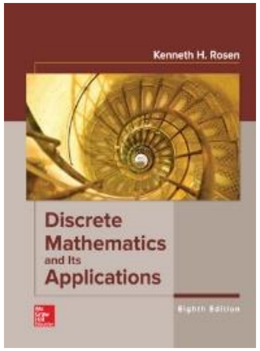
Discrete Mathematics
Lecture 1

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Course Information

- **Number theory**: integers, … (4)
- **Combinatorics**: counting, designs,… (2,6,8)
- **Logic**: propositions, predicates, proofs,… (1)
- **Graph theory**: graphs, trees, set systems ⋯ (10,11)
- **Discrete probability**: discrete distributions ⋯
- **Algebra**: matrices, groups, rings and fields ⋯
- **Theoretical computer science**: algorithms ⋯
- **Information theory**: codes ⋯
- …

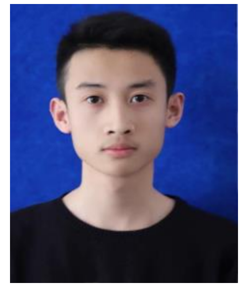


Textbook: Discrete Mathematics and Its Applications (8th edition) Kenneth H. Rosen, William C Brown Pub, 2018.

Course Information

张良峰
zhanglf
week 1-8

乔文汇
qiaowh



陈昱聪
chenyc

郑舸
zhengge

李慕天
limt1

何旭明
hexm
week 9-16

李子阳
lizy5

陈子苓
chenzl

陈雨瑶
chenyy6

Course Information

Course Materials: Lecture slides, homework questions, ...

- **Piazza**: https://piazza.com/class/kzjye4h1zeq4i3
- **Blackboard**: https://egate.shanghaitech.edu.cn/new/index.html

HW Submission: submit a soft copy (pdf/jpg) of HW solutions

- **Gradescope**: https://www.gradescope.com/courses/370554

Q&A: online Q&A, office hours, and tutorial sessions

- **Online Q&As**: post your questions to **Piazza** and get answers
- **Instructor's Office hours**: 20:00-21:00, Wednesday, SIST 2-202.i
- **TAs' Tutorial Sessions**: 19:50-21:30, Monday & Thursday

Evaluation:

- Attendance: 10% (random codes)
- Homework: 30% (no plagiarisms, firm deadline, ...)
- Midterm: 30% (on the first half of the course)
- Final Exam: 30% (on the second half of the course)

Divisibility

NOTATION: $\mathbb{N} = \{0,1,2,\dots\}$; $\mathbb{Z} = \{0,\pm 1,\dots\}$; $\mathbb{Q}$ (rational); $\mathbb{R}$ (real)

DEFINITION: Let $a \in \mathbb{Z} \setminus \{0\}$ and let $b \in \mathbb{Z}$.

- a **divides** b: there is an integer $c \in \mathbb{Z}$ such that $b = ac$
  - 因子 倍数
  - a is a **divisor** of b; b is a **multiple** of a
  - a整除b (a是b的因子)
  - $a|b$: a divides b; $a \nmid b$: a does not divide b
- $n \in \{2,3,\dots\}$ is a **prime** if the only positive divisors of n are 1 and n
  - Example: 2,3,5,7,11,13,17,19,23,29, … are all primes
- If $n \in \{2,3,\dots\}$ is not a prime, then n is called a **composite** 合数
  - Example: n is composite iff $\exists a, b \in (1,n) \cap \mathbb{Z}$ such that $n = ab$

算术基本定理

THEOREM (Fundamental Theorem of Arithmetic) Every integer $n > 1$ can be uniquely 唯一的 written as $n = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1 < \cdots < p_r$ are primes and $e_1, \dots, e_r \geq 1$.

