大学本科小学教育专业教材
初等数论

大学本科小学教育专业教材

初等数论

CHUDENG SHULUN

王进明 主编

人民教育出版社

大学本科小学教育专业教材

初等数论

王进明　主编

人民教育出版社
·北京·

图书在版编目（CIP）数据

初等数论/王进明主编. —北京：人民教育出版社，2002
大学本科小学教育专业教材
ISBN 7-107-15889-9

Ⅰ. 初…
Ⅱ. 王…
Ⅲ. 初等数论—高等学校—教材
Ⅳ. 0156.1

中国版本图书馆 CIP 数据核字（2002）第 062569 号

人民教育出版社 出版发行
（北京沙滩后街 55 号　邮编：100009）
网址：http://www.pep.com.cn
北京市房山印刷厂印装　全国新华书店经销
2002 年 12 月第 1 版　2003 年 7 月第 2 次印刷
开本：890 毫米×1 240 毫米　1/32　印张：7.25
字数：183 千字　印数：2 001－7 000 册
定价：11.20 元

本书编写人员

主　　编：王进明

撰　　稿：（以汉语拼音字母为序）

高思伟　刘　莹　王进明

特约审稿：张君达

大学本科小学教育专业教材编审委员会

如发现印、装质量问题，影响阅读，请与出版社联系调换。

（联系地址：北京市方庄小区芳城园三区 13 号楼　邮编：100078）

大学本科小学教育专业教材

总　　序

为了适应社会主义现代化建设和人民群众对教育需求不断增长的新形势，经国家教育部批准，全国各地相继成立了以培养大学本科学历小学教师为主要任务的初等教育学院（系），大学本科小学教育专业应运而生。该专业的设立是我国初等教育改革和发展的需要，是提高我国小学教师素质的重要举措，也是我国师范教育改革和发展的必然趋势。

《中共中央国务院关于深化教育改革全面推进素质教育的决定》指出：建设高质量的教师队伍是全面推进素质教育的基本保障。目前，培养小学教师的现行课程、教材和教法，已不能完全满足全面推进素质教育的客观要求，受到了前所未有的挑战。新的课程教材建设势在必行。鉴于此，教育部师范教育司组织有关高等学校成立了“面向21世纪培养本科程度小学师资专业建设研究”的全国性总课题组，制订了大学本科小学教育专业培养目标和课程方案，在此基础上形成了“全国小学教育专业建设协作会”，对该专业课程教材建设进行了深入研究。

为了加强对教材编写工作的管理，教育部师范司、教育部课程教材研究所及有关高师院校的领导和专家组成了“大学本科小学教育专业教材编写委员会”。中国教育学会会长顾明远、教育部课程教材研究所原所长吴履平、教育部师范司司长马立为编写委员会顾问，首都师范大学副校长刘新成为编写委员会主任。编写委员会聘请具有丰富教学经验和较高学术水平的学科带头人分别担任各科教材主编，并聘请知名专家审核编写大纲和初稿。为了加强对这套教

材编审工作的领导、协调和统筹，人民教育出版社还成立了“大学本科小学教育专业教材编审委员会”。

本套教材的编写以“教育要面向现代化，面向世界，面向未来”为指针，以党和国家的教育方针以及大学本科小学教育专业培养目标为依据，以思想性、科学性、时代性和师范性为原则，致力于培养未来小学教师的创新精神和实践能力，全面体现“大学本科程度”和“面向小学教育”的要求，力求建立合理的教材结构，以满足21世纪对新型小学教师素质结构的需要。

本套教材是从大多数地区的情况出发而编写的全国通用教材，主要供培养本科层次小学教师的高等院校使用，也可供培养专科层次小学教师的院校使用，还可供广大在职小学教师进修或自学使用。这套教材由人民教育出版社于新世纪第一年开始陆续推出。

本套教材的编写出版得到了教育部师范教育司、高等教育司、社会科学研究与思想政治工作司、课程教材研究所、人民教育出版社，以及部分省市教委（教育厅）和有关高等院校的领导和同志们的大力支持，谨在此一并致谢。

编写出版大学本科小学教育专业系列教材，是我们贯彻国家教育部师范教育课程教材改革精神、全面落实《面向21世纪教育振兴行动计划》的初步尝试，如有不当之处，敬请广大师生不吝指正，以使本套教材日臻完善。

