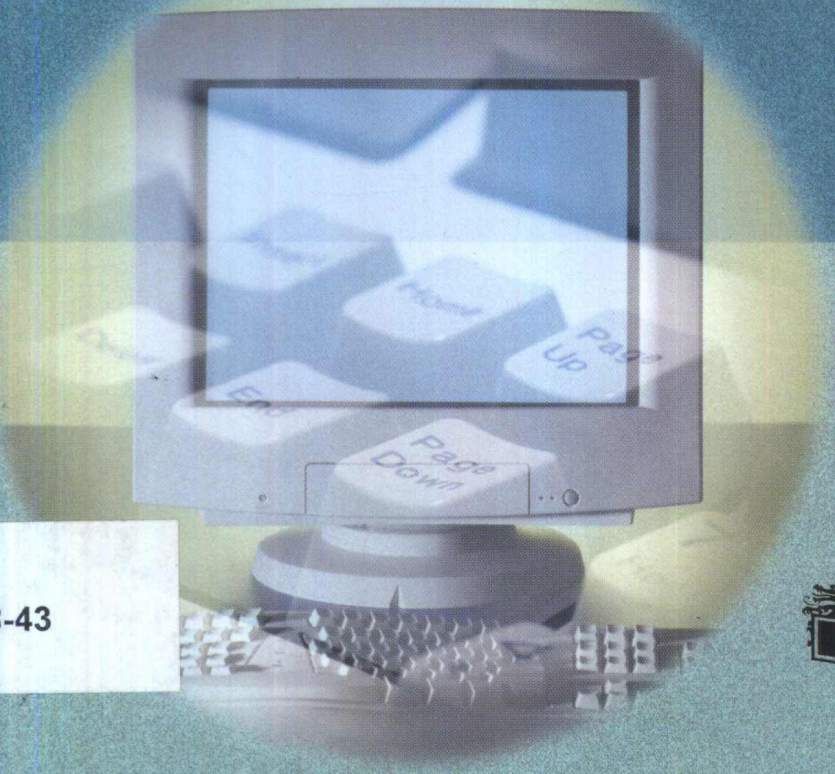
专升本

教育部师范教育司组织编写
中学教师进修高等师范本科(专科起点)教材

离散数学

邓安生　主编
邓安生　黄馥林等　编著



-43

高等教育出版社

324

O158-43
D38

教育部师范教育司组织编写
中学教师进修高等师范本科(专科起点)教材

离 散 数 学

邓安生 主编
邓安生 黄馥林等 编著

高等教育出版社

内容提要

本书根据教育部师范教育司制订的《中学教师进修高等师范本科(专科起点)教学计划》编写。

全书内容分成五篇:预备知识篇,包括整数、排列和组合初步及数学归纳法;数理逻辑篇,包括命题逻辑和一阶谓词逻辑中的基本概念、公式的蕴涵和等值演算、范式及推理理论;集合论篇,包括集合及其运算、二元关系及闭包、部分序关系和等价关系、映射;代数结构篇,包括群、环和格及其基本性质、布尔代数;图论篇,包括图和树、最短路径算法、最优二叉树算法、哈夫曼算法和几种特殊的图。

本书主要面向自学学生,在保证离散数学基本知识结构体系完整的前提下,对教材内容进行了必要的筛选。全书内容严谨而且自足,循序渐进,条理清楚,叙述流畅,重点突出,难点讲解详尽,辅助材料丰富,便于学生自学,也便于教师教学。

本书可作为中学教师进修本科(专科起点)离散数学课程的教材或参考书,也可作其他类"专升本"或成人本科教育的教材。

图书在版编目(CIP)数据

离散数学/邓安生主编.—北京:高等教育出版社,2001.7
ISBN 7-04-009399-5

Ⅰ.离… Ⅱ.①邓… ②黄… Ⅲ.离散数学-师范大学-教材 Ⅳ.0158

中国版本图书馆 CIP 数据核字(2001)第 26161 号

离散数学
邓安生 主编

出版发行	高等教育出版社		
社　　址	北京市东城区沙滩后街 55 号	邮政编码	100009
电　　话	010-64054588	传　　真	010-64014048
网　　址	http://www.hep.edu.cn http://www.hep.com.cn		
经　　销	新华书店北京发行所		
印　　刷	中国青年出版社印刷厂		
开　　本	787×960　1/16	版　　次	2001 年 7 月第 1 版
印　　张	15	印　　次	2001 年 7 月第 1 次印刷
字　　数	270 000	定　　价	13.10 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

