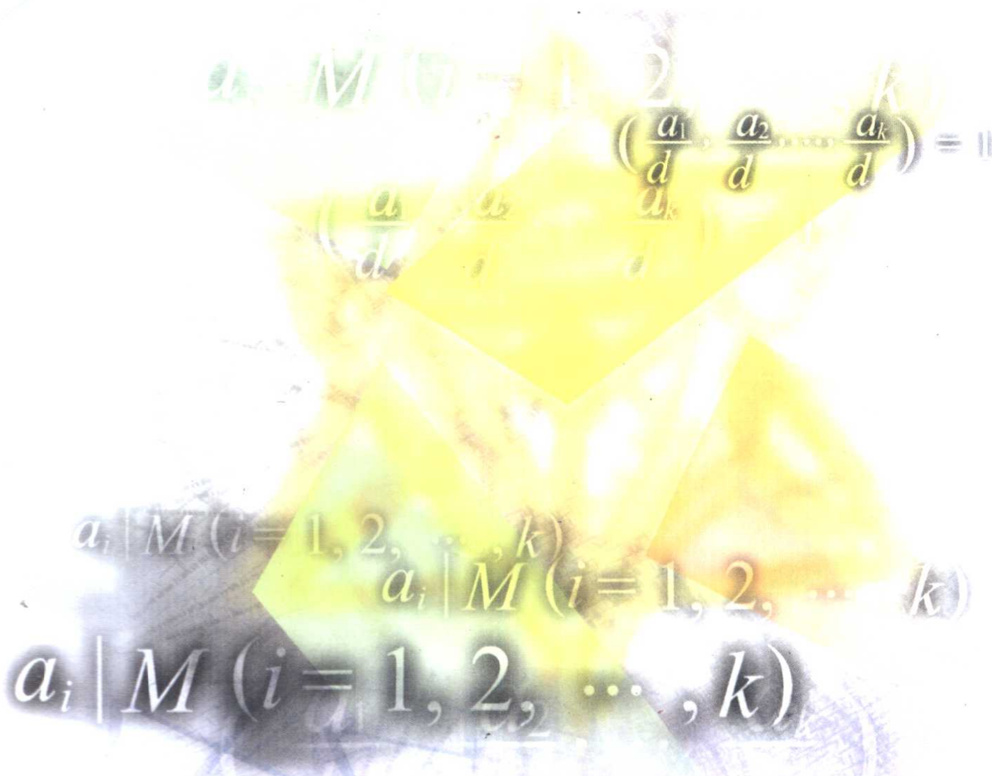
小学教育专业教材

初等数论

CHUDENG SHULUN

⊙ 赵继源 主编



GUANGXI NORMAL UNIVERSITY PRESS
广西师范大学出版社

小学教育专业教材

初等数论

CHUDENG SHULUN

⊙ 赵继源　主编

广西师范大学出版社
·桂林·

图书在版编目（CIP）数据

初等数论/赵继源著.—桂林：广西师范大学出版社，2001.9（2002.8 重印）

小学教育专业教材

ISBN 7-5633-3339-8

Ⅰ.初… Ⅱ.赵… Ⅲ.初等数论－高等学校：师范学校－教材 Ⅳ.O156.1

中国版本图书馆 CIP 数据核字（2001）第 065553 号

广西师范大学出版社出版发行

（桂林市育才路 15 号　邮政编码：541004
网址：http://www.bbtpress.com.cn）

出版人：萧启明

全国新华书店经销

广西民族印刷厂印刷

（广西南宁市明秀西路 53 号　邮政编码:530001）

开本：890mm×1 240mm　1/32

印张：5.875　字数：158 千字

2001 年 9 月第 1 版　2002 年 8 月第 2 次印刷

印数：1 501～7 500　定价：8.00 元

再版说明

ZAIBAN SHUOMING

由广西壮族自治区教育厅组织区内专家自行开发的广西小学教育专业(专科)教材,按照"广西小学教育专业(专科)教材开发总体设计"的部署,于2001年秋季完成了四大类共计19门课程教材的编写出版,这19门课程教材分别是:

