Basic Discrete Mathematics

Review 2

Meng Zhang

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

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

Lecture Schedule

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 $p|a_1a_2...a_n$, then $p|a_i$ for some i.

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.

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.

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 $0 \le x < m$, and all other solutions are congruent modulo m to this solution.)

The Chinese Remainder Theorem: Example

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

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 y_k, i.e., 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 $x = a_1 M_1 y_1 + \ldots + a_n M_n y_n$: $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \pmod{105}$
4. The solutions are all integers x that satisfy $x \equiv 23 \pmod{105}$.

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 $m_1, m_2, \ldots m_n$ 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,

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

Fermat's Little Theorem

FERMAT'S LITTLE THEOREM If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer a we have

$$a^p \equiv a \pmod{p}.$$

RAS Cryptosystem

Pick two large primes p and q. Let $n = pq$. **Encryption key** (n, e) and **decryption key** (n, d) are selected such that

(1) $\gcd(e, (p-1)(q-1)) = 1$

(2) $ed \equiv 1 \pmod{(p-1)(q-1)}$

RSA encryption: $C = M^e \textbf{ mod } n$;
RSA decryption: $M = C^d \textbf{ mod } n$.

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

4 Number Theory and Cryptography

5 Mathematical Induction

6 Recursion

7 Counting

8 Relations

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 Principle of Mathematical Induction

Well-Ordering Property: Every nonempty set of nonnegative integers has a least element.

Principle. (Weak Principle of Mathematical Induction)

(a) Basic Step: the statement $P(b)$ is true

(b) Inductive Step: the statement $P(n-1) \rightarrow P(n)$ is true for all $n > b$

Thus, $P(n)$ is true for all integers $n \geq b$.

Principle (Strong Principle of Mathematical Induction):

(a) Basic Step: the statement $P(b)$ is true

(b) Inductive Step: for all $n > b$, the statement

$$P(b) \wedge P(b+1) \wedge \ldots \wedge P(n-1) \rightarrow P(n) \text{ is true.}$$

Then, $P(n)$ is true for all integers $n \geq b$.

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

Lecture Schedule

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

Recurrence

To specify a function on the basis of a recurrence:

- Basis step (initial condition): Specify the value of the function at zero.
- Recursive step: Give a rule for finding its value at an integer from its values at smaller integers.

Find a closed-form solution? "Top-down" and "bottom-up"

$$
\begin{aligned}
T(n) &= rT(n-1)+a \\
&= r(rT(n-2)+a)+a \\
&= r^2T(n-2)+ra+a \\
&= r^2(rT(n-3)+a)+ra+a \\
&= r^3T(n-3)+r^2a+ra+a \\
&= r^3(rT(n-4)+a)+r^2a+ra+a \\
&= r^4T(n-4)+r^3a+r^2a+ra+a.
\end{aligned}
$$

$$
\begin{aligned}
&T(0)=b \\
&T(1)=rT(0)+a=rb+a \\
&T(2)=rT(1)+a=r(rb+a)+a=r^2b+ra+a \\
&T(3)=rT(2)+a=r^3b+r^2a+ra+a
\end{aligned}
$$

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

Mathematical induction.

Lecture Schedule

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

Counting

Product Rule: If a count of elements can be broken down into a sequence of dependent counts where the first count yields n_1 elements, the second n_2 elements, and k-th count n_k elements, then the total number of elements is

$$n = n_1 \times n_2 \times ... \times n_k$$

Sum Rule:

- A task can be done either in one of n_1 ways or in one of n_2 ways
- None of the set of n_1 ways is the same as any of the set of n_2 ways

The Subtraction Rule:

- A task can be done in either n_1 ways or n_2 ways
- **Principle of inclusion–exclusion**:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

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

Pigeonhole Principle

Assume that there are a set of objects and a set of bins to store them.

The Pigeonhole Principle: If k is a positive integer and $k + 1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

If N objects are placed into k bins, then there is at least one bin containing at least $\lceil N/k \rceil$ objects.

Permutations and Combinations

Theorem: If n is a positive integer and r is an integer with $1 \leq r \leq n$, then there are

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

r-permutations of a set with n distinct elements.

Theorem: For integers n and r with $0 \leq r \leq n$, the number of r-element subsets of an n-element set is

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

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

Combinatorial Proof

Theorem: Let n and r be nonnegative integers with $r \leq n$. Then $C(n, r) = C(n, n - r)$.

Definition: A combinatorial proof of an identity is

- a proof that uses counting arguments to prove that both sides of the identity count the same objects but in different ways
- or a proof that is based on showing that there is a bijection between the sets of objects counted by the two sides of the identity.

