浙江省教育厅重点建设教材

初等数论

于秀源　瞿维建

山东教育出版社

浙江省教育厅重点建设教材

初等数论

于秀源　瞿维建

山东教育出版社

初等数论

于秀源　瞿维建

出 版 者：山东教育出版社
（济南市纬一路 321 号　邮编：250001）
电　　话：(0531)2092663　传真：(0531)2092661
网　　址：http://www.sjs.com.cn
发 行 者：山东教育出版社
印　　刷：山东新华印刷厂临沂厂
版　　次：2004 年 4 月第 1 版
2004 年 4 月第 1 次印刷
印　　数：1—4000
规　　格：850mm × 1168mm　32 开本
印　　张：9.125 印张
字　　数：213 千字
书　　号：ISBN7 - 5328 - 3265 - 1
定　　价：14.80 元

前　言

数论是数学的一个源远流长的分支.长时间以来,数论一直是高等学校数学系的一门重要课程.近几十年来,数论的理论研究和应用研究都有了许多引人瞩目的进展,数论进入了许多学科领域.为适应这一情况,许多高等学校在更多的系或专业开设数论课程,以满足人才培养的需要.

本书是在我们20世纪80年代以来讲授初等数论课使用的讲义的基础上编写而成的,它的读者对象主要是师范院校数学系学生,目的是使他们了解和掌握初等数论的基本理论和方法,具备进行数论理论研究,以及将数论应用于其他学科的能力.在编写本书的时候,也考虑到了其他专业的学生和科技人员对数论知识的需要.

初等数论课有自己的特点.首先,学生在小学、中学学习阶段就已经接触到初等数论中的一些内容和结论,并且具有利用这些知识解决问题的能力.其次,相对而言,初等数论课的理论是比较容易学习的,数论题目却常是比较难做的.此外,初等数论中的许多内容又是数论应用中最常涉及的部分.从这些考虑出发,本书在内容安排上,大致分成三大部分:第一部分包括整除理论、简单的不定方程求解问题.这一部分是初等数论中最基础的内容,其中一些结论,学生在中学里就已经熟悉(尽管可能未经过严格的证明)或者使用了.因此,总的来说,除个别内容外,学生完全可以自学.这一部分很能体现初等数论的"理论易学、题目难做、技巧性强"的特点.根据我们的经验,这一部分的课堂教学除对少数定理或结论

给出讲解和证明外，大部分内容可以学生自学为主.课堂教学主要是通过对大量例题的讲解，使学生加深对定义和定理的理解，学会解题和制设新题的基本技巧，注意对逻辑推理严密性、数学语言规范性、文字叙述准确性的基础训练.这一部分含有较多的例题和习题，可以根据具体的教学情况选讲或全讲.第二部分包括同余和同余方程的基础理论、二次剩余、整数的平方和表示、原根和连分数的基础知识.这是初等数论的重要组成部分，是学生深入学习数论的基础，也是将来从事数论理论研究的基础.这一部分中包含了许多数论中的基本概念、方法和结论.我们认为，对这一部分的教学，要着重使学生充分理解概念、定义的内涵，掌握基本方法，了解重要结论，以及应用这些知识去解决问题.因此，课堂教学应以教师讲解为主，辅以学生的自学.第三部分对数论的应用，特别是在密码学中的应用做了较多的介绍，也介绍了超越数和代数数的基本知识.除了个别内容外，对于学生来说，这一部分都属于新的概念或命题，自学是比较困难的.

本书被浙江省教育厅列为重点建设教材项目，并给以经费资助，为本书的编写提供了许多方便的条件.本书的编写过程中，得到了黄伟娣副研究员（杭州师范学院）、Peter S. J. Shiue 教授（University of Nevada, Las Vegas, USA）和 Joseph Kelleher、Jean Kelleher 夫妇（Edwardsville, Illinois, USA）的许多支持和帮助.山东教育出版社霍亮先生对本书的内容和编排提出了很好的建议.借本书出版的机会，我们向他们表示衷心的感谢.

