国家示范性高等院校“十二五”精品规划教材

离散数学

LISAN SHUXUE

主编◎费洪晓 刘丽珏

天津大学出版社
TIANJIN UNIVERSITY PRESS

国家示范性高等院校“十二五”精品规划教材

离散数学

主　编　费洪晓　刘丽珏
副主编　费雄伟　马提宝

天津大学出版社
TIANJIN UNIVERSITY PRESS

内容提要

本书介绍离散数学的主要内容，包括数论、数理逻辑、集合论、图论、近世代数等近代数学分支的最基本知识，并对离散数学的应用作了初步介绍.

本书适合于高等院校理工科计算机类学生作为专业基础课教材，也适合作为有关科技人员的参考用书.

图书在版编目(CIP)数据

离散数学/费洪晓，刘丽珏主编. —天津：天津大学出版社，2011.8

国家示范性高等院校“十二五”精品规划教材

ISBN 978-7-5618-3974-4

Ⅰ.①离… Ⅱ.①费…②刘… Ⅲ.①离散数学 Ⅳ.①0158

中国版本图书馆 CIP 数据核字(2011)第 129933 号

出版发行	天津大学出版社
出 版 人	杨欢
地　　址	天津市卫津路 92 号天津大学内(邮编：300072)
电　　话	发行部：022－27403647　邮购部：022－27402742
网　　址	www.tjup.com
印　　刷	河间市新成印刷有限公司
经　　销	全国各地新华书店
开　　本	185mm×260mm
印　　张	17.25
字　　数	431 千
版　　次	2011 年 8 月第 1 版
印　　次	2011 年 8 月第 1 次
定　　价	34.00 元

国家示范性高等院校“十二五”精品规划教材编委会

前　言

“离散数学”是专门研究离散量的结构和相互间关系的数学理论与数学方法，是计算机科学中基础理论的核心课程，是计算机类专业最重要的专业基础课之一，是现代数学的重要分支．离散数学形成于上世纪七十年代初期，它随着计算机科学的发展而逐步建立，并不断地扩充与更新．离散数学中的基本概念、基本思想和方法与计算机科学中的数据结构、操作系统、编译理论、算法分析、逻辑设计、系统结构、数据库、容错诊断、机器定理证明等课程联系紧密，广泛用于计算机电路设计、计算机系统设计、计算机应用、软件工程、人工智能和计算机科学理论等方面，是从事计算机设计、研究、应用的专业人员必须掌握的基础知识．我们根据多年的教学实践，编写了这本适用于理工科院校计算机类专业的离散数学教材，它也可供从事计算机工作的科研人员、工程技术人员及其他有关人员参考．

本书介绍了“离散数学”的主要内容，包括数论、数理逻辑、集合论、图论、近世代数等近代数学分支的最基本知识．这对于培养训练学生抽象思维和严密逻辑推理的能力，对于后续课程的学习以及日后从事计算机应用开发和科学研究，都是十分必要的．

全书紧紧抓住了“培养读者学会思考”这一主题，全部内容统一于数理逻辑这一基础．定义和定理的叙述严格而明确，定理的证明与推理过程始终强调“What 代替 How”这一思考问题与科学研究的重要方法，逻辑性强，思路清楚，非常有利于培养学生抽象思维和严密逻辑推理的能力．

为了适应“打好基础，扩大适应面”这一总要求的发展趋势，在取材和内容组织上，本书作了一些特殊考虑．首先，我们重点选择了离散数学最核心、最基础的内容，并在阐述时力求严谨，推演时务求详尽；其次，在图论部分的内容组织上，将无向图和有向图分开介绍，这对学生的理解大有帮助；第三，在介绍近世代数的基本内容时，特别强调非常典型的、在计算机科学中的应用极其广泛的“按模加”和“按素数模乘”这一代数结构；第四，对数

论的基础知识作了一定的介绍，这不仅对后续课程的学习，同时对课程本身的学习大有帮助，还有利于训练学生严密逻辑推理的能力.

本书有针对性地选取了大量习题，其中大部分是基本的，只要熟悉了教材的基本内容即可解决，但也有少数习题难度较大，供掌握较好的读者选做.