通识课教材:《应用哲学方法论》、《科学技术与社会》、《中国文化概论》、《大学语文》;

文科方向专修课教材:《中国文学》、《中国古代文学作品选》、《外国文学作品选析》、《古代汉语》、《文学理论基础》、《名著选读》、《高等数学》;

理科方向专修课教材:《高等数学》、《初等数论》、《数学方法论》、《大学化学》;

教育科学课程教材:《教育原理》、《教育科学研究方法》、《课程与教学》、《发展心理学》.

这19门课程教材编写出版以后,在我区17所开办小教大专班的中师学校投入使用,至今整整使用了一年.其间,在广西小学教育专业建设专家指导委员会及广西小教大专课题组的领导和组织下,由钟海青教授带队到部分学校对这套教材的编写质量和使用状况进行了专题

调查研究，广泛征求师生们的意见，形成了进一步修订并完善教材的思路.在此基础上，召开了小教大专专家指导委员会全体成员和教材主编专题会议，认真研究教材修订和再版的问题.会上，调查组向各位主编通报了师生们对各科教材的使用意见，并提出了修订教材的基本思路.各位主编针对教材使用的信息进行了热烈的讨论，明确了各自修订教材的思路和任务，表示要在吸纳师生意见的基础上进一步解放思想，开拓创新，结合我区小教大专的实际，开发出更能满足广大师生需要，具有广西特色的专用教材.经过半年多的努力，根据“总体设计，分步实施，改革完善，推广应用”的教材建设总目标，教材的修订版终于问世了.这一次教材修订不仅是主编和作者的智慧的再挖掘，而且是各承担小教大专教育的中师学校的广大师生共同参与、努力的结果.对此，我们表示衷心的感谢！

本次修订在加强教材使用对象的针对性(如我区小教大专教育及教育对象的现实基础、我区民族地区的文化特点等)、学生学习的实践性和“与时俱进”的时代性等方面作出了较大的努力.此外，经过修订，教材的科学性和可读性也明显提高.尽管如此，由于我们的科学认识水平和编写能力有限，本套教材仍然会有许多不足之处.我们真诚地希望广大教师和学生在使用该套教材的过程中继续向我们提出宝贵的意见，也希望有关专家不吝赐教.

广西小学教育专业教材编写委员会

2002 年 7 月

说　　明

初等数论是大学专科小学教育专业数学类主修学科的主干课程，教学总时数为72课时.本课程主要研究整数最基本的性质.其中第一章讨论整除理论.整除理论是初等数论的基础，其中心内容是算术基本定理和最大公约数理论.第二章较全面地介绍了同余理论的基本知识.同余理论是初等数论的核心，包含了数论所特有的思想、概念与方法.第三章介绍不定方程.求解不定方程是推进数论发展最主要的课题，本章在整除理论和同余理论的基础上讨论了几类最基本不定方程的解法.第四章介绍了同余方程，它是同余理论的应用和进一步深化，其中包含了我国古代数学家的重要数学成就.

本课程的内容既体现了大学的专科程度，又突出了培养小学教师的师范性，适应小学数学教师职前教育的需要.

本书是在广泛征求开办小学教育大专班的几所师范学校的有关老师意见的基础上编写而成的.与以往使用的同级教材相比，本书在编写过程中作了一些改进：一是精简内容.全书只有四章，属初等数论最基本的内容，其中还将各章较繁杂但又希望学生能了解的部分内容列为选学内容.二是增强教材的可读性.语言力求通俗易懂，对较难的例题和定理证明给出分析过程.同时每章后面附有该章的小结，书末附有习题答案或提示，以方便读者自学.

本教材编写人员及分工为：

第一章由蒋邕平（南宁市师范学校）执笔；第二章、第四章与附录由赵继源（广西师范学院数计系）执笔；第三章由赵飞（广西师范学院数计系）执笔.全书由赵继源统稿，由李忠傧审稿.

