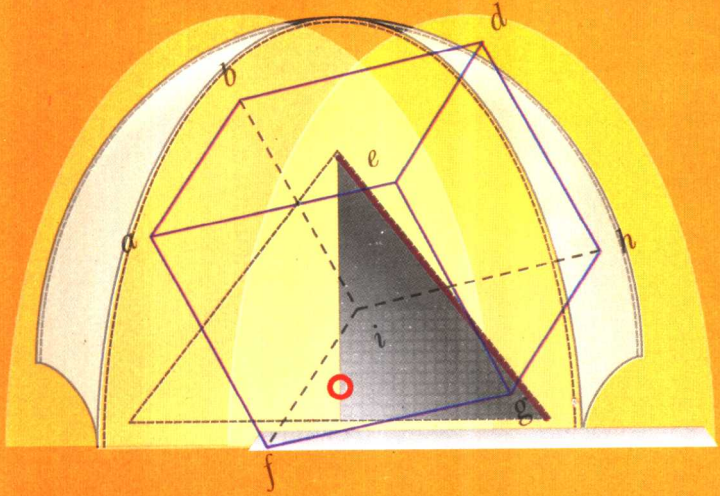
费洪晓 编著

Lisan Shuxue
Jichu Jiaocheng

离散数学基础教程



湖南大学出版社

面向21世纪高等学校数学系列教材

离散数学基础教程

费洪晓　编

湖南大学出版社
2001年·长沙

内 容 提 要

本书系统地介绍了"离散数学"的基本内容和方法，主要内容包括数论、数理逻辑、集合论、图论、近世代数等.这些内容对于培养训练学生抽象思维能力，对于后续课程的学习，以及从事计算机应用开发和科学研究十分必要.

本书语言简朴、通顺、通俗易懂，适合于高等院校本科生作教材，也可供计算机专业师生和科研人员参考.

图书在版编目(CIP)数据

离散数学基础教程/费洪晓编.—长沙：湖南大学出版社，2001.9

ISBN7-81053-422-x/O·31

Ⅰ.离… Ⅱ.费… Ⅲ.离散数学-高等学校-教材细化

Ⅳ.0158

中国版本图书馆 CIP 数据核字(2001)第 065767 号

离散数学基础教程

Lisan Shuxue Jichu Jiaocheng

费洪晓 编

□责任编辑 李立鹏 李 刚 厉 亚

□出版发行 湖南大学出版社

社址 长沙市岳麓山 邮码 410082

电话 0731-8821691 0731-8821315

□经 销 湖南省新华书店

□印 装 湖南航天长宇印刷有限责任公司

□开本 850×1168 32开 □印张 11 □字数 273千

□版次 2001年9月第1版 □2001年9月第1次印刷

□印数 1-5 000册

□书号 ISBN 7-81053-422-x/O·31

□定价 15.00元

前 言

“离散数学”是专门研究离散量的结构和相互关系的数学理论与方法，是计算机科学中基础理论的核心课程，是计算机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20世纪70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、逻辑分析、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．

本书系统地介绍了“离散数学”各分支的主要内容，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．这些内容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．

全书紧紧地抓住了“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，思路清晰，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”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做出.但也有少数习题难度较大，供掌握较好的读者选做.

本书是作者在总结长期学习和教学的基础上，参考大量文献后编写而成的，全部内容均作过多次讲授，并印成讲义实践过.这期间作者的相关工作得到了原长沙铁道学院信息工程学院的大力支持，在此表示衷心感谢.

编　者

2001 年 7 月于中南大学

目 次

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.

我们知道，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的公解的算法，即著名的孙子定理，国外把它叫做中国剩余定理.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都得到了应用.

我们在本篇中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专业的学生是非常有益的.

一方面通过这些内容加深对数的性质的了解，更深入地理解某些其它邻近学科(包括离散数学的其它内容和计算机科学的其它学科)；另一方面，也许更重要的是有利于培养严密逻辑推理的能力.

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(常称为自然数)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 $b = ad$，那么我们称 a 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，有 $2 \mid 4, 2 \nmid 3$

整除关系有下列性质：

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

证　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 显然.

(3) 若 $a|b, b|c$，则 $a|c$.

证 因为 $b|c$，所以存在 d' 使得 $c = d'b$，又因为 $a|b$，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：$a|c$.

(4) 若 $d|a, d|b$，则 $d|(a+b)$.

证 由整除的定义知：存在整数 x_1 和 x_2 使得

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

因此

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

由整除定义知 $d|(a+b)$.

(5) 若 $d|a$，则 $cd|ca$，特别地，$d|ca$，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

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

以上两性质请读者补证.