于秀源

2002.7

目　录

第一章　整除理论

整除理论是初等数论的基础.本章要介绍带余数除法、辗转相除法、最大公约数、最小公倍数、算术基本定理以及它们的一些应用.

第一节　数的整除性

定义 1　设 a,b 是整数,$b \neq 0$,如果存在整数 c,使得

$$a = bc$$

成立,则称 a 被 b 整除,a 是 b 的倍数,b 是 a 的约数(因数或除数),并且使用记号 $b \mid a$;如果不存在整数 c,使得 $a = bc$ 成立,则称 a 不被 b 整除,记为 $b \nmid a$.

显然每个非零整数 a 都有约数 $\pm 1, \pm a$,这四个数称为 a 的平凡约数,a 的另外的约数称为非平凡约数.

被 2 整除的整数称为偶数,不被 2 整除的整数称为奇数.

定理 1　下面的结论成立:

(i) $a \mid b \Leftrightarrow \pm a \mid \pm b$;

(ii) $a \mid b, b \mid c \Rightarrow a \mid c$;

(iii) $b \mid a_i, i = 1,2,\cdots,k \Rightarrow b \mid a_1x_1 + a_2x_2 + \cdots + a_kx_k$,此处 $x_i (i = 1,2,\cdots,k)$ 是任意的整数;

(iv) $b \mid a \Rightarrow bc \mid ac$,此处 c 是任意的非零整数;

(v) $b \mid a, a \neq 0 \Rightarrow \mid b \mid \leqslant \mid a \mid$;

$b \mid a$ 且 $|a| < |b| \Rightarrow a = 0$.

证明(留作习题)

定义 2　若整数 $a \neq 0, \pm 1$,并且只有约数 ± 1 和 $\pm a$,则称 a 是素数(或质数);否则称 a 为合数.

(以后在本书中若无特别说明,素数总是指正素数)

定理 2　任何大于 1 的整数 a 都至少有一个素约数.

证明　若 a 是素数,则定理是显然的.

若 a 不是素数,那么它有两个以上的正的非平凡约数,可设它们为 $d_1, d_2, \cdots, d_k$. 不妨设 d_1 是其中最小的. 若 d_1 不是素数,则存在 $e_1 > 1, e_2 > 1$,使得 $d_1 = e_1 e_2$,因此,e_1 和 e_2 也是 a 的正的非平凡约数. 这与 d_1 的最小性矛盾. 所以 d_1 是素数. 证毕.

推论　任何大于 1 的合数 a 必有一个不超过 $\sqrt{a}$ 的素约数.

证明　使用定理2中的记号,有 $a = d_1 d_2$,其中 $d_1 > 1$ 是最小的素约数,所以 $d_1^2 \leqslant a$. 证毕.

例 1　设 r 是正奇数,证明:对任意的正整数 n,有

$$n + 2 \nmid 1^r + 2^r + \cdots + n^r.$$

解　对于任意的正整数 a, b 以及正奇数 k,有

$$\begin{aligned} a^k + b^k &= (a + b)(a^{k-1} - a^{k-2}b + a^{k-3}b^2 - \cdots + b^{k-1}) \\ &= (a + b)q, \end{aligned}$$

其中,q 是整数.

记 $s = 1^r + 2^r + \cdots + n^r$,则

$$\begin{aligned} 2s &= 2 + (2^r + n^r) + (3^r + (n-1)^r) + \cdots + (n^r + 2^r) \\ &= 2 + (n + 2)Q, \end{aligned}$$

其中,Q 是整数.

若 $n + 2 \mid s$,由上式知 $n + 2 \mid 2$,因为 $n + 2 > 2$,这是不可能的,所以 $n + 2 \nmid s$.