版权所有　侵权必究

前　言

离散数学研究离散量的结构和相互间的关系，是计算机科学中基础理论的核心课程。考虑到离散数学在计算机科学中的重要作用，我们希望学生通过该课程的学习，不仅能够掌握必备的离散数学知识，同时有助于自身数学能力的提高。本书选择离散数学基础理论中的基本内容，充分注重学生的特点，力求讲述自然，条理清楚。

本书共分成五篇，分别讲述预备知识，数理逻辑，集合论，抽象代数和图论的基本知识，并在各章后配有习题工工。

作为必须讲授和最低教学要求部分，全书的内容还可以进一步精选。书中附有“*”号的内容可以作为选修或者只作为学生阅读参考使用，不作基本要求。根据《中学教师进修高等师范本科（专科起点）教学计划》对本课程课时的规定，并依据“专升本”教学的实际情况，建议使用本教材时参考如下的课时分配方案。

	脱产	业余	函授		
			面授	自学	合计
第一章 预备				4	4
第二章 命题逻辑	10	10	8	16	24
第三章 一阶谓词逻辑	8	8	6	12	18
第四章 集合和二元关系	10	10	8	16	24
第五章 群	12	12	8	16	24
第六章 环	4	4	2	4	6
第七章 格和布尔代数	10	10	8	16	24
第八章 图	10	10	8	16	24
第九章 树	6	6	4	8	12
总结	2	2	2		2

本书由东北师范大学和华东师范大学合作编写，东北师范大学计算机科学系邓安生教授任主编，华东师范大学计算机科学系黄馥林教授任副主编。预备知识部分和集合论部分由邓安生执笔；数理逻辑部分由杨沛（华东师范大学）执笔；抽象代数部分由关伟洲（东北师范大学）执笔；图论部分由章炯民（华东师范

大学)执笔;最后由邓安生和黄馥林对全书统稿。

本书由华东师范大学计算机科学系陶增乐教授审阅。

限于作者水平,书中难免存在错误、疏漏和不妥之处,恳请广大读者、教师和专家批评指正。

编 者

2000 年 10 月

试读结束:需要全本请在线购买: www.ertongbook.com

目　录

第一篇　预备知识

第一章　预备 …… 1

1.1　整除、互质和同余 …… 1

1.1.1　整除和质因数分解 …… 1

1.1.2　同余式 …… 7

1.2　排列和组合 …… 11

1.2.1　排列与组合及其简单性质 …… 11

1.2.2　排列和组合的生成 …… 18

1.3　数学归纳法 …… 19

1.3.1　数学归纳法的基本形式 …… 20

1.3.2　数学归纳法的其他形式 …… 21

1.4　小结 …… 25

习题一 …… 25

第二篇　数理逻辑

第二章　命题逻辑 …… 27

2.1　基本概念 …… 27

2.1.1　命题与逻辑联结词 …… 27

2.1.2　命题公式与类型 …… 32

2.2　等值演算 …… 35

2.2.1　等值和基本等值式 …… 35

2.2.2　置换规则 …… 37

2.2.3　联结词的全功能集* …… 39

2.3　范式 …… 40

2.3.1　析取范式和主析取范式 …… 41

2.3.2　合取范式和主合取范式 …… 46

2.4　公式的蕴涵和推理 …… 49

2.5　小结 …… 55

习题二 …… 55

第三章　一阶谓词逻辑 …… 58

3.1　基本概念 …… 58

3.1.1 谓词和量词 …… 58
3.1.2 一阶谓词公式和解释 …… 60
3.2 等值演算和前束范式 …… 64
3.2.1 等值演算 …… 64
3.2.2 前束范式 …… 68
3.3 公式的蕴涵和推理 …… 70
3.4 小结 …… 73
习题三 …… 73

第三篇 集合和关系

第四章 集合和二元关系 …… 75
4.1 集合及其运算 …… 75
4.1.1 集合及其表示 …… 75
4.1.2 集合之间的关系和运算 …… 76
4.1.3 集合恒等式 …… 79
4.2 二元关系及其闭包 …… 81
4.2.1 二元关系及其运算 …… 81
4.2.2 二元关系的性质 …… 84
4.2.3 二元关系的闭包 …… 85
4.3 几种特殊的二元关系 …… 87
4.3.1 等价关系 …… 88
4.3.2 部分序关系 …… 89
4.3.3 相容关系* …… 91
4.4 映射与集合的等势 …… 93
4.4.1 映射的基本概念 …… 94
4.4.2 映射的性质 …… 94
4.4.3 集合的等势* …… 98
4.5 小结 …… 101
习题四 …… 102

