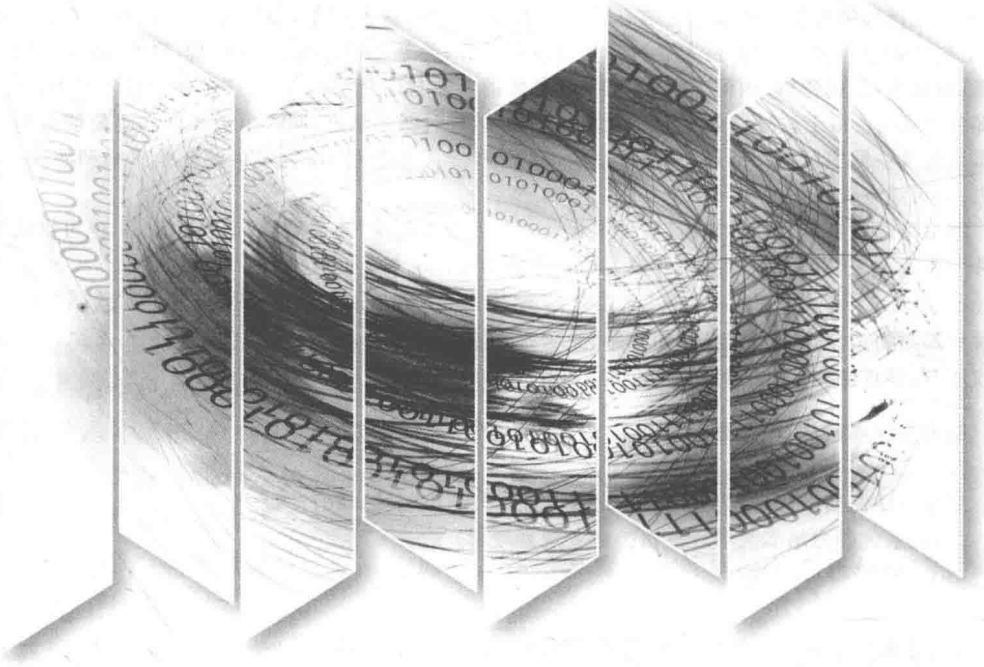
面向系统能力培养大学计算机类专业规划教材

离散数学简明教程

卢 力 编著

清华大学出版社

面向系统能力培养大学计算机类专业规划教材



离散数学简明教程

卢 力 编著

清华大学出版社
北京

内 容 简 介

离散数学是研究离散量的结构和相互间关系的学科，是计算机、软件工程等专业的理论基础.

本书依据教育部计算机科学与技术教学指导委员会编制的《高等学校计算机科学与技术专业规范》和《高等学校计算机科学与技术专业核心课程教学实施方案》进行编写，简要介绍离散数学的集合论、抽象代数、图论和数理逻辑4个部分，主要包括集合及其运算，关系，函数，代数系统，群、环和域，格和布尔代数，图与树，特殊图，命题逻辑，谓词逻辑共10章，“整数的整除与同余”一章作为预备知识供学习集合论和代数系统部分时参考. 由于教材以集合论开头，便于学生学习时循序渐进，同时由于教材内容简明扼要，例题和习题多且包含一些实际应用问题，从而可以调动学生的学习积极性，培养学生的数学思维和解决实际问题的能力，为后续专业课程的学习奠定良好的基础.

本书可作为高等院校计算机、软件工程及相关专业本科生“离散数学”课程的教材，也可供从事计算机、软件工程及相关领域研究和应用开发人员自学或参考.

图书在版编目(CIP)数据

离散数学简明教程/卢力编著. —北京：清华大学出版社，2017
(面向系统能力培养大学计算机类专业规划教材)
ISBN 978-7-302-46062-6

Ⅰ. ①离… Ⅱ. ①卢… Ⅲ. ①离散数学—教材 Ⅳ. ①O158

中国版本图书馆CIP数据核字(2017)第004893号

责任编辑：张瑞庆　赵晓宁
封面设计：常雪影
责任校对：李建庄
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：20.75　　**字　　数**：526千字
版　　次：2017年7月第1版　　**印　　次**：2017年7月第1次印刷
印　　数：1～2000
定　　价：39.50元

产品编号：069439-01

FOREWORD

前　言

离散数学是相对于连续数学而言的. 从数学的发展历程来看,最开始的数学是离散的数学,如计数;后面出现微积分这样连续的数学;随着计算机的出现,离散数学重新找到了它应有的位置.

