教材

离散数学结构（第六版　影印版）

Discrete Mathematical Structures

(Sixth Edition)

Bernard Kolman
Robert C. Busby
Sharon Cutler Ross

高等教育出版社（教育部高等教育司推荐）
Prentice Hall　Pearson Education
出版集团　**2012.3**

参考书目

1. **“离散数学”第四版, 耿素云, 屈婉玲, 张立昂，清华大学出版社.**
2. **离散数学教程，耿素云，屈婉玲，王捍贫，北京大学出版社**
3. **离散数学, 陈莉, 刘晓霞, 高等教育出版社, 2002.8**
4. **离散数学, 孙吉贵,杨风杰, 欧阳丹彤, 李占山, 高等教育出版社,2002,8.**
5. **JH Conway & RK Guy: *The book of numbers,* Springer-Verlag, 1996, ISBN0-387-97993-X (A beautiful book – deeply subtle mathematics presented in an accessible and exciting way).**
6. **P Giblin: *Primes and programming,* Cambridge University Press, 1993, ISBN 0-521-40988-8.**

7. **RL Graham, DE Knuth & O Patashnik: *Concrete mathematics* (2 nd edition), Addison Wesley, 1994, ISBN 0-201-55802-5.**

8. **N Nissanke: *Introductory logic and sets for Computer Scientist*s, Addison-Wesley, 1999, ISBN 0-201-17957-1.**

9. **KH Rosen: *Discrete mathematics and its applications* (4 th edition), McGraw-Hill, 1999,IBN 0-07-116756-0(An excellent book covering a wide range of topics and useful throughout the course).**

考核：（平时作业+平时考勤+期中检测）50%

+期末考试（50%）

主讲教师：曾文艺

计划学时　**3** 学时/周×**17**

概述

一、离散数学的研究对象

离散数学的研究对象是离散量，即，以离散现象作为其研究对象或对象之一，包括，离散量之间的数量关系、空间结构及之间的性质。

二、离散数学的作用

离散数学是伴随着计算机科学的发展而形成的一门学科，现代数学的一个重要分支，作为计算机科学与技术学科、软件工程学科的核心课程。离散数学一方面着重培养学生的抽象思维和逻辑推理能力，掌握离散数学知识进行离散问题的数学建模；另一方面，也是为后续的相关课程（如，数据结构、操作系统、数据库原理、编译理论、数字逻辑理论、算法分析、逻辑程序设计、系统结构、容错诊断、机器定理证明、人工智能等）的学习打下良好的理论基础。

三、本课程的培养目标和主要内容

离散数学着重培养学生的离散问题建模、数学理论、计算机求解方法和技术、算法的初步认识，以及抽象思维和逻辑推理能力，同时加强科学研究方法的学习。

本学期的《离散数学》课程内容主要包括集合论、数论初步、代数结构、数理逻辑、关系和函数。

第一章　集合论基础

1 基础知识 Fundamentals

1.1集合与子集 Sets and Subsets

集合论的起源是 1874 年，29 岁的德国数学家康托尔(Cantor)在“数学杂志”发表关于无穷集合论的第一篇革命性文章，奠定了集合论的思想。
罗素称之为“可能是这个时代所能夸耀的最巨大的工作”，是现代数学的基础。

Zadeh (Fuzzy set，模糊集合), Pawlak (Rough set，粗糙集合), Tanassov(Intuitionistic fuzzy set，直觉模糊集合)

将集合的概念进行拓广。为了区分，我们将称康托的集合为“普通集合”或“经典集合”。

1.1.1　集合的表示

康托尔描述集合：所谓集合是指人们思想中将一些确定的、彼此完全不同的客体的总和考虑为一个整体，这些客体称为该集合的元素。

枚举（穷举）、谓词表示（描述）

1. $A=\{x \mid P(x)\}$

$P(x)$**是谓词 Predicate，表示元素 x 具有某种属性，满足 P(x)，即，具有性质 P 的全体对象，x 是集合 *A* 的元素**

例　$A=\{x \mid 0\le x\le 3 \wedge x\text{是实数}\}$

约定，$\wedge$：并且（且），$\vee$：或者（或）

具有某种属性的全体对象

记号(英文大写字母, A，表示集合, 英文小写字母，a，表示元素)和记法(元素可以列举，也可以满足某种性质)，元素与集合是属于或者不属于的关系。用符号$\in$, $\notin$**表示。**

2.一般来说，集合$A=\{a,b,c,d\}$**中的元素不考**

虑先后次序，也没有重复元素。

$a \in A$**, *a* is in *A*, *a* is an element of *A*.**

$f \notin A$

1.1.2　集合的例子

The set of positive integers and zero

$N = \{0,1,2,3,\cdots\}$　自然数集

The set of all integers(positive and negative integers and zero)

$Z = \{\cdots,-2,-1,0,1,2\cdots\}$　整数集

The set of all　positive integers

$Z^{+} = \{1,2,3,\cdots\}$　$\boldsymbol{Z^{+}}$**=**正整数集

The set of all rational numbers

$Q = \{\frac{n}{m} \mid n,m \in Z\}$　有理数集

The set of real number

$R = \{x \mid x\text{是实数}\}$　实数集

Ø，empty set 空集**.**

1.1.3 子集 subset（包含关系）

$$A \subseteq B \Leftrightarrow \forall x(x \in A \Rightarrow x \in B)$$.

集合相等

$A = B$ **if and only if for every *x*,** $x \in A \Leftrightarrow x \in B$.

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A.$$

例 **For any set *A*, Ø⊆*A*, *A*⊆*A*,**

$\{a,c\} \subseteq \{a,b,c\}$, $\{\{a\}\} \subseteq \{a,\{a\}\}$

$Z^{+} \subseteq N \subseteq Z \subseteq Q \subseteq R$

空集∅是任何集合的子集。

1.1.4 真子集 proper subset（真包含关系）

$$A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B$$

$$\Leftrightarrow A \subseteq B \wedge \exists x(x \in B \wedge x \notin A)$$

$$Z^{+} \subset N \subset Z \subset Q \subset R$$

$\exists$：**存在，exist,** $\forall$ **:一切，any**

1.1.5 全集 universe(论域)U 讨论对象的范围

We always assume that for each discussion there is a universal set U , for any set A in the discussion , $A \subseteq U$, for any element x in the discussion $x \in U$。

问题思考： 子集（包含关系），真子集（真包含关系）对于集合来说，似乎构成一种序关系（大小关系）？相比于实数的大小序关系，这种序关系有什么性质？

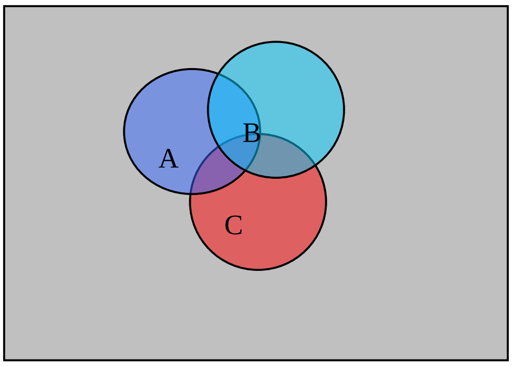
1.1.6 Venn diagrams（文氏图）

使用几何图形来形象地描述集合之间的关系

John Venn 是十九世纪英国的哲学家和数学家，1880 年，维恩（Venn）在《论命题和推理的图表化和机械化表现》一文中首次采用固定位置的交叉环形式，封闭曲线（内部区域），来表示集合及其关系。1881 年，我们称这样的图形为维恩图，也叫韦恩图或维恩图（文氏图）。

Diagrams used to show relationships between sets after the British logician John Venn.

例如：The Universe U is the rectangular box. Each set is represented by a circle and its interior. All possible combinations of the sets must be represented



1.1.7 幂集 power set 与集合族

$$P(A)=\{B \mid B \subseteq A\}$$

由集合 A 的全体子集所组成的集合。

$$P(\{a\}) = \{\varnothing, \{a\}\}$$

$$P(\{a,b\}) = \{\varnothing, \{a\}, \{b\}, \{a,b\}\}$$

$$P(\{a,b,c\}) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$$

$$P(\{a,\{a\}\}) = \{\varnothing, \{a\}, \{\{a\}\}, \{a,\{a\}\}\}$$

$$P(\varnothing) = \{\varnothing\}$$

C 是一个集合，若 C 中的元素都是集合，则称 C 为集合族，若 C={S_d| d∈D}，则称 D 为集合族 C 的标志集（指标集）。

基数：有限集合 *A* 中所包含元素的个数，称为该集合的基数，记为|*A*|. 因此，我们有：

If $|A| = n$, then $|P(A)|=2^n$.

