Basic Discrete Mathematics

Review 1

Meng Zhang

ZJU-UIUC Institute
Zhejiang University
Email: mengzhang@intl.zju.edu.cn

Topics of This Course

Logic and Mathematical Proofs

Sets and Functions

Relations

Graphs I

Graphs II

Trees

Complexity of Algorithms

Number Theory

Cryptography

Groups, Rings, and Fields*

Finite Fields*

Mathematical Induction and Recursion

Counting

Discrete Probability*

Coverage for First Midterm

1. Logic and Mathematical Proofs
2. Sets and Functions
3. Complexity of Algorithms
4. Number Theory

Lecture Schedule

1. Logic and Mathematical Proofs
2. Sets and Functions
3. Complexity of Algorithms
4. Number Theory

Propositional Logic

Proposition: a declarative sentence that is either true or false (not both).

- Conventional letters used for propositional variables are p, q, r, s, ...
- **Truth value** of a proposition: true, denoted by T; false, denoted by F.

Propositional Logic

Proposition: a declarative sentence that is either true or false (not both).

- Conventional letters used for propositional variables are p, q, r, s, ...
- **Truth value** of a proposition: true, denoted by T; false, denoted by F.

Compound propositions are build using logical connectives:

- Negation $\neg$
- Conjunction $\wedge$
- Disjunction $\vee$
- Exclusive or $\oplus$
- Implication $\rightarrow$
- Biconditional $\leftrightarrow$

Tautology and Logical Equivalences

- Tautology: A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it.
  - E.g., $p \vee \neg p$
- Contradiction: A compound proposition that is always false.

Tautology and Logical Equivalences

- Tautology: A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it.
  - E.g., $p \vee \neg p$
- Contradiction: A compound proposition that is always false.

The compound propositions p and q are called logically equivalent, denoted by $p \equiv q$, if $p \leftrightarrow q$ is a tautology.

- E.g., $\neg(p \vee q)$ and $\neg p \wedge \neg q$

Tautology and Logical Equivalences

- Tautology: A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it.
  - E.g., $p \vee \neg p$
- Contradiction: A compound proposition that is always false.

The compound propositions p and q are called logically equivalent, denoted by $p \equiv q$, if $p \leftrightarrow q$ is a tautology.

- E.g., $\neg(p \vee q)$ and $\neg p \wedge \neg q$

That is, two compound propositions are equivalent if they always have the same truth value.

Tautology and Logical Equivalences

- Tautology: A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it.
  - E.g., $p \vee \neg p$
- Contradiction: A compound proposition that is always false.

The compound propositions p and q are called logically equivalent, denoted by $p \equiv q$, if $p \leftrightarrow q$ is a tautology.

- E.g., $\neg(p \vee q)$ and $\neg p \wedge \neg q$

That is, two compound propositions are equivalent if they always have the same truth value.

Determine logically equivalent propositions using:

- Truth table
- Logical Equivalences

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Important Logical Equivalences

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws

Important Logical Equivalences

$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

$$p \rightarrow q \equiv \neg p \vee q$$

Useful Law

Predicate Logic and Quantified Statements

Predicate Logic: make statements with variables: $P(x)$.

Propositional function $P(x) \overset{\text{specify } x}{\Longrightarrow}$ Proposition

Predicate Logic and Quantified Statements

Predicate Logic: make statements with variables: $P(x)$.

Propositional function $P(x) \overset{\text{specify } x}{\Longrightarrow}$ Proposition

Quantified Statements: Universal quantifier $\forall x P(x)$; Existential quantifier $\exists x P(x)$

Statement	When true?	When false?
$\forall$x P(x)	P(x) true for all x	There is an x where P(x) is false.
$\exists$x P(x)	There is some x for which P(x) is true.	P(x) is false for all x.

Propositional function $P(x) \overset{\text{for all/some } x \text{ in domain}}{\Longrightarrow}$ Proposition

Negation and Nest Quantifier

Negation	Equivalent Statement	When Is Negation True?	When False?
$\neg\ \exists x\ P(x)$	$\forall x\ \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\ \forall x\ P(x)$	$\exists x\ \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Negation and Nest Quantifier

Negation	Equivalent Statement	When Is Negation True?	When False?
$\neg\, \exists x\ P(x)$	$\forall x\ \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\, \forall x\ P(x)$	$\exists x\ \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

Statement	***When True?***	***When False?***
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y.	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y.