大学本科小学教育专业教材编写委员会

2000年12月

说　明

初等数论是大学本科小学教育专业理科类必修课程，教学总时数为48课时。本课程主要研究整数最基本的性质。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，本书第一章就是讨论整除理论。同余理论是初等数论的核心，它是数论所特有的思想、概念与方法，本书第二章与第三章较全面地介绍了同余理论的基本知识。第四章用以上建立的整除理论和同余理论介绍了几类最基本不定方程的解法。本书最后一章对一个十分有用的工具——连分数作了简单的介绍。

本书的内容既突出了培养小学教师的师范专业特点，又体现了大学本科教育的需要。编写人员及分工如下：第一章由王进明编写，第二章、第三章由高思伟编写，第四章、第五章由刘莹编写。

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。

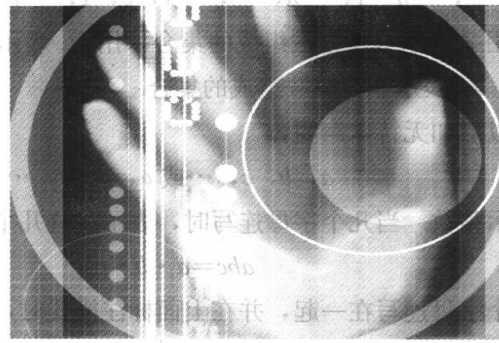
《初等数论》编写组

2001年5月

目　录

第一章　整数的整除性……（1）
§1.1　整除 ……（1）
§1.2　质数与合数 ……（19）
§1.3　最大公约数与最小公倍数 ……（30）
§1.4　算术基本定理 ……（51）
§1.5　数的进位制 ……（66）
§1.6　高斯函数 ……（77）
§1.7　费马(Fermat)数　梅森(Mersenne)数　完全数 …（102）
第二章　同余……（113）
§2.1　同余的定义及基本性质 ……（113）
§2.2　剩余类与剩余系 ……（120）
§2.3　欧拉定理 ……（129）
§2.4　循环小数 ……（135）
第三章　同余方程……（147）
§3.1　一次同余方程 ……（147）
§3.2　一次同余方程组 ……（158）
第四章　不定方程……（171）
§4.1　一次不定方程 ……（171）
§4.2　商高不定方程 ……（186）
第五章　简单连分数……（199）
§5.1　有限连分数与有理数 ……（199）
§5.2　无限连分数与无理数 ……（210）

第一章　整数的整除性



初等数论是研究整数最基本性质的一门十分重要的数学基础课程.

整除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，本章重点讨论整除理论. 首先从数论的最基本概念——整除出发，讨论奇数、偶数的有关性质，引入带余除法和质数、合数概念，介绍质数的基本性质、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辗转相除法，最后介绍 k 进制数、高斯函数、费马数、梅森数、完全数.

§1.1　整　　除

1. 整数

自然数，就是我们所熟悉的

$$0,\ 1,\ 2,\ 3,\ \cdots,\ n,\ n+1,\ \cdots$$

我们用 **N** 表示全体自然数组成的集合.

整数就是指正整数、负整数与零，即

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

我们用 **Z** 表示全体整数组成的集合，用 $\mathbf{N}_+$ 表示全体正整数组成的集合，$\mathbf{Z}_+$ 表示非零整数组成的集合.

以后如无特殊声明，

$$a，b，c，\cdots或\alpha，\beta，\gamma，\cdots$$

均表示整数. 当几个字母连写时，表示将这几个字母连乘起来，如

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

当几个字母连写在一起，并在上面标注横线时，每个字母均代表数字，且最左边的第一个字母不能为零，如 $\overline{abcde}$ 表示个位、十位、百位、千位、万位的数字分别为 e，d，c，b，a 的一个五位数，且 $a\neq 0$. 一般有

$$\overline{a_n a_{n-1}\cdots a_2 a_1 a_0}=\sum_{i=0}^{n} a_i 10^i = a_n\times 10^n + a_{n-1}\times 10^{n-1}+\cdots+a_2\times 10^2 + a_1\times 10 + a_0$$

（a_i 全是 0，1，2，…，9 中的数字，$a_n\neq 0$，$n\in\mathbf{N}$）

表示个位、十位、百位……分别为 a_0，a_1，a_2，…的一个 $n+1$ 位数.

任意两个整数的和、差、积仍是整数，即整数集对加、减、乘法运算封闭. 但整数除以整除，其商不一定是整数，究竟在什么条件下两整数的商才是整数，这正是我们要研究的一个重要内容——整数的整除性.

