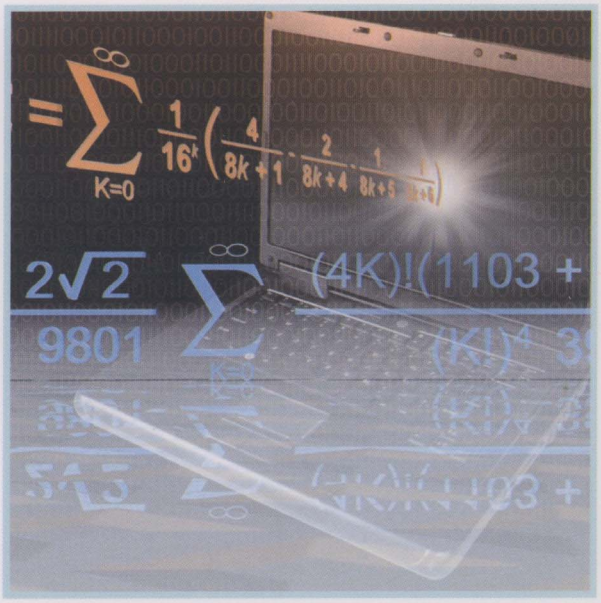
HZ BOOKS
华章教育

网络工程
专业系列教材

数论与有限域

Number Theory and Finite Field

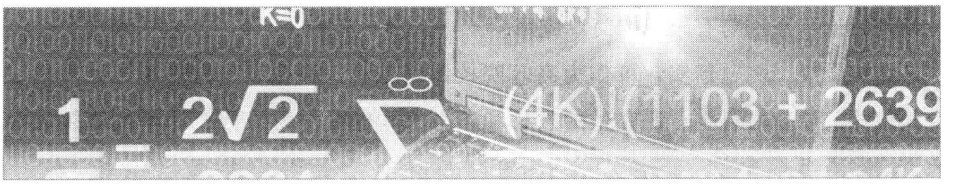
董丽华 胡予濮 曾 勇 编著



- 内容涵盖数论与有限域的核心基础知识
- 叙述简明、推理详尽，展现数论与有限域的本质
- 通过例题揭示数论与有限域在网络工程、编码学、密码学、通信工程等方面的实际应用

机械工业出版社
China Machine Press

网络工程
专业系列教材



Number Theory and Finite Field

数论与有限域

董丽华 胡予濮 曾 勇 编著

机械工业出版社
China Machine Press

本书是初等数论与有限域的入门教材. 全书共分七章，前四章论述了数论中的基础知识，具体内容包括：整数的整除理论、同余理论、数论函数、二次剩余以及原根与指数等内容；随后两章重点论述了近世代数中群、环、域的基本概念，有限域的构造以及有限域中的计算；最后一章则讨论了数论与有限域的简单应用.

本书结构紧凑、例题翔实，可作为高等院校网络工程、通信、信息工程、计算机、信息安全及其他相关专业本科生、研究生的教材和参考书，也可作为通信、计算机等领域中工程技术人员的参考书.

图书在版编目（CIP）数据

数论与有限域/董丽华，胡予濮，曾勇编著. —北京：机械工业出版社，2010.9

（网络工程专业系列教材）

ISBN 978-7-111-31596-4

Ⅰ. 数…　Ⅱ. ①董… ②胡… ③曾…　Ⅲ. ①数论－教材 ②有限域－教材　Ⅳ. ①O156 ②O153.4

中国版本图书馆 CIP 数据核字（2010）第 160782 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）

责任编辑：迟振春

北京京北印刷有限公司印刷

2010 年 10 月第 1 版第 1 次印刷

184mm×260mm · 10.5 印张

标准书号：ISBN 978-7-111-31596-4

定价：25.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991；88361066

购书热线：（010）68326294；88379649；68995259

投稿热线：（010）88379604

读者信箱：hzjsj@hzbook.com

前 言 Preface

长期以来，数论与有限域作为高度抽象的数学学科，对数学理论的发展起到了积极的作用，但其发展一直处于纯理论的研究状态，大多数人并不清楚它们的实际意义. 当今，随着近代计算机科学和应用数学的发展，数论与有限域已经不仅仅是优秀数学家大展才华的场所，在计算方法、编码学、密码学、计算机代数、组合论、通信工程、离散控制系统等许多领域得到日益广泛的实际应用，是许多从事应用和实际工作的工程技术人员必须掌握的数学基础知识. 本书试图使读者在较短时间内切实掌握数论与有限域的基本概念和基础知识，领会数论与有限域的精神实质和思想方法.