广义来讲,离散数学包括两个方面,一个是连续数学的离散化,即计算数学或数值分析的研究内容;另一个就是离散量自身的研究内容. 一般而言,离散数学是研究离散量的结构和相互间关系的学科. 离散结构则是离散数学和组合数学的统称.

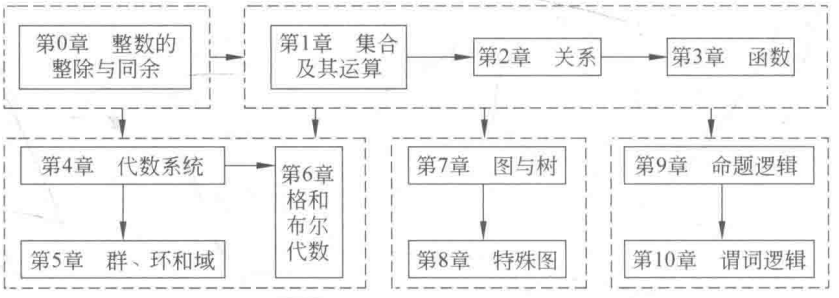
离散数学是计算机、软件工程专业的一门核心基础课程,其主要作用如下:

(1) 离散数学为后继专业课程如数据结构、数据库原理、数字逻辑、信息安全、编译原理、人工智能、操作系统等提供必要的数学基础;

(2) 离散数学为从事计算机科学各方面的工作以及解决计算机科学中遇到的实际问题等提供有力的工具;

(3) 离散数学是现代数学的一个重要分支,通过该课程的学习可以提高逻辑思维与抽象思维能力、创造性思维能力以及分析和解决实际问题的能力等,培养出高素质的人才.

离散数学课程的主要内容可以分为 4 个部分,其导图如下. 课程以离散量为研究对象,内容丰富,涉及面宽,具有 4 个主要的特点:以集合论为基础;高度的抽象性;推理的严密性;应用的广泛性.



本课程概念多、定理多、推理多,并且内容较为抽象. 但由于它是为后继专业知识的学习做必要的数学准备的,因此它研究的内容均比较基础,难度不大. 在学习离散数学的过程中,不必过分关注它的用处以及它在计算机学科中所起的作用,而应从以下几个方面入手,力争学好本课程的全部内容.

(1) 熟读教材,重于细节. 这是学好离散数学不可缺少的一环,要准确理解各个概念和定理的含义,要看懂必要的推理过程.

(2) 独立思考,加强练习. 在熟读教材的基础上,必须通过练习、独立思考来真正获取知识.

FOREWORD

(3) 注重抽象思维能力的培养. 要学好这门课程,必须具有较强的抽象思维能力,才能深入掌握课程内容. 证明技巧的训练,可以促进推理技能的提高、逻辑抽象的深入、思维方式的严谨和理解能力的增强.

本教材是编者根据多年从事离散数学课程教学实践,并在参阅国内同行编著的多本教材的基础上编写完成的,特别是在教学中一直选用洪帆教授主编的《离散数学基础》组织教学,因此受到了许多潜移默化的影响,在此表示衷心的感谢. 教材的编写得到了华中科技大学教材建设项目的资助和清华大学出版社的支持,在此一并表示衷心的感谢.

讲授本教材的基本部分约需 64～80 学时. 教材习题分为 A 类题和 B 类题两类,其中 B 类题多为知识拓展和难度较大的综合题,供学习者选做. 另有思考题散布于教材内容之中. 教材还配有电子教案,与教材配套的习题解答也在整理之中.

限于编者的水平,书中错误和疏漏之处在所难免,敬请读者不吝指正.

编　者

2017 年 4 月于武汉

CONTENTS

目　录

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

第0章　整数的整除与同余

数学是科学之王，数论是数学之王，因此吸引着一些具有数学天赋和灵感的人终生投身于数论的研究. 数论最初是从研究整数开始的，所以也称为整数论，后来进一步发展成为数论. 确切地说，数论是研究整数性质和方程整数解的学科. 数论是一门最古老的数学分支，以严格和简洁著称，既丰富又深刻，问题浅显易懂，但从经验归纳往往又难于证明. 因此，数论具有概念简单易懂但解题过程困难曲折等特点. 长期以来，数论被当作“纯”数学进行研究，但随着密码学等的发展，数论产生的影响越来越大，已成为计算机科学技术和通信工程技术领域的重要数学基础.