2. 整除

定义 1.1 设 a，$b\in\mathbf{Z}$，$b\neq 0$，如果存在整数 q，使 $a=bq$，则称 a 能被 b 整除，或 b 整除 a，记作 $b\mid a$. 否则称 a 不能被 b 整除，记作 $b\nmid a$.

当 $b\mid a$ 时，称 a 是 b 的倍数，b 是 a 的约数. 当 $b\mid a$，且 $b\neq$

$\pm a$，$a\neq 0$，$b\neq\pm 1$ 时，称 b 为 a 的真（非显然）约数.

根据上述定义及整数的有关性质，可推出下列有关整除的性质.

定理 1.1.1

(1) $1\mid a$，$b\mid 0$，$a\mid a$.

(2) 若 $a\mid b$，$|b|<|a|$，则 $b=0$.

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

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

(5) x，y 为任意整数，若 $a\mid b$，$a\mid c$，则 $a\mid(bx+cy)$；反之亦然.

(6) 若 $m\neq 0$，则 $a\mid b$ 的充分必要条件是 $ma\mid mb$.

(7) 若 $a\mid b$，$b\mid a$，则 $a=\pm b$.

(8) 若 a，$b\in\mathbf{N}_+$，$a\mid b$，则 $a\leqslant b$.

(9) 若 a 是 b 的真约数，则 $1<|a|<|b|$.

证明：(1) $\because a=a\times 1$，$0=b\times 0$，$a=a\times 1$，

$\therefore\quad 1\mid a$，$b\mid 0$，$a\mid a$.

(2) $\because a\mid b$，$\therefore$存在整数 q 使得 $b=aq$，即 $|b|=|a|\,|q|$.

$\because |b|<|a|$，$\therefore |a|\,|q|-|a|<0$，即

$$|a|(|q|-1)<0.$$

$\because |a|>0$，$\therefore |q|<1$.

$\because |q|\geqslant 0$，$\therefore q=0$.

$\therefore\quad b=0$.

(3) $\because\ a\mid b$，$\therefore b=aq$，而 $aq=(-a)(-q)$，故 $b=(-a)(-q)$，则 $-a\mid b$；

$\because\ -a\mid b$，$\therefore b=(-a)q_1=a(-q_1)$，

则 $a \mid b$.

(余略)

(4) $\because$ $a \mid b$, $b \mid c$,

$\therefore$ $b=aq_1$, $c=bq_2$, 即 $c=(aq_1)q_2=a(q_1q_2)$. 故 $a \mid c$.

(5) $\because$ $a \mid b$, $a \mid c$,

$\therefore$ $b=aq_1$, $c=aq_2$.

$\because x$, y 是整数,

$\therefore$ $bx+cy=(aq_1)x+(aq_2)y$

$=a(q_1x+q_2y)$,

则 $a \mid (bx+cy)$.

反之, $\because$ $a \mid (bx+cy)$且 x, y 是任意整数, 取 $x=1$, $y=0$ 及 $x=0$, $y=1$, 则有 $bx+cy=b$, $bx+cy=c$, $\therefore a \mid b$, $a \mid c$.

(6) (必要性证明)

$\because a \mid b$, $\therefore b=aq$, 则

$mb=m(aq)=(ma)q$.

$\because m \neq 0$, $\therefore am \neq 0$, 则

$ma \mid mb$.

(充分性证明)

$\because$ $ma \mid mb$, $\therefore mb=(ma)q=m(aq)$.

$\because$ $m \neq 0$, $\therefore b=aq$, 则 $a \mid b$.

故 $m \neq 0$ 时, $a \mid b$ 的充分必要条件是 $ma \mid mb$.

(7) $\because a \mid b$, $b \mid a$,

$\therefore$ $a=bq_2$, $b=aq_1$, 则 $a=(aq_1)q_2=a(q_1q_2)$.

$\because$ $a \neq 0$,

$\therefore$ $q_1q_2=1$.

$\because$ q_1, $q_2 \in \mathbf{Z}$, $\therefore$ $q_1=q_2=1$ 或 $q_1=q_2=-1$, 则 $a=b$ 或 $a=-b$. 故 $a=\pm b$.

(8) $\because$ $a \mid b$, $\therefore b=aq$, 即 $|b|=|a||q|$.

∵a，$b\in\mathbf{N}_+$，∴$b=a\mid q\mid>0$.

而$\mid q\mid\geqslant 1$，∴$a\leqslant b$.

(9) ∵　a是b的真约数，∴$\mid a\mid>1$.

∵　$a\mid b$，∴　$\mid b\mid=\mid a\mid\mid q\mid$.