1.2 集合的运算 Operations on the Sets

1.2.3 并 union

$$A \bigcup B = \{x \mid x \in A \vee x \in B\}$$

1.2.4 交 intersection

$$A \bigcap B = \{x \mid x \in A \wedge x \in B\}$$

1.2.5 余 complement

$$\overline{A} = U - A$$

1.2.6 差 difference

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

1.2.7 对称差 symmetric difference

$$A \oplus B = (A - B) \bigcup (B - A) = \{x \mid x \in A - B \vee x \in B - A\}$$

例 U = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

A= {1, 2, 3, 4, 5}, B = {4, 5, 6, 7, 8}.

Then

$A \cup B$ = {1, 2, 3, 4, 5, 6, 7, 8}

$A \cap B$ = {4, 5}

$\overline{A}$ = {0, 6, 7, 8, 9, 10}

$\overline{B}$ = {0, 1, 2, 3, 9, 10}

A - B = {1, 2, 3}

$\boldsymbol{B - A = \{6, 7, 8\}}$

$\boldsymbol{A \oplus B = \{1, 2, 3, 6, 7, 8\}}$

现在将并、交、余运算进行推广

$\boldsymbol{A \cap B \cap C} = \{x \mid x \in A \wedge x \in B \wedge x \in C\}$

$\bigcap_{i=1}^{n} A_i = \boldsymbol{A_1 \cap A_2 \cap \ldots \cap A_n}$

$= \{x \mid x \in A_1 \wedge x \in A_2 \wedge \cdots \wedge x \in A_n\}$

$\boldsymbol{A \cup B \cup C} = \{x \mid x \in A \vee x \in B \vee x \in C\}$

$\bigcup_{i=1}^{n} A_i = \boldsymbol{A_1 \cup A_2 \cup \ldots \cup A_n}$

$= \{x \mid x \in A_1 \vee x \in A_2 \vee \cdots \vee x \in A_n\}$

1.2.8 集合运算的代数性质

Algebraic Properties of Set Operations

Theorem 1. 集合运算满足如下性质：

交换律 **Commutative Properties**

1. $A \cap B = B \cap A$

2. $A \bigcup B = B \bigcup A$

结合律 **Associative Properties**

3. $A \bigcup (B \bigcup C) = (A \bigcup B) \bigcup C$

4. $A \bigcap (B \bigcap C) = (A \bigcap B) \bigcap C$

分配律 **Distributive Property**

5. $A \bigcap (B \bigcup C) = (A \bigcap B) \bigcup (A \bigcap C)$

6. $A \bigcup (B \bigcap C) = (A \bigcup B) \bigcap (A \bigcup C)$

幂等律 **Idempotent Properties**

7. $A \bigcap A = A$

8. $A \bigcup A = A$

复原律

9. $\overline{\overline{A}} = A$

补余率 **Properties of the Complement**

10. $A \bigcap \overline{A} = \varnothing$

11. $A \bigcup \overline{A} = U$

12. $\overline{\varnothing} = U$

13. $\overline{U} = \varnothing$

德 ·摩根律 **De Morgan's Law**（对偶律）

14. $\overline{A \bigcap B} = \overline{A} \bigcup \overline{B}$

15. $\overline{A\cup B}=\overline{A}\cap\overline{B}$

0-1 律 Properties of a universal set and the empty set

16. $A\cap U=A$

17. $A\cup U=U$

18. $A\cap\varnothing=\varnothing$

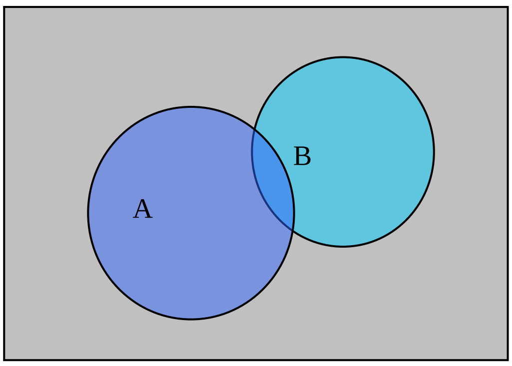
19. $A\cup\varnothing=\mathrm{A}$

1.2.9 集合运算性质的证明

Property 14: **德 摩根律 De Morgan's Law,**

$\overline{A\cap B}=\overline{A}\cup\overline{B}$

由文氏图来说明两个集合互相包含，
进而说明他们相等。



Proof: For any x,

$x \in \overline{A \bigcap B}$

$\Leftrightarrow x \notin A \bigcap B$

$\Leftrightarrow x \in A - B \vee x \in A^c \vee x \in B - A \vee x \in B^c$

$\Leftrightarrow x \in \overline{A} \vee x \in \overline{B}$

$\Leftrightarrow x \in \overline{A} \bigcup \overline{B}$

Thus, we have $\overline{A \bigcap B} \subseteq \overline{A} \bigcup \overline{B}$ **and** $\overline{A} \bigcup \overline{B} \subseteq \overline{A \bigcap B}$。

Hence $\overline{A \bigcap B} = \overline{A} \bigcup \overline{B}$**.**

集合运算的一些其它性质 Some other properties of set operations

20. $A \bigcap B \subseteq A, A \bigcap B \subseteq B$
21. $A \subseteq A \bigcup B, B \subseteq A \bigcup B$
22. $A - B \subseteq A$
23. $A - B = A \bigcap \overline{B}$
24. $A \subseteq B \Leftrightarrow A \bigcap B = A \Leftrightarrow A \bigcup B = B \Leftrightarrow A - B = \phi$
25. $A \oplus B = B \oplus A$
26. $A \oplus A = \phi$
27. $A \oplus \phi = A$

Property 23: $A-B=A\cap\overline{B}$

Proof: For any x,

$$x\in A-B$$
$$\Leftrightarrow x\in A\wedge x\notin B$$
$$\Leftrightarrow x\in A\wedge x\in\overline{B}$$
$$\Leftrightarrow x\in A\cap\overline{B}$$

Thus，we have $A-B=A\cap\overline{B}$ **.**

Example 1： $A-(B\cup C)=(A-B)\cap(A-C)$

Proof 1. (用集合相等的定义)

For any x,

$$x\in A-(B\cup C)$$
$$\Leftrightarrow x\in A\wedge x\notin B\cup C$$
$$\Leftrightarrow x\in A\wedge(x\notin B\wedge x\notin C)$$
$$\Leftrightarrow (x\in A\wedge x\notin B)\wedge(x\in A\wedge x\notin C)$$
$$\Leftrightarrow x\in(A-B)\wedge x\in(A-C)$$
$$\Leftrightarrow x\in(A-B)\cap(A-C)$$

Hence，we have

$A-(B\cup C)=(A-B)\cap($

Proof 2.（用集合运算的性质）

$$A-(B\bigcup C)=A\bigcap\overline{B\bigcup C}$$
$$=A\bigcap(\overline{B}\bigcap\overline{C})=(A\bigcap\overline{B})\bigcap(A\bigcap\overline{C})$$
$$=(A-B)\bigcap(A-C)$$

Example 2：Suppose $A\subseteq B$**, then we have:** $\overline{B}\subseteq\overline{A}$

Proof: Since $A\subseteq B$**, with the property 21, we have:** $A\subseteq B\Leftrightarrow A\bigcup B=B$ **,**
So $\overline{A\bigcup B}=\overline{B}$**. And with De Morgan's Law , we obtain** $\overline{A}\bigcap\overline{B}=\overline{B}$**. Use the property 21 again,** $\overline{A}\bigcap\overline{B}=\overline{B}\Leftrightarrow\overline{B}\subseteq\overline{A}$ **,** $\overline{B}\subseteq\overline{A}$ **is gotten.**

上述集合关系和性质的证明主要使用属于（集合互相包含）和集合的运算性质来证明。

下面，我们使用一种新的方法来刻画集合。

1.2.10 特　征　函　数　Characteristic Function

If *A* is　a subset of a universe *U*,　*A* 的特征函数 the characteristic function f_A of *A* is defined:

$$f_A : U \to \{0,1\}, x \in U \to f_A(x) \in \{0,1\}$$

for each $x \in U$ **,**

$$f_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

注释：集合与其特征函数之间的对应关系是一一对应的。

举例说明特征函数。

Theorem 1 特征函数的性质 Properties of characteristic functions

(a) 集合的交： $A \cap B$**, that is**

$f_{A\cap B}(x) = f_A(x) f_B(x)$**, for all *x*.**

(b) 集合的余：$\overline{A}$， **that is**，

$f_{\overline{A}}(x) = 1 - f_A(x)$ **for all *x*.**

(c) 集合的差：$A - B$, **that is**

$f_{A-B}(x) = f_A(x) - f_A(x) f_B(x)$ **for all *x*.**

因为 $A - B = A \cap \bar{B}$，因此

$$f_{A-B}(x) = f_A(x) f_{\bar{B}}(x) = f_A(x)(1 - f_B(x)) = f_A(x) - f_A(x) f_B(x)$$

