1 Number Theory

1.1 FTA

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

1.2 The Well-Ordering Property

$$\emptyset \neq S \subseteq \mathbb{N} \Rightarrow \min S \in S$$

1.3 Division Algorithm

$$a = bq + r \quad 0 \le r < b \text{ for unique } q, r$$

1.4 Ideal of $\mathbb{Z}$

A nonempty set $I \subseteq \mathbb{Z}$ such that

$$a, b \in I \Rightarrow a + b \in I$$

$$a \in I, r \in \mathbb{Z} \Rightarrow ra \in I$$

$$I \text{ is an ideal of } \mathbb{Z} \Leftrightarrow I = d\mathbb{Z}$$

$$I_1 + I_2 = \{x + y : x \in I_1, y \in I_2\}$$

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$$

1.5 Great Common Divisor

$$\gcd(a, b) = as + bt$$

1.6 Euler's Phi Function

$$\Phi(n) = |\mathbb{Z}_n^*|, \forall n \in \mathbb{Z}^+$$

If $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$\Phi(n) = \Phi(p_1^{e_1}) \cdots \Phi(p_r^{e_r}) = n(1 - p_1^{-1}) \cdots (1 - p_r^{-1})$$

If $n = pq$, then

$$\Phi(n) = (p-1)(q-1)$$

1.7 The Set $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$$

$$\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n : \gcd(a, n) = 1\}$$

1.8 Euler's Theorem

Let $n \ge 1$ and $\alpha \in \mathbb{Z}_n^*$, then $\alpha^{\Phi(n)} = 1$

1.9 Fermat's Little Theorem

If p is a prime and $\alpha \in \mathbb{Z}_p$, then $\alpha^{p-1} = 1$

1.10 Wilson's Theorem

If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$

2 Cryptography

2.1 RSA

$(pk, sk) \leftarrow \mathbf{Gen}(1^n)$:

Choose two n-bit primes $p \neq q$, $N = pq$
Choose e, d s.t. $0 \le e, d < \Phi(N)$, $\gcd(e, \Phi(N)) = 1$
$d = e^{-1} \bmod \Phi(N)$
output $pk = (N, e), sk = (N, d)$

$c \leftarrow \mathbf{Enc}(pk, m)$:

output $c = m^e \bmod N, 0 \le c < N$

$m \leftarrow \mathbf{Dec}(sk, c)$:

output $m = c^d \bmod N, 0 \le m < N$

2.2 Arithmetic Operations

$$a = (a_{k-1} \cdots a_1 a_0)_2, \ b = (b_{l-1} \cdots b_1 b_0)_2$$

$$\ell(a) = \begin{cases} \lfloor \log_2(|a|) \rfloor + 1, & a \neq 0, \\ 1, & a = 0 \end{cases}$$

$$k = \ell(a), l = \ell(b)$$

Addition & Subtraction $a + b$ or $a - b$: $O(k)$
Multiplication $a * b$: $O(k^2)$
Division a/b: $O((k - l + 1) \cdot l)$
Arithmetic Module N $(a \pm b) \bmod N$: $O(\ell(N))$, $(ab) \bmod N$: $O(\ell(N)^2)$
Square-and-Multiply
Square $\quad x_0 = a$

$$x_{k-1} = x_{k-2}^2 \bmod N = a^{2^{k-1}} \bmod N$$

Multiply $a^e \bmod N = (x_0^{e_0} \cdot x_1^{e_0} \cdots x_{k-1}^{e_0}) \bmod N$

2.3 EA

Compute $d = \gcd(a, b)$

2.4 EEA

Compute $d = \gcd(a, b) = as + bt$: $O(\ell(a)\ell(b))$

2.5 Prime Number Theorem

For $x \in \mathbb{R}^+, \pi(x) = \sum_{p \le x}$ Numbers of primes

$$|\mathbb{P}_n| \ge \frac{2^n}{n \ln 2}\left(\frac{1}{2} + O\left(\frac{1}{n}\right)\right) \text{ when } n \to \infty$$

2.6 Linear Congruence Equation

$$ax \equiv b \pmod{n}$$

2.7 CRT

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ \vdots \\ x \equiv b_k \pmod{n_k} \end{cases}$$

