中国科学院研究生教学丛书

算法数论

裴定一　祝跃飞　编著

科学出版社

812
65
1

中国科学院研究生教学丛书

算法数论

裴定一　祝跃飞　编著

科学出版社

北京

内 容 简 介

本书论述了算法数论的基本内容，其中包括：连分数、代数数域、椭圆曲线、素性检验、大整数因子分解算法、椭圆曲线上的离散对数、超椭圆曲线．本书的特点是内容涉及面广，在有限的篇幅内，包含了必要的预备知识和数学证明，尽可能形成一个完整的体系．并且本书的部分内容曾多次在中国科学院研究生院信息安全国家重点实验室和广州大学作为硕士研究生教材使用．

本书可作为信息安全、数论等专业的研究生教材及相关专业的研究人员、高等学校的教师和高年级学生的参考．

图书在版编目(CIP)数据

算法数论/裴定一，祝跃飞编著．—北京：科学出版社，2002
(中国科学院研究生教学丛书/白春礼主编)
ISBN 7-03-010683-0
Ⅰ．算… Ⅱ．①裴…②祝… Ⅲ．算法理论-研究生-教材
Ⅳ．0241
中国版本图书馆 CIP 数据核字(2002)第 053337 号

责任编辑：吕 虹 陈玉琢/责任校对：宋玲玲
责任印制：安春生/封面设计：槐寿明 韦万里
科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
丽源印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2002 年 9 月第 一 版 开本：850×1168 1/32
2002 年 9 月第一次印刷 印张：7 3/4
印数：1—3 000 字数：196 000
定价：19.00 元
(如有印装质量问题，我社负责调换〈新欣〉)

《中国科学院研究生教学丛书》总编委会

主　任：白春礼

副主任：何　岩　师昌绪　杨　乐　汪尔康
沈允钢　黄荣辉　叶朝辉

委　员：朱清时　叶大年　王　水　施蕴渝
余翔林　冯克勤　冯玉琳　高　文
洪友士　王东进　龚　立　吕晓澎
林　鹏

《中国科学院研究生教学丛书》数学学科编委会

主　编：杨　乐

副主编：冯克勤

编　委：王靖华　严加安　文志英　袁亚湘
李克正

《中国科学院研究生教学丛书》序

在21世纪曙光初露，中国科技、教育面临重大改革和蓬勃发展之际，《中国科学院研究生教学丛书》——这套凝聚了中国科学院新老科学家、研究生导师们多年心血的研究生教材面世了．相信这套丛书的出版，会在一定程度上缓解研究生教材不足的困难，对提高研究生教育质量起着积极的推动作用．

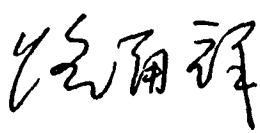
21世纪将是科学技术日新月异，迅猛发展的新世纪，科学技术将成为经济发展的最重要的资源和不竭的动力，成为经济和社会发展的首要推动力量．世界各国之间综合国力的竞争，实质上是科技实力的竞争．而一个国家科技实力的决定因素是它所拥有的科技人才的数量和质量．我国要想在21世纪顺利地实施“科教兴国”和“可持续发展”战略，实现小平同志规划的第三步战略目标——把我国建设成中等发达国家，关键在于培养造就一支数量宏大、素质优良、结构合理，有能力参与国际竞争与合作的科技大军，这是摆在我国高等教育面前的一项十分繁重而光荣的战略任务．

中国科学院作为我国自然科学与高新技术的综合研究与发展中心，在建院之初就明确了出成果出人才并举的办院宗旨，长期坚持走科研与教育相结合的道路，发挥了高级科技专家多，科研条件好，科研水平高的优势，结合科研工作，积极培养研究生；在出成果的同时，为国家培养了数以万计的研究生．当前，中国科学院正在按照江泽民同志关于中国科学院要努力建设好“三个基地”的指示，在建设具有国际先进水平的科学研究基地和促进高新技术产业发展基地的同时，加强研究生教育，努力建设好高级人才培养基地，在肩负起发展我国科学技术及促进高新技术产业发展重任的同时，为国家源源不断地培养输送大批高级科技人才．

此为试读，需要完整PDF请访问：www.ertongbook.com

质量是研究生教育的生命，全面提高研究生培养质量是当前我国研究生教育的首要任务．研究生教材建设是提高研究生培养质量的一项重要的基础性工作．由于各种原因，目前我国研究生教材的建设滞后于研究生教育的发展．为了改变这种情况，中国科学院组织了一批在科学前沿工作，同时又具有相当教学经验的科学家撰写研究生教材，并以专项资金资助优秀的研究生教材的出版．希望通过数年努力，出版一套面向21世纪科技发展，体现中国科学院特色的高水平的研究生教学丛书．本丛书内容力求具有科学性、系统性和基础性，同时也兼顾前沿性，使阅读者不仅能获得相关学科的比较系统的科学基础知识，也能被引导进入当代科学研究的前沿．这套研究生教学丛书，不仅适合于在校研究生学习使用，也可以作为高校教师和专业研究人员工作和学习的参考书．