∵　$b\neq 0$，∴　$\mid b\mid>0$.

由(8)知　$\mid b\mid\geqslant\mid a\mid$.

∵$a\neq\pm b$，∴　$\mid b\mid>\mid a\mid$，

则　　$1<\mid a\mid<\mid b\mid$.

定理得证.

定理 1.1.2　若a，b是给定的两个整数，且$b\neq 0$，则一定存在唯一的一对整数q和r，满足　$a=bq+r$，$0\leqslant r<\mid b\mid$.

证明：

(1) 当$b>0$时，作整数序列

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

若a与上面序列中某一项相等，则$a=bq$，即　$a=bq+r$，$r=0$.

若a与上面序列中任一项均不相等，则必在此序列的某相邻两项之间，即有确定的整数q，使$bq<a<b(q+1)=bq+b$，

∴　$0<a-bq<b=\mid b\mid$.

令$a-bq=r$，则有

$$a=bq+r，0<r<\mid b\mid.$$

(2) 当$b<0$时，作整数序列

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

若a与序列中某一项相等，则$a=bq$，即　$a=bq+r$，$r=0$.

若a与序列中任一项均不相等，则必在此序列的某相邻两项之间，即有确定的整数q，使$bq<a<b(q-1)=bq-b$.

∴　$0<a-bq<-b=\mid b\mid$，

令$a-bq=r$，则有

$$a=bq+r，0<r<\mid b\mid.$$

综上所述，对给定的整数 a，$b(b\neq 0)$，有确定的一对整数 q 和 r，满足

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

对于给定的整数 a，$b(b\neq 0)$，如果有两对整数 q_1，r_1；q_2，r_2 满足

$$a=bq_1+r_1,\ 0\leqslant r_1<|b|, \qquad ①$$

$$a=bq_2+r_2,\ 0\leqslant r_2<|b|. \qquad ②$$

①－②得

$$r_1-r_2=(q_2-q_1)b,\ 0\leqslant|r_1-r_2|<|b|,$$

即 $b\mid(r_1-r_2)$，且 $|r_1-r_2|<|b|$.

由定理 1.1.1 的 (2) 知 $r_1-r_2=0$，则 $r_1=r_2$，从而 $q_1=q_2$.

综上所述，结论成立.

称上述定理中的 q 和 r 分别为**被除数** a 除以**除数** b 的**商和余数**. 此定理又被称为**带余（数）除法定理**，它是初等数论证明中最基本、最直接、最重要的工具. 当 $a=bq+r$，$0\leqslant r<|b|$ 时，$b\mid a$的充要条件是 $r=0$.

例 1　若 $N=2^{2\,000}-2^{1\,998}+2^{1\,996}-2^{1\,994}+2^{1\,992}-2^{1\,990}$，则$9\mid N$.

证明：∵
$$\begin{aligned}N&=2^{2\,000}-2^{1\,998}+2^{1\,996}-2^{1\,994}+2^{1\,992}-2^{1\,990}\\&=2^{1\,990}(2^{10}-2^8+2^6-2^4+2^2-1)\\&=2^{1\,990}(2^2-1)(2^8+2^4+1)\\&=2^{1\,990}\times 3\times 273\\&=9\times 91\times 2^{1\,990},\end{aligned}$$

∴ $9\mid N$.

例 2　已知 $n\in\mathbf{N}$ 且 $4\nmid n$，求证：

$$5\mid(1^n+2^n+3^n+4^n).$$

证明：∵
$$\begin{aligned}&1^n+2^n+3^n+4^n\\&=1^n+2^n+(5-2)^n+(5-1)^n\\&=1^n+2^n+5^n+C_n^1\cdot 5^{n-1}\cdot(-2)+C_n^2\cdot 5^{n-2}\cdot(-2)^2+\cdots+\end{aligned}$$

$$C_n^{n-1}\cdot 5\cdot(-2)^{n-1}+(-2)^n+5^n+C_n^1\cdot 5^{n-1}\cdot(-1)+$$
$$C_n^2\cdot 5^{n-2}\cdot(-1)^2+\cdots+C_n^{n-1}\cdot 5\cdot(-1)^{n-1}+(-1)^n$$
$$=1^n+2^n+(-2)^n+(-1)^n+5t_1+5t_2,$$

(这里 $t_1=5^{n-1}+C_n^1\cdot 5^{n-2}\cdot(-2)+C_n^2\cdot 5^{n-3}\cdot(-2)^2+\cdots$
$+C_n^{n-1}\cdot(-2)^{n-1}$,

$t_2=5^{n-1}+C_n^1\cdot 5^{n-2}\cdot(-1)+C_n^2\cdot 5^{n-3}\cdot(-1)^2+\cdots$
$+C_n^{n-1}\cdot(-1)^{n-1}$)

∵ $4\nmid n$, ∴ $n=4q+r$, $r=1$, 2, 3.

