



Number Theory: Part II

Murat Kantarcioglu

Groups

-
- ★ $Z = \{\dots - 2, -1, 0, 1, 2\}$
 - ★ $Z_+ = \{1, 2, \dots\}$
 - ★ $N = \{0, 1, \dots\}$
 - ★ $Z_N = \{0, 1, \dots, N - 1\}$
 - ★ $Z_N^* = \{i \in Z : 1 \leq i \leq N - 1, \wedge \gcd(i, N) = 1\}$
 - ★ **GROUP:** (G, \cdot)
 - ▶ Closure: $\forall a, b \in G \Rightarrow a \cdot b \in G$
 - ▶ Associativity: $\forall a, b, c \in G \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$
 - ▶ Identity: $\exists \mathbf{1}, \forall a \in G \Rightarrow \mathbf{1} \cdot a = a \cdot \mathbf{1} = a$
 - ▶ Invertibility: $\forall a \in G, \exists b \in G \Rightarrow a \cdot b = \mathbf{1}$

$a \cdot b \pmod n$
 $\in Z_n^*$
 $(Z, +) \quad a + -a = 0$



Facts about Groups

- ★ Let a^{-1} be the inverse of a
- ★ Example groups:
 - ▶ $(\mathbb{Z}_N, + \text{ mod } N), (\mathbb{Z}_N^*, * \text{ mod } N)$
- ★ $a^i = a.a.a.a \dots$ (i times) $(\mathbb{Z}, +) = a^i = \underbrace{a+a+\dots+a}_i$
- ★ If $|G| = m$ then $\forall a \in G, a^m = 1$
- ★ $|G| = m$ is called the order of group G
- ★ S is a subgroup of G if S is a group and $S \subseteq G$
- ★ If S is a subgroup of G then $|S|$ divides $|G|$
 ↓ Finite groups

Cyclic Groups

- ★ The order of g is the least n s.t $g^n = 1 \rightarrow$
 $g^0 = 1 \quad \& \quad g^m = 1 \quad m = |G|$
- ★ Let $\langle g \rangle = \{g^0, g^1, \dots, g^{n-1}\}$
 1 $\langle a \rangle = \{a^0, a^1, \dots, a^{n-1}\}$ $|G| = m$
- ★ g is a Generator of G if $\langle g \rangle = G$
 g^0, g^1, \dots, g^m
- ★ G is a cyclic group if it has a generator
- ★ Discrete Logarithm $DL_{G,g}(a) = i$ implies $g^i = a$

Examples

$$(Z_{11}^*, A \text{ mod } 11)$$

Example 7.9 Let $p = 11$, which is prime. Then $Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ has order $p - 1 = 10$. Let us find the subgroups generated by group elements 2 and 5. We raise them to the powers $i = 0, \dots, 9$. We get:

$$\langle 9 \rangle \quad 6$$

$$\langle 2 \rangle$$

$$= 2^0, 2^1, 2^2, \dots, 2^9$$

i	0	1	2	3	4	5	6	7	8	9	10
$2^i \text{ mod } 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \text{ mod } 11$	1	5	3	4	9	1	5	3	4	9	1

$$|Z_{11}^*| = \phi(11) = 10$$

$$|\langle 5 \rangle| = 5$$

$$5 \mid 10$$

a	1	2	3	4	5	6	7	8	9	10
$\text{DLog}_{Z_{11}^*, 2}(a)$	0	1	8	2	4	9	7	3	6	5

$$\langle x \rangle \text{ subgroup of } 6$$

Cyclic Groups

- ★ If p is a prime then Z_p^* is cyclic group
 - ★ If $|G| = m$ is prime then G is cyclic
 - ★ Prop: If G is cyclic and $|G| = m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$
 $\forall i, m_i = m/p_i$ $g \in G$ is a generator of G iff
 $\forall i, g^{m_i} \neq 1$
 - ▶ Note that $\langle g \rangle$ is a subgroup of G
- $G = Z_{10}^*$ $|G| = 10 = \varphi(10) = 2 \cdot 5$
 $m_1 = 2$ $m_2 = 5$



Cyclic Groups

- ★ $|G| = m$ and g is a generator of G then
 $Gen(G) = \{g^i \in G : i \in Z_m^*\}$ and $|Gen(G)| = \phi(m)$
- ★ To find a generator efficiently,
we need to know the factorization of m
- ★ Assume $p = 2q + 1$ for some primes p, q then
 g is a generator iff $g^2 \bmod p \neq 1$ and $g^q \bmod p \neq 1$
- ★ Note that $Pr(g \text{ is a generator}) = \phi(\phi(p)) / (p - 3) = 0.5$

$$= \frac{\phi(p-1)}{p-3} = \frac{\phi(2q)}{p-3} = \frac{q-1}{2q-3} = \frac{1}{2}$$

Examples

Example 7.15 Let us determine all the generators of the group \mathbf{Z}_{11}^* . Let us first use Proposition 7.13. The size of \mathbf{Z}_{11}^* is $m = \varphi(11) = 10$, and the prime factorization of 10 is $2^1 \cdot 5^1$. Thus, the test for whether a given $a \in \mathbf{Z}_{11}^*$ is a generator is that $a^2 \not\equiv 1 \pmod{11}$ and $a^5 \not\equiv 1 \pmod{11}$. Let us compute $a^2 \pmod{11}$ and $a^5 \pmod{11}$ for all group elements a . We get:

a	1	2	3	4	5	6	7	8	9	10
$a^2 \pmod{11}$	1	4	9	5	3	3	5	9	4	1
$a^5 \pmod{11}$	1	10	1	1	1	10	10	10	1	10