(d) 集合的并：$A \cup B$，

如果 $A \cap B = \phi$,（空集），则

$f_{A\cup B}(x) = f_A(x) + f_B(x)$ **for all x**

一般来说，

$f_{A\cup B}(x) = f_A(x) + f_B(x) - f_A(x) f_B(x)$ **for all *x*.**

$$A \cup B = A \cup (B - A) = A \cup (B \cap \overline{A})$$

$$f_{A\cup B}(x) = f_A(x) + f_{B\cap\overline{A}}(x) = f_A(x) + f_B(x)(1 - f_A(x))$$
$$= f_A(x) + f_B(x) - f_A(x) f_B(x)$$

(e) 集合的幂运算，$A = A \cap A$，**that is**，$f_A^2(x) = f_A(x),\ \forall A \in P(X), x \in A$。

(f) 集合的对称差

$A \oplus B = (A - B) \cup (B - A)$，**that is**，

$f_{A\oplus B}(x) = f_A(x) + f_B(x) - 2 f_A(x) f_B(x)$

for all *x*.

由于 $(A - B) \cap (B - A) = \phi$，故

$$
\begin{aligned}
f_{A\oplus B}(x) &= f_{A-B}(x) + f_{B-A}(x) \\
&= f_A(x) - f_A(x) f_B(x) + f_B(x) \\
&\quad - f_A(x) f_B(x) \\
&= f_A(x) + f_B(x) - 2f_A(x) f_B(x)
\end{aligned}
$$

例： $A-(B\cup C)=(A-B)\cap(A-C)$

Proof 1.（使用集合相等的定义）

Proof 2.（使用集合运算的性质）

Proof 3.（使用特征函数）

For all x, we have:

$$
\begin{aligned}
f_{A-(B\cup C)}(x) &= f_A(x) - f_A(x) f_{B\cup C}(x) \\
&= f_A(x)(1 - f_B(x) - f_C(x) + f_B(x) f_C(x)) \\
&= f_A(x)(1 - f_B(x))(1 - f_C(x))
\end{aligned}
$$

$$
\begin{aligned}
f_{(A-B)\cap(A-C)}(x) &= f_{A-B}(x) f_{A-C}(x) \\
&= f_A(x)(1 - f_B(x)) f_A(x)(1 - f_C(x)) \\
&= f_A{}^2(x)(1 - f_B(x))(1 - f_C(x)) \\
&= f_A(x)(1 - f_B(x))(1 - f_C(x))
\end{aligned}
$$

对偶律的证明:

Proof (of the property 14 $\overline{A \cap B} = \overline{A} \cup \overline{B}$**)**

For any x,

$$f_{\overline{A\cap B}}(x) = 1 - f_{A\cap B}(x) = 1 - f_A(x) f_B(x)$$
$$= 1 - f_A(x) + 1 - f_B(x) - f_A(x) f_B(x) - 1 + f_A(x)$$
$$+ f_B(x)$$
$$= (1 - f_A(x)) + (1 - f_B(x)) - (1 - f_A(x))(1 - f_B(x))$$
$$= f_{\overline{A}\cup\overline{B}}(x)$$

Hence $\overline{A \cap B} = \overline{A} \cup \overline{B}$**.**

分配律 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

证明：

$$f_{A\cap(B\cup C)}(x) = f_A(x)[f_B(x) + f_C(x) - f_B(x) f_C(x)]$$
$$= f_A(x) f_B(x) + f_A(x) f_C(x) - f_A(x) f_B(x) f_C(x)$$
$$f_{(A\cap B)\cup(A\cap C)}(x) = f_A(x) f_B(x) + f_A(x) f_C(x)$$
$$- f_A(x) f_B(x) f_A(x) f_C(x)$$
$$= f_{A\cap(B\cup C)}(x)$$

1.2.11 （有限）集合基数的性质

The cardinality of a finite set

If a set *A* has *n* distinct elements, $n \in N$**,** ***n*** **is called the cardinality of *A* , is denoted by |*A*|.**

$$|\{a,b,c,d\}|=4,\ |\{a, \{a\}\}|=2\ ,\quad |\varnothing|=0.$$

1.2.12 (不交集合的)加法原理 The Addition Principle (of disjoint sets)

设 ***A*, *B*** 是论域 ***U*** 的两个有限子集，***A*, *B*** 不交，即 $A \cap B = \varnothing$，则 $|A \cup B| = |A| + |B|$

由文氏图可以得到。

结论 1：设 ***A*, *B*,*C*** 是论域 ***U*** 的三个有限子集，***A*,*B*,*C*** 互不相交，即 $A \cap B = \varnothing$， $B \cap C = \varnothing$， $A \cap C = \varnothing$，则

$$|A \cup B \cup C| = |A| + |B| + |C|$$

结论 2：设 ***A*, *B*** 是论域 ***U*** 的两个有限子集，

则$|A-B|=|A|-|A\cap B|$

$$A=(A-B)\cup(A\cap B),\ (A-B)\cap(A\cap B)=\phi$$

1.2.11 容斥原理 inclusion-exclusion principle

Theorem 2. 设 *A*, *B* 是有限子集，则 $|A\cup B|=|A|+|B|-|A\cap B|$.

一方面，其结论也可以由文氏图得到。

另一方面，因为

$$A\cup B=(A-B)\cup(A\cap B)\cup(B-A)$$

Theorem 3. 设 *A*, *B*,*C* 是有限子集，则

$$\begin{aligned}&|A\cup B\cup C|\\&=|A|+|B|+|C|-|A\cap B|-|A\cap C|\\&\quad-|B\cap C|+|A\cap B\cap C|\end{aligned}$$

因为

$$|A \cup B \cup C| = |((A \cup B) - C) \cup C|$$
$$= |A \cup B| - |(A \cup B) \cap C| + |C|$$
$$= |A| + |B| - |A \cap B| - |A \cap C|$$
$$- |B \cap C| + |(A \cap C) \cap (B \cap C)| + |C|$$

整理可得上式。

该结论是上述定理的推广。
对于有限集合，我们还可以进行推广。
留作思考。

下面，我们用两个实例来验证上述两个定理。

Example 3　**Let** $A=\{a, b, c, d, e\}$ **and** $B=\{c, e, f, h, k, m\}$**. Verify theorem 2.**

Solution:

$A \cup B=\{a, b, c, d, e, f, h, k, m\}$ **and**

$A \cap B=\{c, e\}$

$|A|= 5$, $|B|= 6$, $|A \cup B|= 9$ **and**

$|A \cap B|= 2$

$|A|+|B|-|A \cap B|= 9$

$|A|+|B|-|A\cap B|=|A\cup B|$

Example 4 **Let A={a, b, c, d, e}, B={a, b, e, g, h} , C={b, d, e, g, h, k, m, n}. Verify theorem 3.**

Solution:

$A\cup B\cup C=\{a, b, c, d, e, g, h, k, m, n\}$,

$A\cap B=\{a, b, e\}$,

$A\cap C=\{b, d, e\}$, $B\cap C=\{b, e, g, h\}$, and

$A\cap B\cap C=\{b, e\}$

$|A|=5$, $|B|=5$, $|C|=8$, $|A\cup B\cup C|=10$,

$|A\cap B|=3$, $|A\cap C|=3$, $|B\cap C|=4$,

$|A\cap B\cap C|=2$.

$$|A|+|B|+|C|-|A\cap B|-|B\cap C|-|A\cap C|+|A\cap B\cap C|$$

$$=5+5+8-3-3-4+2=10=|A\cup B\cup C|$$

Theorem 3 is verified.

推论 Corrallory

$$|\overline{A}\cap\overline{B}\cap\overline{C}|=|\overline{A\cup B\cup C}|$$

$$=|U|-|A|-|B|-|C|+|A\cap B|+|A\cap C|+|B\cap C|-|A\cap B\cap C|$$

问题 1：1000 以内不能被 5，6，或 8 整除的正整数有多少个？

U: 1,2,3,…,1000 的整数，
A: U 中能被 5 整除的整数，
B: U 中能被 6 整除的整数，
C: U 中能被 8 整除的整数，
则，$|U|=1000$，$|A|=200$，$|B|=166$，$|C|=125$.
$|A\cap B|=33$，$|A\cap C|=25$，$|B\cap C|=41$，
$|A\cap B\cap C|=8$.

$$|\overline{A\cap B\cap C}|$$
$$=1000-200-166-125+33+25+41-8$$
$$=600$$

问题 2：将 1,2,3,…,n 做全排列，计算 1 不在第一个位置的排列数。(n-1)(n-1)!