第四篇 代数结构

第五章 群 …… 106
5.1 代数系统 …… 106
5.1.1 代数运算 …… 106
5.1.2 代数系统及其同态和同构 …… 109
5.2 群和子群 …… 112
5.2.1 群的定义及其基本性质 …… 112
5.2.2 子群和子群的判定 …… 114

5.3 变换群和置换群 …… 116
5.3.1 变换群 …… 116
5.3.2 置换群 …… 117
5.4 循环群 …… 121
5.4.1 循环群和生成元 …… 122
5.4.2 循环群的性质 …… 122
5.5 群的陪集分解 …… 127
5.5.1 陪集及其基本性质 …… 127
5.5.2 有限群的陪集分解 …… 130
5.5.3 正规子群和商群 …… 131
5.6 群的同态和同构 …… 133
5.6.1 同态映射的核 …… 133
5.6.2 群同态基本定理 …… 137
5.6.3 群的自同态和自同构 …… 139
5.7 小结 …… 140
习题五 …… 141
第六章 环 …… 144
6.1 环及其基本性质 …… 144
6.1.1 环及其简单性质 …… 144
6.1.2 子环 …… 146
6.1.3 环的分类 …… 146
6.2 环的同态和同构 …… 149
6.2.1 理想子环和商环 …… 149
6.2.2 环同态基本定理 …… 152
6.2.3 素理想和极大理想 …… 153
6.3 域 …… 155
6.3.1 域的特征、素域 …… 155
6.3.2 域的扩张 …… 157
6.4 小结 …… 159
习题六 …… 160
第七章 格和布尔代数 …… 162
7.1 格和子格 …… 162
7.1.1 格的定义 …… 162
7.1.2 子格 …… 165
7.2 格的性质 …… 166
7.2.1 格的基本性质 …… 166
7.2.2 格的对偶原理 …… 168
7.3 几种特殊的格 …… 170

7.3.1 有界格和有余格 …… 170
7.3.2 分配格和模格 …… 171
7.4 布尔代数 …… 174
7.4.1 布尔代数及其基本性质 …… 174
7.4.2 亨廷顿公理 …… 176
7.4.3 有限布尔代数 …… 178
7.5 小结 …… 181
习题七 …… 181

第五篇 图 和 树

第八章 图 …… 185
8.1 图及其表示 …… 185
8.1.1 图的概念 …… 185
8.1.2 图的简单性质 …… 189
8.1.3 子图 …… 190
8.1.4 图的同构 …… 192
8.1.5 图的矩阵表示 …… 193
8.2 图的连通性 …… 195
8.2.1 通路和回路 …… 196
8.2.2 图的连通性 …… 197
8.2.3 最短通路与迪杰斯特拉算法 …… 201
8.3 欧拉图和哈密尔顿图 …… 204
8.3.1 欧拉图 …… 204
8.3.2 哈密尔顿图 …… 207
8.4 平面图 …… 210
8.4.1 平面图的概念 …… 210
8.4.2 平面图的性质和特征 …… 212
8.5 小结 …… 215
习题八 …… 215
第九章 树 …… 219
9.1 无向树 …… 219
9.1.1 无向树及其基本性质 …… 219
9.1.2 最小生成树与克鲁斯卡尔算法 …… 222
9.2 有向树 …… 225
9.2.1 有向树和根树及其简单性质 …… 225
9.2.2 最优二叉树与哈夫曼算法 …… 228
9.3 小结 …… 231
习题九 …… 231

第一篇　预备知识

本篇内容为预备知识．在本篇中将简要地介绍整数论、组合论中的一些最基本的知识和在离散数学中广泛应用的数学归纳法．这些内容是为了使学生能够更加顺利地学好以后各章节的内容而加入的，供学生在学习时参考，它们中的一些知识（如整数论部分）在以后的叙述中被用到，但又不属于本书中任何其他的章节．我们建议学生对本篇所介绍的内容能够认真阅读，因为这些内容不仅是进一步学习离散数学的准备性知识，同时这些知识本身也是很重要的，至少对于学习计算机科学是十分必要的．

本篇内容在教学中可以略去，除极个别的内容需要较高的数学知识以外，其他内容学生只要具有中学的数学基础，就能够进行自学．

第一章　预　　备

1.1　整除、互质和同余

本节讲述整数论中的一些基本知识．通过这一节的学习，学生应该掌握整除的基本概念和基本性质，掌握最高公因的概念、基本性质和用辗转相除求最高公因的方法，学会整数的质因数分解方法，掌握同余的基本概念和基本性质，理解完全剩余系和简化剩余系的概念，了解一次同余方程和一次联立同余方程的求解方法，理解欧拉（Euler）函数的计算方法．