本书在编写过程中力求做到叙述简明，推理详尽，并不假定读者具有很多的数学知识，大学二年级的学生不查看其他参考书籍就能看懂本书.

本教材在编写的过程中参考了许多相关专著、文献和教材，在此向其作者表示衷心的感谢. 另外，在本书的撰写过程中，得到了国家自然科学基金重点项目（项目编号：60473029）、陕西省自然科学基金基础研究计划资助项目（项目编号：2009JQ8005）、中央高校基本科研业务费专项资金项目（项目编号：JY1000090111；JY10000903011）的资助.

由于作者水平有限，不妥之处在所难免，我们诚挚地期待广大读者提出宝贵意见.

编 者

于西安电子科技大学

Suggestions 教学和阅读建议

在一学期30学时的课程学习中，对各章的教学内容可作如下安排：

第1章 整数与同余(4学时)

教学内容：

- ✓ 整数与整除；
- ✓ 带余除法、整数的进制表示法、数制转换；
- ✓ 算术基本定理；
- ✓ 整数分解算法：欧几里得算法、因式分解法、爱拉斯托散方法、试除法；
- ✓ 同余：同余的概念和性质、中国剩余定理、威尔逊定理、费马小定理与欧拉定理.

考核要求：

- ✓ 通过课堂讲解和讨论，学生要能掌握整除的一些判别法则、带余除法、整数的进制表示法、最大公约数与最小公倍数求法、算术基本定理、同余的概念和性质、同余式求解、威尔逊定理、费马小定理与欧拉定理.

第2章 数论函数(4学时)

教学内容：

- ✓ 积性函数：积性函数的定义和基本性质、除数(或因数)和与除数(或因数)个数函数的定义和性质、除数(或因数)和与除数(或因数)个数函数的函数值的求法；
- ✓ 高斯函数$[x]$的性质与应用；
- ✓ 欧拉函数$\phi(x)$的性质与函数值的求法；
- ✓ 默比乌斯函数、默比乌斯反演公式；
- ✓ 完全数.

考核要求：

- ✓ 掌握积性函数的定义和基本性质；
- ✓ 熟悉几种重要的数论函数：除数(或因数)和与除数(或因数)个数函数、高斯函数$[x]$、欧拉函数$\phi(x)$及默比乌斯函数的性质与应用；
- ✓ 了解几种具有特殊性质的数：完全数、梅森数及费马数的定义及性质.

第 3 章　二次剩余(4 学时)

教学内容:

✓ 二次剩余:模素数 p 的简化剩余系中二次剩余和二次非剩余个数;

✓ 勒让德符号:勒让德符号的定义、欧拉判别法及高斯引理、勒让德符号的性质;

✓ 二次互反律;

✓ 雅可比符号:雅可比符号的定义、性质、计算方法;

✓ 二次同余式的解法和解数.

考核要求:

✓ 理解勒让德符号的定义,掌握勒让德符号的性质,会用勒让德符号判定二次剩余;

✓ 掌握二次互反律的证明,会使用二次互反律判定某些不定方程是否有解;

✓ 理解雅可比符号与勒让德符号的关系,掌握雅可比符号的性质,会计算雅可比符号的值;

✓ 会使用雅可比符号判定二次同余式是否有解,会解某些二次同余式.

第 4 章　原根和指数(4 学时)

教学内容:

✓ 原根:整数的阶、原根的定义、原根存在的条件、原根的求法;

✓ 指数的基本性质:指数的定义、指数的性质、指数表.

考核要求:

✓ 掌握整数的阶的定义与求解;

✓ 理解原根的定义,熟悉原根存在的条件,掌握原根的求法;

✓ 理解指数的概念,掌握指数的基本性质.

第 5 章　有限域的概念(4 学时)

教学内容:

✓ 代数系统的定义;

✓ 群:群的定义与性质、子群、陪集与拉格朗日定理;

✓ 环:环的定义与性质、多项式环;

✓ 整环中的因子分解:一些基本概念、主理想整环、欧几里得整环;

✓ 由整环构造域.

考核要求:

✓ 理解群、环的定义与性质;

✓ 熟悉由整环构造域的过程.