本书由中南大学费洪晓、刘丽珏担任主编，负责全书的总体策划、统稿和定稿工作. 湖南城市学院费雄伟与黑龙江农业经济职业学院马提宝担任副主编. 长沙理工大学谢文彪、中南大学沈海澜参与了部分内容的编写工作. 在本书的编写过程中，中南大学邹北骥、施荣华、王小玲、余腊生、陈再良等老师参与了大纲的讨论，提出了许多宝贵的意见，在此一并表示感谢. 此外，在编写本书的过程中，编者参考了大量的文献资料，在此也向这些文献资料的作者表示感谢.

由于计算机科学技术发展迅速加上编者水平有限，书中遗漏和不妥之处难免恳请读者批评.

编者

2011 年 7 月

目　　录

第一篇　数论

第一章　数论基础 …… 2
1.1　整数、整除和最大公约数 …… 2
1.2　关于素数的某些初等事实 …… 8
1.3　同余 …… 13
1.4　同余方程 …… 20
1.5　二次剩余 …… 26
1.6　数论在密码学中的应用 …… 35

第二篇　数理逻辑

第二章　命题逻辑 …… 39
2.1　命题的概念与表示 …… 39
2.2　逻辑联结词 …… 40
2.3　命题演算的合式公式 …… 43
2.4　等价与蕴涵 …… 49
2.5　功能完备集及其他联结词 …… 55
2.6　对偶与范式 …… 58
2.7　命题演算的推理理论 …… 63
第三章　谓词逻辑 …… 68
3.1　谓词的概念与表示 …… 68
3.2　命题函数与量词 …… 69
3.3　谓词演算的合式公式 …… 71
3.4　变元的约束 …… 74
3.5　谓词公式的解释 …… 76
3.6　谓词演算的永真式 …… 78
3.7　谓词演算的推理理论 …… 82
3.8　自动定理证明 …… 86

第三篇　集合论

第四章　集合 …… 91
4.1　集合的概念与表示 …… 91

4.2 集合的运算 …… 97
4.3 Venn 氏图及容斥原理 …… 101
4.4 集合的划分 …… 104
4.5 自然数集与数学归纳法 …… 107
第五章 二元关系 …… 113
5.1 Cartesian 积 …… 113
5.2 关系的概念与表示 …… 115
5.3 关系的性质 …… 118
5.4 逆关系和复合关系 …… 121
5.5 关系的闭包 …… 128
5.6 有序关系 …… 131
5.7 相容关系与等价关系 …… 137
5.8 关系数据库初步 …… 142
第六章 函数 …… 145
6.1 函数的概念 …… 145
6.2 复合函数与逆函数 …… 149
6.3 基数的概念 …… 154
6.4 基数的比较 …… 160

第四篇 图论

第七章 无向图 …… 165
7.1 三个古老的问题 …… 165
7.2 若干基本概念 …… 166
7.3 路径、圈及连通性 …… 173
7.4 Euler 图和 Hamilton 图 …… 177
7.5 平面图 …… 183
7.6 图的着色 …… 188
7.7 树与生成树 …… 193
第八章 有向图 …… 197
8.1 有向图的概念 …… 197
8.2 有向图的可达性、连通性和顶点基 …… 198
8.3 根树及其应用 …… 205

第五篇 代数系统

第九章 代数结构基础 …… 212
9.1 代数系统的概念 …… 212

9.2 代数系统之间的联系 …… 216
9.3 同余关系与商代数 …… 219
9.4 半群与独异点 …… 223
9.5 群的基本性质 …… 227
9.6 变换群与循环群 …… 232
9.7 Lagrange 定理与群同态定理 …… 237
9.8 环与域 …… 242
第十章 格与布尔代数 …… 247
10.1 格的概念与性质 …… 247
10.2 分配格、有界格与有补格 …… 252
10.3 布尔代数 …… 256
10.4 布尔表达式与布尔函数 …… 260
10.5 布尔代数在电路分析中的应用 …… 261

第一篇　数　　论

初等数论是主要用算术方法研究整数性质的一个数学分支，它是数学中最古老的分支之一.

