Discrete Mathematics
Lecture 2

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Summary of Lecture 1

Divide, Divisor, Multiple, Prime, Composite

Fundamental Theorem of Arithmetic: $n = p_1^{e_1} \cdots p_r^{e_r}$

The Well-Ordering Property: $\emptyset \neq S \subseteq \mathbb{N} \Rightarrow \min S \in S$

Division Algorithm: $a = bq + r; 0 \leq r < b$ for unique q, r

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

- $a, b \in I \Rightarrow a + b \in I; a \in I, r \in \mathbb{Z} \Rightarrow ra \in I$

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

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

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

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: $a \cdot 1 + b \cdot 0 \in d\mathbb{Z}$ $d|a$ $a \cdot 0 + b \cdot 1 \in d\mathbb{Z}$

    $d|b$
  - d is greatest: Suppose that d' is a common divisor of a, b
    - $d'|a, d'|b$ $d' | = a \cdot x + b \cdot y \Rightarrow d' | (ax + by)$
    - $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \Rightarrow d = as + bt$ 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
  - $d' = p_1^{e_1} \cdots p_r^{e_r}$
    - $d'|a \Rightarrow e_i \le \alpha_i$ for all $i \in [r]$; $d'|b \Rightarrow e_i \le \beta_i$ for all $i \in [r]$
      - $e_i \le \min\{\alpha_i, \beta_i\}$ 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 $p_i \nmid N$

gcd (N, N+1) = 1

Equivalence Relation

$A \times B = \{(a,b) \mid a \in A, b \in B\}$

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

二元关系

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 "$=$"

等价关系

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

从集合到自己的二元关系

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

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

a所在的等价类 → $$[a]_R = \{x \in A: xRa\}$$

集合A中与a存在某种二元关系的元素的集合

Congruence 同余

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 剩余类

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

Residue Class

THEOREM: Let $n \in \mathbb{Z}^+, a, b \in \mathbb{Z}$. Then

$$[a]_n \cap [b]_n = \emptyset \text{ or } [a]_n = [b]_n.$$

- $[a]_n \cap [b]_n = \emptyset$: done
- $[a]_n \cap [b]_n \neq \emptyset$
  - $\exists c \in [a]_n \cap [b]_n$
  - $c \equiv a \pmod{n}, c \equiv b \pmod{n}$
  - $a \equiv b \pmod{n}$
  - $\exists t \in \mathbb{Z}$ such that $a = b + nt$
  - 推论 $[a]_n = \{a + nx : x \in \mathbb{Z}\} = \{b + nt + nx : x \in \mathbb{Z}\} = [b]_n$

COROLLARY: $[a]_n = [b]_n$ iff $a \equiv b \pmod{n}$.

COROLLARY: $\{[0]_n, [1]_n, \dots, [n-1]_n\}$ is a partition of $\mathbb{Z}$.

- $[a]_n \cap [b]_n = \emptyset$ for all $a, b \in \{0, 1, \dots, n-1\}$
- $\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$

$\mathbb{Z}_n$

DEFINITION: Let n be any positive integer. We define $\mathbb{Z}_n$ to be set of all residue classes modulo n.

- $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$
  - $\mathbb{Z}_n = \{0,1,\dots,n-1\}$;
- $\mathbb{Z}_n = \{[1]_n, [2]_n, \dots, [n]_n\}$
  - $\mathbb{Z}_n = \{1,2,\dots,n\}$

EXAMPLE: Two representations of the set $\mathbb{Z}_6$

- $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$
  $= \{0,1,2,3,4,5\}$
- $\mathbb{Z}_6 = \{[-3]_6, [-2]_6, [-1]_6, [0]_6, [1]_6, [2]_6\}$
  $= \{-3,-2,-1,0,1,2\}$

$\mathbb{Z}_n$

DEFINITION: Let $n \in \mathbb{Z}^+$. For all $[a]_n, [b]_n \in \mathbb{Z}_n$, define

- **addition**: $[a]_n + [b]_n = [a+b]_n$
- **subtraction**: $[a]_n - [b]_n = [a-b]_n$
- **multiplication**: $[a]_n \cdot [b]_n = [a \cdot b]_n$

Well-defined? If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$a \pm b \equiv a' \pm b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