INSTITUTE
Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Validity of Argument Form:

The argument form with premises $p_1, p_2, ..., p_n$ and conclusion q is valid, if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q \text{ is a tautology.}$$

Note: According to the definition of $p \to q$, we do not worry about the case where $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ is false.

Rules of Inference for Propositional Logic

Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \land (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \land (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \lor q$ $\neg p$ $\therefore q$	$((p \lor q) \land \neg p) \to q$	Disjunctive syllogism

Rules of Inference for Propositional Logic

$\begin{array}{rl} & p \\ \hline \therefore & p \vee q \end{array}$	$p \rightarrow (p \vee q)$	Addition
$\begin{array}{rl} & p \wedge q \\ \hline \therefore & p \end{array}$	$(p \wedge q) \rightarrow p$	Simplification
$\begin{array}{rl} & p \\ & q \\ \hline \therefore & p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\begin{array}{rl} & p \vee q \\ & \neg p \vee r \\ \hline \therefore & q \vee r \end{array}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

Rules of Inference for Propositional Logic

Rule of Inference	***Name***
$\forall x P(x)$ $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore \exists x P(x)$	Existential generalization

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Methods of Proving Theorems

A proof is a valid argument that establishes the truth of a mathematical statement.

- **Direct proof**

  $p \to q$ is proved by showing that if p is true then q follows

- **Proof by contrapositive**

  show the contrapositive $\neg q \to \neg p$

- **Proof by contradiction**

  show that $(p \wedge \neg q)$ contradicts the assumptions

- **Proof by cases**

  give proofs for all possible cases

- **Proof of equivalence**

  $p \leftrightarrow q$ is replaced with $(p \to q) \wedge (q \leftarrow p)$

Proof Exercise 1

Prove that $\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Proof Exercise 1

Prove that $\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof: Suppose that $\sqrt{2}$ is rational. Then, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest terms.)

Since $\sqrt{2} = a/b$, it follows that $2b^2 = a^2$. By the definition of an even integer, it follows that a^2 is even, so a is even (see Exercise 16).

Since a is even, $a = 2k$ for some integer k. Thus, $b^2 = 2k^2$. This implies that b^2 is even, so b is even.

As a result, a and b have a common factor 2, which contradicts our assumption.

Proof Exercise 2

Show that there exist irrational numbers x and y such that x^y is rational.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Proof Exercise 2

Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have two irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ with $x^y = \sqrt{2}^{\sqrt{2}}$ rational.

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We have $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ is rational.

Note that although we do not know which case works, we know that one of the two cases has the desired property.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Lecture Schedule

1 Logic and Mathematical Proofs

2 Sets and Functions

3 Complexity of Algorithms

4 Number Theory

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Sets

A set is an unordered collection of objects.

- listing (enumerating) the elements
- if enumeration is hard, use ellipses (...)
- definition by property, using the set builder

$$\{x \mid x \text{ has property } P \text{ or property } P(x))\}$$

Sets

A set is an unordered collection of objects.

- listing (enumerating) the elements
- if enumeration is hard, use ellipses (...)
- definition by property, using the set builder

$$\{x \mid x \text{ has property } P \text{ or property } P(x))\}$$

Proof of Subset:

- Showing $A \subseteq B$: if x belongs to A, then x also belongs to B.
- Showing $A \not\subseteq B$: find a single $x \in A$ such that $x \notin B$.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Sets

A set is an unordered collection of objects.

- listing (enumerating) the elements
- if enumeration is hard, use ellipses (...)
- definition by property, using the set builder

$$\{x \mid x \text{ has property } P \text{ or property } P(x))\}$$

Proof of Subset:

- Showing $A \subseteq B$: if x belongs to A, then x also belongs to B.
- Showing $A \nsubseteq B$: find a single $x \in A$ such that $x \notin B$.

Prove $A = B$?

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Cardinality, Power Set, Tuples, and Cartesian Product

Cardinality: If there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a finite set and n is the cardinality of S, denoted by $|S|$.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Cardinality, Power Set, Tuples, and Cartesian Product

Cardinality: If there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a finite set and n is the cardinality of S, denoted by $|S|$.

Power Set: Given a set S, the power set of S is the set of all subsets of the set S, denoted by $\mathcal{P}(S)$.

Cardinality, Power Set, Tuples, and Cartesian Product

Cardinality: If there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a finite set and n is the cardinality of S, denoted by $|S|$.