公元前三世纪，古希腊数学家 Euclid 证明了素数的个数是无穷的，并给出了求两个正整数的最大公因子的算法. 我国古代的《孙子算经》中给出了求一次同余方程组公解的算法，即著名的孙子定理，国外把它叫作中国剩余定理. 从 17 世纪到 19 世纪，Fermat、Euler、Legendre、Gauss 等人的工作大大发展和丰富了初等数论的内容. 特别是 1801 年，Gauss 出版了著名的 *Disquisitiones Arithmeticae*. 在这本书中，Gauss 证明了互逆定理、原根存在的充分必要条件等重要结果. 随着初等数论的不断发展，它的内容也越来越丰富，并促使数学中新分支的发展.

近几十年来，初等数论在计算机科学、组合数学、代数编码、信号的数字处理等领域内得到了广泛的应用，而且许多较深刻的结果也都得到了应用.

本篇介绍初等数论中最基础的内容：整除性、最大公约数、素数的基本性质、同余、同余方程、二次剩余等，学习这些内容对计算机类专业的学生是非常有益的. 一方面通过这些内容的学习加深对数的性质的了解，能够更深入地理解其他邻近学科（包括离散数学的其他内容和计算机科学的其他学科）；另一方面，更加主要的是有利于培养学生严密逻辑推理的能力. 本篇还介绍了数论知识在计算机密码学中的初步应用.

第一章　数论基础

1.1　整数、整除和最大公约数

数论中很大一部分内容是研究整数性质的. 所谓整数,乃指下列数之一:

$$\cdots, -2, -1, 0, 1, 2, \cdots$$

特别是研究正整数的性质. 所谓正整数,乃指下列数之一:

$$1, 2, 3, 4, \cdots$$

另有非负整数,乃指下列数之一:

$$0, 1, 2, 3, 4, \cdots$$

显然,正整数和非负整数都是整数的一部分.

在本篇中,小写英文字母一律代表整数,除非有特别声明.

定义 1.1.1　设 a, b 是整数,若存在一个整数 d 使得 $b = ad$,则称 a 可整除 b,记作 $a \mid b$,并称 a 为 b 的一个因子(或称为约数、因数),b 为 a 的倍数;否则称 a 不可整除 b,记作 $a \nmid b$.

例 1.1.1　根据定义 1.1.1,有 $2 \mid 4, 2 \nmid 3$.

整除关系有许多重要性质.

(1) 对于任意的整数 a,皆有: $\pm 1 \mid a, \pm a \mid a, a \mid 0$.

证明　由整除性的定义直接可知.

因为对于任意的整数 a,皆有 $\pm 1 \mid a$ 和 $\pm a \mid a$,因此常称 ± 1 和 $\pm a$ 为 a 的平凡因子.

注: 若 b 是 a 的因子,而 b 既不等于 ± 1,也不等于 $\pm a$,则称 b 为 a 的非平凡因子(或真因子).

(2) 若 d 是 $a(\neq 0)$ 的非平凡因子,则

$$1 < |d| < |a|.$$

证明　显然成立.

(3) 若 $a \mid b, b \mid c$,则 $a \mid c$.

证明　因为 $b \mid c$,所以存在 d' 使得 $c = d'b$,又因为 $a \mid b$,所以存在 d'' 使得 $b = d''a$. 故

$$c = d'b = d'(d''a) = (d'd'')a,$$

因为 $d'd''$ 是整数,由整除的定义知: $a \mid c$.

(4) 若 $d \mid a, d \mid b$,则 $d \mid (a + b)$.

证明　由整除的定义知: 存在整数 x_1 和 x_2 使得

$$a = dx_1, \ b = dx_2,$$

因此

$$a + b = d(x_1 + x_2),$$

由整除的定义知: $d \mid (a + b)$.

(5) 若 $d \mid a$,则 $cd \mid ca$,特别地,$d \mid ca$,其中 c 为任意整数.

(6) 若 $d|a_1, d|a_2, \cdots, d|a_n$，且 $c_1, c_2, \cdots, c_n$ 是 n 个整数，则

$$d|\sum_{i=1}^{n} a_i c_i .$$

性质(5)、(6)请读者自己证明.

定理 1.1.1 设 a 和 b 是任意两个整数，且 $b>0$，则存在唯一的一对整数 q 和 r 使得：

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

式中的 r 称为 b 除 a 所得的最小非负剩余(或简称为余数)，用 $a \bmod b$ 表示；q 称为 b 除 a 的不完全商.