本节介绍整数论中的一些最基本的知识．为了叙述上的简便，如果不特别说明，在本节中所出现的表示数的符号均假定为整数．

1.1.1　整除和质因数分解

两个整数的和、差、积仍然是整数，但是用一个不等于0的整数去除另一个整数所得到的结果不一定是整数．我们已经学过“6除以2等于3”（即$6\div 2=3$）这样简单的事实，其中6称为**被除数**，2称为**除数**，3称为**商**．当然也知道用2

去除 7 是除不尽的,“7 除以 2”的**余数**为 1. 所谓整数的整除性就是研究有关整数之间能否整除的问题.

定义 1.1.1 设 a,b 是整数. 若存在整数 c,使得 $a=bc$,则称 a 是 b 的**倍数**,b 是 a 的**因数**,也称 b **整除** a,a 被 b 整除.

根据整除的定义,下述结论是显然的.

(1) ± 1 能整除任意整数,任意整数均能整除 0.

(2) 0 能够整除 0,除了 0 以外,0 不能整除其他整数.

若 a 整除 b,则记为 $a\mid b$,否则记为 $a\nmid b$. 整数的整除具有如下的基本性质,这些性质的证明极为简单,读者可以直接根据定义自行完成.

定理 1.1.1 设 a,b,c 是整数,

(1) 若 $a\mid b,b\mid c$,则 $a\mid c$.

(2) 若 $a\mid b$,则 $a\mid bc$.

(3) 若 $a\mid b,b\mid a$,则 $a=\pm b$.

(4) 若 $a\mid b,a\mid c$,则对任意的整数 s 和 t,有 $a\mid(sb+tc)$. ▌

定理 1.1.2(带余除法定理) 设 a 和 b 是整数并且 $b\neq 0$,则存在惟一的整数 q 和 r,使得

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

证明 先证明 q 和 r 的存在性.

当 $b>0$ 时,考虑 b 的倍数

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

将 b 的这些倍数和 a 进行比较,易知必存在 q,使得

$$qb\leqslant a<(q+1)b$$

现在令 $r=a-qb$,这时有

$$a=qb+r,\quad \text{其中 } 0\leqslant r<b.$$

当 $b<0$ 时,$-b>0$. 因而由上述讨论可知,存在 q 和 r,使得

$$a=q(-b)+r,\quad \text{其中 } 0\leqslant r<-b=|b|.$$

总之,无论 $b>0$ 还是 $b<0$,都存在整数 q 和 r,使得

$$a=qb+r,\quad \text{其中 } 0\leqslant r<|b|.$$

再证明 q 和 r 的惟一性.

设 q_1,r_1 和 q_2,r_2 满足

$$a=q_1b+r_1,\quad \text{其中 } 0\leqslant r_1<|b|$$

$$a=q_2b+r_2,\quad \text{其中 } 0\leqslant r_2<|b|$$

则 $(q_1-q_2)b=r_1-r_2$,由于 $|r_1-r_2|<|b|$,所以 $|(q_1-q_2)b|<|b|$,这时只能 $q_1=q_2$,因而 $r_1=r_2$.

试读结束:需要全本请在线购买: www.ertongbook.com

综上所述，定理成立．▌

带余除法定理中的式子 $a = qb + r$（其中 $0 \leqslant r < |b|$）也称为**长除式**，在整数理论中占有十分重要的地位．

若 d 既是 a 的因数又是 b 的因数，则称 d 是 a 和 b 的**公因数**，简称公因；若 m 既是 a 的倍数又是 b 的倍数，则称 m 是 a 和 b 的**公倍数**，简称公倍．

定义 1.1.2 d 称为是 a 和 b 的**最高公因**，如果

(1) $d \mid a$ 并且 $d \mid b$．即 d 是 a 和 b 的公因数．

(2) 若 d' 是 a 和 b 的公因数，则 $d' \mid d$．即 d 能被 a 和 b 的所有公因数整除．

定义 1.1.3 m 称为是 a 和 b 的**最低公倍**，如果

(1) $a \mid m$ 并且 $b \mid m$．即 m 是 a 和 b 的公倍数．

(2) 若 m' 也是 a 和 b 的公倍数，则 $m \mid m'$．即 m 能整除 a 和 b 的所有公倍数．

显然，若 d 是 a 和 b 的最高公因，则 $-d$ 也是 a 和 b 的最高公因．类似地，若 m 是 a 和 b 的最低公倍，则 $-m$ 也是 a 和 b 的最低公倍．也就是说，两个整数的最高公因和最低公倍如果存在，则其最高公因和最低公倍除了相差一个正负号以外是惟一确定的．因此，以后所提及的最高公因和最低公倍均假定是非负整数①．