Let $N_i = n/n_i$ for every $i \in [k]$, $\exists s_i, t_i, N_i s_i + n_i t_i = 1$
Let $b = b_1 N_1 s_1 + \cdots + b_k N_k s_k$, then

$$x \equiv b \pmod{n}$$

2.8 DLOG & CDH

$f_{\mathrm{DLOG}}(q, G, g; h) = \log_g h$, $f_{\mathrm{CDH}}(q, G, g; A, B) = g^{ab}$

2.9 Diffie-Hellman Key Exchange

Alice: $a \leftarrow \mathbb{Z}_q, A = g^a$, send (q, G, g, A) to Bob
Bob: $b \leftarrow \mathbb{Z}_q, B = g^b$, send B to Alice; output $k = A^b$
Alice: output $k = B^a$

3 Group Theory

3.1 Group

Closure $\forall a, b \in G, a \star b \in G$
Associative $\forall a, b, c \in G, a \star (b \star c) = (a \star b) \star c$
Identity $\exists e \in G, \forall a \in G, a \star e = e \star a = a$
Inverse $\forall a \in G, \exists b \in G, a \star b = b \star a = e$
Commutative (Abelian Group) $\forall a, b \in G, a \star b = b \star a$

3.2 Field

$(\mathbb{F}, +, \cdot)$

3.3 Polynomial

Let $f(X) = f_t X^t + \cdots + f_1 X + f_0 \in \mathbb{Z}_p[X]$ and $\alpha \in \mathbb{Z}_p$, then $\exists q(X) = q_{t-1} X^{t-1} + \cdots + q_0 \in \mathbb{Z}_p[X]$ s.t.

$$f(X) = (X - \alpha)q(X) + f(\alpha)$$

$$\begin{aligned} q_{t-1} &= f_t \\ q_{t-2} &= f_{t-1} + f_t \alpha \\ &\vdots \\ q_0 &= f_1 + f_2 \alpha + \cdots + f_t \cdot \alpha^{t-2} \end{aligned}$$

$f(X) \in \mathbb{Z}_p[X]$ has $\le \deg(f)$ roots in $\mathbb{Z}_p$

3.4 Order

The order of a group G is the cardinality of G.
When $|G| < \infty, \forall a \in G$, the order of a is the least integer $l > 0$ s.t. $a^l = 1$ ($la = 0$ for additive group)
$\forall a \in G, a^{|G|} = 1$

3.5 Cyclic Group

Abelian group $(G, \cdot)$ is a cyclic group if $\exists g \in G$ s.t. $G = \langle g \rangle$

4 Combinatorics

4.1 Functions

Let $A, B \neq \emptyset$ be two sets. A function(map) $f : A \to B$ assigns a unique element $b \in B$ for all $a \in A$
injective $f(a) = f(b) \Rightarrow a = b$
surjective $f(A) = B$
bijective injective and surjective

4.2 Cantor's Diagonal Argument

$$|A| \neq |\mathbb{Z}^+|$$

4.3 Cantor's Theorem

Let A be any set, then $|A| < |\mathcal{P}(A)|$

4.4 The Halting Problem

There is no Turing machine computing

$$\mathbf{HALT}(P, I) = \begin{cases} \text{“halts”} & \text{if } P(I) \text{ halts;} \\ \text{“loops forever”} & \text{if } P(I) \text{ loops forever.} \end{cases}$$

4.5 Countable an Uncountable

A set A is countable if $|A| < \infty$ or $|A| = |\mathbb{Z}^+|$; otherwise, it is said to be uncountable

4.6 Schröder-Bernstein Theorem

If $|A| \le |B|$ and $|B \le |A|$, then $|A| = |B|$
$\aleph_0 = |\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)| = 2^{\aleph_0} = |[0,1)| = |(0,1)| = |\mathbb{R}| = c$

4.7 Permutations of Set

An n-element set has $P(n, r) = \dfrac{n!}{(n-r)!}$ and has n^r different r-permutations with repetition.