编写期间，得到广西师范学院教务处的大力支持和帮助，谨此致

谢.

由于时间仓促,水平有限,疏漏之处在所难免,敬请广大读者不吝赐教.

《初等数论》编写组

2001年3月

M U L U

第一章 整数的整除性

第二章　同余理论

第三章　不定方程

第四章　同余方程

第一章

整数的整除性

ZHENGSHU DE ZHENGCHUXING

初等数论是研究整数最基本性质的数学分支,是一门十分重要的数学基础课程.

整除性理论是初等数论的基础,其中心内容是最大公约数理论和算术基本定理.本章引入了带余除法和质数、合数的概念,介绍了质数的基本性质、最大公约数与最小公倍数的有关性质与理论,进而证明算术基本定理并研究带余数除法的发展——辗转相除法,最后介绍数的进位制及高斯函数等.

§1.1　整除

一、整数

我们知道,所谓整数是指

$$\cdots,-n-1,-n,\cdots,-1,0,1,\cdots,n,n+1,\cdots.$$

全体整数组成的集合用 **Z** 表示,即

$$\mathbf{Z}=\{\cdots,-n-1,-n,\cdots,-1,0,1,\cdots,n,n+1,\cdots\}$$
$$=\{0,\pm1,\pm2,\cdots,\pm n,\pm(n+1),\cdots\}.$$

正整数是指 $1,2,3,\cdots,n,n+1,\cdots$.

用 $\mathbf{N}$ 或 $\mathbf{Z}^+$ 表示全体正整数组成的集合.

以后,若无特别说明,我们将用字母

$$a,b,c,\cdots\text{或}\ \alpha,\beta,\gamma,\cdots$$

表示整数.

当几个字母连写时,表示连乘积,如

$$abc=a\cdot b\cdot c.$$

当几个字母连写并在上面标有横线时,字母均代表 0,1,2,…,9 等阿拉伯数字,如

$$\overline{abc}=100a+10b+c\ (a\neq0)$$

表示百位、十位、个位数字分别为 a,b,c 的三位数.

两个整数的和、差、积仍是整数,即整数中加、减、乘法运算是封闭的,但商就不一定是整数,只有在一定条件下才是整数.下面我们讨论数的整除性.

定义 1.1 设 $a,b\in\mathbf{Z},b\neq0$,如果存在 $q\in\mathbf{Z}$,使 $a=bq$,则称 a 能被 b 整除或 b 整除 a,记作 $b\mid a$.如果 q 不存在,则称 a 不能被 b 整除,记作 $b\nmid a$.

例如:$2\mid6,-23\mid2001,8\mid0,4\nmid10$ 等等.

当 $b\mid a$时,称 a 是 b 的倍数,b 是 a 的约数.

若 $b\mid a$,且 $b\neq\pm a,a\neq0,b\neq\pm1$,则称 b 是 a 的真约数(或非显然约数).

由整除定义出发,可以推出整除的基本性质:

(1) $1\mid a,b\mid0,c\mid c(c\neq0)$;

(2) 若 $a\mid b$,且 $|b|<|a|$,则 $b=0$;

(3) 若 $a\mid b$,则 $(\pm a)\mid(\pm b),|a|\,\big|\,|b|$,反之亦然;

(4) 若 $a\mid b$,且 $b\mid c$,则 $a\mid c$(传递性);

(5) 若 $a\mid b$,且 $b\mid a$,则 $a=\pm b$;

(6) 若 $a\mid b$,且 $a\mid c$,则 $a\mid(bx+cy)$,x,y为任意整数;

(7) 若 $m\neq 0$,则 $a\mid b$的充要条件是$ma\mid mb$;

(8) 若 $a\mid b$,且 $a,b\in\mathbf{N}$,则 $a\leqslant b$;

(9) 若 a 是b 的真约数,则 $1<|a|<|b|$;

(10) 若 $c\mid a$,且$c\nmid b$,则 $c\nmid(a\pm b)$;

(11) 若 $b\mid a$,且 $c\mid d$,则 $bc\mid ad$;

(12) 若 $a=b+c$,且 $d\mid a$,$d\mid b$,则 $d\mid c$;

(13) n 个连续自然数之积,必能被 $n!$ 整除;

(14) 若 $n\in\mathbf{Z}^{+}$且 $a\neq b$,则$(a-b)\mid(a^{n}-b^{n})$.