Power Set: Given a set S, the power set of S is the set of all subsets of the set S, denoted by $\mathcal{P}(S)$.

Tuples: The ordered n-tuple $(a_1, a_2, ..., a_n)$ is the ordered collection that has a_1 as its first element and a_2 as its second element and so on.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Cardinality, Power Set, Tuples, and Cartesian Product

Cardinality: If there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a finite set and n is the cardinality of S, denoted by $|S|$.

Power Set: Given a set S, the power set of S is the set of all subsets of the set S, denoted by $\mathcal{P}(S)$.

Tuples: The ordered n-tuple $(a_1, a_2, ..., a_n)$ is the ordered collection that has a_1 as its first element and a_2 as its second element and so on.

Cartesian Product: Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$:

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

Set Operations

Union: Let A and B be sets. The union of the sets A and B, denoted by $A \cup B$, is the set $\{x \mid x \in A \vee x \in B\}$.

Intersection: The intersection of the sets A and B, denoted by $A \cap B$, is the set $\{x \mid x \in A \wedge x \in B\}$.

Complement: If A is a set, then the complement of the set A (with respect to U), denoted by $\bar{A}$ is the set $U - A$, $\bar{A} = \{x \in U \mid x \notin A\}$

Difference: Let A and B be sets. The difference of A and B, denoted by $A - B$, is the set containing the elements of A that are not in B.
$A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \bar{B}$.

Principle of inclusion–exclusion: $|A \cup B| = |A| + |B| - |A \cap B|$

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Set Identities

$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws

Set Identities

$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

A	B	$\overline{A}$	$\overline{B}$	$\overline{A \cap B}$	$\overline{A} \cup \overline{B}$
1	1	0	0	0	0
1	0	0	1	1	1
0	1	1	0	1	1
0	0	1	1	1	1

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

- $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:
  -
  -
  -

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

- $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:
  - Suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, $\neg((x \in A) \wedge (x \in B))$ is true.
  -
  -

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

- $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:
  - Suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, $\neg((x \in A) \wedge (x \in B))$ is true.
  - By applying De Morgan's law, $\neg(x \in A) \vee \neg(x \in B))$. Thus, $x \notin A$ or $x \notin B$. Using the definition of the complement of a set, $x \in \bar{A}$ or $x \in \bar{B}$.
  -

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

- $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:
  - Suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, $\neg((x \in A) \wedge (x \in B))$ is true.
  - By applying De Morgan's law, $\neg(x \in A) \vee \neg(x \in B))$. Thus, $x \notin A$ or $x \notin B$. Using the definition of the complement of a set, $x \in \bar{A}$ or $x \in \bar{B}$.
  - By the definition of union, we see that $x \in \bar{A} \cup \bar{B}$.Thus, $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$.

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

- $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:
  - Suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, $\neg((x \in A) \wedge (x \in B))$ is true.
  - By applying De Morgan's law, $\neg(x \in A) \vee \neg(x \in B))$. Thus, $x \notin A$ or $x \notin B$. Using the definition of the complement of a set, $x \in \bar{A}$ or $x \in \bar{B}$.
  - By the definition of union, we see that $x \in \bar{A} \cup \bar{B}$.Thus, $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$.
- $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: using membership tables.
Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$
Proof 3: Using set builder and logical equivalences

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Proof of Set Identities

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: using membership tables.
Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$
Proof 3: Using set builder and logical equivalences

$$
\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement} \\
&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol} \\
&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection} \\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equivalences} \\
&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol} \\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} && \text{by definition of complement} \\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} && \text{by definition of union} \\
&= \overline{A} \cup \overline{B} && \text{by meaning of set builder notation}
\end{aligned}
$$

Function

Let A and B be two sets. A function from A to B, denoted by $f : A \to B$, is an assignment of exactly one element of B to each element of A.

Function

Let A and B be two sets. A function from A to B, denoted by $f : A \to B$, is an assignment of exactly one element of B to each element of A.

- **One-to-one (injective) function**:
  - A function f is called one-to-one or injective if and only if $f(x) = f(y)$ implies $x = y$ for all x, y in the domain of f.

Function

Let A and B be two sets. A function from A to B, denoted by $f : A \to B$, is an assignment of exactly one element of B to each element of A.