“桃李不言，下自成蹊．”我相信，通过中国科学院一批科学家的辛勤耕耘，《中国科学院研究生教学丛书》将成为我国研究生教育园地的一丛鲜花，也将似润物春雨，滋养莘莘学子的心田，把他们引向科学的殿堂，不仅为科学院，也为全国研究生教育的发展作出重要贡献．



前　言

算法数论是一门对数论问题进行算法设计和算法分析的学科．它的历史可以追溯到古希腊 Eratosthenes 氏筛法构造素数表．但真正成为一门学科，是在 20 世纪中叶，一方面是由于计算机科学的发展和计算复杂度理论的建立，为算法数论奠定了理论基础；另一方面是数论发展的内部推动力，如对数论中某些问题（如一些猜想）给出肯定与否的回答过程中，收集依据时涉及到一些大数据量的实例验证，而这已经超出了人们的手算能力，只能借助计算机编程来完成；更重要的是由于一些基于数论的公钥密码方案的提出和对其攻击所涉及到的一些数论问题求解算法的发现．

公钥密码是在 20 世纪 70 年代中期提出的一类新型的密码，它尤其适合在计算机网络环境下使用，具有加密信息，管理密钥和数字签名等功能，能保证信息的机密性、完整性和不可否认性．迄今为止，所提出的公钥密码，其安全性都建立在某个数学难题的基础之上，所谓“数学难题”，确切地说是求解这个数学问题，目前还没有多项式时间的算法被发现．例如，大整数因子分解，有限域或椭圆曲线离散对数等问题．只要选择适当的参数，在现有的技术条件下，这些问题都是很难解决的，这就为相应的公钥密码的安全性奠定了基础．在解决这些难题方面所取得的任何重大进展，都会对相应的公钥密码的使用产生巨大的影响．

RSA 公钥密码、ElGamal 公钥密码和椭圆曲线公钥密码是目前影响最大的三类公钥密码．前者是在 70 年代中叶提出来的，它的安全性依赖于大整数因子分解的难度，后两者的安全性分别

信赖于计算有限域离散对数和椭圆曲线离散对数的难度．椭圆曲线公钥密码是80年代中叶提出来的，由于其自身具有一些其它公钥体制无法比拟的优势，近十年来是公钥密码研究的一个十分活跃的方向，研究所获得的许多相关的椭圆曲线的算法，大大丰富了算法数论的理论．

因子分解和离散对数是算法数论研究的两个核心问题．本书的主要内容是介绍这两个问题的基本理论，及迄今为止所提出的主要算法的基本原理．这部分内容包含在第九至第十一章．第九章介绍 Miller-Rabin 概率型素性检验方法，以及分别利用特征和、椭圆曲线的肯定型检验方法．第十章重点介绍椭圆曲线因子分解方法及数域筛法．第十一章包含有关有限域及椭圆曲线上的离散对数的主要结果．其余各章（除第六章外）都是为这最后三章作准备的．第一至第五章介绍初等数论的有关知识，第七章介绍代数数论的有关预备知识，第八章介绍椭圆曲线的有关预备知识．第六章介绍前五章的初等数论知识在密码学中的一些应用．为了本书的系统性，添加了一个附录，介绍了一些代数和有限域的一些算法．

本书的选材是经过精心考虑的，内容的涉及面很广，但在有限的篇幅内，包含了必要的预备知识和数学证明，尽可能形成一个较完整的体系．考虑到信息安全专业的研究生有来自数学本科和非数学本科两类，在利用本教材时，可以根据需要，选择不同的章节组成一个学期的教学．对于来自数学本科的学生，前五章可以较快地通过，而把重点放在后面几章．对于来自非数学本科的学生，第七至第十一章有关代数数论和椭圆曲线的章节可以考虑不讲．本书的部分内容曾多次在中国科学院研究生院信息安全国家重点实验室和广州大学作为硕士研究生教材使用．

本书的编写和出版得到国家自然科学基金跨学科重点项目“电子商务系统中的信息安全理论和技术的研究”（批准号19931010），国家“973”项目“信息与网络安全体系结构”（批

准号 G1999035804）和“中国科学院研究生教材基金”的资助，特此感谢.

作　者

2001 年 4 月

目　录

此为试读,需要完整PDF请访问: www.ertongbook.com

第一章　整数的因子分解

§1.1　唯一分解定理

数论是研究自然数 1,2,3,…的性质的一门数学分支. 自然数是人们日常生活中用得最多的一类数. 在历史上,人们很早就开始数论的研究,使数论成为内容十分丰富的一个分支. 数论在信息安全,计算机科学,数字信号处理等现代重要科技领域有重要的应用,所以,数论至今仍是一门充满活力,蓬勃发展的分支.