第 6 章　有限域的抽象性质(4 学时)

教学内容:

- ✓ 有限域的加法结构;
- ✓ 乘法结构:元素的阶、本原元;
- ✓ 最小多项式与本原多项式.

考核要求:

- ✓ 了解有限域的加法结构与乘法结构;
- ✓ 掌握元素的阶与本原元的定义、性质与求解;
- ✓ 理解有限域上多项式中最小多项式和本原多项式的概念,熟悉利用不可约多项式构造有限域的过程.

第 7 章　数论与有限域的应用(6 学时)

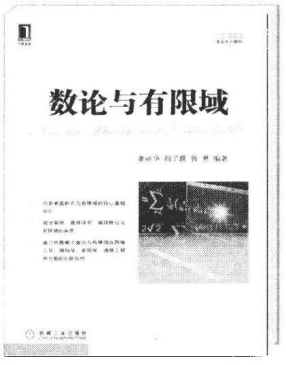
教学内容:

- ✓ 同余式的简单应用:正整数能否被除尽、弃九法、计算星期几、循环赛;
- ✓ 二次剩余的应用:Blum 通信游戏、欧拉伪素数;
- ✓ 信息加密:文件集合的加密、RSA 公钥密码体制;
- ✓ 正交拉丁方;
- ✓ 阿达玛阵;
- ✓ 纠错码:循环码与循环冗余校验码.

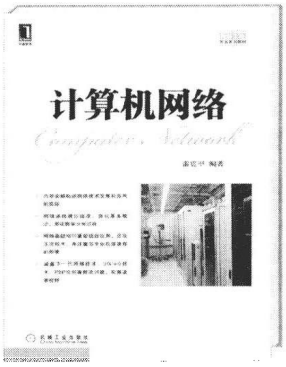
考核要求:

- ✓ 了解同余式在正整数能否被除尽、弃九法、计算星期几及循环赛的日程安排中的应用;
- ✓ 了解二次剩余在 Blum 通信游戏中的作用及欧拉伪素数的定义;
- ✓ 了解中国剩余定理在文件集合的加密中的应用;
- ✓ 了解大数分解对 RSA 公钥密码体制的作用;
- ✓ 了解正交拉丁方的定义、性质及构造;
- ✓ 了解阿达玛阵的定义、性质及构造;
- ✓ 了解数论与有限域在循环码与循环冗余校验码的构造过程中的应用.

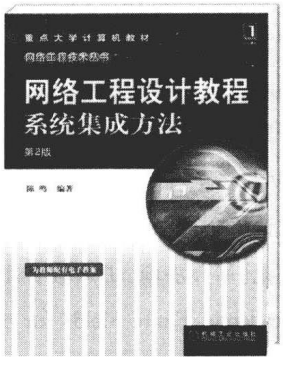
好 书 推 荐



作者：董丽华 胡予濮 曾 勇
书号：978-7-111-31596-4
定价：25.00元

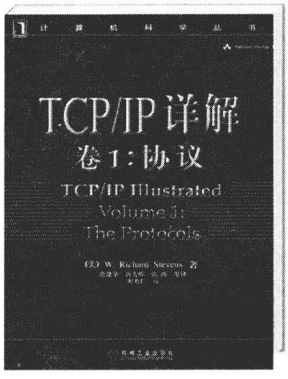


作者：雷震甲
书号：978-7-111-30649-8
定价：33.00元

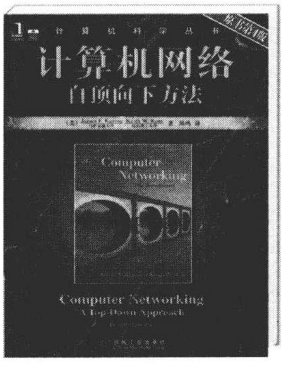


作者：陈鸣
书号：978-7-111-23711-2
定价：33.00元

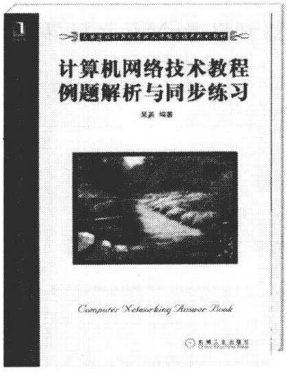
作者：陈鸣 常强林 岳振军
书号：978-7-111-20682-8
定价：45.00元