证明 (1) 存在性.

令 α 为一实数，用 $[\alpha]$ 表示 α 的整数部分，即不超过 α 的最大整数，那么

$$[\alpha]\leqslant\alpha<[\alpha]+1,$$

即

$$0\leqslant\alpha-[\alpha]<1.$$

现取 $\alpha=\frac{a}{b}$，则有

$$0\leqslant\frac{a}{b}-\left[\frac{a}{b}\right]<1,$$

从而

$$0\leqslant a-b\left[\frac{a}{b}\right]<b.$$

取 $q=\left[\frac{a}{b}\right], r=a-b\left[\frac{a}{b}\right]$ 得

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

(2) 唯一性.

设 q、r 与 q_1、r_1 是两对商与余数，即

$$a=qb+r=q_1b+r_1(\text{其中 } 0\leqslant r<b, 0\leqslant r_1<b),$$

故

$$b(q-q_1)=(r_1-r),$$

这说明 (r_1-r) 是 b 的倍数，但是

$$-b<(r_1-r)<b,$$

所以，$r_1-r=0$，即 $b(q-q_1)=0$.

总之，有

$$q=q_1 \text{且 } r=r_1.$$

当 $a \bmod b=0$，即 $b|a$ 时，则称 b 除 a 为零剩余. 计算 $a \bmod b$ 也称 a 对 b 取模(或 a 对模 b 取余)，这一点在 1.3 节还要深入讨论.

定义 1.1.2 若 $d|a_1, d|a_2, \cdots, d|a_n$，则称 d 为 $a_1, a_2, \cdots, a_n$ 的公因子.

定义 1.1.3 设 d 是 $a_1, a_2, \cdots, a_n$ 的公因子，若对 $a_1, a_2, \cdots, a_n$ 的任一公因子 c 都有 $c\leqslant d$，则称 d 为 $a_1, a_2, \cdots, a_n$ 的最大公因子，记作 $d=\mathrm{GCD}(a_1, a_2, \cdots, a_n)$，或简单地记作 $d=(a_1, a_2, \cdots, a_n)$.

另常用 $\mathrm{LCM}(a_1, a_2, \cdots, a_n)$ 表示 $a_1, a_2, \cdots, a_n$ 的最小公倍数.

定义 1.1.4 若$(a_1,a_2,\cdots,a_n)=1$,则称$a_1,a_2,\cdots,a_n$互素(也称互质). 如果$a_1,a_2,\cdots,a_n$中的每一个数都与其他数互素,则称$a_1,a_2,\cdots,a_n$是两两互素的.

例 1.1.2 根据定义,有:$(2,3)=1,(4,6)=2,(4,6,8)=2$;而3,4,5是两两互素的.

最大公因子有下列性质.

(1) 若$a\mid b$,则$(a,b)=|a|$.

证明 由最大公因子的定义直接可证明.

(2) 若$(a,b)=d$,则$\left(\frac{a}{d},\frac{b}{d}\right)=1$.

证明 显然$\left(\frac{a}{d},\frac{b}{d}\right)\geqslant 1$. 令$\left(\frac{a}{d},\frac{b}{d}\right)=c$,则$c\mid\left(\frac{a}{d}\right)$且$c\mid\left(\frac{b}{d}\right)$.

根据整除的性质(5),有

$$cd\mid a \text{ 且 } cd\mid b,$$

即cd是a和b的公因子,所以$cd\leqslant(a,b)=d$,这表明$c\leqslant 1$.

总之,有

$$c=\left(\frac{a}{d},\frac{b}{d}\right)=1.$$

(3) 若$a=bq+r$,那么$(a,b)=(b,r)$.

证明 记$d=(a,b),c=(b,r)$.

由$d\mid a$且$d\mid b$可知$d\mid(a-bq)$,即$d\mid r$,从而d是b和r的公因子,所以$d\leqslant c$.

另一方面,由$c\mid b$且$c\mid r$可知$c\mid(bq+r)$即$c\mid a$,从而c是a和b的公因子,所以$c\leqslant d$.

综上,有$c=d$,即$(a,b)=(b,r)$.

这一性质提示了一个通常所熟知的求最大公因子的有效方法,即著名的Euclid算法(或称辗转相除法).