Squares and non-squares

- ★ $a \in G$ is called a square or a quadratic residue (QR) if $\exists b \in G$ s.t $b^2 = a$ in G
- ★ $QR(G) = \{a \in G : a \text{ is a QR in } G\}$
- ★ We will focus on the QRs in Z_N^* , especially where $N = p$
- ★ a is called Square mod N or quadratic residue mod N if $a \in QR(Z_N^*)$



Squares mod p

- ★ We focus on Z_p^*
- ★ Define Legendre symbol of a as $J_p(a)$ where

$$J_p(a) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ 0 & \text{if } a = 0 \text{ mod } p \\ -1 & \text{if } a \text{ is a non-square mod } p \end{cases}$$

$$\text{QR}(Z_{11}^*) = \{1, 3, 4, 5, 9\}$$

a	1	2	3	4	5	6	7	8	9	10
$a^2 \text{ mod } 11$	1	4	9	5	3	3	5	9	4	1

$$J_p(2) = -1$$

$$J_p(4) = 1$$

Squares mod p

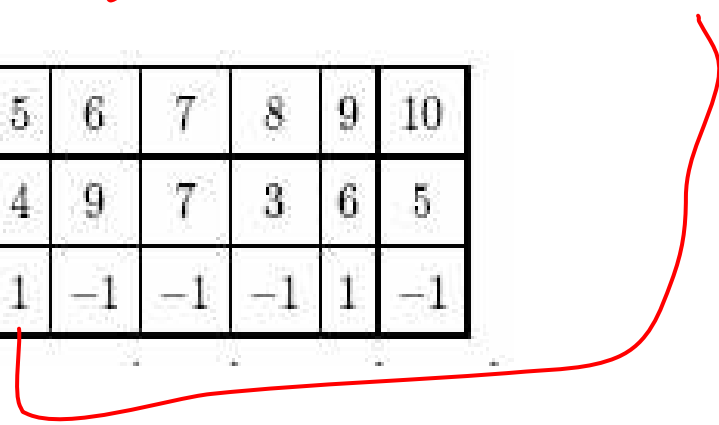
★ Let $p \geq 3$ and let g is a generator of Z_p^* . Then $QR(Z_p^*) = \{g^i : i \in Z_{p-1}, i = 0 \pmod 2\}$

★ $|QR(Z_p^*)| = \frac{p-1}{2}$

★ For example, for Z_{11}^*

$5 \pmod{11}$
 $5^2 \cdot 5^2 \cdot 5 = 3 \cdot 3 \cdot 5 = 1 \pmod{11}$

a	1	2	3	4	5	6	7	8	9	10
$DLog_{Z_{11}^*, 2}(a)$	0	1	8	2	4	9	7	3	6	5
$J_{11}(a)$	1	-1	1	1	1	-1	-1	-1	1	-1





Squares mod p

★ Lemma 7.18: Let $p \geq 3$ be a prime then

$$\forall a \in \mathbb{Z}_p^*, J_p(a) = a^{\frac{p-1}{2}} \pmod{p}$$

★ Let $p \geq 3$ be a prime then

$$\forall g \text{ generator of } \mathbb{Z}_p^*, g^{\frac{p-1}{2}} = -1 \pmod{p}$$

$$\begin{aligned} g^{\frac{p-1}{2}} &= -1 \pmod{p} \\ g^{\frac{p-1}{2}} &= a \quad \Rightarrow a^2 = g^{p-1} = 1 \pmod{p} \\ &\Rightarrow a = 1 \text{ or } -1 \pmod{p} \end{aligned}$$



Squares mod p

★ Proof of Lemma 7.18: We need to prove

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is a non-square mod } p \end{cases}$$

★ Let $i = DL_{Z_p^*, g}(a)$, if a is square mod p then i is even

$$a^{\frac{p-1}{2}} = (g^i)^{\frac{p-1}{2}} = (g^{p-1})^{i/2} = 1 \pmod{p}$$

★ if a is a non-square mod p then i is odd

$$a^{\frac{p-1}{2}} = (g^i)^{\frac{p-1}{2}} = g^{(i-1)\frac{p-1}{2} + \frac{p-1}{2}} = g^{\frac{p-1}{2}} = -1 \pmod{p}$$



Squares mod p

★ Let $p \geq 3$ be a prime then $\forall a, b \in Z_p^*$

$$J_p(ab \bmod p) = J_p(a) \cdot J_p(b)$$

★ Let $p \geq 3$ be a prime and g is generator of Z_p^* ,
 $\forall x, y \in Z_{p-1}$ then $J_p(g^{xy} \bmod p) = 1$ iff

$$x = g^x$$

$$y = g^y$$

$$J_p(g^x \bmod p) = 1 \vee J_p(g^y \bmod p) = 1$$

Squares mod p

★ Prop. 7.22: Let $p \geq 3$ is a prime and let g is a generator of Z_p^* then given $x \leftarrow Z_{p-1}; y \leftarrow Z_{p-1}$

$$\Pr [J_p(g^{xy}) = 1] = \frac{3}{4}$$

$$\frac{|\text{QR}(Z_p^*)| = \frac{p-1}{2}}{|Z_p^*| = p-1} = \frac{1}{2}$$

$$2^3 = 1 \pmod{7}$$