定理 1.1.3 任意整数 a 和 b 都有最高公因，并且可以表示成为 a 和 b 的倍数之和 $sa + tb$ 的形式．

证明 若 $a = b = 0$，这时 a 和 b 的最高公因为 0，定理显然成立．以下设 a 和 b 不同时为 0．令

$$d = \min\{sa + tb \mid sa + tb > 0\}$$

往证 d 是 a 和 b 的最高公因．

不失一般性，设 $d = s_0 a + t_0 b$．显然 a 和 b 的公因数一定能整除 d，故以下只需再证明 d 是 a 和 b 的公因数．令

$$a = qd + r, \quad \text{其中 } 0 \leqslant r < d$$

若 $r \neq 0$，则 $r = a - qd = (1 - qs_0)a + (-qt_0)b$，这就是说，$r$ 具有 $sa + tb$ 的形式并且 $0 < r < d$，与 d 的定义矛盾，所以 $d \mid a$．同理可得 $d \mid b$．

总之，d 是 a 和 b 的具有 $sa + tb$ 形式的最高公因，定理成立．▌

显然，在 $a = qb + r$ 中，a 和 b 的公因数与 b 和 r 的公因数是完全相同的，也就是说，d 是 a 和 b 的公因数当且仅当 d 是 b 和 r 的公因数．

---

① a 和 b 的最高公因和最低公倍也称为 a 和 b 的**最大公因数**和**最小公倍数**，一般记为 $\gcd(a,b)$ 和 $\operatorname{lcm}(a,b)$，有时分别用符号 (a,b) 和 $[a,b]$ 表示．

定理 1.1.4 任意整数 a 和 b 都有最低公倍，若 d 和 m 分别是 a 和 b 的最高公因和最低公倍，则 $dm=|ab|$.

证明 显然，只需证明定理当 a 和 b 均为非负数时成立即可.

当 $a=b=0$ 时，$d=0$ 并且 $m=0$，这时定理成立. 以下设 a 和 b 不同时为 0，这时 $d\neq 0$.

令 $m=\frac{ab}{d}$，为证明定理成立，只需证 m 是 a 和 b 的最低公倍. 首先，由于 $\frac{a}{d}$ 和 $\frac{b}{d}$ 都是整数，故 m 是 a 和 b 的公倍数；其次，对 a 和 b 的任意公倍数 m'，必存在 x 和 y，使得 $m'=ax=by$. 根据定理 1.1.3，可设 $d=sa+tb$，两边同乘以 x，得 $dx=sm'+tbx$，故 $b\mid dx$，因而 $\frac{b}{d}\mid x$. 故存在 z，使得 $x=\frac{b}{d}z$. 于是有

$$m'=ax=\left(\frac{ab}{d}\right)z=mz$$

即 $m\mid m'$.

综上所述，定理成立. ▌

定理 1.1.4 给出了利用两个整数的最高公因求其最低公倍的方法. 下面给出求任意两个整数的最高公因，并将其表示成为它们的倍数之和的方法，这种方法称为**辗转相除**.

对于任意整数 a 和 b，若 $b=0$，显然 a 是 a 和 b 的最高公因，因而以下不妨假定 $b\neq 0$.

由定理 1.1.2，可得到一系列长除式：

$$\begin{aligned}
a&=q_1b+r_1, && \text{其中 } 0\leqslant r_1<|b|\\
b&=q_2r_1+r_2, && \text{其中 } 0\leqslant r_2<r_1\\
&\vdots\\
r_{k-2}&=q_kr_{k-1}+r_k, && \text{其中 } 0\leqslant r_k<r_{k-1}\\
&\vdots\\
r_{n-2}&=q_nr_{n-1}+r_n, && \text{其中 } 0\leqslant r_n<r_{n-1}\\
r_{n-1}&=q_{n+1}r_n.
\end{aligned}$$

由于 $r_1,r_2,\cdots,r_k,\cdots$ 均为非负整数并且逐次减小，故一直做下去必然减小到 0. 所以不妨设 $r_{n+1}=0$，于是 r_n 必是 a 和 b 的最高公因.

