Finite groups

Mathematical Cryptography,
Lectures 9 - 10

Contents

Multiplicative order of elements

If G is a finite group of order n, then by Euler's theorem, for any element $a \in G$ is $a^n = 1$ in G. However, for a particular a the number n may not be the smallest exponent to which we must power a to get 1.

Definition

Let $(G, \cdot)$ be a group with the identity element 1, $a \in G$.
The smallest positive integer $r > 0$ such that $a^r = 1$ in G is called the *multiplicative order of the element* a in G. We denote it $\mathrm{r}(a)$.
If no such $r \in \mathbb{N}$ exists, we say that a has an infinite order.

Example

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8, \}$, $|\mathbb{Z}_9^*| = \varphi(9) = 6$
$\mathrm{r}(8) = 2$, $\mathrm{r}(4) = 3$, $\mathrm{r}(2) = 6$

Multiplicative order of elements

Notes

- Knowledge of the order of a makes the exponentiation a^k in G easier: we can calculate modulo $\mathrm{r}(a)$ in the exponent.
- In the additive group $(G, +)$ with the identity element 0, the order of a is the smallest $r > 0$ such that $ra = \underbrace{a + \ldots + a}_{r \text{ times}} = 0$.
- The order of the element a in the group G equals to the order of the cyclic subgroup $\langle a \rangle$ generated by a. (This actually is an alternative definition.)

Multiplicative order of elements

Proposition

Let G be a finite group.
For each $a \in G$ holds $\mathrm{r}(a) \mid |G|$

Euler's Theorem

Let G be a finite group.
For each $a \in G$ is $a^{|G|} = 1$ in G.

Remark

Since, we have given a proof of the Euler's theorem only for abelian groups, but we did not need commutativity for the Lagrange's theorem. Thanks to it (due to the previous statement), we have prooved the Euler's theorem for non-commutative groups too.

Multiplicative order of elements

Proposition

Let G be a finite group, $a, b \in G$.

- $a^k = 1$ in G if and only if $\mathrm{r}(a) \mid k$
- $\mathrm{r}(a^{-1}) = \mathrm{r}(a)$
- Let G be an Abelian group (or at least $ab = ba$).
  If $\mathrm{r}(a)$, $\mathrm{r}(b)$ are relatively prime, then $\mathrm{r}(ab) = \mathrm{r}(a)\,\mathrm{r}(b)$.

Proposition

Let G_1, G_2 be finite groups, $(a_1, a_2) \in G_1 \times G_2$.

- $\mathrm{r}(a_1, a_2) = \mathrm{lcm}(\mathrm{r}(a_1), \mathrm{r}(a_2))$

Multiplicative order of elements

Proposition

Let G be a finite group, $a \in G$.

- $\mathrm{r}(a^k) = \frac{\mathrm{r}(a)}{\gcd(k, \mathrm{r}(a))}$
- Especially, if $d \mid \mathrm{r}(a)$ then $r(a^d) = \frac{\mathrm{r}(a)}{d}$.

Consequence

- $\mathrm{r}(a^k) = \mathrm{r}(a)$ if and only if $\gcd(k, \mathrm{r}(a)) = 1$
- The number of generators of a cyclic subgroup $\langle a \rangle$ is $\varphi(\mathrm{r}(a))$.

Example

$\mathbb{Z}_9^* = \langle 2 \rangle$, since $\mathrm{r}(2) = 6 = |\mathbb{Z}_9^*|$.
Each element b of order 6 in $\mathbb{Z}_9^*$ has the form 2^k, where $\gcd(k, 6) = 1$. Hence $k \in \{1, 5\}$ and $b \in \{2^1 = 2, 2^5 = 5\}$.

Cyclic groups

Definition

A group G is called the *cyclic group* if for some $a \in G$ is $G = \langle a \rangle$.
The element a is called the *generator* of the group G.

Proposition

- Cyclic groups are abelian.
- A finite group G of order n is cyclic if and only if it contains an element a of order $\mathrm{r}(a) = n$.
- The number of generators of a cyclic group of order n is $\varphi(n)$.
  The probability of finding a generator by choosing $a \in G$ at random is $\frac{\varphi(n)}{n}$.

Cyclic groups

Proposition

An element $a \in G$ is a generator of a finite group G of order n if and only if one of the conditions is satisfied:

- $a^r \neq 1$ for every $r < n$, where $r \mid n$
- $a^r \neq 1$ for every $r = \frac{n}{p}$, where p is a prime and $p \mid n$

Examples

- The groups $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$ are cyclic with the generator 1.
- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8, \}$, $|\mathbb{Z}_9^*| = \varphi(9) = 6$, $\mathrm{r}(2) = 6$, so the group $(\mathbb{Z}_9^*, \cdot)$ is cyclic with the generator 2.
- The group $(\mathbb{Z}_8^*, \cdot)$ is not cyclic, since $a^2 = 1$ for every $a \in \mathbb{Z}_8^* = \{\pm 1, \pm 3\}$.