A: 1 在第一个位置的排列数

思考：进一步，所有 i，i=1,2,..,n 都不在第 i 个位置的个数。其排列数是

$n!(1-1/1!+1/2!-1/3!+\dots+(-1)^n 1/n!)$

$e^{-1}= 1-1/1!+1/2!-1/3!+\dots+(-1)^n 1/n!+\dots$

Homework

P11： 8(a),(f)

P12： 24

P13： 38，45，46

1.3 序列 Sequences

从数列想象序列

序列：按照一定次序排列的对象，**A sequence is simply a list of objects arranged in a definite order**

1,0,1,1,0,0,1

0,1,1,2,3,5,8,13,…,

1,4,9,16,25,…

于是，就有第一个元素，第二个元素，依次类推。

到第 **n** 个元素终止的序列叫有限 **finite** 序列，否则是无限 **infinite** 序列。

序列中元素值如何确定？有无显式的表达式？

a_n 的计算？a_n 的计算表达式（通解）。

递归 **recursived** 序列

递归：用前一项或者前若干项来定义后一项的方法叫递归，**recursive.**

注释：使用递归定义必须满足两个条件：首先，定义初值（给出原始值），然后，给出递归算法（给出计算方法）。

Example

$$c_1 = 5,\quad c_n = 2c_{n-1},\quad 2 \le n \le 6,$$

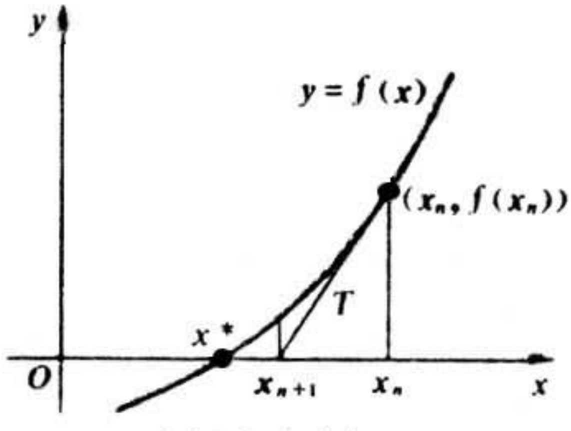
于是得到递归序列：**5，10，20，40，80，160.**

Fibonacci 序列

0, 1, 1, 2, 3, 5, 8, $a_n = a_{n-1} + a_{n-2}$ **…,**

牛顿求根迭代法：利用泰勒公式，在 x_0 处展开，且展开到一阶，即

$f(x) = f(x_0) + (x - x_0)f'(x_0)$，令 **f(x)=0**，则整个过程如下图：



牛顿法求实根图示

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

一般来说，序列中的对象可以是数值，数字，也可以是字符。如，**s, t, u, d, y.**或者 **a, b, a,**

b, a, b, …, 通常，我们使用 $a_1, a_2, a_3, a_4, \cdots\cdots,$ 来表示。特别地，字符或符号组成的序列称为**字符串 String**。

数列是大家非常熟悉的概念，数列是序列的特殊情形（特例），数列又被我们称之为“数组”。

数组 **array** 是表示序列的一种有效方法，它是实现线性表 **linear list**（序列）在计算机中进行表示的重要方式。

Remark: 数组与维数有关，一维数组就是数列，二维数组就是矩阵。从数学的角度来看，我们可以定义 **n** 维数组。

如何使用计算机来表示集合？换言之，我们的目的就是想利用计算机来表示集合，并进行集合的相关运算。

集合的序列刻画、序列的运算。

集合所对应的序列

The set corresponding to a sequence

即：使用序列中的数字或字符来刻画集合。

利用特征函数，我们可以对集合进行刻画。

计算机中**用序列 sequence 来表示一个集合**，

首先，我们将有限全集中的全体元素以一定的次序进行排列。全集的基数，$|U|$。

其次，A 是一个有限全集 U 的一个子集，A 的特征函数值就可以按照全集元素的次序**由数字 0，1 所组成的序列来刻画，该序列就可以作为集合 A 的表示。**其中，所得到的序列中的对象“1”的个数就是集合 A 中所有元素的个数。

例 **U={1,2,3,4,5,6}, A={1,2}, B={2,4,6}, C={4,5,6}**

则 $f_U = 111111,\quad f_A = 110000,$

$f_B = 010101$ ， $f_C = 000111$，

U

1	**1**	**1**	**1**	**1**	**1**

A

1	**1**	**0**	**0**	**0**	**0**

B

0	**1**	**0**	**1**	**0**	**1**

C

0	**0**	**0**	**1**	**1**	**1**

于是，利用计算机来进行对应位置的数值运算（特征函数的计算公式），以达到集合运算的目的。

从而，将集合运算转化为函数的数值运算。

众所周知，概念的运算及推理均可以归结为集合运算，因此，机器证明就变得可能了。

可数集合 **countable set**，不可数集合 **uncountable set**

一个集合称为可数的 **countable**，如果它与

自然数集合的某个子集一一对应，即，集合中的元素可以排成一列，第一个，第二个，第三个，…；否则就是不可数 **uncountable** 集合。

简单地理解，可数集合的全体元素可以一个一个地数出来，第一个，第二个，第三个，……，因此，有限集合都是可数集合。从数学的角度来说，集合中的每个元素与自然数集 **N** 的每个元素之间可以建立一对一的关系。

例如，自然数集合是无限集合，但它是可数的。推而广之，能够与自然数集合产生对应关系（一一对应）的集合就是可数集合。例如，整数集、偶数集、有理数集是可数集合。这些无限集合是可数的，虽然它们是无限集合。

相关结论：

1) 可数集合的子集是可数集合。
2) 可数个可数集合的并集是可数集合。

3) A，B 是可数集合，则 AxB 是可数集合。

4) 有限个可数集合的乘积集合是可数集合。

$$a_{11} = (1, 1) \to a_{12}$$

$$a_{13} \to a_{14}$$

$$a_{21}$$

$$\downarrow \quad a_{22} \quad a_{23}$$

$$a_{31}$$

$$a_{32}$$

$$a_{41}$$

$$\downarrow \quad \iddots$$

$$a_{51}$$

实数集是无限集合，但它是不可数集合。

However, not all infinite sets are not

countable. 需要注意的是：不是所有的无限集合都是不可数的。

康托给出了一个评判标准：如果两个集合 A，B 的元素可以建立一一对应关系，则它们的基数相等。

接下来，我们来说明实数集是不可数的。

首先，我们给出一个映射，

$$f:(0,1)\to R=(-\infty,+\infty)$$

$$x\to \tan(x-\frac{1}{2})\pi$$

可以证明，该映射是一一映射。

其次，“如果两个集合之间存在一一对应的话，则这两个集合的基数是一样的”。均为可数或不可数。

这表明，实数集 **R** 与集合（**0**，**1**）的基数是相同的。

最后，我们来说明（0，1）区间内的实数是不可数的。

反证：假设（0，1）区间内的实数是可数的，那么，我们则有一个序列 $d_1, d_2, d_3, \cdots, d_n, \cdots$ 来列出(0, 1)区间内的所有实数。每个 $i \in N$，$0<d_i<1$，

因此，我们可以用十进制小数来表示 d_i：

$$d_1 = 0.a_{11}a_{12}a_{13}\cdots$$

$$d_2 = 0.a_{21}a_{22}a_{23}\cdots$$

$$d_3 = 0.a_{31}a_{32}a_{33}\cdots$$

…

其中 $a_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}, \forall i, j$ 。

现在，我们来构造另外一个实数

$$d = 0.b_1 b_2 b_3 \cdots b_n \cdots$$

$$b_n = \begin{cases} 1, & if \quad a_{nn} = 2 \\ 2, & otherwise \end{cases}$$

不难看出 $d \in (0,1)$ 。

对任意 $k \in N, d_k = 0.a_{k1}a_{k2}...a_{kk}\cdots$，因为 $b_k \neq a_{kk}$，

故，

这与 $d_1,d_2,d_3,\cdots,d_n,\cdots$ 列出（0，1）区间内所有的实数矛盾。因此，（0，1）区间内的实数不可数，故，全体实数不可数。

结论：实数集合的开区间、闭区间、半开半闭区间均是不可数集合。

数论初步

1.4 整除 Divide

定理 1 （带余除法）对任意两个整数 n，m，$n>0$,存在整数 q, r, $0\leqslant r<n$，使 $m=qn+r$，q 和 r 都是唯一确定的。

q 叫做商 quotient, r 叫做余数 reminder.