如果令

$$S_0=0,T_0=1,S_1=1,T_1=q_1$$

则反复使用递推公式①

$$S_k = q_k S_{k-1} + S_{k-2}, T_k = q_k T_{k-1} + T_{k-2}$$

可以十分方便地求出 S_k 和 T_k. 在递推过程中,有 $r_k = (-1)^{k-1} S_k a + (-1)^k T_k b$.

例 1.1.1 求 301 和 133 的最高公因,并将其表示为它们的倍数之和.

解 记 $a=301, b=133$. 由于

$$301 = 2\times 133 + 35,\ 133 = 3\times 35 + 28,\ 35 = 1\times 28 + 7,\ 28 = 4\times 7 + 0$$

故 $q_1=2, r_1=35; q_2=3, r_2=28; q_3=1, r_3=7; q_4=4, r_4=0$. 于是 7 是 301 和 133 的最高公因.

从 $S_0=0, T_0=1, S_1=1, T_1=2$ 开始递推,可得 $S_2=3, T_2=7, S_3=4, T_3=9$. 所以有 $7=(-1)^2\times 4\times 301 + (-1)^3\times 9\times 133 = 4\times 301 + (-9)\times 133$. ▌

定义 1.1.4 若 a 和 b 除了 ± 1 以外没有其他的公因数,则称 a 和 b 是**互质**的.

显然,a 和 b 互质当且仅当 a 和 b 的最高公因为 1,当且仅当存在 s 和 t,使得 $sa + tb = 1$.

定理 1.1.5 对于整数 a, b, c,下述性质成立

(1) 若 a 和 b 互质并且 $a \mid bc$,则 $a \mid c$.

(2) 若 a 和 b 互质并且 a 和 c 互质,则 a 和 bc 互质.

(3) 若 a 和 b 互质,并且 $a \mid c, b \mid c$,则 $ab \mid c$.

证明 在此仅证明(2),(1)和(3)的证明请读者自己完成.

由于 a 和 b 互质并且 a 和 c 互质,所以有 s_1, t_1, s_2, t_2,使得

$$s_1 a + t_1 b = 1, s_2 a + t_2 c = 1$$

将上述两个式子左端和右端分别相乘,有

$$(s_1 s_2 a + t_1 s_2 b + s_1 t_2 c)a + (t_1 t_2)bc = 1$$

所以 a 和 bc 互质. ▌

用数学归纳法②,很容易将上述定理推广到一般情形,其证明略去.

(1) 若 a 和 $b_1, b_2, \cdots, b_n$ 都互质并且 $a \mid b_1 b_2 \cdots b_n c$,则 $a \mid c$.

(2) 若 a 和 $b_1, b_2, \cdots, b_n$ 都互质,则 a 和 $b_1 b_2 \cdots b_n$ 互质.

(3) 若 $a_1, a_2, \cdots, a_n$ 两两互质并且都整除 b,则 $a_1 a_2 \cdots a_n \mid b$.

定义 1.1.5 设 p 是一个大于 1 的正整数,若 p 除了 1 和 p 以外没有其他

---

① 对这个递推公式的推导和解释需要高等代数中有关矩阵的知识,故在此略去.

② 关于数学归纳法,请参见第 1.3 节.

的正因数,则称 p 为**质数**①.

设 p 是质数,对任意整数 a,或者 $p \mid a$,或者 $p \nmid a$,当 $p \mid a$ 时 p 和 a 不互质,当 $p \nmid a$ 时 p 和 a 互质,因此 p 和 a 互质当且仅当 $p \nmid a$.

定理 1.1.6 设 p 为质数,且 $p \mid a_1 a_2 \cdots a_n$,则 p 整除 $a_1, a_2, \cdots, a_n$ 之一.

证明 若对任意 a_i,有 $p \nmid a_i$,则 p 和 a_i 互质,其中 $1 \leqslant i \leqslant n$,于是 p 和 $a_1 a_2 \cdots a_n$ 互质. 所证矛盾. ▌

定理 1.1.7(算术基本定理) 任意大于 1 的正整数 n 都可以写成质数的乘积

$$n = p_1 p_2 \cdots p_m$$

其中 $p_1, p_2, \cdots, p_m$ 是质数. 如果不考虑乘积中的质数的排列顺序,则这个写法是惟一的.

证明 设 $n > 1$,对 n 作数学归纳法.