Cyclic groups

Example

The group $\mathbb{Z}_{19}^* = \mathbb{Z}_{19} \setminus \{0\}$ is given.

- $|\mathbb{Z}_{19}^*| = \varphi(19) = 18 = 2 \cdot 3^2$.
  Thus, possible orders of elements are $1, 2, 3, 6, 9, 18$.
- Let's find a generator in $\mathbb{Z}_{19}^*$. We check (randomly) $a = 2$.
  $2^6 = 7 \neq 1$ (hence also $2^2 \neq 1$, $2^3 \neq 1$), $2^9 = -1 \neq 1$,
  so $\mathrm{r}(2) = 18$ and 2 is a generator in $\mathbb{Z}_{19}^*$.
- The probability of hitting a generator is $P = \frac{\varphi(18)}{18} = \frac{1}{3}$.
- Determine $\mathrm{r}(8)$ and use it to calculate 8^{195} in $\mathbb{Z}_{19}$:
  $\mathrm{r}(8) = \mathrm{r}(2^3) = \frac{18}{3} = 6$, $8^{195} = 8^3 = 18$ in $\mathbb{Z}_{19}$.

Cyclic groups

Theorem

- Every infinite cyclic group is isomorphic to the group $(\mathbb{Z}, +)$.
- Every cyclic group of order n is isomorphic to the group $(\mathbb{Z}_n, +)$.

The corresponding isomorphism is the exponentiation $f : k \mapsto a^k$, where a is a generator of the group.

Cyclic groups

Subgroups of finite cyclic groups

- Subgroups in $(\mathbb{Z}_n, +)$ are of the form $d\mathbb{Z}_n = \langle d \rangle$, where $d \mid n$.
  The subgroup $d\mathbb{Z}_n = \{di, 1 \leq i \leq \frac{n}{d}\}$ has $\frac{n}{d}$ elements.
  Moreover, $d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n$, just when $d_2 \mid d_1$, just when $\frac{n}{d_1} \mid \frac{n}{d_2}$.
- Let $G = \langle a \rangle$ be a cyclic group of order n.
  Subgroups in $(G, \cdot)$ are of the form $G^d = \langle a^d \rangle$, where $d \mid n$.
  The subgroup $G^d = \{a^{id}, 1 \leq i \leq \frac{n}{d}\}$ has $\frac{n}{d}$ elements.
  Moreover, $G^{d_1} \subseteq G^{d_2}$, just when $d_2 \mid d_1$, just when $\frac{n}{d_1} \mid \frac{n}{d_2}$.

Cyclic groups

Proposition

Let $G = \langle a \rangle$ be a cyclic group of order n.

- Every subgroup of a cyclic group is cyclic.
- For every $r \mid n$, there is only one subgroup of order r in G. This is the subgroup $H_r = \langle b \rangle$, where $b = a^{\frac{n}{r}}$ is an element of order r.
- Let H_r be a subgroup of order r and H_s a subgroup of order s. Then $H_r \subseteq H_s$, just when $r \mid s$.

Consequence

- Let $G = \langle a \rangle$ be a cyclic group of order n. If $r \mid n$, then there are just $\varphi(r)$ elements of order r in G.
- The formula for the Euler's function holds: $\sum_{r|n} \varphi(r) = n$.

Cyclic groups

Solving equations $x^k = 1$

Let $G = \langle a \rangle$ be a cyclic group of order n.

- If $r \mid n$, then the equation $x^r = 1$ has exactly r solutions in G, these are elements of the only subgroup of order r in G. So the solutions are of the form $x = b^i$, where $b = a^{\frac{n}{r}}$ is an element of order r and $1 \leq i \leq r$.
- For any $k \in \mathbb{N}$, the equation $x^k = 1$ has exactly $d = \gcd(k, n)$ solutions in G, and it reduces to the equation $x^d = 1$.

Consequence

If the group $(\mathbb{Z}_n^*, \cdot)$ is cyclic and $n > 2$, then the equation $x^2 = 1$ has exactly two solutions in $\mathbb{Z}_n$, namely $x = \pm 1$.
In $\mathbb{Z}_2$, $x^2 = 1$ has only one solution $x = 1 = -1$.