初等数论是用初等数学的方法来研究整数性质和方程整数解的学科. 本章将重点介绍整数的整除和同余，它们是初等数论中两个最重要的概念，也是初等数论的基础，在计算机的数据表示、数据传输以及数据保密等方面起着非常重要的作用.

0.1　整除及带余除法

0.1.1　整数

整数、正整数、负整数分别是集合$\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$，$\{1,2,3,\cdots\}$，$\{\cdots,-3,-2,-1\}$中的元素.

奇数、偶数分别是集合$\{\cdots,-5,-3,-1,1,3,5,\cdots\}$，$\{\cdots,-6,-4,-2,0,2,4,6,\cdots\}$中的元素.

常用$\mathbf{Z}$表示所有整数构成的集合，$\mathbf{Z}^+$表示所有正整数构成的集合，$\mathbf{N}$表示所有非负整数即自然数构成的集合，小写字母$a,b,c,d,\cdots$表示整数.

整数的加、减、乘、除四则运算的符号分别用$+$、$-$、$\times$或$\cdot$、$/$表示.

当几个小写英文字母在一起时，表示将这几个整数相乘，例如$ab=a\times b$，$abc=a\times b\times c$.

当n是正整数时，a^n表示由n个相同的整数a相乘所得的积. 记$a^1=a$.

用记号$|a|$来表示整数a的绝对值，即

$$|a|=\begin{cases}a, & a\geqslant 0\\ -a, & a<0\end{cases}$$

最小整数公理(良序性)　正整数集合$\mathbf{Z}^+$的任意非空子集都存在一个最小的正整数.

显然，正整数集合$\mathbf{Z}^+$具有良序性，但是整数集合$\mathbf{Z}$并不具有良序性，因为没有最小值.

在整数的加、减、乘、除四则运算中，

整数$+$整数$=$整数，　整数$-$整数$=$整数，　整数$\times$整数$=$整数

但是整数除整数却不一定得到整数，这正是将要研究的整数的整除性.

0.1.2 整除的概念与性质

定义 0.1 设 a,b 是两个整数，$a\neq 0$. 如果存在整数 q，使得 $b=aq$，则称 ***a* 整除 *b***，或 ***b* 被 *a* 整除**，记为 $a|b$，又称 a 是 b 的**因子**或**因数**，b 是 a 的**倍数**. 此时 q 可表示为 $q=b/a$. 如果找不到这样的整数 q，则称 ***a* 不整除 *b***，记为 $a\nmid b$.

例如：$2|6$，而 $-4\nmid 6$，同时 6 的因子分别为 $\pm 1,\pm 2,\pm 3,\pm 6$.

根据整除的定义，显然有

(1) 设 a 是任一非零整数，则 $a|0$，即 0 是任一非零整数的倍数.

(2) 设 a 是任一整数，则 $\pm 1|a$，即 1 和 -1 是任一整数的因数.

(3) 设 a 是任一非零整数，则 $a|a$，即任一非零整数是其自身的倍数，也是其自身的因数.

非零整数 a 的因子 $\pm 1,\pm a$ 称为 a 的**平凡因子**，其他的因子(如果存在的话)称为 a 的**非平凡因子**或**真因子**.

显然，若整数 b 是 a 的真因子，则有 $1<|b|<|a|$.

定义 0.2 设 a,b 是两个整数，形如 $ax+by$ 的数称为 a 与 b 的**线性组合**，其中 x,y 是任意的整数.

两个整数的线性组合可推广到有限个整数的情形.

定理 0.1 设 a,b,c 为整数，则有

(1) $a|b$ 当且仅当 $a|-b$ 当且仅当 $-a|b$ 当且仅当 $-a|-b$ 当且仅当 $|a||b|$.

(2) 若 $a|b$ 且 $b|a$，则 $b=a$ 或者 $b=-a$.

(3) 若 $a|b$ 且 $b|c$，则 $a|c$.

(4) $c|a$ 且 $c|b$ 当且仅当对任意的 $x,y\in\mathbf{Z}$，都有 $c|(ax+by)$.

(5) 若 $a|b$ 且 $b\neq 0$，则 $|a|\leqslant|b|$.

(6) $a|b$ 当且仅当 $ca|cb$，其中 $c\neq 0$.

证明 (1) 证明 $a|b$ 当且仅当 $a|-b$，其余证法类似.