当 $n = 2$ 时定理显然成立. 设 $n \leqslant k$ 时$(k \geqslant 2)$定理成立,当 $n = k + 1$ 时

(1) 若 n 是质数,定理显然成立.

(2) 若 n 不是质数,设 p 是 n 的大于 1 的最小正因数,显然,p 是质数. 令 $n = pa$,这时 $1 < a < n$. 由于 p 是由 n 所惟一确定的,故 a 也是由 n 所惟一确定的. 根据归纳假设,a 可以惟一地分解成质数的乘积,所以 n 也可以惟一地分解成质数的乘积.

综上所述,由数学归纳法原理,定理成立. ▌

由定理 1.1.7 可知,任意大于 1 的正整数 n 都可以写成 $p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ 的形式,这里,$p_1, p_2, \cdots, p_m$ 是满足 $p_1 < p_2 < \cdots < p_m$ 的质数,$r_1, r_2, \cdots, r_m$ 是正整数. $p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ 称为 n 的**标准分解式**.

定理 1.1.8 (欧几里德定理)质数是无穷多的.

证明 若只有有限多个质数,则不妨设 $p_1, p_2, \cdots, p_n$ 为所有的质数,令

$$N = p_1 p_2 \cdots p_n + 1$$

由于 $N > 1$,N 不是质数,故必有质数 p 满足 $p \mid N$. 但 $p_1, p_2, \cdots, p_n$ 均不能整除 N,所以 p 是不同于 $p_1, p_2, \cdots, p_n$ 的质数,这与 $p_1, p_2, \cdots, p_n$ 是所有的质数矛盾. ▌

设 n 是一个大于 1 的正整数,可以证明,若 n 没有小于等于$\sqrt{n}$的质因数,则 n 必为质数. 当 n 不是很大时,可以使用**筛法**方便地找出 n 以内的所有质数. 在 $2, 3, \cdots, n$ 中,2 是最小的质数;将 2 和 2 的倍数删去以后,最小的数为 3,3 是

① 质数也称为**素数**,如果一个正整数 $n(n > 1)$不是质数,则称之为**合数**. 1 之所以被摒于质数和合数之外,是因为它完全不具有质数以及合数所具有的重要的数论性质.

第二个最小的质数;再将 3 和 3 的倍数删去以后,最小的数是 5,5 是第三个最小的质数;如此继续下去,直到求出 n 以内的全部质数.

1.1.2 同余式

"同余"也称为合同,是对整除性的另一种表达方式.这种表达方式的好处在于整数的同余与数的相等在性质上十分类似,因而可以用我们比较熟悉的方法来处理有关整除性的一些问题①.

定义 1.1.6 设 $m\neq 0$,整数 a 和 b 称为**模 m 同余**,记为 $a\equiv b(\mathrm{mod}\ m)$,当且仅当 $m\mid(a-b)$.

显然,$m\mid x$ 当且仅当 $-m\mid x$.因而以后在讨论整数模 m 同余时,均假定 m 为正整数.

容易证明,同余有以下基本性质,其证明请读者自己完成.

定理 1.1.9 设 a,b,c 是整数,则

(1) $a\equiv a(\mathrm{mod}\ m)$.

(2) 若 $a\equiv b(\mathrm{mod}\ m)$,则 $b\equiv a(\mathrm{mod}\ m)$.

(3) 若 $a\equiv b(\mathrm{mod}\ m)$,$b\equiv c(\mathrm{mod}\ m)$,则 $a\equiv c(\mathrm{mod}\ m)$.

(4) 若 $a\equiv b(\mathrm{mod}\ m)$,$c\equiv d(\mathrm{mod}\ m)$,则 $a\pm b\equiv c\pm d(\mathrm{mod}\ m)$,$ac\equiv bd(\mathrm{mod}\ m)$.

(5) 若 $ac\equiv bc(\mathrm{mod}\ m)$且 c 和 m 互质,则 $a\equiv b(\mathrm{mod}\ m)$.

(6) 设 p 是质数.若 $ac\equiv bc(\mathrm{mod}\ p)$且 $p\nmid c$,则 $a\equiv b(\mathrm{mod}\ p)$. ▌

记 I 是所有整数的集合.对于 $m>0$,如果用 m 去除一个整数,所得到的余数只能是 $0,1,\cdots,m-1$ 这 m 个数中的一个,因此,在模 m 下所有整数的集合 I 被分成 m 个部分②:

$$mI,mI+1,\cdots,mI+(m-1)$$

其中,$mI+r$ 表示所有被 m 除以后余数为 r 的整数的集合,称为模 m 的一个**剩余类**,这里,$r=0,1,\cdots,m-1$.于是,在模 m 下,整数集合 I 被分成 m 个剩余类.

