CS6260 Discrete Math Cheatsheet

Set Definitions

- $\mathbb{Z}$: Set of all integers
- $\mathbb{Z}_+$: Set of all positive numbers including 0
- $\mathbb{Z}_-$: Set of all negative numbers
- $\mathbb{Z}_\mathbb{N}$: Set of positive numbers from 0 to N - 1
- $\mathbb{Z}^*_N$: Set of all integers co-prime to N
  Note that if N is a prime this includes all numbers from 1 to N - 1 $\implies$ order is N - 1
- ϕ(N): order of group $\mathbb{Z}^*_N$
- Set of squares or Quadratic Residue: **QR**($\mathbb{Z}^*_p$)= $\{a \in \mathbb{Z}^*_p$: a is a square mod p$\}$ = $\{g^i : 0 \le i \le p-2$ and i is even$\}$
  for generator $g \in G$ and $p \ge 3$

Terms

- **Order of a group:** Number of elements in a group
- **Order of a group element:** smallest integer $n \ge 1 : g^n = \mathbf{1}$
- **Subgroup:** Set $S \subseteq G$ is a sub-group if S is a group under the same operation as G
- **Subgroup from group element:** For any $g \in G$, $\langle g \rangle = \{g^0, g^1, \dots g^{o(g)-1}\}$ is a sub-group
- **Generator:** $g \in G$ is a generator if $\langle g \rangle = G$
- **Cyclic Group:** A group G is cyclic if it contains a generator
- **Safe Prime:** Prime p is a safe prime if p =2q + 1, where q is also a prime
- **Square or Quadratic Residue:** a is a square modulo p if $\exists$ b : $b^2 \equiv a \pmod{p}$

What is a Group

A group is a non-empty set on which a binary operation $\cdot$ is defined. It satisfies the following properties:

- **Closure**: $\forall a, b \in G, a \cdot b \in G$
- **Associativity**: $\forall a, b, c \in G, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **Identity**: $\forall a \in G, \exists\ \mathbf{1} \in G : a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$
- **Invertibility**: $\forall a \in G, \exists$ unique $b \in G : a \cdot b = b \cdot a =$**1**

Group Operations

Operation	Definition	Running Time
Addition	a + b	O(|a| + |b|) i.e. Linear
Mult/Div/Mod	a.b// q,r: a = qb + r // r	O(|a|.|b|) i.e. Quadratic
Extended GCD	Returns d, a', N'	O(|a|.|N|) i.e. Quadratic
Mod Inverse	a' $\pmod{N}$; a' from EXT_GCD	Quadratic
Exponentiation	$a^n = a \cdot a \cdot \dots$ n times	O($2^{\|n\|}$) i.e. Exponential
Fast Modular exponentiation	$y_{\|n\|} = 1; y_{\|n\|-1} = y^2_{\|n\|} \cdot a^{b_{\|n\|-1}}$	Cubic for $\mathbb{Z}^*_p$

Jacobi/Legendre Symbol

The Legendre or Jacobi symbol of a modulo p is defined as:

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

Suchithra Ravi

Computing discrete logs

- For a general cyclic group $G = \langle g \rangle$ and $x \in G$ best algorithm is $O(\sqrt{|G|})$ = exponential

  Better algorithms for specific groups but no polynomial time algorithm known.
- For G = $\mathbb{Z}_p^*$, can compute in $O(e^{1.92(lnq)^{(\frac{1}{3}(ln(lnq))^{\frac{2}{3}}}})$
- For an elliptic curve group G with prime order p, can compute in $O(\sqrt{p})$

Computing cyclic groups

- FINDPRIME(K):

  Randomly choose p from all k bit numbers until CHECKPRIME(p) and CHECKPRIME($\frac{p-1}{2}$) are true

  CHECKPRIME(p): O(|N|) randomized algorithm available

  Probability of finding prime randomly from range 1 to N = $\frac{1}{ln(N)}$
- FINDGENERATOR(G):

  For G = $\mathbb{Z}_p^*$, pick g at random from G -{1} until $g^2 \neq \mathbf{1}$ and $g^q \neq \mathbf{1}$

  $\mathbb{Z}_p^*$ has q - 1 generators and choosing from set of p -2

  $\implies$ probability of finding generator = $\frac{1}{2}$

Computing Legendre symbol

TEST_SQ(p,a) for any a and prime $p \geq 3$:
s $\leftarrow a^{\frac{p-1}{2}} \pmod p$
If s = 1 return 1 else return -1

Useful properties

- $a^m = \mathbf{1}\ \forall a \in G$ and $m = |G|$
- $a^i = a^{i \pmod m}\ \forall a \in G$ and $i \in \mathbb{Z}$
- For $a, N \in G$ and (a,N) $\neq$ (0, 0), if d = gcd(a,N), $\exists$ weights $a', N' \in \mathbb{Z}$: $d = a \cdot a' + N \cdot N'$
- If q, r = INT_DIV(a,N), gcd(a,N) = gcd (N,r)
- S is a subgroup of G if $x, y^-1 \in S \forall x, y \in S$
- |S| divides |G| i.e. Order of S divides order of G

- If p is a prime, $\mathbb{Z}_p^*$ is cyclic
- If m= |G| is a prime number for group G, G is cyclic
- If |G| is prime, then every $g \in G - \{\mathbf{1}\}$ is a generator
- It is "easy" to find a generator for $\mathbb{Z}_p^*$ if prime factorization of p-1 is known, but not otherwise $\implies$ easy to find if p is a safe prime
- $g \in \mathbb{Z}_p^*$ is a generator iff $g^2 \neq \mathbf{1}$ and $g^q \neq \mathbf{1}$
- $\mathbb{Z}_p^*$ has q - 1 generators

Useful properties

- J_p(a) = 1 iff $Dlog_{g,\mathbb{Z}_p^*}$(a) is even for generator $g \in \mathbb{Z}_p^*$
- For prime $p \geq 3$ and generator $g \in \mathbb{Z}_p^*$: $J_p(g^{xy} \pmod p) = 1$ iff $J_p(g^x \pmod p) = 1$ or $J_p(g^y \pmod p) = 1\ \forall x, y \in \mathbb{Z}_p^*$

  $\because |\mathbb{Z}_p^*|$ = p-1
- For any $a, b \in \mathbb{Z}$, $J_p(a \cdot b) = J_p(a) \cdot J_p(b)$
- For any $a \in \mathbb{Z}_p^*$, $J_p(a^{-1}) = J_p(a)$
- A generator is always a non-square
- For $p \geq 3$ and generator $g \in \mathbb{Z}_p^*$, $|\mathrm{QR}(\mathbb{Z}_p^*)| = \frac{p-1}{2}$, i.e. half of the elements of the set are squares and half are non-squares.