定理 1.1.2(Euclid 算法) 若a和b是正整数,且

$$\begin{aligned}
&a=bq_1+r_1, && 0<r_1<b,\\
&b=r_1q_2+r_2, && 0<r_2<r_1,\\
&r_1=r_2q_3+r_3, && 0<r_3<r_2,\\
&\vdots && \vdots\\
&r_k=r_{k+1}q_{k+2}+r_{k+2}, && 0<r_{k+2}<r_{k+1},
\end{aligned}$$

那么,当k足够大时,比如$k=t$,有

$$r_t=r_{t+1}q_{t+2},$$

并且

$$(a,b)=r_{t+1}.$$

证明 非负整数序列$b>r_1>r_2>r_3>\cdots$必有终点,所以,这些余数中最后将出现零. 假定$r_{t+2}=0$,那么$r_t=r_{t+1}q_{t+2}$.

根据最大公因子的性质(3),可知

$$(a,b)=(b,r_1)=(r_1,r_2)=(r_2,r_3)=\cdots=(r_t,r_{t+1})=r_{t+1}.$$

例 1.1.3 用Euclid算法计算(343,280)的过程如下:

①$343=280\times 1+63$,

②$280=63\times4+28$,

③$63=28\times2+7$,

④$28=7\times4$,

所以,$(343,280)=7$.

当 a 和 b 中有一个或两个都是负数时,由于

$$(a,b)=(-a,b)=(a,-b)=(-a,-b),$$

仍可利用 Euclid 算法求得(a,b).

定理 1.1.3 对于任意的整数 a 和 b,必存在整数 x 和 y 使得

$$ax+by=(a,b).$$

证明 可用多种方法来证明此定理,下面介绍两种.

【法一】 根据 Euclid 算法,有

$$(a,b)=r_{t+1}=r_{t-1}-r_tq_{t+1},$$

它将 r_{t-1} 和 r_t 用整系数组合起来表示了(a,b). 又因为

$$r_{t-2}=r_{t-1}q_t+r_t,$$

故

$$r_t=r_{t-2}-r_{t-1}q_t.$$

于是

$$(a,b)=r_{t-1}-(r_{t-2}-r_{t-1}q_t)q_{t+1}=r_{t-2}(-q_{t+1})+r_{t-1}(1+q_tq_{t+1}),$$

即将(a,b) 表示成了 r_{t-2} 和 r_{t-1} 的整系数组合,再利用

$$r_{t-3}=r_{t-2}q_{t-1}+r_{t-1}$$

消去 r_{t-1},便可将(a,b) 表示成 r_{t-3} 和 r_{t-2} 的整系数组合:

$$(a,b)=r_{t-3}x_1+r_{t-2}y_1(\text{其中 } x_1 \text{ 和 } y_1 \text{ 是两个整数}),$$

如此继续下去,最后必可将(a,b) 表示成 a 和 b 的整系数组合:

$$(a,b)=ax+by.$$

例 1.1.4 在例 1.1.3 中,有:

$$\begin{aligned}(343,280)&=7=63-28\times2\\&=63-(280-63\times4)\times2\\&=9\times63-2\times280\\&=9\times(343-280)-2\times280\\&=9\times343-11\times280,\end{aligned}$$

这样就找到了使

$$343x+280y=(343,280)$$

成立的 x 和 y: $x=9,y=-11$.

【法二】 若 a 和 b 中有一个为 0,则命题显然成立. 现不妨设 $a\neq0,b\neq0$. 构造集合:

$$S=\{ax+by\mid x,y \text{ 为整数}\},$$

由于 $a\neq0,b\neq0$,故 S 必非空且 S 含有正整数,令

$$S_+=\{s\mid s\in S \text{ 且 } s>0\},$$

S_+ 中必有最小数 d,事实上,$d=(a,b)$,这是因为:

(1) 由 $d\in S$ 可知,存在整数 x 和 y 使得: $ax+by=d$. 令

$$a = dq + r \text{ (其中 } 0 \leqslant r < d),$$

由于

$$r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq),$$

所以 $r \in S$; 又 $0 \leqslant r < d$ 且 d 为 S_+ 中最小者,这样 $r = 0$,即 $d \mid a$. 同理 $d \mid b$.