如果整数 m 是 n 的倍数, $n>0$, 即存在整数 q， 使 $m=qn$， (r=0)，就称 **n 整除 m**，记为 **n|m**。同时 **n|m is read " n devides m".** 否则,

就说 n 不整除 m，记为 $n \nmid m$.

整除的性质：

定理 2. 设 a, b, c 是整数，

(a) $a|b,\ a|c \Rightarrow a|(bx+cy)$，x,y 是整数（线性组合）

(b) $a|b,\ a|c,\ b>c \Rightarrow a|(b-c)$

(c) $a|b$ 或 $a|c \Rightarrow a|bc$

(d) $a|b,\ b|c \Rightarrow a|c$（传递性）

(e) $a|b \Rightarrow ma|mb, m\neq 0$, m 是非零整数

(f) $a|b,\ b|a \Rightarrow |a|=|b|$

1.4.1 素数 prime

一个正整数 p>1，如果只能被 p 和 1 整除，则称 p 是素数。

如何判断 p 是素数？

算法 1：计算从 2 到 p-1 关于 p 的整除性；

例如，考虑 p=97 是否为素数？

计算从 2 到 96 关于 p=97 的整除性。

算法 2：

1. 如果 p=2，则 p 是素数，否则继续，
2. 如果 2|*p*，*p* 不是素数，否则继续，
3. 求最大整数 *K*，$k \le \sqrt{p}$，继续，
4. 看是否有奇数 *D*，$1 < D \le K$，如果 *D*|*p*，则 p 不是素数，否则 p 是素数。

例如，考虑 p=97 是否为素数？
最大整数 K=9，计算从 3 到 9 的奇数关于 p=97 的整除性，即，D=3, 5, 7, 9。

算法的数学理论根据：

对于一个自然数 p，如果 p 不是素数（合数），则其可以分解成 p=mn，那么 m,n 中必然有一个大于等于 $\sqrt{p}$，另一个小于等于 $\sqrt{p}$，也就是说一个合数必然有一个因子是小于等于 $\sqrt{p}$。所以，对于一个自然数 p，只要检验其有没有小于等于 $\sqrt{p}$ 的因子就可以了。

由第 2 步可知，p 不是偶数，故在第 4 步，我们只要考虑奇数就可以，而不用考虑偶数的情形。

算法的有效性与计算复杂性：

关于算法 1，我们需要从 2 到 p-1 进行循环检验，需要执行 p-2 次。计算量的数量级为 p。

关于算法 2，我们需要从 2 到 k 进行循环检验，需要执行 k/2 次。计算量的数量级为 $\sqrt{p}$ /2。

1.4.2 因数分解 factoring

定理 设 p,a_1,a_2,…,a_n 是整数，且 p 是素数。

如果 p| $a_1a_2\ldots a_n$，则 p| $a_1 \vee$ p| $a_2 \vee \ldots \vee$ p| a_n 。

定理 3. **（唯一分解定理）任意一个正整数 n，都可以唯一地分解为素数因数的连乘积：**

$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$，**其中** $p_1 < p_2 < \cdots < p_s$ **是整除 n 的所有互不相同的素数因数，正整数** k_i，$1 \le i \le s$ **分别是素数因数** p_i **的次数（幂）。**

例　9=3^2，　24=2^3·3，30=2·3·5。

1.4.3　最大公约数 Greatest　Common Divisor （GCD）

公约数 Common Divisor

如果$a,b,k \in Z^+$，　$k|a$, $k|b$, 则称 k 是 a,b 的公约数，或公因子（公共的约数，公共的因子）。

公约数中的最大者称之为最大公约数 d，记作 d=GCD(a,b) or d=(a,b).

例如，两个整数，12 与 18，1，2，3，6 均是他们的公约数，6 是他们的最大公约数。

定理 4.

(a)设 d=GCD(a,b)，则存在两个整数 s, t 使 $d=sa+tb$.

(b)如果 c 是 a,b 的公约数，则 $c|d$.

Proof:

令 x=sa+tb 是这种形式的最小正整数，对于任何公约数 c，有 c|a，c|b，因此，c|x，且 $c \le x$. 表明 x=sa+tb 比任何公约数 c 都大。

接下来，证明 x=sa+tb 是 a,b 的公约数。

首先，证明 x=sa+tb 是 a 的公约数。

考虑整数 a 与 x，由带余除法可知，我们有 $a=qx+r$，其中 $0 \leqslant r < x$，　则

$r = a-qx= a-q(sa+tb)=a-qsa-qtb=(1-qs)a+(-qt)b$

因此，r 是 sa+tb 这种形式的整数。

如果 $r \neq 0$，则 r 既是 sa+tb 这种形式的正整数，并且，$0 \leqslant r < x$，表明 r 与 x 的最小性相矛盾，因此，r=0. 这表明　$x|a$. 即 x 是 a 的约数。

同理，可以证明 $x|b$. 即 x 是 b 的约数。

因此，x 是 a,b 的公约数。

We complete the proof of Theorem.

Corollory　**d=GCD(a, b) if and only if**

(a) d|a and d|b.

(b) whenever c|a and c|b, then c|d.

Theorem 5. If $a,b \in Z^+$

(a) $GCD(a, b)= GCD(a,a \pm b)=GCD(a, a \pm qb)$

(b) If $0<a \leqslant b$ and $a|b$, then $GCD(a,b)=a$.

如何计算最大公约数和 s, t?

Euclidean Algorithm 欧几里德算法

用 Euclid 辗转相除法可以得到 GCD(a,b), 不妨假设 $a \geqslant b>0$，则有:

$a=q_1b+r_1, \quad 0 \leqslant r_1<b,$

$b=q_2r_1+r_2, \quad 0 \leqslant r_2<r_1,$

$r_1=q_3r_2+r_3, \quad 0 \leqslant r_3<r_2,$

....

$r_{n-2}=q_nr_{n-1}+r_n, \quad 0 \leqslant r_n<r_{n-2},$

$r_{n-1}=q_{n-1}r_n+r_{n+1}, \quad r_{n+1}=0.$

余数 r_n（非负整数）越来越小，最后等于 0，即，$r_{n+1}=0$。

$GCD(a,b)=r_n,$

这是因为

$GCD(a,b)=GCD(b,r_1)=GCD(r_1,r_2)=...=GCD(r_{n-1},r_n)=r_n$

假设 r_3 是最大公约数，相应地有：

$d=r_3=r_1-q_3r_2= r_1-q_3(b- q_2r_1)= (1+ q_3q_2)\, r_1 -q_3b$

$= (1+ q_3q_2)(a-q_1b) -q_3b$

$=(1+ q_3q_2)\, a-[(1+ q_3q_2)q_1+ q_3]\, b=as+tb$

定义　如果 GCD(a, b)=1，则称 a, b 互素。

Proposition 6

(a)　a, b 互素当且仅当存在整数 s 和 t 使 *sa+tb=1*,

GCD(a,b)=1　iff　*sa+tb=1*, s, t are integers.

充分性，由上述定理 4，显然成立。

必要性，如果存在 d，使得 a=dm, b=dn，则有

sdm+tdn=1，则 d(sm+tn)=1, d=1

(b)　两个整数 a÷GCD(a,b), b÷GCD(a,b) 互素

(c)　(a, b)=1, (a, c)=1，则 (a, bc)=1.

(d)　a|bc, (a,b)=1 ，则 a|c .

(e)　If (a, b)=1, then (a, bc)=(a, c).

EXAMPLE 4　金库内有 3 根同样粗细的金条，分别长 135、243 和 558（单位：寸）。现在要把它们截成相等的小段，要求小段要最长。问一共可以把这些金条分成几段，每段几寸。

GCD（135，243，558）=9，共有 104 段，每段 9 英寸。

最小公倍数 Least Common Multiple

设 $a, b, k \in Z^+$，$a|k$, $b|k$, 称 k 是 a,b 的公倍数。公倍数中最小的一个 c 称之为最小公倍数，记作 c=LCM(a,b)。

设 a,b 互素，则 LCM(a,b)=ab.

Theorem 6.　$GCD(a,b) \cdot LCM(a,b) = ab$.

同余运算

余数相同（被除数，除数），通过整除运算得到，5÷3，8÷3，余数相同，为 2.