- **One-to-one (injective) function**:
  - A function f is called one-to-one or injective if and only if $f(x) = f(y)$ implies $x = y$ for all x, y in the domain of f.
- **Onto (surjective) function**:
  - A function f is called onto or surjective if and only if for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$.

Function

Let A and B be two sets. A function from A to B, denoted by $f : A \to B$, is an assignment of exactly one element of B to each element of A.

- **One-to-one (injective) function**:
  - A function f is called one-to-one or injective if and only if $f(x) = f(y)$ implies $x = y$ for all x, y in the domain of f.
- **Onto (surjective) function**:
  - A function f is called onto or surjective if and only if for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$.
- **One-to-one (bijective) correspondence**
  - One-to-one and onto

Proof for One-to-One and Onto

Suppose that $f : A \to B$.

To show that f is *injective*	Show that if $f(x) = f(y)$ for all $x, y \in A$, then $x = y$
To show that f is not *injective*	Find specific elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
To show that f is *surjective*	Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$
To show that f is not *surjective*	Find a specific element $y \in B$ such that $f(x) \neq y$ for all $x \in A$

Inverse Function and Composition of Functions

Inverse function: Let f be a one-to-one correspondence (bijection) from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Inverse Function and Composition of Functions

Inverse function: Let f be a one-to-one correspondence (bijection) from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$.

Let f be a function from B to C and let g be a function from A to B. The composition of the functions f and g, denoted by $f \circ g$, is defined by $(f \circ g)(x) = f(g(x))$.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Inverse Function and Composition of Functions

Inverse function: Let f be a one-to-one correspondence (bijection) from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$.

Let f be a function from B to C and let g be a function from A to B. The composition of the functions f and g, denoted by $f \circ g$, is defined by $(f \circ g)(x) = f(g(x))$.

The floor function assigns a real number x the largest integer that is $\leq x$, denoted by $\lfloor x \rfloor$. E.g., $\lfloor 3.5 \rfloor = 3$.

Inverse Function and Composition of Functions

Inverse function: Let f be a one-to-one correspondence (bijection) from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$.

Let f be a function from B to C and let g be a function from A to B. The composition of the functions f and g, denoted by $f \circ g$, is defined by $(f \circ g)(x) = f(g(x))$.

The floor function assigns a real number x the largest integer that is $\leq x$, denoted by $\lfloor x \rfloor$. E.g., $\lfloor 3.5 \rfloor = 3$.

The ceiling function assigns a real number x the smallest integer that is $\geq x$, denoted by $\lceil x \rceil$. E.g., $\lceil 3.5 \rceil = 4$.

Sequences

A sequence is a function from a subset of the set of integers (typically the set $\{0, 1, 2, ...\}$ or $\{1, 2, 3, ...\}$) to a set S.

We use the notation a_n to denote the image of the integer n. $\{a_n\}$ represents the ordered list $\{a_1, a_2, a_3, ...\}$

Recursively Defined Sequences: provide

- One or more initial terms
- A rule for determining subsequent terms from those that precede them.

Cardinality of Sets

A set that is either finite or has the same cardinality as the set of positive integers $\mathbf{Z}^+$ is called countable.

If there is a one-to-one function from A to B, the cardinality of A is less than or equal to the cardinality of B, denoted by $|A| \leq |B|$.

Theorem: If there is a one-to-one correspondence between elements in A and B, then the sets A and B have the same cardinality.

Theorem: If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Lecture Schedule

1 Logic and Mathematical Proofs
2 Sets and Functions
3 Complexity of Algorithms
4 Number Theory

Big-O Notation

Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers.We say that $f(x)$ is $O(g(x))$ if there are constants C and k such that

$$|f(x)| \leq C|g(x)|,$$

whenever $x > k$. [This is read as "$f(x)$ is big-oh of $g(x)$."]

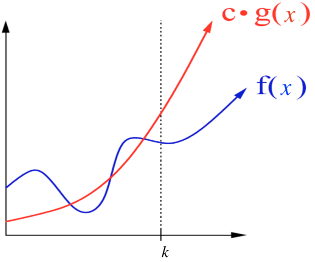
ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Big-O Notation

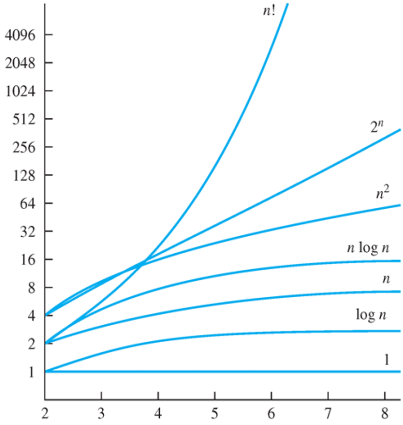
Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers.We say that $f(x)$ is $O(g(x))$ if there are constants C and k such that

$$|f(x)| \leq C|g(x)|,$$

whenever $x > k$. [This is read as "$f(x)$ is big-oh of $g(x)$."]