(证明留给读者)

定理 1.1　设 $a,b\in\mathbf{Z}$,且 $b\neq 0$,则一定存在唯一的一对整数 q 和 r,满足

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

证明　(构造法)作整数序列

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

则 a 必在上述序列的某两项之间,即存在一个整数 q,使得

$$q|b|\leqslant a<(q+1)|b|,$$

于是 $a-q|b|\geqslant 0$,$a-q|b|<|b|$.

令 $a-q|b|=r$,那么 $0\leqslant r<|b|$.

因此,当 $b>0$ 时,我们有 $a=qb+r$;当 $b<0$ 时,我们有 $a=(-q)b+r$.

这样,我们就证明了 q,r 的存在性.

下面我们来证明 q,r 的唯一性.

假设 $a=q_1b+r_1$,$0\leqslant r_1<|b|$.

那么$(q-q_1)b=r_1-r$,$0\leqslant|r_1-r|<|b|$,

即$|q-q_1|\cdot|b|<|b|$.

因此$|q-q_1|<1$.

但 $q, q_1 \in \mathbf{Z}$,所以 $q = q_1$,于是 $r = r_1$.

此即 q, r 是唯一的.

综上所述,定理成立.

例如 $a = 23, b = 5$ 时,$23 = 4 \times 5 + 3$,这时 $q = 4, r = 3$. 又如 $a = 23, b = -5$ 时,$23 = (-4) \times (-5) + 3$,这时 $q = -4, r = 3$.

定理 1.1 又称带余(数)除法定理. 当 $r \neq 0$ 时,称 q 是被除数 a 除以除数 b 的不完全商(数),称 r 为(最小非负)余数,该定理是初等数论证明中最重要、最基本、最直接的工具.

显而易见,$b \mid a$的充要条件是$r = 0$.

例 1 两个整数相除,商数是12,余数是 26,被除数、除数、商数及余数的和等于 454,求被除数是多少?

解 设除数是 x,被除数是 y. 根据带余除法及题意得:

$$\begin{cases} y = 12x + 26, \\ y + x + 12 + 26 = 454. \end{cases} \text{解之得} \begin{cases} x = 30, \\ y = 386. \end{cases}$$

故被除数是 386.

例 2 2001除以某自然数,商为 50,求除数和余数.

解 设除数为 x,余数为 y. 由题意有:

$$2001 = 50x + y, 0 \leqslant y < x,$$

故$\begin{cases} 50x \leqslant 2001, \\ 50x + x > 2001. \end{cases}$ 解得 $\begin{cases} x \leqslant 40\dfrac{1}{50}, \\ x > 39\dfrac{12}{51}. \end{cases}$

而 $x \in \mathbf{Z}$,故取 $x = 40$,从而 $y = 1$.

因此所求除数为 40,余数为 1.

例 3 已知 $N = 2^{1996} - 2^{1994} + 2^{1992} - 2^{1990} + 2^{1988} - 2^{1986}$. 求证:$9 \mid N$.

证明 $\because$

$$\begin{aligned} N &= 2^{1986} \times (2^{10} - 2^8 + 2^6 - 2^4 + 2^2 - 1) \\ &= 2^{1986} \times 819 \\ &= 9 \times 91 \times 2^{1986} \end{aligned}$$

$\therefore \quad 9 \mid N$.

例 4 若 $a \neq b, n \in \mathbf{Z}^+$，则 $(a-b) \mid (a^n - b^n)$.