若 $a|b$，则存在整数 e，使得 $b=ae$，因此 $(-b)=a(-e)$，所以 $a|-b$.

同法可证，若 $a|-b$，则 $a|b$. 故 $a|b$ 当且仅当 $a|-b$.

(2) 若 $a|b$ 且 $b|a$，则存在整数 e 和 f，使得 $b=ae$ 且 $a=bf$，于是 $ef=1$.

由于 e 与 f 是整数，因而 $e=f=1$ 或 $e=f=-1$. 故 $b=a$ 或者 $b=-a$.

(3) 若 $a|b$ 且 $b|c$，则存在整数 e 和 f，使得 $b=ae$ 且 $c=bf$，于是 $c=a(ef)$.

由于整数 e 与 f 的乘积仍然是整数，因而 $a|c$.

(4) 由于 $c|a$ 且 $c|b$，故存在整数 e 和 f，使得 $a=ce$ 且 $b=cf$，因而

$$ax+by=cex+cfy=c(ex+fy)$$

由于 $ex+fy$ 仍然是整数，因而 $c|(ax+by)$.

反之，令 $x=1,y=0$ 和 $x=0,y=1$，则分别有 $c|a$ 且 $c|b$.

此性质常称为**整除的组合性质**.

(5) 若 $a|b$，则由 $b\neq 0$ 知，存在整数 $e\neq 0$，使得 $b=ae$，故 $|b|=|a||e|$. 又因为 $|e|\geqslant 1$，因此 $|a|\leqslant|b|$.

(6) 若 $a|b$，则存在整数 e，使得 $b=ae$，因此 $cb=(ca)e$，所以 $ca|cb(c\neq 0)$.

同法可证，若 $ca|cb(c\neq 0)$，则 $a|b$. 故 $a|b$ 当且仅当 $ca|cb(c\neq 0)$. ■

推论 0.1　设 $a_1,a_2,\cdots,a_n,b$ 为整数，若 $b|a_1,b|a_2,\cdots,b|a_n$，则对任意的整数 $c_1,c_2,\cdots,c_n$，有 $b|(c_1a_1+c_2a_2+\cdots+c_na_n)$.

证明　由定理 0.1(4)立得. ■

推论 0.2　设 a,b 为整数，若 $a|b$ 且 $|b|<|a|$，则 $b=0$.

证明　由定理 0.1(5)立得. ■

【例 0.1】　证明：若 n 是奇数，则 $8|(n^2-1)$.

证明　若 n 是奇数，则存在整数 k，使得 $n=2k+1$，于是

$$n^2-1=(2k+1)^2-1=4k(k+1)$$

因为 k 与 $k+1$ 中有一个为偶数，所以 $8|(n^2-1)$.

【例 0.2】　证明：若 $3|n,5|n$，则 $15|n$.

证明　若 $3|n$，则存在整数 s，使得 $n=3s$，故 $5|3s$. 显然 $5|5s$，故有 $5|(2\times 5s-3\times 3s)$，即 $5|s$，因而存在整数 t，使得 $s=5t$，所以 $n=3(5t)=15t$，于是 $15|n$.

【例 0.3】　设 a,b 为两个非零整数，且有整数 s,t，使得 $as+bt=1$，证明：

(1) 若 $m|a$ 且 $m|b$，则 $m=\pm 1$.

(2) 若 $a|n$ 且 $b|n$，则 $ab|n$.

证明：(1) 若 $m|a$ 且 $m|b$，则 $m|(as+bt)$. 由题设 $as+bt=1$ 知 $m|1$，故 $m=\pm 1$.

(2) 由题设 $as+bt=1$，有

$$n=n\times 1=n(as+bt)=(na)s+(nb)t$$

再由 $a|n$ 且 $b|n$，有 $ab|nb$ 且 $ab|an$，因此 $ab|((na)s+(nb)t)$，即 $ab|n$.

定义 0.3　设整数 $a\neq 0,a\neq\pm 1$，如果它没有真因数，则称 a 为**素数**或**质数**、**不可约数**，否则称 a 为**合数**.

例如，2,3,5,7,11,13,…都是素数；4,6,8,9,10,12,…都是合数. 通常用 p 或 $p_1,p_2,p_3,\cdots$ 表示素数.

由素数和合数的定义知，整数集合可分为三类：素数集合、合数集合和 $\{0,1,-1\}$.