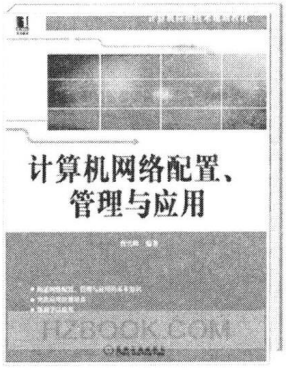
作者：W.Richard Stevens
译者：范建华 等
中文版书号：978-7-111-07566-0
定价：45.00元
英文版书号：978-7-111-09505-7
定价：39.00元



作者：James F. Kurose;
Keith W. Ross
译者：陈鸣
书号：978-7-111-16505-7
定价：66.00元



作者：吴英
书号：978-7-111-27675-3
定价：25.00元



作者：曹雪峰
书号：978-7-111-30124-0
定价：30.00元

教师服务登记表

尊敬的老师：

您好！感谢您购买我们出版的 _____ 教材。

机械工业出版社华章公司为了进一步加强与高校教师的联系与沟通，更好地为高校教师服务，特制此表，请您填妥后发回给我们，我们将定期向您寄送华章公司最新的图书出版信息！感谢合作！

个人资料（请用正楷完整填写）

教师姓名		□先生 □女士	出生年月		职务		职称：□教授 □副教授 □讲师 □助教 □其他
学校			学院			系别	
联系电话	办公： 宅电： 移动：			联系地址及邮编			
				E-mail			
学历		毕业院校		国外进修及讲学经历			
研究领域							

主讲课程	现用教材名	作者及出版社	共同授课教师	教材满意度
课程： □专 □本 □研 人数： 学期：□春□秋				□满意 □一般 □不满意 □希望更换
课程： □专 □本 □研 人数： 学期：□春□秋				□满意 □一般 □不满意 □希望更换

样书申请			
已出版著作		已出版译作	
是否愿意从事翻译/著作工作 □是 □否		方向	
意见和建议			

填妥后请选择以下任何一种方式将此表返回：（如方便请赐名片）

地 址：北京市西城区百万庄南街1号 华章公司营销中心 邮编：100037

电 话：(010) 68353079 88378995 传真：(010)68995260

E-mail:hzedu@hzbook.com markerting@hzbook.com 图书详情可登录http://www.hzbook.com网站查询

目 录 Contents

第1章 Chapter1

整数与同余

数论是数学的一个分支，研究一类特殊数的性质和相互关系. 在数论所研究的数中，最重要的是正整数集合. 更具体地说，特别重要的是素数. 而伟大的德国数学家高斯发明的同余语言，使得我们在研究整除性关系的时候，变得像研究方程一样容易. 在本章中，介绍整数与同余.

1.1 整数

1.1.1 整数的定义

我们把…，−3，−2，−1，0，1，2，3，…叫做整数，其中 1，2，3，4，…叫做正整数，又叫做自然数；1，3，5，7，…叫做奇数；2，4，6，8，…叫做偶数.

以后，如果没有特别声明，我们将用黑正体的大写英文字母 **Z** 表示由所有整数构成的集合，同时用小写英文字母 $a,b,c,d,\cdots$ 表示整数，特别地

1）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 $ab=a\times b, abc=a\times b\times c$.

2）当 n 是一个大于 1 的正整数时，a^n 表示由 n 个相同的整数 a 相乘所得的积，a^{b^n} 表示由 b^n 个相同的整数 a 相乘所得的积，而 $a^{b^{c^n}}$ 则表示由 b^{c^n} 个相同的整数 a 相乘所得的积.

3）用记号 $|a|$ 来表示整数 a 的绝对值，即

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

例如，$|2|=|-2|=2$.

下面我们给出由所有正整数构成的集合的一个重要性质，利用此性质可以证明整数集合 **Z** 中的许多重要结果.

最小整数公理（良序性） *每个正整数集的非空子集中都存在着一个最小的正整数.*

注 虽然正整数集合具有良序性，但是由于许多整数的子集（例如所有负整数构成的集合以及所有小于 200 的偶数构成的集合）中都不具有最小值，因而由所有整数构成的集

合 $\mathbf{Z}$ 并不具有良序性.

在整数范围内,我们有

$$\text{整数}+\text{整数}=\text{整数};$$
$$\text{整数}-\text{整数}=\text{整数};$$
$$\text{整数}\times\text{整数}=\text{整数}.$$

但是整数除整数却不一定得整数,究竟什么样的整数除什么样的整数才能得到整数呢? 这个问题,就是下面我们要研究的整数的整除性.