证明 将 $a^n - b^n$ 分解因式，得

$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.

而 $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}$ 为关于 a, b 的整式，

故 $(a-b) \mid (a^n - b^n)$.

例 5 若 $n \in \mathbf{Z}^+$，则 $23 \mid (5^{2n+1} + 2^{n+4} + 2^{n+1})$.

证明 $\because$
$$\begin{aligned} 5^{2n+1} + 2^{n+4} + 2^{n+1} &= 5 \times 25^n + 16 \times 2^n + 2 \times 2^n \\ &= 5 \times 25^n + 18 \times 2^n \\ &= 23 \times 2^n + 5 \times (25^n - 2^n), \end{aligned}$$

而 $23 \mid 23 \times 2^n, (25-2) \mid (25^n - 2^n)$,

故 $23 \mid 5 \times (25^n - 2^n)$.

$\therefore\ 23 \mid [23 \times 2^n + 5 \times (25^n - 2^n)]$,

即 $23 \mid (5^{2n+1} + 2^{n+4} + 2^{n+1})$.

二、奇数与偶数

因为一个整数被 2 除的余数只能是 0 或 1，因此把所有整数分为奇数和偶数两大类. 奇数指的是

$$\cdots, -5, -3, 1, 3, 5, \cdots$$

这样的数，偶数指的是

$$\cdots, -4, -2, 0, 2, 4, \cdots$$

这样的数，我们可以把对整数问题的研究转化为对奇数和偶数的研究，研究整数的奇偶性也是研究整数性质的基础. 这里我们全面深入地学习奇数与偶数的性质和奇偶性分析法.

定义 1.2 如果 $2 \mid a$，称 a 为偶数，常用 $2k(k \in \mathbf{Z})$ 表示. 大于 0 的偶数(即正偶数)也叫双数.

如果 $2 \nmid a$，称 a 为奇数，常用 $2k+1(k \in \mathbf{Z})$ 表示. 大于 0 的奇数(即正奇数)也叫单数.

从上述定义出发易得下面的性质：

性质 1 若干个偶数的和、差、积仍是偶数.

任意一个整数与偶数的积仍是偶数.

n 个偶数的积是 2^n 的倍数($n \geqslant 2$).

性质 2 双数个奇数的和或差是偶数.

单数个奇数的和或差仍是奇数.

若干个奇数的积仍是奇数.

性质 3 任一奇数与任一偶数不相等.

性质 4 任意奇数的平方除以8的余数是 1.

事实上,对于任一个奇数 $2k+1, k \in \mathbf{Z}$,

$$\begin{aligned}(2k+1)^2 &= 4k^2+4k+1 \\ &= 4k(k+1)+1.\end{aligned}$$

而 $k(k+1)$ 为偶数,故 $4k(k+1)$ 为 8 的倍数,

所以,$(2k+1)^2$ 除以 8 的余数是 1.

例 6 若 $x, y \in \mathbf{Z}$,且 $x^2-4y=1$,试讨论 x, y 的奇偶性.

解 由 $x^2-4y=1$,得

$x^2=2\times 2y+1$ 为奇数.

$\therefore$ x 是奇数.

又 $y=\dfrac{1}{4}(x^2-1)$,

由性质 4 知,奇数的平方减去 1 的差为 8 的倍数,

故 x^2-1 为 8 的倍数.

$\therefore$ $\dfrac{1}{4}(x^2-1)$ 为 2 的倍数.

$\therefore$ y 是偶数.

例 7 能否在下式的各□内填入"+"或"-",使下式成立?

1□2□3□4□5□6□7□8□9 = 10.

解法 1 因为1□2中的□内不管填"+"或"-",结果必为奇数,所以,(1□2)□3 = 奇数□3 = 偶数,于是

1□2□3□4 与 5□6□7□8 均为偶数.

$\therefore$ 1□2□3□4□5□6□7□8□9

= (1□2□3□4)□(5□6□7□8)□9

= 偶数□偶数□9