Examples:

  - $(Z_n, +_n)$ is a group of order n.
  - The set $(Z_n, \times_n)$ is not a group, since not all elements have multiplicative inverses.

- Set Z_n^* is a group of order $\varphi(n)$ under the operation of multiplication modulo n, with identity element 1.

Order of an element of a group

- Definition: Let $a \in Z_n^*$. The order of a, denoted ord (a), is the least positive integer k such that $a^k \equiv 1 \pmod{n}$.
- Fact: If the order of $a \in Z_n^*$ is k, and $a^s \equiv 1 \pmod{n}$, then k divides s. In particular, $k \mid \varphi(n)$.
- Example: $Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

  $\varphi(21) = \varphi(7)\varphi(3) = 12 = \left| Z_{21}^* \right|$. The orders of elements in Z_{21}^* are

$a \in Z_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
order of a	1	6	3	6	2	6	6	2	3	6	6	2

- In a finite group, the order of a group element divides the order of its group

Subgroup of a group

- Definition: A subset H of a group G is a subgroup of G if H is itself a group under the operation in G.

  Note: Every group G has at least two subgroups: G itself and the subgroup $\{e\}$, containing only the identity element. All other subgroups are said to be proper subgroups.

- Lagrange theorem: For any finite group G, the order of subgroup H of group G divides the order of G.

Cyclic Group

- A group G is called cyclic if, for $a \in G$, every element $x \in G$ is of the form a^n, where n is some integer. The element a is then called a generator of G.
- There can be more than one generator of a cyclic group.
- Every cyclic group is abelian.
- Ex: The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic.

  $G = \{ i, i^2, i^3, i^4\}$, $G = \{ -i, (-i)^2, (-i)^3, (-i)^4\}$,

  i and $-i$ are generators of G.

Theorem: If a finite group of order n contains an element of order n, the group must be cyclic.

Ex: $Z_7^* = \{1, 2, 3, 4, 5, 6\}, \times_7 \}$ is cyclic.

a	1	2	3	4	5	6
Order of a	1	3	6	3	6	2

O(3) = 6 and O(5) = 6.

Definition: Let $\alpha \in Z_n^*$. If the order of α is $\varphi(n)$, then α is said to be a generator or a primitive element of Z_n^* or primitive root modulo n.

3 and 5 are the primitive elements of Z_7^*.

Primitive root modulo *n*

n	Primitive roots
6	5
7	3, 5
9	2, 5
10	3, 7
11	2, 6, 7, 8
13	2, 6, 7, 11

Properties of generators of Z_n^*

- Z_n^* has a generator iff $n = 2, 4, p^k$ or $2p^k$, where p is an odd prime and $k \geq 1$. If p is a prime, then Z_p^* has a generator.
- If α is a generator of Z_n^*, then $Z_n^* = \{\alpha^i \bmod n \mid 0 \leq i \leq \varphi(n) - 1\}$.
- Suppose that α is a generator of Z_n^*. Then $\beta = \alpha^k \bmod n$ is also a generator of Z_n^* iff gcd $(k, \varphi(n)) = 1$. It follows that if Z_n^* is cyclic, then the number of generators is $\varphi(\varphi(n))$.

P3: If α is a generator of Z_n^*, then $\beta = \alpha^k \bmod n$ is also a generator of Z_n^* then gcd $(k, \varphi(n)) = 1$.

Proof: Given α is a generator of Z_n^*.

Let $\beta = \alpha^k \bmod n$ is also a generator of Z_n^*

$\alpha \in Z_n^*$

$\Rightarrow \alpha = (\alpha^k)^m = \alpha^{km}$

$\Rightarrow \alpha^{km-1} \equiv 1 \bmod n$

$\Rightarrow \varphi(n)$ divides $km - 1$

$\therefore km - 1 = q\varphi(n)$, where q is a positive integer

$\therefore km - q\varphi(n) = 1 \Rightarrow \gcd(k, \varphi(n)) = 1.$

P3: If α is a generator of Z_n^*, and gcd (k, $\varphi(n)$) = 1 then $\beta = \alpha^k \bmod n$ is also a generator of Z_n^*.