FTA Proof

(i) 存在性 (ii) 唯一性

数归

Proof of existence: by mathematical induction on the integer n

- $n = 2$: $2 = 2^1$ is a product of prime powers
- **Induction hypothesis**: suppose there is an integer $k > 2$ such that the theorem is true for all integer n such that $2 \leq n < k$

  第2类数归

  假设 $n<k$ 时成立

  证 $n=k$ 时成立
- Prove the theorem is true for $n = k$
  - $n = k$ is a prime
    - $n = k$ is a product of prime powers
  - $n = k$ is composite
    - There are integers n_1, n_2 such that $1 < n_1, n_2 < n$ and $n = n_1 n_2$
    - By induction hypothesis, $n_1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $n_2 = q_1^{\beta_1} \cdots q_s^{\beta_s}$
      - $p_1, \ldots, p_r, q_1, \ldots, q_s$ are primes; $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \geq 1$
    - $n = n_1 n_2 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdots q_s^{\beta_s}$ is a product of prime powers

存在性 □

Division Algorithm 带余除法

良序公理

任何一个非空集合都有最小元素

The Well-Ordering Property: Every non-empty subset of $\mathbb{N}$ (the set of nonnegative integers) has a least element.

THEOREM (Division Algorithm) Let $a, b \in \mathbb{Z}$ and $b > 0$. Then there are unique $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ and $a = bq + r$.

- **Existence:** Let $S = \{a - bx\colon\ x \in \mathbb{Z} \text{ and } a - bx \geq 0\}$. Then

  S中元素 $\quad r = a - bq \quad$ x可为负

  - $S \neq \emptyset$ and $S \subseteq \mathbb{N}$
    - S has a least element, say $r = a - bq \geq 0$

存在且唯一

    - If $r \geq b$, then $r - b = a - b(q+1) \in S$ and $r - b < r$.
      - The contradiction shows that $0 \leq r < b$.
- **Uniqueness:** Suppose that $q', r' \in \mathbb{Z}, 0 \leq r' < b$ and $a = bq' + r'$
  - Recall that $a = bq + r, 0 \leq r < b$.
    - Then $b(q - q') = r' - r \in (-b, b)$
      - It must be the case that $q = q'$ and thus $r = r'$

$\mathbb{Z}$

Ideal 理想

非空集

DEFINITION: Let $I \subseteq \mathbb{Z}$ be ~~nonempty~~. I is caled an **ideal** of $\mathbb{Z}$ if

- $a, b \in I \Rightarrow a + b \in I$; and
- $a \in I, r \in \mathbb{Z} \Rightarrow ra \in I$
  - Example: $d\mathbb{Z} = \{0, \pm d, \pm 2d, \dots\}$ is an ideal of $\mathbb{Z}$ for all $d \in \mathbb{Z}$

THEOREM: Let I be an ideal of $\mathbb{Z}$. Then $\exists d \in \mathbb{Z}$ such that $I = d\mathbb{Z}$

- If $I = \{0\}$, then $d = 0$;
- Otherwise, let $S = \{a \in I: a > 0\}$.
  - $S \subseteq \mathbb{N}$ and $S \neq \emptyset$
  - due to well-ordering property, S has a least element, say $d \in S$.
    - $d\mathbb{Z} \subseteq I$
      - $d \in I \Rightarrow dr \in I$ for any $r \in \mathbb{Z}$
    - $I \subseteq d\mathbb{Z}$
      - $\forall x \in I, x = dq + r, 0 \leq r < d$
      - $r = x - dq \in I, 0 \leq r < d$
      - $r = 0$ // otherwise, there is a contradiction
      - $x = dq \in d\mathbb{Z}$

Ideal

DEFINITION: Let I_1, I_2 be ideals of $\mathbb{Z}$. Then the **sum** of I_1 and I_2 is defined as $I_1 + I_2 = \{x + y: x \in I_1, y \in I_2\}$

THEOREM: If I_1, I_2 are ideals of $\mathbb{Z}$, then $I_1 + I_2$ is an ideal of $\mathbb{Z}$.