所以,$d \leqslant (a,b)$.

(2) 显然对于任意的整数 x 和 y 有 $(a,b) \mid (ax + by)$,从而 $(a,b) \mid d$.

综合(1)和(2),得证.

注: 定理可以这样推广,对于任意的整数 $a_1, a_2, \cdots, a_n$,必存在整数 $t_1, t_2, \cdots, t_n$ 使得:

$$a_1t_1 + a_2t_2 + \cdots + a_nt_n = (a_1, a_2, \cdots, a_n)$$

根据这一定理有以下推论.

推论 1 如果 $d \mid ab$ 且 $(d,a) = 1$,那么 $d \mid b$.

证明 因为 $(d,a) = 1$,所以存在整数 x 和 y 满足

$$ax + dy = 1,$$

故

$$abx + dby = b,$$

现在,$d \mid db$ 且 $d \mid ab$,所以 $d \mid b$.

推论 2 设 $(a,b) = d$ 且 $c \mid a, c \mid b$,那么 $c \mid d$.

证明 因为存在整数 x 和 y 使得

$$d = ax + by,$$

而 $c \mid a$ 且 $c \mid b$,故 $c \mid d$.

注: (1) 这一结论也可从 Euclid 算法中得到;

(2) 根据这一结论,有 $(a,b,c) = ((a,b),c)$,从而可用归纳法证明递推式

$$(a_1, a_2, \cdots, a_n) = ((a_1, a_2, \cdots, a_{n-1}), a_n)$$

成立.

推论 3 若 $a \mid m, b \mid m$,并且 $(a,b) = 1$,那么 $ab \mid m$.

证明 因为 $a \mid m$,所以存在整数 q 使得 $m = aq$. 又 $b \mid m$,即 $b \mid aq$,而 $(a,b) = 1$,故由推论 1 可知 $b \mid q$. 因此存在整数 r 使得 $q = br$,于是 $m = aq = abr$,即 $ab \mid m$.

推论 4 $(ac,bc) = (a,b)c$,此处 $c > 0$.

证明 因为存在整数 x 和 y 使得

$$ax + by = (a,b),$$

故

$$acx + bcy = (a,b)c,$$

从而 $(ac,bc) \mid (a,b)c$.

另一方面,易知 $(a,b)c \mid ac, (a,b)c \mid bc$,所以 $(a,b)c \mid (ac,bc)$.

综合上面两点可得

$$(ac,bc) = (a,b)c.$$

注: 这一结论也可从 Euclid 算法中得到.

推论 5 若 $(a,b) = 1$,则 $(ac,b) = (c,b)$.

证明 一方面,显然

$$(ac,b) \mid ac,\ (ac,b) \mid bc.$$

故由推论 2 得

$$(ac,b) \mid (ac,bc).$$

又由推论 4 得

$$(ac,bc) = (a,b)c = c,$$

即得$(ac,b) \mid c$. 从而(ac,b)是 c 和 b 的公因子,所以

$$(ac,b) \leqslant (c,b).$$

另一方面,由$(c,b) \mid ac$ 和$(c,b) \mid b$ 可知,$(c,b) \leqslant (ac,b)$.

综上,本推论得证.

推论 6 若 $a_1,a_2,\cdots,a_m$中的每一个与 $b_1,b_2,\cdots,b_n$ 中的每一个互素,则 $a_1a_2\cdots a_m$ 与 $b_1b_2\cdots b_n$ 互素.

证明 略(反复应用推论 5 的结论即可得证).

习 题 1.1

1. 设 α 为一实数,且 $\alpha = p + \beta$,其中 p 为整数. 证明: $[\alpha] = p + [\beta]$.

2. 设 α 和 β 为实数,证明不等式:

(1) $[\alpha] + [\beta] \leqslant [\alpha + \beta] \leqslant [\alpha] + [\beta] + 1$;

(2) $[\alpha - \beta] \leqslant [\alpha] - [\beta] \leqslant [\alpha - \beta] + 1$.