Big-O Estimates for Some Functions



Big-Omega Notation

Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers.We say that $f(x)$ is $\Omega(g(x))$ if there are positive constants C and k such that

$$|f(x)| \geq C|g(x)|$$

whenever $x > k$. [This is read as "$f(x)$ is big-Omega of $g(x)$."]

Big-Omega Notation

Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers.We say that $f(x)$ is $\Omega(g(x))$ if there are positive constants C and k such that

$$|f(x)| \geq C|g(x)|$$

whenever $x > k$. [This is read as "$f(x)$ is big-Omega of $g(x)$."]

Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers.We say that $f(x)$ is $\Theta(g(x))$ if

- $f(x)$ is $O(g(x))$ and
- $f(x)$ is $\Omega(g(x))$.

When $f(x)$ is $\Theta(g(x))$, we say that $f(x)$ is big-Theta of $g(x)$, that $f(x)$ is of order $g(x)$, and that $f(x)$ and $g(x)$ are of the same order.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Lecture Schedule

1 Logic and Mathematical Proofs

2 Sets and Functions

3 Complexity of Algorithms

4 Number Theory

Division

Divisibility: We say that a divides b if there is an integer c such that $b = ac$, or equivalently b/a is an integer.

- If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb + nc)$ whenever m and n are integers.

Division

Divisibility: We say that a divides b if there is an integer c such that $b = ac$, or equivalently b/a is an integer.

- If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb + nc)$ whenever m and n are integers.

Congruence Relation: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$, denoted by $a \equiv b \pmod{m}$.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Division

Divisibility: We say that a divides b if there is an integer c such that $b = ac$, or equivalently b/a is an integer.

- If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb + nc)$ whenever m and n are integers.

Congruence Relation: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$, denoted by $a \equiv b \pmod{m}$.

The integers a and b are congruent modulo m if and only if there is an integer k such that

$$a = b + km.$$

Congruence: Properties

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Congruence: Properties

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

Corollary: Let m be a positive integer and let a and b be integers. Then,

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m$$

Primes

A integer p that is greater than 1 is called a prime if the only positive factors of p are 1 and p.

- If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Primes

A integer p that is greater than 1 is called a prime if the only positive factors of p are 1 and p.

- If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Let a and b be integers, not both 0. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, denoted by $\gcd(a, b)$. Let $a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n}$. Then,

$$\gcd(a, b) = p^{\min(a_1, b_1)} p^{\min(a_2, b_2)} ... p^{\min(a_n, b_n)}$$

Primes

A integer p that is greater than 1 is called a prime if the only positive factors of p are 1 and p.

- If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Let a and b be integers, not both 0. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, denoted by $\gcd(a, b)$. Let $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$. Then,

$$\gcd(a, b) = p^{\min(a_1, b_1)} p^{\min(a_2, b_2)} \ldots p^{\min(a_n, b_n)}$$

The least common multiple of a and b is the smallest positive integer that is divisible by both a and b, denoted by $\operatorname{lcm}(a, b)$.Let $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$. Then,

$$\operatorname{lcm}(a, b) = p^{\max(a_1, b_1)} p^{\max(a_2, b_2)} \ldots p^{\max(a_n, b_n)}.$$

Euclidean Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations can be time consuming since we need to find all factors of the two integers.

For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Step 3: $14 = 7 \cdot 2 + 0$

$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

GCD as Linear Combinations

Bezout'S Theorem: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

This equation is called Bezout's identity.

GCD as Linear Combinations

Bezout'S Theorem: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

This equation is called Bezout's identity.

We can use extended Euclidean algorithm to find Bezout's identity.

GCD as Linear Combinations

Bezout'S Theorem: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

This equation is called Bezout's identity.

We can use extended Euclidean algorithm to find Bezout's identity.

Lemma: If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

GCD as Linear Combinations

Bezout'S Theorem: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

This equation is called Bezout's identity.