例 2　设 $A = \{d_1, d_2, \cdots, d_k\}$ 是 n 的所有约数的集合,则

$$B = \{\frac{n}{d_1}, \frac{n}{d_2}, \cdots, \frac{n}{d_k}\}$$

也是 n 的所有约数的集合.

证　注意到以下三点：

(i) A 和 B 的元素个数相同；

(ii) 若 $d_1 \in A$，即 $d_i \mid n$，则 $\frac{n}{d_i} \mid n$，反之亦然；

(iii) 若 $d_i \neq d_j$，则 $\frac{n}{d_i} \neq \frac{n}{d_j}$，

显见结论成立.

例 3　以 $d(n)$ 表示 n 的正约数的个数，例如：$d(1) = 1, d(2) = 2, d(3) = 2, d(4) = 3, \cdots$，问

$$d(1) + d(2) + \cdots + d(1997)$$

是否为偶数？

解　对于 n 的每个约数 d，都有 $n = d \cdot \frac{n}{d}$，因此，n 的正约数 d 与 $\frac{n}{d}$ 是成对地出现的. 只有当 $d = \frac{n}{d}$，即 $n = d^2$ 时，d 和 $\frac{n}{d}$ 才是同一个数. 故当且仅当 n 是完全平方数时，$d(n)$ 是奇数.

因为 $44^2 < 1997 < 45^2$，所以在 $d(1), d(2), \cdots, d(1997)$ 中恰有 44 个奇数，故 $d(1) + d(2) + \cdots + d(1997)$ 是偶数.

例 4　设凸 $2n$ 边形 M 的顶点是 $A_1, A_2, \cdots, A_{2n}$，点 O 在 M 的内部，用 $1, 2, \cdots, 2n$ 将 M 的 $2n$ 条边分别编号，又将 $OA_1, OA_2, \cdots, OA_{2n}$ 也同样进行编号，若把这些编号作为相应的线段的长度，证明：无论怎么编号，都不能使得 $\triangle OA_1A_2, \triangle OA_2A_3, \cdots, \triangle OA_{2n}A_1$ 的周长都相等.

解　假设这些三角形的周长都相等，记为 s. 则

$$2ns = 3(1 + 2 + \cdots + 2n) = 3n(2n + 1),$$

即

$$2s = 3(2n + 1),$$

因此 $2 \mid 3(2n + 1)$,这是不可能的,这个矛盾说明这些三角形的周长不可能全都相等.

例 5 设整数 $k \geqslant 1$,证明:

(i) 若 $2^k \leqslant n < 2^{k+1}, 1 \leqslant a \leqslant n, a \neq 2^k$,则 $2^k \nmid a$;

(ii) 若 $3^k \leqslant 2n - 1 < 3^{k+1}, 1 \leqslant b \leqslant n, 2b - 1 \neq 3^k$,则 $3^k \nmid 2b - 1$.

解 (i) 若 $2^k \mid a$,则存在整数 q,使得 $a = q2^k$. 显然 q 只可能是 0 或 1. 此时 $a = 0$ 或 2^k,这都是不可能的,所以 $2^k \nmid a$;

(ii) 若 $3^k \mid 2b - 1$,则存在整数 q,使得 $2b - 1 = q3^k$,显然 q 只可能是 0,1 或 2. 此时 $2b - 1 = 0, 3^k$ 或 $2 \cdot 3^k$,这都是不可能的,所以 $3^k \nmid 2b - 1$.

例 6 写出不超过 100 的所有的素数.

解 将不超过 100 的正整数排列如下:

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

按以下步骤进行:

(i) 删去 1,剩下的后面的第一个数是 2,2 是素数;

(ii) 删去 2 后面的被 2 整除的数,剩下的 2 后面的第一个数是

3,3 是素数;

(iii) 再删去 3 后面的被 3 整除的数,剩下的 3 后面的第一个数是 5,5 是素数;

(iv) 再删去 5 后面的被 5 整除的数,剩下的 5 后面的第一个数是 7,7 是素数 ……

照以上步骤可以依次得到素数 $2,3,5,7,11,\cdots$.