3. 设 α 和 β 为实数,证明不等式:

$$[2\alpha] + [2\beta] \geqslant [\alpha] + [\alpha + \beta] + [\beta].$$

4. 设 α 为实数,n 为正整数,证明:

(1) $\left[\dfrac{[\alpha]}{n}\right] = \left[\dfrac{\alpha}{n}\right]$;

(2) $\left[\dfrac{[n\alpha]}{n}\right] = [\alpha]$;

(3) $[\alpha] + \left[\alpha + \dfrac{1}{n}\right] + \cdots + \left[\alpha + \dfrac{n-1}{n}\right] = [n\alpha]$.

5. 证明: 若 n 是奇数,则 $16 \mid (n^4 + 4n^2 + 11)$.

6. 证明: 若$(m-n) \mid (mx + ny)$,则$(m-n) \mid (my + nx)$.

7. 用 Euclid 算法求出$(323,221)$,并找出使

$$323x + 221y = (323,221)$$

成立的 x 和 y. 对另一对数: 578 和 442 作相同的计算.

8. 证明: 若$(a,b) = 1, c \mid (a+b)$,则$(a,c) = (b,c) = 1$.

9. 证明: $(a,b,c)(ab,bc,ca) = (a,b)(b,c)(c,a)$.

10. 证明: 若$(a,b) = 1$,则$(a+b, a-b) = 1$ 或 2.

11. 证明: 若$(a,b) = 1$,则$(a+b, a^2 - ab + b^2) = 1$ 或 3.

12. 设$(a,b) = d, c > 0$,且 $c \mid a, c \mid b$. 证明: $\left(\dfrac{a}{c}, \dfrac{b}{c}\right) = \dfrac{d}{c}$.

1.2 关于素数的某些初等事实

正整数可以按以下方式分成三类:

(1) 数 1;

(2) 不能被除了 1 和其本身之外的任何正整数整除的数,这类数叫素数或质数;

(3) 除(1) 和(2) 中包含的正整数以外,其他的正整数组成一类,称为复合数或合数,任一合数除了 1 和其本身之外还能被第三个正整数整除.

或者说,合数是含有非平凡因子的正整数,素数是没有非平凡因子的大于 1 的正整数.

例 1.2.1 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97 是 100 以内的全部 25 个素数,2 是全体素数中唯一的偶数,除 2 以外的素数称为奇素数. 常用 p,q 等字母来表示素数.

两个相差 2 的素数称为一对孪生素数. 例如,11 和 13、17 和 19、29 和 31 是三对孪生素数.

素数有很多重要性质,在计算机科学中有广泛的应用. 素数的性质是数论最早的研究课题之一,著名的华罗庚教授及陈景润、王元研究员,潘承洞教授等对素数论的研究都作出了重要的贡献.

定理 1.2.1 若 p 为素数,则对于任一整数 a 有: 要么 $(p,a)=1$,要么 $p\mid a$.

证明 因为 p 仅有正因子 1 和 p,故 $(p,a)=1$,或 $(p,a)=p$ 亦即 $p\mid a$.

常称 a 的素数因子为 a 的素因子.

定理 1.2.2 设 a 是大于 1 的正整数,且所有不超过 $\sqrt{a}$ 的正整数 $x(x>1)$ 都不能整除 a,则 a 是素数.

证明 反证法.

假定 a 不是素数,那么存在正整数 b 和 c 是 a 的非平凡因子使得

$$a=bc,$$

由条件知: $b>\sqrt{a}$, $c>\sqrt{a}$,从而有

$$bc>\sqrt{a}\cdot\sqrt{a}=a=bc,$$

矛盾.

这一定理表明,若 a 是合数,则 a 必有不超过 $\sqrt{a}$ 的非平凡因子,事实上必有不超过 $\sqrt{a}$ 的素因子. 著名的 Eratosthenes 筛选法就是利用这一原理求出所有不大于给定正整数 a 的素数的.

定理 1.2.3 若 p 是素数,且 $p\mid a_1a_2\cdots a_m$,则存在 $a_k(1\leqslant k\leqslant m)$,使得 $p\mid a_k$.

证明 由定理 1.1.3 之推论 1 和定理 1.2.1 直接可得.

定理 1.2.4 素数的个数为无限个.

证明 反证法.

假设只有有限个(不妨设 n 个) 素数,并设它们是 $p_1,p_2,\cdots,p_n$. 考虑正整数

$$m=p_1p_2\cdots p_n+1,$$