当 $r=1$ 时, $(-2)^n=(-2)^{4q+1}=(-2)^{4q}(-2)=-2\cdot 2^{4q}=-2^{4q+1}=-2^n$, $(-1)^{4q+1}=-1$, 此时

$1^n+2^n+(-2)^n+(-1)^n=0$, 结论成立.

当 $r=2$ 时, $(-2)^n=(-2)^{4q+2}=2^{4q+2}$,

$(-1)^n=(-1)^{4q+2}=1$, 此时

$1^n+2^n+(-2)^n+(-1)^n=2+2\cdot 2^{4q+2}=2+2\times 4^{2q+1}$, 而

$$4^{2q+1}=(5-1)^{2q+1}$$
$$=5^{2q+1}-C_{2q+1}^1\cdot 5^{2q}+C_{2q+1}^2 5^{2q-1}-\cdots-1,$$

∴ $2+2\times 4^{2q+1}$
$=2\times(5^{2q+1}-C_{2q+1}^1 5^{2q}+C_{2q+1}^2 5^{2q-1}-\cdots+C_{2q+1}^{2q}5)$.

故当 $r=2$ 时, $5\mid(1^n+2^n+(-2)^n+(-1)^n)$.

当 $r=3$ 时, 与 $r=1$ 时类似, 也有

$$5\mid(1^n+2^n+(-2)^n+(-1)^n).$$

综上所述, 已知 $n\in\mathbf{N}$ 且 $4\nmid n$ 时,

$$5\mid(1^n+2^n+3^n+4^n).$$

例 3　b 是非零整数, 若 d_1, d_2, …, d_k 是它的全体约数, 则 $\frac{b}{d_1}$, $\frac{b}{d_2}$, …, $\frac{b}{d_k}$ 也是它的全体约数.

证明: ∵ 当 $d_i\mid b$ 时, $b=d_iq_i$ $(i=1, 2, \cdots, k)$,

∴ $\frac{b}{d_i}=q_i$ 是整数.

$$\because\quad b=d_i\times\frac{b}{d_i},\ \therefore\quad \frac{b}{d_i}\Big|b,\ \text{即}$$

$\frac{b}{d_1}$，$\frac{b}{d_2}$，…，$\frac{b}{d_k}$均为b的约数，且当$d_i\neq d_j$时，$\frac{b}{d_i}\neq\frac{b}{d_j}$. 这样一来，$\frac{b}{d_1}$，$\frac{b}{d_2}$，…，$\frac{b}{d_k}$是$k$个两两不同的$b$的约数，由于$b$的约数的个数是一定的，所以结论成立.

例4　若$n\in\mathbf{Z}$，$k\in\mathbf{N}_+$，则

$$\frac{n(n-1)\cdots(n-k+1)}{k!}$$

的值是整数.

证明：当$n=0$时，$n(n-1)\cdots(n-k+1)=0$，$k!\mid 0$，结论成立.

当$n>0$时，如果$n\geqslant k$，则

$\frac{n(n-1)\cdots(n-k+1)}{k!}=C_n^k$，$C_n^k$表示从$n$个元素中取$k$个元素的组合数. 组合数是整数，结论成立.

当$0<n<k$时，在n，$n-1$，…，$n-k+1$这k个数中一定有一个数是0，即

$n(n-1)\cdots(n-k+1)=0$，$k!\mid 0$，结论成立.

当$n<0$时，令$n=-n'$，$n'>0$，则

$$\begin{aligned}&\frac{n(n-1)\cdots(n-k+1)}{k!}\\=&\frac{-n'(-n'-1)\cdots(-n'-k+1)}{k!}\\=&(-1)^k\frac{n'(n'+1)\cdots(n'+k-1)}{k!}.\end{aligned}$$

$\because\quad n'+k-1\geqslant k$，

$$\therefore\quad \frac{n'(n'+1)\cdots(n'+k-1)}{k!}=C_{n'+k-1}^k.$$

$\because\quad C_{n'+k-1}^k$是组合数，$\therefore\ (-1)^kC_{n'+k-1}^k$是整数，结论成立.