- $\forall\, a, b \in I_1 + I_2, a + b \in I_1 + I_2$
  - $\exists x_1, x_2 \in I_1, y_1, y_2 \in I_2$ such that $a = x_1 + y_1; b = x_2 + y_2$
  - $a + b = (x_1 + x_2) + (y_1 + y_2) \in I_1 + I_2$
- $\forall a \in I_1 + I_2, r \in \mathbb{Z},\ ra \in I_1 + I_2$
  - $\exists x \in I_1, y \in I_2$ such that $a = x + y$
  - $ra = (rx) + (ry) \in I_1 + I_2$

EXAMPLE: $3\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$; $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$

- $3\mathbb{Z} + 5\mathbb{Z} \subseteq \mathbb{Z}$: this is obvious
- $\mathbb{Z} \subseteq 3\mathbb{Z} + 5\mathbb{Z}$:
  - For every $n \in \mathbb{Z},\ n = 3 \cdot (2n) + 5 \cdot (-n) \in 3\mathbb{Z} + 5\mathbb{Z}$

QUESTION: $a\mathbb{Z} + b\mathbb{Z} =?$

Greatest Common Divisor

DEFINITION: Let $a, b \in \mathbb{Z}$ and at least one of them is nonzero.

- **common divisor**: an integer d such that $d|a, d|b$
- **greatest common divisor** $\gcd(a, b)$**:** the largest common divisor
  - **relatively prime**: $\gcd(a, b) = 1$

THEOREM: Let $a, b \in \mathbb{Z}$ and at least one of them is nonzero.

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

- $\{a, b\} \neq \{0\} \Rightarrow a\mathbb{Z} + b\mathbb{Z} \neq \{0\}$

without loss of generalorsity

- There exists $d \in \mathbb{Z} \setminus \{0\}$ such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. W.l.o.g., $d > 0$.
  - d is a common divisor of a, b: $a \cdot 1 + b \cdot 0 \in d\mathbb{Z}$
  - d is greatest: Suppose that d' is a common divisor of a, b
    - $d'|a, d'|b$
    - $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \Rightarrow d = as + bt$ for some integers s, t
      - $d'|d$ and thus $d' \leq d$

?

THEOREM: There exist $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$.

FTA Proof

THEOREM: If $a, b, c \in \mathbb{Z}, c|ab$ and $\gcd(c, a) = 1$, then $c|b$.

- There exist s, t such that $1 = \gcd(a, c) = as + ct$.
  - $b = bas + bct$
  - $c|ab, c|ct \Rightarrow c|(bas + bct) \Rightarrow c|b$

THEOREM: If p is a prime and $p|ab$, then $p|a$ or $p|b$.

- $p|a$: done
- $p \nmid a \Rightarrow \gcd(p, a) = 1$
  - $\gcd(p, a) = 1 \wedge p|ab \Rightarrow p|b$

Fundamental Theorem of Arithmetic: proof of uniqueness

- Suppose that $n = p_1 \cdots p_r = q_1 \cdots q_s$, where p_i, q_j are all primes
  - $p_1|n \Rightarrow p_1|q_1 \cdots q_s \Rightarrow p_1|q_j$ for some $j \Rightarrow p_1 = q_j$
  - W.l.o.g., we suppose that $j = 1$. Then $p_2 \cdots p_r = q_2 \cdots q_s$
  - The theorem is true by induction.

FTA Applications

THEOREM: Suppose that $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, b = p_1^{\beta_1} \cdots p_r^{\beta_r}$. Then

$$d := p_1^{\min(\{\alpha_1,\beta_1\})} \cdots p_r^{\min(\{\alpha_r,\beta_r\})} = \gcd(a,b).$$

- d is a common divisor of a, b
- d is largest among the common divisors
  - Suppose that d' is a common divisor of a, b
  - $d' = p_1^{e_1} \cdots p_r^{e_r}$
    - $d'|a \Rightarrow e_i \leq \alpha_i$ for all $i \in [r]$; $d'|b \Rightarrow e_i \leq \beta_i$ for all $i \in [r]$
      - $e_i \leq \min\{\alpha_i, \beta_i\}$ for all $i \in [r]$

THEOREM: There are infinitely many primes.