Proof: Given α is a generator of Z_n^* and gcd (k, $\varphi(n)$) = 1

gcd (k, $\varphi(n)$) = 1, therefore $\exists\ m$ & t s.t., $k\,t + m\,\varphi(n) = 1$

$\therefore \quad \alpha \equiv \alpha^{k\,t\,+\,m\,\varphi(n)} \bmod n$

$\Rightarrow \quad \alpha \equiv \alpha^{k\,t}\ (\alpha^{\varphi(n)})^{m} \bmod n$

$\Rightarrow \quad \alpha \equiv (\alpha^{k})^{t} \bmod n$

Thus, every power of α can be expressed as a power of α^k.

i.e., every element of Z_n^* can be expressed as power of α^k. Thus α^k is also a generator of Z_n^*.

Theorem: Every subgroup of a cyclic group is cyclic

Proof: Let G be a cyclic group $G = \langle a \rangle$

Let H be a proper subgroup of G. Therefore, the elements of H will be the integral powers of a.

Let m be the least positive integer such that $a^m \in H$

Let a^s be any arbitrary element of H.

$s = mq + r; \quad 0 \leq r < m$

$a^m \in H \Rightarrow (a^m)^q \in H \Rightarrow a^{-mq} \in H \Rightarrow a^{s-mq} \in H \Rightarrow a^r \in H$

Since m is the least positive integer, such that $a^m \in H$, therefore $r = 0$.

Hence $s = mq$, therefore $a^s = a^{mq} = (a^m)^q$

Hence every element of H can be written as $(a^m)^q$.

Therefore H is cyclic.

Theorem: Every group of prime order is cyclic.

Proof: Let p be a prime and G be a group of order p.

Then G contains more than one element.

Let $a \in G, a \neq e$

$\langle a \rangle$ contains more than one element.

The $|\langle a \rangle|$ divides $|G|$ i.e. p.

Since $|\langle a \rangle| > 1$ and $|\langle a \rangle|$ divides a prime, therefore $|\langle a \rangle| = p = |G|$

Implies $\langle a \rangle = G$.

Hence G is cyclic.

Examples: Groups of prime order

Consider Z_{11}^* a multiplicative group.

$H_1 = \{1, 3, 4, 5, 9\}$, ord $(H_1) = 5$

It is a group under $\times_{\text{mod } 11}$.

$H_1 = \{3^0, 3^1, 3^2, 3^3, 3^4\}$ under mod 11

$(H_1, \times_{\text{mod } 11})$ is a cyclic group.

$H_2 = \{1, 10\}$ is also cyclic group with $\times_{\text{mod } 11}$

Discrete logarithm

- Let G be a finite cyclic group of order n. Let α be a generator of G, and let $\beta \in G$. The discrete logarithm of β to the base α, denoted $\log_\alpha \beta$, is the unique integer x, $0 \leq x \leq n - 1$, s.t. $\beta = \alpha^x$.
- Ex: $\alpha = 3$ and $\beta = 19683$, since $3^9 = 19683$

  $\therefore \log_3 19683 = 9$

Discrete logarithm problem

- Definition DLP: Given a prime p, a generator α of Z_p^*, and an element $\beta \in Z_p^*$, find the integer x, $0 \leq x \leq p - 2$, s.t. $\alpha^x \equiv \beta \pmod{p}$.
- Example: Let $p = 97$. Z_{97}^* is a cyclic group of order 96.

  A generator of Z_{97}^* is $\alpha = 5$.

  Since $5^{32} \equiv 35 \pmod{97}$ therefore $\log_5 35 = 32$ in Z_{97}^* .
- Definition GDLP: Given a finite cyclic group G of order n, a generator α of G, and an element $\beta \in G$, find the integer x, $0 \leq x \leq n - 1$, such that $\alpha^x \equiv \beta \pmod{n}$.

Selecting cyclic group and generators

- The discrete log function is a one-way function (hard to compute) for some cyclic groups G.
- Z_p^* for a prime p, is a cyclic group
- Fact: Let G be a cyclic group and let $n = |G|$. Let $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime factorization of n, and let $n_i = n/p_i$ for $i = 1, ..., n$. Then $\alpha \in G$ is a generator of G if and only if for all $i = 1, ..., n$

$$\alpha^{n_i} \neq 1$$

- Fact. Let G be a cyclic group of order n and let α is a generator of Z_p^* . Then Gen $(G) = \{\alpha^i \in G$ s.t. gcd $(i, n) = 1\}$ and $|\text{Gen}(G)| = \varphi(n)$

References

- Topics in Algebra by I.N. Herstein
- Handbook on Applied Cryptography by Alfred J. Menezes, Pall C. van Oorschot, Scott A. Vanstone