We can use extended Euclidean algorithm to find Bezout's identity.

Lemma: If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Lemma: If p is prime and $p|a_1a_2 \ldots a_n$, then $p|a_i$ for some i.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Linear Congruences

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

Linear Congruences

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Linear Congruences

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Modular Inverse: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

Linear Congruences

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Modular Inverse: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

Solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

$$x \equiv \bar{a}b \pmod{m}.$$

Modular Inverse

Modular Inverse: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

When does inverse exist?

Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. The inverse is unique modulo m. That is,

- there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and
- every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.

Modular Inverse

Modular Inverse: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

When does inverse exist?

Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. The inverse is unique modulo m. That is,

- there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and
- every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.

If we obtain an arbitrary inverse of a modulo m, how to obtain the inverse that is less than m?

Modular Inverse

How to find inverses?

Using extended Euclidean algorithm:

Example: Find an inverse of 101 modulo 4620. That is, find $\bar{a}$ such that $\bar{a} \cdot 101 \equiv 1 \pmod{4620}$.

With extended Euclidean algorithm, we obtain $\gcd(a, b) = sa + tb$, i.e., $1 = -35 \cdot 4620 + 1601 \cdot 101$. It tells us that -35 and 1601 are Bezout coefficients of 4620 and 101. We have

$$1 \textbf{ mod } 4620 = 1601 \cdot 101 \textbf{ mod } 4620.$$

Thus, 1601 is an inverse of 101 modulo 4620.

The Chinese Remainder Theorem

Systems of linear congruences have been studied since ancient times.

今有物不知其数 三三数之剩二 五五数之剩三 七七数之剩二 问物几何

About 1500 years ago, the Chinese mathematician Sun-Tsu asked: "There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?"

- $x \equiv 2 \pmod{3}$
- $x \equiv 3 \pmod{5}$
- $x \equiv 2 \pmod{7}$

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

The Chinese Remainder Theorem

Theorem (The Chinese Remainder Theorem): Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then, the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$.
(That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

The Chinese Remainder Theorem

Proof: To show such a solution exists: Let $M_k = m/m_k$ for $k = 1, 2, ..., n$ and $m = m_1 m_2 ... m_n$. Thus, $M_k = m_1 ... m_{k-1} m_{k+1} ... m_n$.

The Chinese Remainder Theorem

Proof: To show such a solution exists: Let $M_k = m/m_k$ for $k = 1, 2, ..., n$ and $m = m_1 m_2 ... m_n$. Thus, $M_k = m_1 ... m_{k-1} m_{k+1} ... m_n$.

Since $\gcd(m_k, M_k) = 1$, there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \pmod{m_k}$. Let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n.$$

It is checked that x is a solution to the n congruences:

The Chinese Remainder Theorem

Proof: To show such a solution exists: Let $M_k = m/m_k$ for $k = 1, 2, ..., n$ and $m = m_1 m_2 ... m_n$. Thus, $M_k = m_1 ... m_{k-1} m_{k+1} ... m_n$.

Since $\gcd(m_k, M_k) = 1$, there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \pmod{m_k}$. Let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n.$$

It is checked that x is a solution to the n congruences:

$$x \textbf{ mod } m_k = (a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n) \textbf{ mod } m_k$$

Since $M_k = m/m_k$, we have $x \textbf{ mod } m_k = a_k M_k y_k \textbf{ mod } m_k$. Since $M_k y_k \equiv 1 \pmod{m_k}$, we have $a_k M_k y_k \textbf{ mod } m_k = a_k \textbf{ mod } m_k$. Thus,

$$x \equiv a_k \pmod{m_k}.$$

The Chinese Remainder Theorem

How to prove the uniqueness of the solution modulo m?

Proof: Suppose that x and x' are both solutions to all the congruences. As x and x' give the same remainder, when divided by m_k, their difference $x - x'$ is a multiple of each m_k for all $k = 1, 2, ..., n$.

The Chinese Remainder Theorem

How to prove the uniqueness of the solution modulo m?

Proof: Suppose that x and x' are both solutions to all the congruences. As x and x' give the same remainder, when divided by m_k, their difference $x - x'$ is a multiple of each m_k for all $k = 1, 2, ..., n$.

As m_1, m_2, . . . , m_n be pairwise relatively prime positive integers, their product m divides $x - x'$, and thus x and x' are congruent modulo m, i.e., $x \equiv x' \pmod{m}$.