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

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

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

证 (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 $\alpha = a/b$,则有

$$0 \leqslant a/b - [a/b] < 1,$$

从而

$$0 \leqslant a - b[a/b] < b,$$

即 $q = [a/b], r = a - b[a/b]$ 立得

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

(2) 唯一性.

设 q、r 与 q_1、r_1 是两对这样的商与余数,即

$a = qb + r = q_1 b + r_1$, 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,我们有

$$q = q_1, \text{且 } r = r_1.$$

当 $a \bmod b = 0$,即 $b \mid a$ 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 $d \mid a_1, d \mid a_2, \cdots, d \mid a_n$,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 $d = GCD(a_1, a_2, \cdots, a_n)$,或简单地记作 $d = (a_1, a_2, \cdots, a_n)$.

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(也有称互质的). 如果 $a_1, a_2, \cdots, a_n$ 中的每一个数都与其它数互素,则称 $a_1, a_2, \cdots, a_n$ 是两两互素的.

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

最大公因子有下列性质：

(1) 若 $a|b$，则 $(a,b) = |a|$.

证 由最大公因子的定义直接可知.

(2) 若 $(a,b) = d$，则 $(a/d,b/d) = 1$.

证 显然 $(a/d,b/d) \geqslant 1$. 令 $(a/d,b/d) = c$，则 $c|(a/d)$ 且 $c|(b/d)$. 根据整除的性质(5)，有

$$cd|a, \qquad \text{且 } cd|b,$$

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，我们有

$$c = (a/d,b/d) = 1.$$

(3) 若 $a = bq + r$，那么 $(a,b) = (b,r)$.

证 我们记 $d = (a,b), c = (b,r)$.

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

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

综上，有 $c = d$，也即 $(a,b) = (b,r)$.

这一性质提示了一通常所熟知的求最大公因子的有效方法，即 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，$b \neq 0$，且

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

那么，当 k 足够大时，比如 $k=t$，我们有

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

并且

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

证 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 $280 = 63 \times 4 + 28$,

③ $63 = 28 \times 2 + 7$,

④ $28 = 7 \times 4$,

所以，$(343,280) = 7$.

当 a 和 b 中有一个或两个都是负数时，由于

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

故我们仍可利用 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 可用多种方法来证明此定理，我们介绍两种.

【法 1】 根据 Euclid 算法

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

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}的一个整系数的组合. 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}的一个整系数的组合:

$$(a,b) = r_{t-3}x_1 + r_{t-2}y_1,$$

其中:x_1和y_1是两个整数,如此继续下去,最后必可将(a,b)表示成a和b的一个整系数的组合

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

例 1.1.4 在例 1.1.3 中,我们有

$$(343,280) = 7 = 63 - 28 \times 2 = 63 - 2 \times (280 - 63 \times 4)$$
$$= 9 \times 63 - 2 \times 280$$
$$= 9 \times (343 - 280) - 2 \times 280$$
$$= 9 \times 343 - 11 \times 280.$$

这样就找到了使

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

成立的x和y:$x = 9, y = -11$.

【法 2】 若a和b中有一个为 0,则命题显然成立. 现不妨设$a \neq 0, b \neq 0$. 我们构造集合:

$$S = \{ax + by \mid x,y \text{ 为整数}\}.$$

由于$a \neq 0, b \neq 0$,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

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

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

$$(a,b)|d.$$

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

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

推论 1 如果 $d|ab$ 且 $(d,a)=1$，那么 $d|b$.

证 因为 $(d,a)=1$，所以存在有整数 x 和 y 满足：

$$ax+dy=1,$$

故

$$abx+dby=b.$$

现在，$d|db$ 且 $d|ab$，所以 $d|b$.

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

证 因为存在有整数 x 和 y 使得

$$d=ax+by,$$

而 $c|a$ 且 $c|b$，故 $c|d$.

注 (1)这一结论也可以从Euclid算法中得到.(2)根据这一结论，我们有 $(a,b,c)=((a,b),c)$，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 $a|m,b|m$，并且 $(a,b)=1$，那么 $ab|m$.

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

推论 4 $(ac,bc)=(a,b)c$，此处设 $c>0$.

证 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 这一结论也可以从 Euclid 算法中得到.

推论 5 若$(a,b)=1$，则$(ac,b)=(c,b)$.

证 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，$(ac,bc)=(a,b)c=c$，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$a_1a_2\cdots a_n$与$b_1b_2\cdots b_n$互素.

证 略(反复应用推论 5 的结论即可).

1.1 习题

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

2. 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. 证明不等式：

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

4. 设 n 为正整数，证明：

(1)$[[\alpha]/n]=[\alpha/n]$；

(2)$[[n\alpha]/n]=[\alpha]$；

(3)$[\alpha]+[\alpha+1/n]+\cdots+[\alpha+(n-1)/n]=[n\alpha]$.

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