4.8 Combinations of Set

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

of r-combinations of an n element set with repetition, # of natural number solutions of the equation

$x_1 + x_2 + \cdots + x_n = r$ are $\binom{n+r-1}{r}$

4.9 Multiset

$A = \{n_1 \cdot a_1, n_2 \cdot a_2, \dots, n_k \cdot a_k\}$ is an $(n_1 + n_2 + \cdots n_k)$-multiset

4.10 Permutations of Multiset

A has exactly $\dfrac{(n_1 + n_2 + \cdots + n_k)!}{n_1!n_2!\cdots n_k!}$ permutations

4.11 Combination of Multiset

An r-subset(multiset) of A is r-combination of A

4.12 Shortest Path

of shortest paths from $(0,0)$ to (p,q) is $\dfrac{(p+q)!}{p!q!}$

4.13 T-Route

There is a T-route from $A = (a, \alpha)$ to $B = (b, \beta)$ only if (1) $b > a$; (2) $b - a \geq |\beta - \alpha|$ (3) $2 \mid (b + \beta - a - \alpha)$

4.14 Numbers of T-Routes

of T-routes from $A = (a, \alpha)$ to $B = (b, \beta)$ is

$$\frac{(b-a)!}{(\frac{b-a}{2} + \frac{\beta-\alpha}{2})!(\frac{b-a}{2} - \frac{\beta-\alpha}{2})!}$$

# of T-routes that intersect the x-axis is

$$\frac{(b-a)!}{(\frac{b-a}{2} + \frac{\beta+\alpha}{2})!(\frac{b-a}{2} - \frac{\beta+\alpha}{2})!}$$

4.15 Solution of Bertrand's Ballot Problem

The sequence $x_1 x_2 \dots x_{2n}$ is a ballot

The probability that A never trials B is $p_n = C_n / \binom{2n}{n}$

4.16 Catalan Number

of solutions of the equation system

$$\begin{cases} x_1 + x_2 + \cdots + x_{2n} = n \\ x_1 + x_2 + \cdots + x_i \leq i/2, i = 1, 2, \dots, 2n-1 \\ x_i \in \{0, 1\}, i = 1, 2, \dots, 2n \end{cases}$$

$$C_n = \frac{(2n)!}{n!(n+1)!}$$

4.17 Inverse Binomial Transform

The binomial transform of $\{a_n\}_{n \geq s}$ is $\{b_n\}_{n \geq s}$ s.t.

$$b_n = \sum_{k=s}^{s} \binom{n}{k} a_k$$

The inverse binomial transform of $\{b_n\}_{n \geq s}$ is $\{a_n\}_{n \geq s}$ s.t.

$$a_n = \sum_{k=s}^{s} (-1)^{n-k} \binom{n}{k} b_k$$

4.18 Distribution Problems

Type 1 n labeled $\to$ k labeled: $|S| = k^n$

$n \to i$: $N_1 = \dfrac{n!}{n_1!n_2!\cdots n_k!}$

Type 2 n unlabeled $\to$ k labeled: $|S| = \binom{n+k-1}{n}$

Type 3 n labeled $\to$ k unlabeled: $|S| = \sum_{j=1}^{k} S_2(n, j)$

Type 4 n unlabeled $\to$ k unlabeled: $|S| = \sum_{j=1}^{k} p_j(n)$

4.19 Stirling number of the second kind $S_2(n, j)$

$$S_2(n,j) = \frac{1}{j!} \sum_{i=0}^{j-1} (-1)^i \binom{j}{i} (j-i)^n \text{ when } n \geq j \geq 1$$

$$S_2(n,j) = S_2(n-1, j-1) + jS_2(n-1, j)$$

4.20 Partitions of Integers

For $n \in \mathbb{Z}^+$, $p_j(n+j) = \sum_{k=1}^{j} p_k(n)$,

$$p_k(n) = p_{k-1}(n-1) + p_k(n-k)$$

4.21 Characteristic Roots

Characteristic equation: $r^k - c_1 r^{n-1} - c_2 r^{n-2} - \cdots - c_k = 0$

4.22 LHRR

$$a_n = \sum_{i=1}^{k} c_i a_{n-i}, \text{ where } n \geq k, \{c_i\}_{i=1}^{k} \text{ are constants, } c_k \neq 0$$

No multiple roots $\{r_1, \dots, r_k\}$: $x_n = \sum_{j=1}^{k} \alpha_j r_j^n$

Multiple roots $\{m_1 \cdot r_1, \dots m_t \cdot r_t\}$: $x_n = \sum_{j=1}^{t} (\sum_{\ell=0}^{m_j - 1} \alpha_{j,\ell} n^\ell) r_j^n$