- Suppose there are only n primes: $p_1, \ldots, p_n$
- By FTA, $N = p_1 \cdots p_n + 1$ must be the product of primes
- $\exists i \in [n]$ such that $p_i | N$
- But $p_i \nmid N$

Equivalence Relation

DEFINITION: Let A, B be two sets. A **binary relation** from A to B is a subset $R \subseteq A \times B$. // aRb means $(a, b) \in R$

EXAMPLE: $R = \{(a, a): a \in \mathbb{Z}^+\}$ is a binary relation from $\mathbb{Z}^+$ to $\mathbb{Z}^+$

- aRb means that $a = b$; R is "$=$"

DEFINITION: Let A be a set. An **equivalence relation** R on A is a binary relation R from A to A such that

- **Reflexive**: aRa for all $a \in A$
- **Symmetric**: $aRb \Rightarrow bRa$ for all $a, b \in A$
- **Transitive**: $aRb, bRc \Rightarrow aRc$ for all $a, b, c \in A$

DEFINITION: The **equivalence class** of $a \in A$ is the set

$$[a]_R = \{x \in A: xRa\}$$

Congruence

THEOREM: Let $n \in \mathbb{Z}^+$. Then $R = \{(a, b) \in \mathbb{Z}^2 : n|(a - b)\}$ is an equivalence relation on $\mathbb{Z}$ (from $\mathbb{Z}$ to $\mathbb{Z}$).

- R is a binary relation from $\mathbb{Z}$ to $\mathbb{Z}$
  - Reflexive: $n|(a - a) \Rightarrow aRa$
  - Symmetric: $aRb \Rightarrow n|(a - b) \Rightarrow n|(b - a) \Rightarrow bRa$
  - Transitive: $aRb, bRc \Rightarrow n|(a - b), n|(b - c) \Rightarrow n|(a - c) \Rightarrow aRc$

DEFINITION: Let $n \in \mathbb{Z}^+$ and $R = \{(a, b) \in \mathbb{Z}^2 : n|(a - b)\}$.

- The notation $\boldsymbol{a \equiv b}$ **(mod** $\boldsymbol{n}$**)** means that aRb.
  - $a \equiv b \pmod{n}$ is called a **congruence**
    - Read as: a is **congruent** to b modulo n
    - n is called the **modulus** of the congruence
  - $\boldsymbol{a \not\equiv b}$ **(mod** $\boldsymbol{n}$**)**: $(a, b) \notin R$, or equivalently $n \nmid (a - b)$
    - Read as: a is not congruent to b modulo n

Congruence

THEOREM: Let $n \in \mathbb{Z}^+$. For any $a \in \mathbb{Z}$, there is a unique integer r such that $0 \leq r < n$ and $a \equiv r \pmod{n}$.

- **Existence**: by division algorithm, $\exists\ q, r \in \mathbb{Z}$ s.t. $0 \leq r < n, a = qn + r$
  - $a \equiv r \pmod{n}$
- **Uniqueness**: suppose that $0 \leq r' < n$ and $a \equiv r' \pmod{n}$
  - $|r - r'| < n$ and $r \equiv r' \pmod{n}$
    - $|r - r'| < n$ and $n|(r - r')$
      - $r = r'$

DEFINITION: Let $a, n \in \mathbb{Z}$ and $n > 0$. Then there are unique integers q, r such that $0 \leq r < n$ and $a = nq + r$.

- We define $a \bmod n$ as r.

Residue Class

DEFINITION: Let $\alpha \in \mathbb{R}$.

- $\lfloor \alpha \rfloor$: **floor** of α, the largest integer $\leq \alpha$
- $\lceil \alpha \rceil$: **ceiling** of α, the smallest integer $\geq \alpha$
  - If $a = bq + r$, then $q = \lfloor a/b \rfloor$ and $r = a - bq$

DEFINITION: Let $a \in \mathbb{Z}, n \in \mathbb{Z}^+$. We denote the equivalence class of a under the equivalence relation mod n with $[a]_n$ and call it the **residue class of** a mod n.

- $[a]_n = a + n\mathbb{Z} = \{a + nx : x \in \mathbb{Z}\}$
  - any element of $[a]_n$ is a **representative** of $[a]_n$

EXAMPLE: $[0]_6 = \{0, \pm 6, \pm 12, \dots\}$; $[1]_6 = \{\dots, -11, -5, 1, 7, 13, \dots\}$; …