抽象数学化

模函数 f_n, **mod-n function**

设 $m,n\in \mathbb{Z}^+$, $m-r=qn$

记作 $f_n(m)=r$, 或 $m\equiv r(\mathrm{mod}\ \ n)$, 简记 $m\equiv r(n)$.

Proposition

(i) $a\equiv b(n)$ **if and only if** $n|a-b$.

(ii) $a\equiv b(n)$ **and** $b\equiv c(n)$ **then** $a\equiv c(n)$

同余关系是等价关系（满足自反性，对称性，传递性）

(iii) *if* $a\equiv b(n)$ **and** $c\equiv d(n)$ **then**

$$(a\pm c)\equiv(b\pm d)(n)$$

(iV)*if* $a\equiv b(n)$ **then** $ka\equiv kb(n)$

(V)*if* $a\equiv b(n)$ **and** $c\equiv d(n)$ **then** $ac\equiv bd(n)$

因为 **a=pn+b, c=qn+d,** 因此，

ac=(pn+b)(qn+d)=pqn^2 +bqn+dpn+bd=(pqn+bq+dp)n+bd

同余关系保持加法，乘法运算的封闭性。

定理

(1) 设 m 是一个正整数，a、b、c∈Z，若 ac≡bc（m)，c|m，则 a≡b（m/c)。

(2) 设 m 是一个正整数，a、b、c∈Z，若 ac≡bc（m)，GCD(c, m) = 1，则有

a≡b (mod m)

(3) 设 m 是一个正整数，a、b、c∈Z，若 ac≡bc（m)，GCD(c,m)=d，则 a≡b（m/d）。

证明: (1) ac-bc=mq，并且 m=ck，于是我们有 a-b=qk=q(m/c)，因此，**a≡b（m/c)。**

(2) 因为 ac≡bc（mod m)，则 ac-bc=mq

有 m| ac-bc 即 m| (a-b)c。

又已知 GCD(c, m) = 1,因此,得到 m| (a-b),即

$$a \equiv b \pmod{m}$$

(3) ac-bc=mq, (a-b)c/d=q(m/d), 即，(m/d)|(a-b)c/d, 并且 m/d 与 c/d 互素，故，(m/d)|(a-b)，即，a≡b（m/d）。

进一步思考:

1） 2017 年 9 月 1 日是周五，那么 2018 年 9 月 1 日是星期几？

2） 3^406 写成十进制数时的个位数是什么？

3） 任意一个十进制的 n 位数与其各位上的各数字之和关于模 3 同余。

例如，1236 与（1+2+3+6）被 3 整除，

136 与（1+3+6）关于 3 同余，余数为 1。

数学理论根据？

思考：　2017 年 9 月 1 日是周五，问 2018 年 9 月 1 日是星期几？

星期是一个以 7 天为周期的循环，$365=52*7+1\equiv1 \pmod 7$

因此，2018 年 9 月 1 日是星期六。

3^{406} 写成十进制数时的个位数是什么？

$3^4=81\equiv1 \pmod{10}$

$3^{404}\equiv1^{101} \pmod{10} \equiv1 \pmod{10}$

$3^{406}=3^{404}*3^2\equiv9 \pmod{10}$

从而，个位数字是 9

因此，3^{406} 写成十进制数时的个位数是 9。

任意一个十进制的 n 位数与其各位上的各数字之和关于 3 同余。

思路：若 a,b,c,d 为整数，m 为正整数，若

a≡b(mod m), c≡d(mod m)，则

1）a^n≡b^n(mod m)（幂方保运算）

因为：由前述结论，我们有：ac≡bd(mod m)，推而广之，当 n 是大于 0 的整数时，我们有 a^n≡b^n(mod m)。

或者：存在 q, a=b+mq, 由二项式定理展开，有 a^n=(b+mq)^n=b^n+mK

2）(ax+cy)≡(bx+dy)(mod m), x,y 为整数(线性保运算）

因为：存在 p, q, a=b+mq, c=d+mp

ax=bx+mqx, cy=dy+mpy

ax+cy=bx+dy+m(qx+py)

3）f(a)≡f(b)(mod m), f(x)为任一整系数多项式（整系数多项式保运算）

$$f(x) = p_0x^n + p_1x^{n-1} + p_2x^{n-2} + \cdots + p_n$$

$$f(a) = p_0a^n + p_1a^{n-1} + p_2a^{n-2} + \cdots + p_n$$

$$f(b) = p_0 b^n + p_1 b^{n-1} + p_2 b^{n-2} + \cdots + p_n$$

4）十进制的 n 位数: $A = \sum_{i=0}^{n} a_i * 10^i = f(10)$

各位上的数字之和: $B = \sum_{i=0}^{n} a_i = \sum_{i=0}^{n} a_i * 1^i = f(1)$

其中， $f(x) = \sum_{i=0}^{n} a_i * x^i$

因为 **10≡1(mod 3)**，因此，**f(10)≡f(1)(mod 3)**，即，**A≡B(mod 3).**

整数分解的应用----密码模型及其应用

代数结构 **algebraic structures**

〈**A, f_1, f_2, f_3**〉

A 是论域 **Universe**（全集），**f_1, f_2, f_3** 是论域 **A** 上的运算，可以是一元运算，可以是二元

运算，也可以是三元，n 元运算，二者构成代数结构(非空集合，封闭性)。

例如，A 是论域（全体实数集合），f_1, f_2, f_3 分别是实数上的加法、减法、乘法运算，这些运算是实数上的二元运算。

(R,+), (R, -), (R,×), (R,+, -, ×)构成代数结构。

注释：论域关于其上的运算必须满足封闭性。

例如：自然数集关于加法、乘法运算封闭，（N, +），（N,×）；

自然数集关于减法不封闭，（N, -）。

对于代数结构(A, *)，集合 A 中所有元素 a 和运算*，若存在元素 e，使得 e*a=a，则称 e 为关于运算“*”的左单位元，若 a*e=a，则称 e 为关于运算“*”的右单位元；若 e*a =a*e= a，则称 e 为关于运算“*”的单位元

（既是左单位元，又是右单位元）。

注释：（R,+），(R,×)构成代数结构。

对于加法，0 是单位元；

对于乘法，1 是单位元；

例如：在实数集 R 中定义新运算“*”如下：二元运算 x*y=xy-2x-2y+6，求运算“*”的左单位元。

解: 设左单位元为 e，因此我们有，e*x=ex-2e-2x+6=x，(x-2)(e-3)=0，所以, e=3.

同理，设右单位元为 e，因此我们有，x*e=xe-2x-2e+6=x，(x-2)(e-3)=0，所以, e=3.

故 e=3 是关于运算“*”的单位元（既是左单位元，又是右单位元）。

注意：左、右单位元若存在，则二者相等。

因为 e=e*i=i

例如，**2*2** 的矩阵类，其中 **a**$\neq$0, b 是实数，关于矩阵乘法，其右单位元是:

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

无穷多个右单位元，但左单位元没有。

另外，非零实数集合{**R-0**，÷}，存在一个右单位元，**1**。

定理 **1.**（单位元的唯一性） 设〈**A, ***〉是一个代数结构，***是 A** 上的二元运算，**e** 是关于运算"*****"的单位元 **identity**，即对任意 **x∈A, x*e=e*x=x**，则 **e** 是唯一的单位元。

Proof. Assume i be another identity for operation *，then e=e*i=i.

同余运算，

对于加法运算，单位元是 **0**，因为**(0+a) mod m = a mod m**；

同理，因为**(pm+a) mod m = a mod m**；

约定：单位元小于 m.

对于乘法运算，单位元是 1，因为(1×a) mod m = a mod m

同理，因为[(1+km)×a] mod m = a mod m

约定：单位元小于 m

对于集合 A 中所有元素 a，运算*和单位元 e，若存在元素 y，使得 y*a=e，则称 y 为 a 关于运算“*”的左逆元，若 a*y=e，则称 y 为 a 关于运算“*”的右逆元；若 y*a=a*y=e，则称 y 为 a 关于运算“*”的逆元（既是左逆元，又是右逆元）。

注释：（R,+），(R,×)构成代数结构。

对于加法，0 是单位元，-a 是逆元；

对于乘法，1 是单位元，1/a= a^{-1} 是逆元；

同余运算，

对于 $a\in Z$, 存在 $b\in Z$, 使得 $a+b \equiv 0 \pmod m$)，则称 b 是 a 的加法逆元，记 b= - a。其中，- a 仅仅是一种符号，而非相反数。

如，a= 2 , m=7, 加法运算的单位元为 0，则 a 的加法逆元 b， b ＝5，记 b ＝- a＝5;

对 $a\in Z$，存在 $b\in Z$，使得 $a\times b \equiv 1 \pmod m$)，则称 b 是 a 的乘法逆元，记 $b= a^{-1}$。其中， a^{-1} 仅仅是一种符号，而非倒数。

如，a= 2 , m=7, 乘法运算的单位元为 1，则 a 的乘法逆元 b， b ＝4，记 $b= a^{-1}=4$;

定理 2.　设〈A, *〉是一个代数结构，*是 A 上的二元运算，e 是关于运算“*”的单位元，且该运算“*”满足结合律，$x\in A$, 如果 x 有逆元 y，即 $x*y=y*x=e$, 则逆元 y 唯一。

Proof.　Assume $z\in A$, be another * inverse for　x, then

$z*e=z*(x*y)=(z*x)*y=e*y=y$.