- Hence, $[a]_n \pm [b]_n = [a']_n \pm [b']_n$; $[a]_n \cdot [b]_n = [a']_n \cdot [b']_n$
  - $a \equiv a' \pmod{n} \Rightarrow n|(a-a') \Rightarrow \exists x$ such that $a - a' = nx$
  - $b \equiv b' \pmod{n} \Rightarrow n|(b-b') \Rightarrow \exists y$ such that $b - b' = ny$
    - $(a+b) - (a'+b') = nx + ny$
    - $(a-b) - (a'-b') = nx - ny$
    - $ab - a'b' = a(b-b') + b'(a-a') = any + b'nx$

$\mathbb{Z}_n^*$

DEFINITION: Let $n \in \mathbb{Z}^+$ and $[a]_n \in \mathbb{Z}_n$. $[s]_n \in \mathbb{Z}_n$ is called an **inverse** of $[a]_n$ if $[a]_n[s]_n = [1]_n$.

- **division**: If $[a]_n\ [s]_n = [1]_n$, define $\frac{[b]_n}{[a]_n} = [b]_n \cdot [s]_n$

THEOREM: Let $n \in \mathbb{Z}^+$. $[a]_n \in \mathbb{Z}_n$ has an inverse iff $\gcd(a, n) = 1$.

- Only if: $\exists\ s$ s. t. $[a]_n[s]_n \equiv [1]_n$; $\exists\ t, as - 1 = nt$; $\gcd(a, n) = 1$
- If: $\exists\ s, t$ s. t. $as + nt = 1$; $as \equiv 1 \pmod n$

DEFINITION: Let $n \in \mathbb{Z}^+$. Define $\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n\colon \gcd(a, n) = 1\}$

- If n is prime, then $\mathbb{Z}_n^* = \{1,2, \dots, n - 1\}$
- If n is composite, then $\mathbb{Z}_n^* \subset \mathbb{Z}_n$

EXAMPLE: $\mathbb{Z}_5^* = \{1,2,3,4\}$; $\mathbb{Z}_6^* = \{1,5\}$; $\mathbb{Z}_8^* = \{1,3,5,7\}$

Euler's Phi Function

QUESTION: How many elements are there in $\mathbb{Z}_n^*$?

- $|\mathbb{Z}_n^*|$ is the number of integers $a \in [n]$ such that $\gcd(a, n) = 1$

DEFINITION: (Euler's Phi Function) $\phi(n) = |\mathbb{Z}_n^*|, \forall n \in \mathbb{Z}^+$.

- $\phi(n)$ is the number of integers $a \in [n]$ such that $\gcd(a, n) = 1$

THEOREM: Let p be a prime. Then $\forall e \in \mathbb{Z}^+, \phi(p^e) = p^{e-1}(p-1)$.

- Let $x \in [p^e]$.
- $\gcd(x, p^e) \neq 1$ iff $p|x$

  iff $x = p, 2p, \dots, p^{e-1} \cdot p$

  - $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

EXAMPLE: $\phi(3^2) = 3(3-1) = 6$

- $\mathbb{Z}_9^* = \{1,2,\cancel{3},4,5,\cancel{6},7,8,\cancel{9}\}$

EXAMPLE: $\phi(p) = p - 1$

- $\mathbb{Z}_p^* = \{1,2, \dots, p-1\}$

Euler's Phi Function

QUESTION: Formula of $\phi(n)$ for general integer n?

THEOREM: If $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, \dots, p_k$ and integers $e_1, \dots, e_k \geq 1$, then $\phi(n) = \phi\left(p_1^{e_1}\right) \cdots \phi\left(p_k^{e_k}\right)$.

Hence, $\phi(n) = n(1 - p_1^{-1}) \cdots \left(1 - p_k^{-1}\right)$.

- There are many proofs. We will see in the future.

COROLLARY: If $n = pq$ for two different primes p and q, then $\phi(n) = (p-1)(q-1)$.

EXAMPLE: $\phi(10) = (2-1)(5-1) = 4; n = 10; p = 2, q = 5$

- $\mathbb{Z}_{10}^* = \{1,\cancel{2},3,\cancel{4},\cancel{5},\cancel{6},7,\cancel{8},9,\cancel{10}\}$

Euler's Theorem

THEOREM (Euler) Let $n \geq 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} = 1$.