通常,我们用$\mathbb{Z}$表示整数集合,整数即为

$$0, \pm 1, \pm 2, \cdots,$$

自然数就是正整数.

定理 1.1　*设 a 和 b 为整数,$b>0$,则存在整数 q 和 r,使*

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

r 称为 b 除 a 所得的最小正剩余.

证明　以$\left[\frac{a}{b}\right]$表示不超过分数$\frac{a}{b}$的最大整数,则

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

取 $q=\left[\frac{a}{b}\right]$, $r=a-\left[\frac{a}{b}\right]b$,即证得定理.

当 b 除 a 的最小正剩余 r 为零时,称 b 为 a 的因子,a 为 b 的倍数,记为 $b\mid a$.

若 b 为 a 的因子,$b\neq 1$, $b\neq a$ 这时称 b 为 a 的真因子,显然有 $0<|b|<|a|$,这里 $|a|$ 为 a 的绝对值.

若 $b\neq 0$, $c\neq 0$,显然:

1. 若 $b\mid a$, $c\mid b$,则 $c\mid a$;

2. 若 $b\mid a$,则 $bc\mid ac$;

3. 若 $c|d$, $c|e$,则对任意 m,n 有 $c|dm+en$.

自然数 $p(\neq 1)$,若仅以 1 和自身 p 为其因子,称 p 为素数. 非素数的自然数 $n(\neq 1)$称为复合数.

设 M 为整数的一个子集合,它对加,减法封闭,即若 $m,n\in M$,则 $m\pm n\in M$,则 M 称为模. a 为任一整数,a 的所有的倍数就组成一个模. 相反的结论也成立,即

定理 1.2 任一非零模,必为一正整数的诸倍数组成的集合.

证明 设 d 为该模中最小正整数,则模中其它数必为 d 之倍数. 若不然,设 n 为模中 d 之非倍数,由定理 1.1,存在整数 q 及 r,使

$$n = qd + r, 0 < r < d.$$

由于 $r=n-qd$ 也属于此模,这与 d 为该模中最小正整数的假设相矛盾,故模中其它各数都为 d 的倍数. 因 d 在模中,所以 d 的任一倍数也在模中. 定理即证.

命 a,b 为二整数,集合

$$\{ma + nb \mid m,n \in \mathbb{Z}\}$$

即为一模,此模中最小正整数 d 称为 a,b 的最大公因子,记为 $d=(a,b)$.

由定理 1.2 的证明,不难证得下述定理:

定理 1.3 (a,b)具有下述性质:

1. 有整数 x,y,使 $(a,b)=ax+by$.
2. 对任二整数 x,y,必有 $(a,b)|ax+by$.
3. 若 $c|a$, $c|b$,则 $c|(a,b)$.

由于 3,我们也称(a,b)为 a,b 的最大公因子.

定理 1.4 设 p 为素数且 $p|ab$,则 $p|a$ 或 $p|b$.

证明 若 $p\nmid a$,则$(a,p)=1$,由定理 1.3,知有二整数 x,y,使

$$ax + py = 1,$$

所以

$$abx + pyb = b.$$

由于 $p \mid ab$，可见 $p \mid b$，证毕.

定理 1.5(唯一分解定理) 任一自然数 n 皆可唯一地表为素数之积

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}. \tag{1.1}$$

这里，$p_1 < p_2 < \cdots < p_k$ 为素数，$a_1, a_2, \cdots, a_k$ 为自然数.

证明 我们首先证明 n 可以表为素数之积，然后再证明上述表法唯一.

若 n 为素数，定理显然成立. 当 n 不是素数时，设 p_1 是 n 的最小的真因子，则 p_1 一定是素数，因 p_1 的真因子也是 n 的真因子，所以 p_1 不能有真因子. 设 $n = p_1 n_1 (1 < n_1 < n)$，对 n_1 重复上述推理，得 $n = p_1 p_2 n_2$，p_2 为素数，$1 < n_2 < n_1$，执行此法，得 $n > n_1 > n_2 > \cdots > 1$，此项手续，最多不能超过 n 次，最后必得

$$n = p_1 p_2 \cdots p_l,$$

也可排为(1.1)中的形式.