The Chinese Remainder Theorem

How to prove the uniqueness of the solution modulo m?

Proof: Suppose that x and x' are both solutions to all the congruences. As x and x' give the same remainder, when divided by m_k, their difference $x - x'$ is a multiple of each m_k for all $k = 1, 2, ..., n$.

As m_1, m_2, . . . , m_n be pairwise relatively prime positive integers, their product m divides $x - x'$, and thus x and x' are congruent modulo m, i.e., $x \equiv x' \pmod{m}$.

This implies that given a solution x with $0 \leq x < m$, all other solutions are congruent modulo m to this solution.

The Chinese Remainder Theorem: Example

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

The Chinese Remainder Theorem: Example

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

1. Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

The Chinese Remainder Theorem: Example

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

1. Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
2. Compute the inverse of M_k modulo m_k:
   - $35 \cdot 2 \equiv 1 \pmod{3}$ $y_1 = 2$
   - $21 \equiv 1 \pmod{5}$ $y_2 = 1$
   - $15 \equiv 1 \pmod{7}$ $y_3 = 1$

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

The Chinese Remainder Theorem: Example

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

1. Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
2. Compute the inverse of M_k modulo m_k:
   - $35 \cdot 2 \equiv 1 \pmod{3}$ $y_1 = 2$
   - $21 \equiv 1 \pmod{5}$ $y_2 = 1$
   - $15 \equiv 1 \pmod{7}$ $y_3 = 1$
3. Compute a solution x:
   $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \pmod{105}$

The Chinese Remainder Theorem: Example

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

1. Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
2. Compute the inverse of M_k modulo m_k:
   - $35 \cdot 2 \equiv 1 \pmod{3}$ $y_1 = 2$
   - $21 \equiv 1 \pmod{5}$ $y_2 = 1$
   - $15 \equiv 1 \pmod{7}$ $y_3 = 1$
3. Compute a solution x:
   $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \pmod{105}$
4. The solutions are all integers x that satisfy $x \equiv 23 \pmod{105}$.

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, \ldots m_n$ by back substitution.

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, ...m_n$ by back substitution.

Example:

(1) $x \equiv 1 \pmod 5$
(2) $x \equiv 2 \pmod 6$
(3) $x \equiv 3 \pmod 7$

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, \ldots m_n$ by back substitution.

Example:

(1) $x \equiv 1 \pmod{5}$
(2) $x \equiv 2 \pmod{6}$
(3) $x \equiv 3 \pmod{7}$

According to (1), $x = 5t + 1$, where t is an integer.

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, ...m_n$ by back substitution.

Example:

(1) $x \equiv 1 \pmod{5}$
(2) $x \equiv 2 \pmod{6}$
(3) $x \equiv 3 \pmod{7}$

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2 \pmod{6}$, which means that $t \equiv 5 \pmod{6}$. Thus, $t = 6u + 5$, where u is an integer.

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, ...m_n$ by back substitution.

Example:

(1) $x \equiv 1 \pmod{5}$
(2) $x \equiv 2 \pmod{6}$
(3) $x \equiv 3 \pmod{7}$

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2 \pmod{6}$, which means that $t \equiv 5 \pmod{6}$. Thus, $t = 6u + 5$, where u is an integer.

Substituting $x = 5t + 1$ and $t = 6u + 5$ into (3), we have $30u + 26 \equiv 3 \pmod{7}$, which implies that $u \equiv 6 \pmod{7}$. Thus, $u = 7v + 6$, where v is an integer.

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, \ldots m_n$ by back substitution.

Example:

(1) $x \equiv 1 \pmod{5}$
(2) $x \equiv 2 \pmod{6}$
(3) $x \equiv 3 \pmod{7}$

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2 \pmod{6}$, which means that $t \equiv 5 \pmod{6}$. Thus, $t = 6u + 5$, where u is an integer.

Substituting $x = 5t + 1$ and $t = 6u + 5$ into (3), we have $30u + 26 \equiv 3 \pmod{7}$, which implies that $u \equiv 6 \pmod{7}$. Thus, $u = 7v + 6$, where v is an integer.

Thus, we must have $x = 210v + 206$. Translating this back into a congruence,

$$x \equiv 206 \pmod{210}.$$

ZJU-UIUC INSTITUTE
Zhejiang University-University of Illinois at Urbana-Champaign Institute
浙江大学伊利诺伊大学厄巴纳香槟校区联合学院