4.23 LNRR

$$a_n = \sum_{i=0}^{k} c_i a_{n-i} + F(n), \{c_i\}_{i=1}^{k} \text{ are constants, } c_k, F(n) \neq 0$$

Particular Solutions

$F(n) = (f_l n^l + \cdots + f_1 n + f_0) s^n = f(n) s^n$

s: a root of characteristic equation, m: multiplication of s

$$x_n = (p_l n^l + \cdots + p_1 n + p_0) s^n n^m$$

General Solutions

Particular solution of LNRR + General solution of the associated LHRR

4.24 Generating Function

$$A(x) = \sum_{r=0}^{\infty} a_r x^r, B(x) = \sum_{r=0}^{\infty} b_r x^r$$

$$A(x) \pm B(x) = \sum_{r=0}^{\infty} (a_r \pm b_r) x^r, A(x) \cdot B(x) = \sum_{r=0}^{\infty} (\sum_{j=0}^{r} a_j b_{r-j}) x^r$$

$A(x)$ has an inverse iff $a_0 \neq 0$.

4.25 $(1 + \alpha x)^u$

The extended binomial coefficient

$$\binom{u}{n} = \begin{cases} u(u-1)\cdots(u-n+1)/n! & n > 0 \\ 1 & n = 0 \end{cases}$$

Let x be a real number with $|x| < 1$,

$$(1+x)^u = \sum_{r=0}^{\infty} \binom{u}{r} x^r$$

4.26 Counting Combinations with GFs

$a_r = |\{(r_1, \dots, r_n) : r_i \in R_i, r_1 + \cdots + r_n = r\}|$

$$\sum_{r=0}^{\infty} a_r x^r = \prod_{i=1}^{n} \sum_{r_i \in R_i} x^{r_i}$$

4.27 Counting Permutations with GFs

$a_r = \sum_{r_1 \in R_1, \dots, r_n \in R_n, r_1 + \cdots r_n = r} \frac{r!}{r_1! \cdots r_n!}$

$$\sum_{r=0}^{\infty} \frac{a_r}{r!} x^r = \prod_{i=1}^{n} \sum_{r_i \in R_i} \frac{x^{r_n}}{r_n!}$$

4.28 Partial Fraction Decomposition

Let $Q(x), P(x)$ be two polynomial s.t. $\deg(Q) > \deg(P)$. If $Q(x) = (1 - r_1 x)^{m_1} \cdots (1 - r_t x)^{m_t}$ for distinct non-zero numbers $r_1, \dots, r_t$ and integers $m_1, \dots, m_t \geq 1$, then there exist unique coefficients $\{\alpha_{j,u} : j \in [t], u \in [m_j]\}$ such that

$$\frac{P(x)}{Q(x)} = \sum_{j=1}^{t} \sum_{u=1}^{m_j} \frac{\alpha_{j,u}}{(1 - r_j x)^u}$$

4.29 Principle of IE

Let S be a finite set, $A_1, A_2, A_n \subseteq S$, then

$$|\bigcup_{i=1}^{n} A_i| = \sum_{t=1}^{n} (-1)^{t-1} \sum_{1 \leq i_1 < \cdots < i_t \leq n} |A_{i_1} \cap \cdots \cap A_{i_t}|$$

$$|\bigcap_{i=1}^{n} A_i| = \sum_{t=1}^{n} (-1)^{t-1} \sum_{1 \leq i_1 < \cdots < i_t \leq n} |A_{i_1} \cup \cdots \cup A_{i_t}|$$

4.30 Cover

A cover of a finite set A is a family $\{A_1, A_2, \dots A_n\}$ of subsets of A such that $\bigcup_{i=1}^{n} A_i = A$.

4.31 Pigeonhole Principle

Let A be a set with $\geq N$ elements. Let $\{A_1, A_2, \dots, A_n\}$ be a cover of A, then $\exists k \in [n], |A_k| \geq \lceil N/n \rceil$.