以后约定，素数和合数是正整数，因为 a 是素数(合数)当且仅当 $-a$ 是素数(合数).

定义 0.4　设 $x\in\mathbf{R}$(实数集合)，$[x]$ 表示不超过 x 的最大整数，称为 x 的**整数部分**；$\{x\}$ 表示 $x-[x]$，称为 x 的**小数部分**.

例如：$[3.14]=3,\{3.14\}=0.14;[-3.14]=-4,\{-3.14\}=0.86$.

0.1.3　带余除法

定理 0.2(带余除法)　设 a,b 是两个整数，$b\neq 0$，则存在唯一的一对整数 q 和 r，使得

$$a=qb+r,\quad 0\leqslant r<|b| \tag{0.1}$$

并分别称 q 与 r 为 b 除 a 的**商**和**余数**.

证明　如果 $b>0$，则 b 的倍数由小到大排列为

$$\cdots,-4b,-3b,-2b,-b,0b,b,2b,3b,4b,\cdots$$

如果 $b<0$，则 b 的倍数由小到大排列为

$$\cdots,4b,3b,2b,b,0b,-b,-2b,-3b,-4b,\cdots$$

整数 a 同 b 的这些倍数相比可能出现以下两种情形：

(1) 存在整数 q，使得 $a=qb$，此时取 $r=0$，则式(0.1)成立.

(2) 当 $b>0$ 时，存在整数 q，使得 $qb\leqslant a<(q+1)b$，因此有 $0\leqslant a-qb<b$.

当 $b<0$ 时，存在整数 q，使得 $qb\leqslant a<(q-1)b$，因此有 $0\leqslant a-qb<-b$.

于是 $0\leqslant a-qb<|b|$. 令 $r=a-qb$，则 $a=qb+r$，$0\leqslant r<|b|$.

此即证明了 q 和 r 的存在性.

假设分别存在整数 q 与 r，以及 q_1 与 r_1，使得

$$a=qb+r,\quad 0\leqslant r<|b|$$

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

两式相减得：$r_1-r=(q-q_1)b$. 于是 $b|(r_1-r)$，且 $|r_1-r|=|(q-q_1)b|$.

因为 $0\leqslant r<|b|$，$0\leqslant r_1<|b|$，故有 $|r_1-r|<|b|$.

若 $q\neq q_1$，则 $|(q-q_1)b|\geqslant|b|$，而 $|r_1-r|<|b|$，矛盾. 故必有 $q=q_1$，$r=r_1$. 即商 q 和余数 r 都是唯一的. ■

显然，若 $a=qb+r$，$0\leqslant r<|b|$，则 $b|a$ 当且仅当 $r=0$.

一般情况下，约定 $b>0$，则式(0.1)表示为

$$a=qb+r,\quad 0\leqslant r<b \tag{0.2}$$

其中 r 常记为 $\mathrm{res}_b(a)$.

推论 0.3 设整数 $a>0$，则任一整数被 a 除后所得到的最小非负余数是且仅是 $0,1,2,\cdots,a-1$ 这 a 个数中的一个.

注意：这是带余除法定理的直接推论，是整数的进制表示法的基础.

【例 0.4】 证明：任意给出的 5 个整数中，必有三个数之和被 3 整除.

证明：设 $a_1\sim a_5$ 为 5 个整数，且由带余除法有

$$a_i=3q_i+r_i,\quad 0\leqslant r_i<3,i=1,2,3,4,5$$

分别考虑以下两种情况：

(1) 若在 $r_1\sim r_5$ 中数 0,1,2 都出现，不妨设 $r_1=0$，$r_2=1$，$r_3=2$，则

$$a_1+a_2+a_3=3(q_1+q_2+q_3)+3$$

可被 3 整除.

(2) 若在 $r_1\sim r_5$ 中数 0,1,2 至少有一个不出现，则至少有三个取相同的值，不妨设 $r_1=r_2=r_3=r(r=0,1$ 或 $2)$，因而

$$a_1+a_2+a_3=3(q_1+q_2+q_3)+3r$$

可被 3 整除.

0.1.4 整数的进制表示法

整数通常是以十进制表示的，除此之外，还有二进制表示等，下面对此进行讨论.

定理 0.3 设整数 $b>1$，则任意正整数 n 都可以唯一表示为

$$n=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0 \tag{0.3}$$

称此表达式为正整数 n 的 ***b* 进制表示**，记为