- $\alpha^{\phi(n)}, 1$ are both residue classes modulo n
- Suppose that $\alpha = [a]_n$ for $a \in \mathbb{Z}$. Then $\alpha^{\phi(n)} = 1$ is $([a]_n)^{\phi(n)} = [1]_n$
- How to prove?
  - Consider the map $f\colon \mathbb{Z}_n^* \to \mathbb{Z}_n^* \quad [x]_n \mapsto [a]_n \cdot [x]_n$
  - We show that f is injective
    - $f([x]_n) = f([y]_n)$
    - $[a]_n \cdot [x]_n = [a]_n \cdot [y]_n$
    - $[ax]_n = [ay]_n$
    - $n|a(x-y)$
    - $n|(x-y)$, this is because $\gcd(n,a) = 1$
      - $[x]_n = [y]_n$

Euler's Theorem

THEOREM (Euler) Let $n \geq 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} = 1$.

- $\alpha^{\phi(n)}, 1$ are both residue classes modulo n
- Suppose that $\alpha = [a]_n$ for $a \in \mathbb{Z}$. Then $\alpha^{\phi(n)} = 1$ is $([a]_n)^{\phi(n)} = [1]_n$
- How to prove?
  - Consider the map $f\colon \mathbb{Z}_n^* \to \mathbb{Z}_n^* \quad [x]_n \mapsto [a]_n \cdot [x]_n$
  - Suppose that $\mathbb{Z}_n^* = \left\{[x_1]_n, \dots, \left[x_{\phi(n)}\right]_n\right\}$.
    - $f([x_1]_n) \cdots f\left(\left[x_{\phi(n)}\right]_n\right) = [x_1]_n \cdots \left[x_{\phi(n)}\right]_n$
    - $[ax_1]_n \cdots \left[ax_{\phi(n)}\right]_n = [x_1]_n \cdots \left[x_{\phi(n)}\right]_n$
    - $\left[a^{\phi(n)} x_1 \cdots x_{\phi(n)}\right]_n = \left[x_1 \cdots x_{\phi(n)}\right]_n$
      - $n \mid (a^{\phi(n)} - 1) x_1 \cdots x_{\phi(n)}$
        - $n \mid (a^{\phi(n)} - 1)$, this is because $\gcd\left(n, x_1 \cdots x_{\phi(n)}\right) = 1$
          - $\left[a^{\phi(n)}\right]_n = [1]_n$, i. e., $([a]_n)^{\phi(n)} = [1]_n$

Fermat's Little Theorem

EXAMPLE: Understand Euler's theorem with $\mathbb{Z}_{10}^* = \{1,3,7,9\}$.

- $n = 10, \phi(n) = 4,$
- $1^4 \equiv 1 \pmod{10} \Rightarrow ([1]_{10})^4 = [1]_{10}$
- $3^4 = 81 \equiv 1 \pmod{10} \Rightarrow ([3]_{10})^4 = [1]_{10}$
- $7^4 = 2401 \equiv 1 \pmod{10} \Rightarrow ([7]_{10})^4 = [1]_{10}$
- $9^4 = 6561 \equiv 1 \pmod{10} \Rightarrow ([9]_{10})^4 = [1]_{10}$
    - Consider the map $f: \mathbb{Z}_{10}^* \to \mathbb{Z}_{10}^* \quad [x]_n \mapsto [9]_n \cdot [x]_n$
    - $f([1]_{10}) = [9]_{10} \cdot [1]_{10} = [9]_{10}; f([3]_{10}) = [7]_{10}; f([7]_{10}) = [3]_{10}, f([9]_{10}) = [1]_{10}$
    - f is injective
    - $f([1]_{10})f([3]_{10})f([7]_{10})f([9]_{10}) = [9]_{10}[7]_{10}[3]_{10}[1]_{10}$

Fermat's Little Theorem: If p is a prime and $\alpha \in \mathbb{Z}_p$.

Then $\alpha^p = \alpha$.

- This is a corollary of Euler's theorem for $n = p$
- By Euler's theorem, $\alpha^{p-1} = 1$
    - $\alpha^p = \alpha$