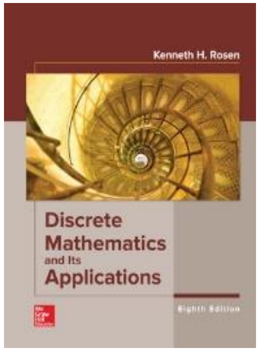
Discrete Mathematics

prime, fundamental theorem of arithmetic, well-ordering property, division algorithm, ideal, great common divisor

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

Course Information

Course Materials: Lecture slides, homework questions, …

- **Piazza**: https://piazza.com/class/lsym548ojzg5xr/
- **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/742757 **(DPVK3Y)**

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**: TBD

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)

Elementary Number Theory

Divisibility

- primes, division algorithm, greatest common divisor, fundamental theorem of arithmetic

Congruences

- congruence, residue classes, Euler’s theorem

Application (Public-key encryption)

- RSA, modular arithmetics, square and multiply, Euclidean algorithm, prime number generation, CRT

Application (Key exchange)

- groups, subgroups, cyclic groups, DLog, Diffie-Hellman key exchange

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 $b = ac$
  - a is a **divisor** of b; b is a **multiple** of a
  - $a|b$: 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**
  - Example: n is composite iff $\exists a, b \in (1, n) \cap \mathbb{Z}$ such that $n = ab$

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

- Euclid (300 BC)-> Al-Farisi (1319)-> Prestet (1689)->Euler (1770)->Legendre (1798)->Gauss (1801)

FTA Proof

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 $2 \leq n < k$
- 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 $n_2 = q_1^{\beta_1} \cdots q_s^{\beta_s}$
            - $p_1, \dots, p_r, q_1, \dots, q_s$ are primes; $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s \geq 1$
        - $n = n_1 n_2 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdots q_s^{\beta_s}$ is a product of prime powers

Division Algorithm

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

Ideal

DEFINITION: Let $I \subseteq \mathbb{Z}$ be nonempty. I is called 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 $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$.

- $\{a, b\} \neq \{0\} \Rightarrow a\mathbb{Z} + b\mathbb{Z} \neq \{0\}$
- 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 $\gcd(a, b) = as + bt$.