Homework

P44：　1 (a), (b); 3 (a); 8 (a), (b)

现在，我们来集中考虑与同余相关的一些问题。

非零元有逆元

定理　设 a 与 m 互素且 a、m 为正整数，$a<m$，则存在 b 满足

$$ab \equiv 1 (\mathrm{mod}\ m)$$

故，称 b 为 a 的逆元，记 $b= a^{-1}$，满足 $ab=a\,a^{-1} \equiv 1(\mathrm{mod}\ m)$.

证明：在同余的乘法运算中，我们知道 1 是乘法运算的单位元。由 $(a,m)=1$ 可知，存在整数 s，t，使得 $as+tm=1$，因此有 $as \equiv 1(\mathrm{mod}\ m)$，表明存在整数 s，使得 $as \equiv 1(\mathrm{mod}\ m)$，即，整数 a 的逆元是存在的。

同余方程 **$ax \equiv b(m)$**

(1)若$(a, m)=1$，

首先，求解方程 **$ay \equiv 1(\mathrm{mod}\ m)$,得到 a 的逆元 $y=a^{-1}$；**

其次，$ax \equiv b(m)$有唯一解，其解为 $x \equiv a^{-1}b(m)$。其唯一性是指 $a^{-1}b$ 模 m 以后所得到的数值唯一（即，小于 m）。

证明：由$(a,m)=1$，因此，存在整数 a^{-1},使得 $aa^{-1} \equiv 1(m)$,于是 $aa^{-1}-1=mq$，故，两边同时乘以 b，可得到：$aa^{-1}b-b=mqb$,

即，$aa^{-1}b \equiv b(m)$，因此，我们有解 $x \equiv a^{-1}b(m)$。

唯一性： 假设 x，y 是同余方程的解，故均满足 $ax \equiv b(m)$，$ay \equiv b(m)$,则 $ax-b=mp$, $ay-b=mq$，$a(x-y)=m(p-q)$，则 $m|a(x-y)$，由于$(a, m)=1$，于是 $m|(x-y)$，因此，$x=y+mk$,故，x,y 在均小于 m 的情况下，$x=y$.

需要注意的是：$a^{-1}b+m$, $a^{-1}b+2m$,...也能够满

足同余方程。

因为，$a(a^{-1}b+m)=aa^{-1}b+ma$

$=b+mqb+ma=b+(qb+a)m$

所以，$a(a^{-1}b+m)\equiv b(m)$

例如，$3x\equiv 2(4)$，由于$(3,4)=1$，于是，首先求解 $3y\equiv 1(4)$，于是有，$3^{-1}=3, 7, 11,...,$

其次，$3^{-1}b=3^{-1}2=6$，14，22,...，$x=3^{-1}2\equiv 2(4)$，

即，$x=2$ 是唯一解.

2 是比模 4 小的唯一解，但 2+1*4，2+2*4，也能够满足同余方程。

例如，$2x\equiv 2(3)$，由于$(2,3)=1$，于是，首先求解 $2y\equiv 1(3)$，于是有，$2^{-1}=2, 5, 8,...,$

其次，$2^{-1}b=2^{-1}2=4$，10，16,...，$x=2^{-1}2\equiv 1(3)$，

即，$x=1$ 是唯一解。

1 是比模 3 小的唯一解，但 1+1*3，1+2*3，也能够满足同余方程。

(2)若 GCD(a, m)=d，

$ax\equiv b(m)$ 有解的充分必要条件是 $d|b$，即，b

是 d 的倍数。

这时 $ax\equiv b(m)$ 有 d 个解

证明:由于 GCD(a, m)=d,因此,a=dp, m=dk, 由同余方程可知, ax-b=mq, b=ax-mq=d(px-kq), a,m 均是 d 的倍数,因此,d 是 b 的因数(约数),故,d|b,

由于 GCD(a, m)=d,则 GCD(a/d, m/d)=1,因此,对于同余方程$(a/d)x\equiv(b/d)(\mathrm{mod}\ m/d)$来说,它有唯一解 $x\equiv(a/d)^{-1}b/d(\mathrm{mod}\ m/d)$,并且,我们知道:

$x\equiv (a/d)^{-1}b/d\ (\mathrm{mod}\ m/d)$,

$x+m/d$, $x+2m/d$, ……, $x+(d-1)m/d$

也能够满足同余方程$(a/d)x\equiv b/d(\mathrm{mod}\ m/d)$。

接下来,我们来说明满足同余方程 $(a/d)x\equiv b/d(\mathrm{mod}\ m/d)$的 x 也满足同余方程 $ax\equiv b(\mathrm{mod}\ m)$。

首先,唯一解满足:$(a/d)x-b/d=(m/d)q$,两边同时乘以 d,于是,有 $ax-b=mq$,

即,唯一解满足同余方程 $ax\equiv b(m)$。这表明

同余方程 $(a/d)x\equiv(b/d)(m/d)$ 的唯一解 $x\equiv(a/d)^{-1}b/d(m/d)$ 满足同余方程 $ax\equiv b(m)$，即 $ax-b=mq$。是同余方程 $ax\equiv b(m)$的解

进一步，我们有：

$a(x+m/d)-b=ax+(a/d)m-b=m(q+a/d)$,

即，$a(x+m/d)\equiv b(m)$，表明 $x+m/d$ 满足同余方程 $ax\equiv b(m)$，是同余方程 $ax\equiv b(m)$的解?

同理，

$a(x+2m/d)-b=ax+(2a/d)m-b=m(q+2a/d)$,

即，$a(x+2m/d)\equiv b(m)$，表明 $x+2m/d$ 满足同余方程 $ax\equiv b(m)$，是同余方程 $ax\equiv b(m)$的解?

……

类似地，我们有：$a(x+(d-1)m/d)\equiv b(m)$，

表明 $x+(d-1)m/d$ 满足同余方程 $ax\equiv b(m)$，是同余方程 $ax\equiv b(m)$的解

因此，$x, x+m/d, x+2m/d, \ldots, x+(d-1)m/d$ 均是同余方程 $ax\equiv b(m)$的解，并且互不相同。

故，同余方程 $ax\equiv b(m)$ 有 d 个互不相同的

解。

例，9x≡6(12)

因为：d=(9,12)=3，并且 3|6，即，d|b，因此，我们有 d=3 个不同的解。

首先，求解同余方程(a/d)x≡(b/d)(mod m/d)，即，3x≡2(4)，得到 x≡2(4)，

然后，计算 x+k*m/d, k=0,1,2,...,d-1，它们是同余方程 9x≡6(12)的解，即，x=2，2+12/3=6，2+2*12/3=10。

因此，x≡2(12), x≡6(12), x≡10(12) 是同余方程 9x≡6(12)的 3 个互不相同的解。

例，同余方程 9x≡4 (12)无解。

因为：d=(9,12)=3，但是 $3 \nmid 4$，因此，同余方程 9x≡4 (12)无解。

同余方程组

$$
\begin{aligned}
&x \equiv b_1 (\bmod m_1) \\
&x \equiv b_2 (\bmod m_2) \\
&\cdots\cdots \\
&x \equiv b_k (\bmod m_k)
\end{aligned}
$$

其中 $m_i,\ i = 1, 2, 3, \cdots k,$ 是两两互素的 **k** 个正整数。

孙子定理：如上所述，设

$$m = m_1 m_2 \cdots m_k = \prod_{i=1}^{k} m_i = m_i M_i$$

则同余方程组有唯一解

$$x \equiv (b_1 M_1' M_1 + b_2 M_2' M_2 + \cdots b_k M_k' M_k)(\bmod m)$$

其中，$M_i' M_i \equiv 1 (\bmod m_i),\ 1 \le i \le k$

$$M_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k = \prod_{i=1, j \ne i}^{k} m_j$$