These two types of proofs are called double counting proofs and bijective proofs, respectively.

The Binomial Theorem

Let x and y be variables, and let n be a nonnegative integer:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

Corollary: Let n be a nonnegative integer,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Theorem: Let n and k be positive integers with $n \geq k$. Then,

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Labelling and Trinomial Coefficients

If we have k_1 labels of one kind (e.g., red), k_2 labels of a second kind (e.g., blue), and $k_3 = n - k_1 - k_2$ labels of a third kind (e.g., green).

How many different ways to label n distinct objects?

$$\begin{aligned}\binom{n}{k_1}\binom{n-k_1}{k_2} &= \frac{n!}{k_1!(n-k_1)!}\frac{(n-k_1)!}{(k_2)!(n-k_1-k_2)!} \\ &= \frac{n!}{k_1!k_2!(n-k_1-k_2)!} = \frac{n!}{k_1!k_2!k_3!}\end{aligned}$$

This is called a trinomial coefficient and denote it as

$$\binom{n}{k_1 \quad k_2 \quad k_3} = \frac{n!}{k_1!k_2!k_3!},$$

where $k1 + k2 + k3 = n$.

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

Solving Linear Homogeneous Recurrence Relations

Definition: A linear homogeneous relation of degree k with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k},$$

where c_1, c_2, . . . , c_k are real numbers, and $c_k \neq 0$.

By induction, such a recurrence relation is uniquely determined by this recurrence relation and k initial conditions a_0, a_1, ... , a_{k-1}.

Solving Linear Homogeneous Recurrence Relations

The characteristic equation (CE) is:

$$r^k - \sum_{i=1}^{k} c_i r^{k-i} = 0.$$

Theorem: Suppose that there are t roots $r_1, \ldots, r_t$ with multiplicities $m_1, \ldots, m_t$. Then,

$$\begin{aligned} a_n = \ & (\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n \\ & + (\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha_{2,m_2-1} n^{m_2-1}) r_2^n \\ & + \cdots + (\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n \end{aligned}$$

- Solving the roots with CE
- Solving the α_i for all i using initial conditions

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 Nonhomogeneous Recurrence Relations

Definition: A linear nonhomogeneous relation with constant coefficients may contain some terms $F(n)$ that depend only on n

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k} + F(n).$$

The recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k}$ is called the associated homogeneous recurrence relation.

Theorem: If $\{a_n^{(p)}\}$ is any particular solution to the linear nonhomogeneous relation with constant coefficients,

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k} + F(n),$$

Then all its solutions are of the form

$$a_n = a_n^{(p)} + a_n^{(h)},$$

where $\{a_n^{(h)}\}$ is any solution to the associated homogeneous recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k}$.

Linear Nonhomogeneous Recurrence Relations

Suppose that $\{a_n\}$ satisfies the linear nonhomogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n),$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and

$$F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n,$$

where $b_0, b_1, \ldots, b_t$ and s are real numbers. When s is not a root of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form

$$(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

When s is a root of this characteristic equation and its multiplicity is m, there is a particular solution of the form

$$n^m (p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

Linear Nonhomogeneous Recurrence Relations

Find all solutions of the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2} + 7^n$.

Solution:

- $a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$
- Let $a_n^{(p)} = C \cdot 7^n$:

  $$C \cdot 7^n = 5C \cdot 7^{n-1} - 6C \cdot 7^{n-2} + 7^n.$$

  Thus, $C = 49/20$, and $a_n^{(p)} = (49/20)7^n$.
- Solve α_i in $a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n + (49/20)7^n$ using initial conditions.

Generating Function

The generating function for the sequence $a_0, a_1, \ldots, a_k, \ldots$ of real numbers is the infinite series

$$G(x) = a_0 + a_1 x + \ldots + a_k x^k + \ldots = \sum_{k=0}^{\infty} a_k x^k.$$

Example:

- The sequence $\{a_k\}$ with $a_k = 3$

$$\sum_{k=0}^{\infty} 3x^k$$

- The sequence $\{a_k\}$ with $a_k = 2^k$

$$\sum_{k=0}^{\infty} 2^k x^k$$

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

Generating Function: Finite Series

A finite sequence $a_0, a_1, \ldots, a_n$ can be easily extended by setting $a_{n+1} = a_{n+2} = \ldots = 0$.

The generating function $G(x)$ of this infinite sequence $\{a_n\}$ is a polynomial of degree n, i.e.,

$$G(x) = a_0 + a_1 x + \ldots + a_n x^n.$$

Example: What is the generating function for the sequence $a_0, a_1, \ldots, a_m$, with $a_k = C(m, k)$?

$$G(x) = C(m, 0) + C(m, 1)x + C(m, 2)x^2 + \ldots + C(m, m)x^m.$$

Based on binomial theorem, $G(x) = (1 + x)^m$.