1.1.2 整除

定义 1.1.1 设 a,b 是两个给定的整数且 $a\neq 0$. 如果存在整数 c 使得 $b=ac$,则称 a 整除 b,记为 $a|b$,有时也称 a 是 b 的因子(或因数),b 是 a 的倍数;反之,若找不到这样的整数 c,则称 a 不整除 b,记为 $a\nmid b$.

例如,易知 $3|6$,而 $3\nmid 5$,同时 6 的因子分别为 $\pm 1,\pm 2,\pm 3,\pm 6$.

定理 1.1.1 设 a,b,c 是满足条件 $a|b$ 且 $b|c$ 的整数,则 $a|c$.

证明:由于 $a|b$ 且 $b|c$,知存在整数 e 和 f 使得 $b=ae$ 且 $c=bf$,于是

$$c=bf=(ae)f=a(ef).$$

由于整数 e 与 f 的乘积仍然是整数,因而 $a|c$. ■

例如,由于 $11|66$ 且 $66|198$,由定理 1.1.1 就有 $11|198$.

定理 1.1.2 设 a,b,c 是满足条件 $c|a$ 且 $c|b$ 的整数,则 $\forall m,n\in\mathbf{Z}$,有 $c|(ma+nb)$.

证明:由于 $c|a$ 且 $c|b$,知存在整数 e,f 使得 $a=ce,b=cf$,进而

$$ma+nb=mce+ncf=c(me+nf).$$

由于 $me+nf$ 仍然是整数,因而 $c|(ma+nb)$. ■

例如,由于 $3|21$ 且 $3|33$,由定理 1.1.2 就有 $3|(5\times 21-3\times 33)$,即 $3|6$.

另外,我们有如下定义:

定义 1.1.2 一个大于 1 的正整数,若只能被 1 和其本身整除,而不能被其他正整数整除,则称其为素数(或质数),通常记为 p 或 $p_1,p_2,p_3,\cdots$.

例如,2,3,5,7,11,13,…都是素数.

这里需要注意的是,虽然 1 也是具有这类性质的数,但大家约定 1 不称为素数,因为若 1 是素数,则 100 可以写成

$$100=1\times 1\times 1\times 1\times\cdots\times 1\times 2\times 2\times 5\times 5,$$

这里等式的右边我们爱写几个 1 就可以写几个 1,这样一个自然数写成素数之积的形式就

不唯一了.但是若 1 不是素数,那么一个自然数则可以唯一地写成若干素数之积,这一结论就是后面我们要证明的算术基本定理.

定义 1.1.3　大于 1 的不是素数的自然数称为合数.

例如,4,6,8,9,10,12,…都是合数.

由上述素数与合数的定义 1.1.2 与 1.1.3 可知,全体正整数可分为三类:1,全体素数以及全体合数.

1.2　整数的进位制表示法

在生产劳动和日常生活中,数的进位制表示法有很多种.我们最常用、最熟悉的是十进制,例如十寸为一尺,十尺为一丈,十两为一斤等.除了我们有十根手指外,以十作为基底没有任何其他的原因,下面我们将看到,任意的正整数都可以作为基底.例如:一年等于十二个月,是十二进制;一小时等于六十分,一分等于六十秒,是六十进制;中药店的秤一斤等于十六两,是十六进制;鞋是以双计算的,一双等于二只,是二进制.

为了研究整数的进位制表示,需要引入如下初等数论的证明中最重要、最基本、最直接的工具——带余除法,也称为除法算法.

1.2.1　带余除法

定理 1.2.1(带余除法)　设 a 是正整数,b 是整数,则一定存在唯一的整数 q 和 r,使得 $b=qa+r$,其中 $0\leqslant r<a$,并分别称 q 与 r 为 a 除 b 的商和余数.

证明:(唯一性)假设存在整数 q 与 r,以及整数 q_1 与 r_1,使得

$$b=qa+r,0\leqslant r<a,\text{且 } b=q_1a+r_1,0\leqslant r_1<a.$$

则将两式相减,得到:

$$r_1-r=(q-q_1)a.$$

由于 $q-q_1$ 仍然是整数,因而 $a\mid(r_1-r)$.同时,由假设 $0\leqslant r<a$ 且 $0\leqslant r_1<a$,得到 $-a<r_1-r<a$.于是由 $a\mid(r_1-r)$,得到 $r_1-r=0$,即 $r_1=r$.进一步地,由 $qa+r=q_1a+r_1$ 且 $r_1=r$,得到 $q_1=q$,即商 q 和余数 r 都是唯一的.