证明：构造同余方程的解。 首先，考虑

$$
\begin{aligned}
&l_i \equiv 1 (\bmod m_i) \\
&l_i \equiv 0 (\bmod m_j),\ \ j \ne i
\end{aligned}
$$

由于 $m_i,\ i=1,2,3,\cdots k,$ 两两互素，故

$$(M_i, m_i)=1,\ \textit{there exists}\ M_i' \ \textit{such that}\\ M_i'M_i \equiv 1(\bmod m_i),\ \textit{and}\ M_i'M_i \equiv 0(\bmod m_j),\ j\neq i$$

因此，$b_1M_1'M_1$ 满足同余方程：

$$\begin{aligned} &x\equiv b_1(\bmod m_1)\\ &x\equiv 0(\bmod m_2)\\ &\cdots\cdots\\ &x\equiv 0(\bmod m_k)\end{aligned}$$

同理，$b_2M_2'M_2$ 满足同余方程：

$$\begin{aligned} &x\equiv 0(\bmod m_1)\\ &x\equiv b_2(\bmod m_2)\\ &\cdots\cdots\\ &x\equiv 0(\bmod m_k)\end{aligned}$$

以此类推，因此，我们有

$$x=b_1M_1'M_1+b_2M_2'M_2+\cdots b_kM_k'M_k$$

满足同余方程组：

$$\begin{aligned}
&x \equiv b_1 (\bmod m_1) \\
&x \equiv b_2 (\bmod m_2) \\
&\cdots\cdots \\
&x \equiv b_k (\bmod m_k)
\end{aligned}$$

进一步，假设 x, y 均能满足上述同余方程组，则

$$\begin{aligned}
&x - y \equiv 0 (\bmod m_1) \\
&x - y \equiv 0 (\bmod m_2) \\
&\cdots\cdots \\
&x - y \equiv 0 (\bmod m_k)
\end{aligned}$$

由于

$$m_i,\ i = 1, 2, 3, \cdots k,$$

两两互素，故 **x-y** 整除 **m**，是 **m** 的倍数，因此，

$$x \equiv (b_1 M_1' M_1 + b_2 M_2' M_2 + \cdots b_k M_k' M_k)(\bmod m)$$

是上述同余方程组的唯一解。

例如：今有一物，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？

$$x \equiv 2(\bmod 3),\ x \equiv 3(\bmod 5),\ x \equiv 2(\bmod 7)$$

$$M_1 = 5\times 7 = 35,\quad M_1' M_1 \equiv 1(\bmod 3),\ M_1' = 2$$

$$M_2 = 3\times 7 = 21,\quad M_2' M_2 \equiv 1(\bmod 5),\ M_2' = 1$$

$$M_3 = 3\times 5 = 15,\quad M_3' M_3 \equiv 1(\bmod 7),\ M_3' = 1$$

$$\begin{aligned} x &\equiv (2\times 2\times 35 + 3\times 1\times 21 + 2\times 1\times 15)(\bmod 3\times 5\times 7) \\ &\equiv (140+63+30)(\bmod 105) \equiv 233(\bmod 105) \\ &\equiv 23(\bmod 105) \end{aligned}$$

韩信点兵，多多益善：有兵若干，若列成 **5** 行纵队，则末行 **1** 人；若列成 **6** 行纵队，则末行 **5** 人；若列成 **7** 行纵队，则末行 **4** 人；若列成 **11** 行纵队，则末行 **10** 人；问兵员几人？

$$x \equiv 1(\bmod\ 5),\ x \equiv 5(\bmod\ 6),\ x \equiv 4(\bmod\ 7),\ x \equiv 10(\bmod\ 11)$$

$$M_1 = 6\times7\times11 = 462,\quad M_1' M_1 \equiv 1 (\bmod 5),\ M_1' = 3$$

$$M_2 = 5\times7\times11 = 385,\quad M_2' M_2 \equiv 1 (\bmod 6),\ M_2' = 1$$

$$M_3 = 5\times6\times11 = 330,\quad M_3' M_3 \equiv 1 (\bmod 7),\ M_3' = 1$$

$$M_4 = 5\times6\times7 = 210,\quad M_4' M_4 \equiv 1 (\bmod 11),\ M_4' = 1$$

$$\begin{aligned} x \equiv\ & (1\times3\times462 + 5\times1\times385 \\ & + 4\times1\times330 + 10\times1\times210)(\bmod 5\times6\times7\times11) \\ \equiv\ & 6731 (\bmod\ 2310) \equiv 2111 (\bmod\ 2310) \end{aligned}$$

1.5 矩阵（二维数组）

1.5.3 Boolean matrix 布尔矩阵

每个元素的值非 **0** 即 **1**

矩阵也是一种集合（详细在关系中进行论述），因此，我们有以下运算：（布尔矩阵的并、交、余运算）

Operations on Boolean Matrix

1.5.4 布尔矩阵的运算

Let A= $\left(a_{ij}\right)_{m\times n}$ **, B=** $\left(b_{ij}\right)_{m\times n}$ **be** $m\times n$ **Boolean matrix.**

并 **Join of A and B,** $C = A\bigcup B$ **=** $\left(c_{ij}\right)_{m\times n}$

$c_{ij} = a_{ij} \vee b_{ij}$

交 **Meet of A and B,** $D = A\bigcap B$ **=** $\left(d_{ij}\right)_{m\times n}$

$d_{ij} = a_{ij} \wedge b_{ij}$

余 **Complment of A,** $E = A^{c}$ **=** $\left(e_{ij}\right)_{m\times n}$

$e_{ij} = 1 - a_{ij}$ **,** $e_{ij} = \begin{cases} 1 & a_{ij} = 0 \\ 0 & a_{ij} = 1 \end{cases}$

Example 11. Let A= $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ **,**

B= $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ **.**

Join of A and B,

$$C = A \bigcup B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Meet of A and B,

$$D = A \bigcap B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

余 Complment of A, $E = A^c = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

类似于代数矩阵，我们可以定义布尔矩阵的乘积运算。

积

Let A=$\left(a_{ij}\right)_{m\times p}$ **be** $m\times p$ **Boolean matrix, B=**$\left(b_{ij}\right)_{p\times n}$ **be** $p\times n$ **Boolean matrix.**

Boolean product of A and B , denoted $A\circ B=\left(f_{ij}\right)$

$$f_{ij}=\bigvee_{k=1}^{p}(a_{ik}\wedge b_{kj})$$

for i=1,2,..,m, j=1,2,..,n.

Obviously, $A\circ B$ **is the** $m\times n$ **Boolean matrix.**

Example 12. Let A=$\begin{pmatrix}1&1&0\\0&1&0\\1&1&0\\0&0&1\end{pmatrix}$**,**

B= $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$ **.**

Product of A and B,

$$A \circ B = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

1.5.5 布尔矩阵运算的性质

Theorem 4. 如果 **A,B,C** 是相应的（满足运算需要的行和列的要求）布尔矩阵，则

1. (a) $A \cup B = B \cup A$.

(b) $A \cap B = B \cap A$.

2. (a) $(A \cup B) \cup C = A \cup (B \cup C)$.

(b) $(A \cap B) \cap C = A \cap (B \cap C)$.

3. (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

4. $(A \circ B) \circ C = A \circ (B \circ C)$.

矩阵是线性代数中重要的工具。布尔矩阵与

代数矩阵的区别就是矩阵中元素的取值、矩阵乘法的表达式以及所代表的相应意义。

阅读材料：

模糊集合(Fuzzy set)：1965 年美国控制论专家 Zadeh 教授所提出，目前广泛应用于各种智能系统领域。边界不确定（模糊）的概念

特征函数变化为隶属函数

$$f_A : U \to \{0,1\}, x \in U \to f_A(x) \in \{0,1\}$$

$$\mu_A : U \to [0,\ 1], x \in U \to \mu_A(x) \in [0,\ 1]$$

可以发现，普通集合是模糊集合的特殊情形。

由此研究模糊集合的运算性质。

并： $A \cup B,\ \mu_{A \cup B}(x) = \max(\mu_A(x),\ \mu_B(x))$

交： $A \cap B,\ \mu_{A \cap B}(x) = \min((\mu_A(x),\ \mu_B(x))$

$$A^c,\ \mu_{A^c}(x) = 1 - \mu_A(x)$$

余：

补余率 Properties of the Complement（普通集合）

10. $A \cap \overline{A} = \varnothing$，**11.** $A \cup \overline{A} = U$

补余率 Properties of the Complement（模糊集合）不成立

由此开展一系列的关于模糊集合的理论研究与应用的技术开发。