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

Operations of Generating Functions

Theorem: Let $f(x) = \sum_{k=0}^{\infty} a_k x_k$, and $g(x) = \sum_{k=0}^{\infty} b_k x^k$. Then,

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$$

$$f(x)g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k$$

Example 2: To obtain the corresponding sequence of $G(x) = 1/(1 - ax)^2$ for $|ax| < 1$:

Consider $f(x) = 1/(1 - ax)$ and $g(x) = 1/(1 - ax)$. Since the sequence of $f(x)$ and $g(x)$ corresponds to 1, a, a^2, ..., we have

$$G(x) = f(x)g(x) = \sum_{k=0}^{\infty} (k+1) a^k x^k.$$

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

Generating Functions

- For $|x| < 1$, function $G(x) = 1/(1-x)$ is the generating function of the sequence 1, 1, 1, 1, . . . ,

$$1/(1-x) = 1 + x + x^2 + ...$$

- For $|ax| < 1$, function $G(x) = 1/(1-ax)$ is the generating function of the sequence 1, a, a^2, a^3, . . . ,

$$1/(1-ax) = 1 + ax + a^2x^2 + ...$$

- For $|x| < 1$, $G(x) = 1/(1-x)^2$ is the generating function of the sequence 1, 2, 3, 4, 5, . . .

$$1/(1-x)^2 = 1 + 2x + 3x^2 + ...$$

Example 1

Solve the recurrence relation $a_k = 3a_{k-1}$ for $k = 1, 2, 3, \dots$ and initial condition $a_0 = 2$.

Let $G(x)$ be the generating function for the sequence $\{a_k\}$, that is, $G(x) = \sum_{k=0}^{\infty} a_k x^k$. We aim to first derive the formulation of $G(x)$.

$$
\begin{aligned}
G(x) - 3xG(x) &= \sum_{k=0}^{\infty} a_k x^k - 3\sum_{k=1}^{\infty} a_{k-1} x^k \\
&= a_0 + \sum_{k=1}^{\infty} (a_k - 3a_{k-1}) x^k \\
&= 2,
\end{aligned}
$$

Thus, $G(x) - 3xG(x) = (1 - 3x)G(x) = 2$:

$$G(x) = \frac{2}{(1-3x)}.$$

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

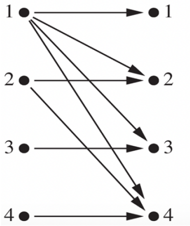
Cartesian Product

Let $A = \{a_1, a_2, ..., a_m\}$ and $B = \{b_1, b_2, ..., b_n\}$, the Cartesian product $A \times B$ is the set of pairs $\{(a_1, b_1), (a_2, b_2), ..., (a_1, b_n), ..., (a_m, b_n)\}$.

Let A and B be two sets. A binary relation from A to B is a subset of a Cartesian product $A \times B$.

A relation on the set A is a relation from A to itself.

We use the notation aRb to denote $(a, b) \in R$, and $a \not R b$ to denote $(a, b) \notin R$.



R	1	2	3	4
1	×	×	×	×
2		×		×
3			×	
4				×

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

Summary on Properties of Relations

- Reflexive Relation: A relation R on a set A is called reflexive if $(a, a) \in R$ for every element $a \in A$.
- Irreflexive Relation: A relation R on a set A is called irreflexive if $(a, a) \notin R$ for every element $a \in A$.
- Symmetric Relation: A relation R on a set A is called symmetric if $(b, a) \in R$ whenever $(a, b) \in R$ for all $a, b \in A$.
- Antisymmetric Relation: A relation R on a set A is called antisymmetric if $(b, a) \in R$ and $(a, b) \in R$ implies $a = b$ for all $a, b \in A$.
- Transitive Relation: A relation R on a set A is called transitive if $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$ for all $a, b, c \in A$.

Combining Relations

Definition: Let R be a relation from a set A to a set B and S be a relation from B to C. The composite of R and S is the relation consisting of the ordered pairs (a, c) where $a \in A$ and $c \in C$ and for which there is a $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$.

Example: Let $A = \{1, 2, 3\}$, $B = \{0, 1, 2\}$, and $C = \{a, b\}$:

- $R = \{(1, 0), (1, 2), (3, 1), (3, 2)\}$
- $S = \{(0, b), (1, a), (2, b)\}$
- $S \circ R = \{(1, b), (3, a), (3, b)\}$