(存在性)考虑由所有形如 $b-ka$ 的整数构成的集合

$$T=\{b-ka,k=0,\pm1,\pm2,\cdots\},$$

设集合 S 为 T 中所有非负整数构成的集合,则集合 S 非空(只要取满足条件 $k<b/a$ 的整数 k,$b-ka$ 就是正数),进而由正整数集的良序性知,集合 S 中必有一个最小值,不妨设为 $r=b-qa$,同时由集合 S 的构造过程知 $r\geqslant0$.接下来我们证明 $r<a$.

如果 $r \geqslant a$，那么由 a 是正整数，即 $a>0$，得到

$$r > r-a = b-qa-a = b-(q+1)a \geqslant 0,$$

即在集合 S 中存在一个小于 r 的非负整数 $b-(q+1)a$，这与 $r=b-qa$ 是集合 S 的最小值相矛盾，因而有 $0 \leqslant r < a$. ■

推论 1.2.1 设 $a>0$，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.

这是带余除法定理的直接推论，是如下进位制表示法的基础.

定理 1.2.2 设正整数 $b>1$，那么每个正整数 n 都可以唯一地表示为如下形式：

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

我们称此表达式为正整数 n 的 b 进制表示，记为 $(n)_b = (a_k, a_{k-1}, \cdots, a_1, a_0)_b$，其中 k 是非负整数，整数 a_j 满足条件 $0 \leqslant a_j \leqslant b-1 (j=0,1,\cdots,k)$，且首系数 a_k 不为 0.

证明之前我们先来看一个例子.

例 1.2.1 给出整数 2345 的十进制表示.

解：在定理 1.2.2 中取

$$b = 10, a_0 = 5, a_1 = 4, a_2 = 3, a_3 = 2,$$

且当 $i \geqslant 4$ 时取 $a_i = 0$，则可以得到

$$2345 = 2 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 5.$$

这就是我们最常用、最熟悉的十进制.

一般地，在十进制中任一个正整数 N 都能够写成

$$N = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_3 \times 10^3 + a_2 \times 10^2 + a_1 \times 10 + a_0,$$

其中 $0 \leqslant a_i \leqslant 9$，$i$ 是 0 到 n 中的任一个整数.

接下来，利用带余除法来证明定理 1.2.2.

证明：首先，以 b 除 n，得到

$$n = bq_0 + a_0, 0 \leqslant a_0 \leqslant b-1.$$

如果 $q_0 \neq 0$，继续以 b 除 q_0，得到

$$q_0 = bq_1 + a_1, 0 \leqslant a_1 \leqslant b-1.$$

继续这个过程，依次得到

$$q_1 = bq_2 + a_2, 0 \leqslant a_2 \leqslant b-1,$$

$$q_2 = bq_3 + a_3, 0 \leqslant a_3 \leqslant b-1,$$

$$\cdots$$

$$q_{k-2} = bq_{k-1} + a_{k-1}, 0 \leqslant a_{k-1} \leqslant b-1,$$

$$q_{k-1} = b \cdot 0 + a_k, 0 \leqslant a_k \leqslant b-1.$$

当商为 0 时，结束这个过程.

由上面第一个方程，得到

$$n = bq_0 + a_0,$$

接下来，将第二个方程 $q_0 = bq_1 + a_1 (0 \leqslant a_1 \leqslant b-1)$ 代入上式得到

$$n = b(bq_1 + a_1) + a_0 = b^2 q_1 + a_1 b + a_0$$

继续以 $q_1, q_2, \cdots, q_{k-2}, q_{k-1}$ 进行替换，依次得到

$$\begin{aligned} n &= b^3 q_2 + a_2 b^2 + a_1 b + a_0 \\ &\cdots \\ &= b^{k-1} q_{k-2} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0 \\ &= b^k q_{k-1} + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \\ &= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \end{aligned}$$

其中 $0 \leqslant a_j \leqslant b-1 (j=0,1,\cdots,k)$，且 $a_k \neq 0$，这里假定 $a_k = q_{k-1}$ 是最后一个不为零的商，因而得到了希望证明的表达式.

下面来证明唯一性.