对任意整数 a,b 来说,若 $a\equiv b(\mathrm{mod}\ m)$,则 $m\mid(a-b)$,因此存在 q 使得 $a=qm+b$,所以 a 和 m 的最高公因等于 b 和 m 的最高公因.这说明,在模 m 的任意一个剩余类 $mI+r$ 中,只要有一个元素和 m 互质,则所有其他元素都和 m 互质.也就是说,$mI+r$ 中的元素或者都和 m 互质,或者都和 m 不互质.

---

① 在第 4.3 节将会看到,非负整数上的整除关系是一种部分序关系,而整数上的同余关系是一种等价关系.等价关系具有比部分序关系更为丰富的结果.

② 参见第 4.3 节中的等价关系与等价划分.

当 $mI+r$ 的所有元素都和 m 互质时，不妨称剩余类 $mI+r$ 和 m 是互质的．在模 m 下，所有和 m 互质的剩余类的个数称为 m 的**欧拉**[①]**函数值**，记为 $\varphi(m)$．

对于模 m，在每一个剩余类中各取一个数所得到的 m 个数称为模 m 的一个**完全剩余系**；如果在每一个和 m 互质的剩余类中，各取一个数所得到的 $\varphi(m)$ 个数称为模 m 的一个**简化剩余系**．由于 $1,2,\cdots,m$ 就是模 m 的一个完全剩余系，所以 $\varphi(m)$ 等于不大于 m 的和 m 互质的正整数的个数．

定理 1.1.10（一次同余方程） 设 a 和 m 互质．对任意的 b，在模 m 下有惟一的 x 满足

$$ax\equiv b(\mathrm{mod}\ m).$$

证明 先证明存在性．由于 a 和 m 互质，故有 s 和 t 使得 $sa+tm=1$，所以 $sab+tmb=b$．令 $x=sb$，则 $ax\equiv b(\mathrm{mod}\ m)$．

再证明惟一性．设 x_1 和 x_2 都满足同余方程 $ax\equiv b(\mathrm{mod}\ m)$，则由 $ax_1\equiv b(\mathrm{mod}\ m)$ 和 $ax_2\equiv b(\mathrm{mod}\ m)$ 可知 $ax_1\equiv ax_2(\mathrm{mod}\ m)$．而 a 和 m 互质，故 $x_1\equiv x_2(\mathrm{mod}\ m)$．∎

在定理 1.1.10 中，s 可以用前面介绍的最高公因理论求出，所以该定理的证明实际上提示了一个求解一次同余方程的方法．满足方程 $ax\equiv b(\mathrm{mod}\ m)$ 的解有无穷多个，但它们在模 m 下都是同余的，即相差 m 的倍数．在习惯上，我们给出的解一般是满足这个方程的最小非负整数．如果方程中的模 m 不是很大，可以比较容易地用尝试的方法找到解，即让 x 从 0 开始，以后每次加 1，直到找出满足方程的 x 为止．

例 1.1.2 求解同余方程 $8x\equiv 7(\mathrm{mod}\ 9)$．

解 用在最高公因理论中给出的方法，可以求得 $8\times 8+(-7)\times 9=1$，于是令 $x=8\times 7=56$ 即可满足要求，由于 $56\equiv 2(\mathrm{mod}\ 9)$，所以可令 $x=2$．∎

定理 1.1.11（中国剩余定理） 设 $m_1,m_2,\cdots,m_k$ 两两互质，则对任意的 $a_1,a_2,\cdots,a_k$，在模 $m_1m_2\cdots m_k$ 下有惟一的 x 满足

$$\begin{cases} x\equiv a_1(\mathrm{mod}\ m_1)\\ x\equiv a_2(\mathrm{mod}\ m_2)\\ \quad\vdots\\ x\equiv a_k(\mathrm{mod}\ m_k). \end{cases}$$

证明 由于 $m_1,m_2,\cdots,m_k$ 两两互质，故对于 $1\leqslant i\leqslant k$，m_i 和 $\prod\limits_{j\neq i}m_j$ 互质．于是由定理 1.1.10，存在 c_i 使得 $c_i\prod\limits_{j\neq i}m_j\equiv 1(\mathrm{mod}\ m_i)$．现在令 $l_i=$

① 欧拉(Leonhard Euler)，瑞士数学家．

试读结束：需要全本请在线购买： www.ertongbook.com