Cyclic groups

Example

Solve the equation $x^{21} = 1$ in the group Z_{19}^*.

- We already know that $|\mathbb{Z}_{19}^*| = \varphi(19) = 18$ and 2 is the generator of $\mathbb{Z}_{19}^*$.
- The element a solves the equation $x^{21} = 1$ just when $\mathrm{r}(a) \mid 21$. Moreover, $a \in \mathbb{Z}_{19}^*$, so $\mathrm{r}(a) \mid 18$. Hence $\mathrm{r}(a) \mid \gcd(21, 18) = 3$ and the equation reduces to $x^3 = 1$.
- We find the element b of order 3: $b = 2^{\frac{18}{3}} = 2^6 = 7$. The equation has three solutions: $x_1 = 7$, $x_2 = 7^2 = 11$, $x_3 = 7^3 = 1$.

Cyclic groups

Proposition

Every group of prime order is cyclic.

Note

The previous statement says nothing about the groups $\mathbb{Z}_n^*$. The group $\mathbb{Z}_p^*$ has order $\varphi(p) = p - 1$, which is not a prime!

The structure of groups $\mathbb{Z}_n^*$ will be discussed in the next lecture. Let's mention forward the following proposition, which is based on the fact that $\mathbb{Z}_p$ is a field.

Proposition

The group $\mathbb{Z}_p^*$ is cyclic for every prime p.

m−th powers and square roots

Proposition

Let $G = \langle a \rangle$ be a cyclic group of order n and let $m \in \mathbb{N}$.
The map $\rho_m : G \to G : x \mapsto x^m$ is a group homomorphism.
Let $d \mid n$, so $n = rd$.

- $Ker\, \rho_d = \{g \in G, g^d = 1\} = \langle a^{\frac{n}{d}} \rangle = \langle a^r \rangle$ has d elements.
- $Im\, \rho_d = \{g^d, g \in G\} = \langle a^d \rangle$ has $\frac{n}{d} = r$ elements.

Both subgroups have the same structure, so for $|G| = rd$ there is

- $Ker\, \rho_r = Im\, \rho_d$, $Im\, \rho_r = Ker\, \rho_d$.

For general $m \in \mathbb{N}$, $\rho_m = \rho_d$, where $d = \gcd(m, |G|)$.

m−th powers and roots

Consequence

Let G be a cyclic group of order n and let $d \mid n$.
An element $b \in G$ is a d-th power, $b = c^d$ for some $c \in G$,
if and only if $b^{\frac{n}{d}} = 1$ in G.

Euler's criterion for $\mathbb{Z}_p^*$

Let p be an odd prime.

- The element $b \in \mathbb{Z}_p^*$ is a square ($b = c^2$) iff $b^{\frac{p-1}{2}} = 1$.
  In this case, b has two square roots $\pm c$.
- The element $b \in \mathbb{Z}_p^*$ is a non-square ($b \neq c^2$) iff $b^{\frac{p-1}{2}} = -1$.
- The product of two elements is a square just when either both are squares or both are non-squares.

m−th powers and square roots

Consequence

Let p be an odd prime number.

- $-1 \in \mathbb{Z}_p^*$ is a square iff $p \equiv 1 \pmod 4$.
- $-1 \in \mathbb{Z}_p^*$ is a non-square iff $p \equiv 3 \pmod 4$.

Note

Complex numbers over $\mathbb{Z}_p$ form a field only if $p \equiv 3 \pmod 4$.
$\mathbb{Z}_p[i] = \mathbb{Z}_p[x]/x^2 + 1$, the polynomial $x^2 + 1$ is irreducible over $\mathbb{Z}_p$ only if it has no root in $\mathbb{Z}_p$, which is if -1 is a non-square.

m−th powers and square roots

Example

The group $\mathbb{Z}_{19}^*$ has order 18 and the generator is $a = 2$.

- The equation $x^3 = 1$ is solved by
  $x \in \{2^{6i} = 7^i, 1 \leq i \leq 3\} = \{7, 11, 1\}$.
- These are just all the elements of $(\mathbb{Z}_{19}^*)^6$.
- The element $b = 3$ is a non-square, since $3^9 = -1$ in $\mathbb{Z}_{19}^*$.
- The element $b = 5$ is a square, since $5^9 = 1$ in $\mathbb{Z}_{19}^*$.
  Thus, the equation $x^2 = 5$ has two solutions $x = \pm c$, and we find $c = 9$ by brute force. Thus $x_1 = 9$, $x_2 = -9 = 10$.

Literature

- Shoup: A Computational Introduction to Number Theory and Algebra. Chapter 6.5. http://shoup.net/ntb/