假设有如下两个等于 n 的表达式，即

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

其中 $0 \leqslant a_j < b, 0 \leqslant c_j < b, j=0,1,\cdots,k$，且 $a_k \neq 0$. 将两式相减，得到

$$(a_k - c_k) b^k + (a_{k-1} - c_{k-1}) b^{k-1} + \cdots + (a_1 - c_1) b + (a_0 - c_0) = 0.$$

若两式不同，则必定存在一个最小的整数 $j (0 \leqslant j \leqslant k)$，使得 $a_j \neq c_j$，因此有

$$b^j ((a_k - c_k) b^{k-j} + \cdots + (a_{j+1} - c_{j+1}) b + (a_j - c_j)) = 0,$$

即

$$(a_k - c_k) b^{k-j} + \cdots + (a_{j+1} - c_{j+1}) b + (a_j - c_j) = 0,$$

进而

$$\begin{aligned} a_j - c_j &= (c_k - a_k) b^{k-j} + \cdots + (c_{j+1} - a_{j+1}) b \\ &= b((c_k - a_k) b^{k-j-1} + \cdots + (c_{j+1} - a_{j+1})), \end{aligned}$$

即

$$b \mid (a_j - c_j).$$

然而由 $0 \leqslant a_j < b, 0 \leqslant c_j < b$，得到 $-b < a_j - c_j < b$，进而由 $b \mid (a_j - c_j)$ 得到 $a_j = c_j$. 这与我们的假设（两个表达式不同）相矛盾，因而以 b 为基底的 n 的表达式是唯一的. 结论得证. ■

1.2.2　整数的二进制表示法

在十进制中，由于利用 0,1,2,3,4,5,6,7,8,9 这十个数字符号就可以表示出任意大

小的数，因而十进制被普遍应用. 但是，随着数字电子计算机的出现和发展，除十进制外，其他进位制的作用也愈来愈显著了.

在电子数字计算机中普遍采用的是二进制表示法，即在正整数 n 的 b 进制表示中取 $b=2$，例如，整数 1023 用二进制数可以表示为

$$1023=1\times 2^9+1\times 2^8+1\times 2^7+1\times 2^6+1\times 2^5+1\times 2^4+1\times 2^3+1\times 2^2+1\times 2+1,$$

我们知道 1023 用十进制表示只需四位，但是由上式我们看到 1023 用二进制数表示却需要十位，读写和观察都非常不便. 在编制计算程序及控制台的实际工作中，为了弥补这一不足，在二进制的基础上人们采用了八进制和十六进制的表示方法，其中以八进制用得最多.

在八进制中有 0,1,2,3,4,5,6,7 这八个数字符号，由低位向高位是“逢八进一”的，同一个数所在的位数相差一位，其值就有八倍之差，所以在八进制中有

$$(0)_8=0,(1)_8=1,(2)_8=2,(3)_8=3,(4)_8=4,$$
$$(10)_8=8,(100)_8=8^2=64,(1000)_8=8^3=512,\cdots.$$

例 1.2.2 $(73)_8$ 化为十进制数等于什么？

解：$(73)_8=7\times 8+3=56+3=59$.

例 1.2.3 $(112)_8$ 化为十进制数等于什么？

解：$(112)_8=1\times 8^2+1\times 8+2=74$.

1.2.3 数制转换

由于数字电子计算机中的数是采用二进制的，因此要在数字电子计算机中进行运算时，必须首先把需要运算的十进制数“翻译”成二进制数输入到机器中；计算所得到的二进制数结果也必须“翻译”成十进制数再输出给人们. 因此必须掌握各种计数制相互换算的方法.

正整数 n 的 b 进制表示法的证明过程给出了一个寻找任意整数 n 的以 b 为基底的展开式的方法. 具体地，为了得到任意整数 n 的以 b 为基底的展开式，按以下步骤进行：

1)以 b 除 n，得到余数 a_0.

2)以 b 除商 $[n/b]=q_0$，得到余数 a_1.

3)继续这一过程，依次地以 b 除商，直到商值为 0 时终止.

如此就可以得到整数 n 的以 b 为基底的展开式.

换言之，为了得到整数 n 的以 b 为基底的展开式，需要连续地应用带余除法，每一次以商来替换被除数，当商值为 0 时停止，随后依次“由后向前”读取余数列表，找到 n 的以 b 为基底的展开式.

例 1.2.4 计算 233 的以 2 为基底的展开式.