5 Propositional Logic

5.1 Logical Operators

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

5.2 Type of WFFs

Tautology: truth value is **T** for all truth assignment
Contradiction: truth value is **F** for all truth assignment
Contingency: neither tautology or contradiction

5.3 Logical Equivalence

Proving $A \equiv B$ (1) $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$ (2) $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$ (3) $A \leftrightarrow B$ is a tautology

5.4 Tautological Implications

Proving $A \Rightarrow B$ (1) $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$ (2) $B^{-1}(\mathbf{F}) \subseteq A^{-1}(\mathbf{F})$ (3) $A \to B$ is a tautology (4) $A \wedge \neg B$ is a contradiction

5.5 Rules of Replacement

$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q) \quad \neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$
$$P \vee (P \wedge Q) \equiv P \wedge (P \vee Q) \equiv P$$
$$P \to Q \equiv \neg P \vee Q \quad P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$$

6 Predicate Logic

6.1 From Natural Language to WFFs

$\forall x(P(x) \to Q(x))$ $\exists x(P(x) \wedge Q(x))$

6.2 Type of WFFs

A WFF is **logically valid** if it is **T** in every interpretation
A WFF is **unsatisfiable** if it is **F** in every interpretation
A WFF is **satisfiable** if it is **T** in some interpretation

6.3 Logical Equivalence

$A \equiv B$ iff $A \leftrightarrow B$ is **logically valid**

6.4 De Morgan's Laws for Quantifiers

$$\neg \forall x P(x) \equiv \exists x \neg P(x), \neg \exists x P(x) \equiv \forall x \neg P(x)$$

6.5 Distributive Laws for Quantifiers

$$\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$$
$$\exists x(P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$$

6.6 Rules of Substitution

$(P) \wedge (Q) \Rightarrow P \wedge Q$	Conjunction
$P \wedge Q \Rightarrow P$	Simplification
$P \Rightarrow P \vee Q$	Addition
$P \wedge (P \to Q) \Rightarrow Q$	Modus Ponens
$\neg Q \wedge (P \to Q) \Rightarrow \neg P$	Modus Tollens
$\neg P \wedge (P \vee Q) \Rightarrow Q$	Disjunctive Syllogism
$(P \to Q) \wedge (Q \to R) \Rightarrow (P \to R)$	Hypothetical Syllogism
$(P \vee Q) \wedge (\neg P \vee R) \Rightarrow Q \vee R$	Resolution
$P \Rightarrow Q \to R \equiv P \wedge Q \Rightarrow R$	Conclusion Premise

6.7 Tautological Implications

$\forall x P(x) \vee \forall x Q(x) \Rightarrow \forall x(P(x) \vee Q(x))$
$\exists x(P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x)$
$\forall x(P(x) \to Q(x)) \Rightarrow \forall x P(x) \to \forall x Q(x)$
$\forall x(P(x) \to Q(x)) \Rightarrow \exists x P(x) \to \exists x Q(x)$
$\forall x(P(x) \leftrightarrow Q(x)) \Rightarrow \forall x P(x) \leftrightarrow \forall x Q(x)$
$\exists x(P(x) \leftrightarrow Q(x)) \Rightarrow \exists x P(x) \leftrightarrow \exists x Q(x)$
$\forall x(P(x) \to Q(x)) \wedge \forall x(Q(x) \to R(x)) \Rightarrow \forall x(P(x) \to R(x))$
$\forall x(P(x) \to Q(x)) \wedge P(a) \Rightarrow Q(a)$

6.8 Rules of Inference for $\forall, \exists$

$\forall x P(x) \Rightarrow P(a)$	Universal Instantiation
$P(a) \Rightarrow \forall x P(x)$	Universal Generalization
$\exists x P(x) \Rightarrow P(a)$	Existential Instantiation
$P(a) \Rightarrow \exists x P(x)$	Existential Generalization

7 Graph

7.1 Types of Graph

7.2 Handshaking Theorem

Let $G = (V, E)$ be an undirected graph, then
$2|E| = \sum_{v \in V} \deg(v)$ and $|\{v \in V : \deg(v) \text{ is odd}\}|$ is even.
Let $G = (V, E)$ be an directed graph, then

$$\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|$$

7.3 Edge Contraction

Let $G = (V, E)$ be a simple graph and $e = \{u, v\} \in E$
Define $G/e = (V', E')$, where $V' = (V - \{u, v\}) \cup \{w\}$ and $E' = \{e' \in E : e' \cap e = \emptyset\} \cup \{\{w, x\} : \{u, x\} \in E \text{ or } \{v, x\} \in E\}$