今设

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$$

为 n 的二个分解式，$p_1 < p_2 < \cdots < p_k$，$q_1 < q_2 < \cdots < q_l$ 都为素数，利用定理 1.4，任一 p_i 必为某一 q_j，任一 q_i 也必为某一 p_j，故 $k = l$，$p_i = q_i (1 \leqslant i \leqslant k)$，又若 $a_1 > b_1$，则

$$p_1^{a_1 - b_1} p_2^{a_2} \cdots p_k^{a_k} = p_2^{b_2} \cdots p_k^{b_k},$$

左边为 p_1 的倍数，右边不是 p_1 的倍数，这是不可能的，同样 $a_1 < b_1$ 也不可能，故 $a_1 = b_1$. 类似地，可证得 $a_i = b_i (i = 1, 2, \cdots k)$，唯一性得证.

给定一自然数 n，当它很大时，例如一百多位的十进制数，要将它因子分解，实非易事. 在第十章将讨论一些大整数因子分解的算法，随之而来的一个问题是如何判断一个数是否是素数，在第九章将讨论几个素性判断的方法.

§1.2 辗转相除法(欧氏除法)

若 a,b 为二自然数,$a\geqslant b$,以(a,b)表示 a 和b 的最大公因子.由定理 1.3 知有二整数 x,y,使

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

如何计算(a,b),又如何找到上述 x 和y,定理 1.1 实际上已经给出了我们所要的算法.

首先用 b 除a 得到商q_0,余数 r_0,即

$$a = q_0 b + r_0, \quad 0 \leqslant r_0 < b. \tag{1.2}$$

如果 $r_0=0$,那么 b 是a 的因子,a,b 的最大公因子就是b.如果 $r_0\neq 0$,用 r_0 除 b 得到商q_1,余数 r_1

$$b = q_1 r_0 + r_1, \quad 0 \leqslant r_1 < r_0. \tag{1.3}$$

如果 $r_1=0$,那么 r_0 除尽 b,由(1.2)r_0 也除尽 a,r_0 是 a,b 的公因子.反之,任何一个除尽 a,b 的数,由(1.2),也除尽 r_0,因此 r_0 是 a,b 的最大公因子.如果 $r_1\neq 0$,则用 r_1 除 r_0 得到商 q_2,余数 r_2

$$r_0 = q_2 r_1 + r_2, \quad 0 \leqslant r_2 < r_1. \tag{1.4}$$

如果 $r_2=0$,那么由(1.3)可知 r_1 是 r_0,b 的公因子,由(1.2)知 r_1 也是 a,b 的公因子.反之,如果一整数除得尽 a,b,那么由(1.2),它一定除得尽 r_0,由(1.3),它一定除得尽 r_1,所以 r_1 是 a,b 的最大公因子.

若 $r_2\neq 0$,再用 r_2 除 r_1,重复上述过程,依次得到 $b>r_0>r_1>r_2>\cdots$,逐步小下来,而又都非负.经过有限步后,一定会有某个 r 为零.若设 r_n 是第一个出现的零,则 r_{n-1}就是 a,b 的最大公因子.我们所得到的一串算式:

$$\begin{aligned} a &= q_0 b + r_0, \\ b &= q_1 r_0 + r_1, \\ r_0 &= q_2 r_1 + r_2, \end{aligned}$$

$$r_1 = q_3 r_2 + r_3,$$
$$\vdots$$
$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1},$$
$$r_{n-2} = q_n r_{n-1}.$$

由第一式可得

$$r_0 = a - q_0 b,$$

由第二式可得

$$r_1 = b - q_1 r_0 = -q_1 a + (1 + q_0 q_1) b,$$

一般地,对任一 $r_i (0 \leqslant i \leqslant n-1)$,都有二整数 x_i, y_i,使

$$r_i = x_i a + y_i b,$$

由于

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ &= (x_{i-2} a + y_{i-2} b) - q_i (x_{i-1} a + y_{i-1} b) \\ &= (x_{i-2} - q_i x_{i-1}) a + (y_{i-2} - q_i y_{i-1}) b, \end{aligned}$$

所以,有递推公式

$$x_0 = 1, \quad x_1 = -q_1, \quad x_i = x_{i-2} - q_i x_{i-1},$$
$$y_0 = -q_0, \quad y_1 = 1 + q_0 q_1, \quad y_i = y_{i-2} - q_i y_{i-1}.$$

这样,我们可以找到二整数 x, y,使

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

看一个例子:求 4862 和 2156 的最大公因子.我们有

$$\begin{aligned} 4862 &= 2 \times 2156 + 550, \\ 2156 &= 3 \times 550 + 506, \\ 550 &= 506 + 44, \\ 506 &= 11 \times 44 + 22, \\ 44 &= 2 \times 22. \end{aligned}$$

可见(4862,2156)=22,利用上述算式可得

$$\begin{aligned} 550 &= 4862 - 2 \times 2156, \\ 506 &= -3 \times 4862 + 7 \times 2156, \\ 44 &= 4 \times 4862 - 9 \times 2156, \end{aligned}$$

此为试读,需要完整PDF请访问: www.ertongbook.com