由定理 2 推论可知,不超过 100 的合数必有一个不超过 10 的素约数,因此在删去 7 后面被 7 整除的数以后,就得到了不超过 100 的全部素数.

在例 6 中所使用的寻找素数的方法,称为 Eratosthenes 筛法.它可以用来求出不超过任何固定整数的所有素数.在理论上这是可行的,但在实际应用中,这种列出素数的方法需要大量的计算时间,是不可取的.

例 7　证明:存在无穷多个正整数 a,使得

$$n^4 + a(n = 1,2,3,\cdots)$$

都是合数.

解　取 $a = 4k^4$,对于任意的 $n \in \mathbf{N}$,有

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

因为

$$n^2 + 2k^2 - 2nk = (n - k)^2 + k^2 \geqslant k^2,$$

所以,对于任意的 $k = 2,3,\cdots$ 以及任意的 $n \in \mathbf{N}$,$n^4 + a$ 是合数.

例 8　设 $a_1, a_2, \cdots, a_n$ 是整数,且

$$a_1 + a_2 + \cdots + a_n = 0,$$

$$a_1 a_2 \cdots a_n = n,$$

则 $4 \mid n$.

解　如果 $2 \nmid n$,则 $n, a_1, a_2, \cdots, a_n$ 都是奇数.于是 $a_1 + a_2 +$

$\cdots + a_n$ 是奇数个奇数之和，不可能等于零，这与题设矛盾，所以 $2 \mid n$，即在 $a_1, a_2, \cdots, a_n$ 中至少有一个偶数. 如果只有一个偶数，不妨设为 a_1，那么 $2 \nmid a_i (2 \leqslant i \leqslant n)$. 此时有等式

$$a_2 + \cdots + a_n = -a_1,$$

在上式中，左端是 $(n-1)$ 个奇数之和，右端是偶数，这是不可能的，因此，在 $a_1, a_2, \cdots, a_n$ 中至少有两个偶数，即 $4 \mid n$.

例 9 若 n 是奇数，则 $8 \mid n^2 - 1$.

解 设 $n = 2k + 1$，则

$$n^2 - 1 = (2k+1)^2 - 1 = 4k(k+1).$$

在 k 和 $k+1$ 中有一个是偶数，所以 $8 \mid n^2 - 1$.

例 9 的结论虽然简单，却是很有用的. 例如，使用例 3 中的记号，我们可以提出下面的问题：

问题 $d(1)^2 + d(2)^2 + \cdots + d(1997)^2$ 被 4 除的余数是多少？

例 10 证明：方程

$$a_1^2 + a_2^2 + a_3^2 = 1999 \tag{1}$$

无整数解.

解 若 a_1, a_2, a_3 都是奇数，则存在整数 A_1, A_2, A_3，使得

$$a_1^2 = 8A_1 + 1, a_2^2 = 8A_2 + 1, a_3^2 = 8A_3 + 1,$$

于是

$$a_1^2 + a_2^2 + a_3^2 = 8(A_1 + A_2 + A_3) + 3.$$

由于 1999 被 8 除的余数是 7，所以 a_1, a_2, a_3 不可能都是奇数.

由式(1)，a_1, a_2, a_3 中只能有一个奇数，设 a_1 为奇数，a_2, a_3 为偶数，则存在整数 A_1, A_2, A_3，使得

$$a_1^2 = 8A_1 + 1, a_2^2 = 8A_2 + r, a_3^2 = 8A_3 + s,$$

于是

$$a_1^2 + a_2^2 + a_3^2 = 8(A_1 + A_2 + A_3) + 1 + r + s,$$

其中 r 和 s 是整数，而且只能取值 0 或 4. 这样 $a_1^2 + a_2^2 + a_3^2$ 被 8 除的余数只可能是 1 或 5，但 1999 被 8 除的余数是 7，所以这样的 a_1，a_2, a_3 也不能使式(1) 成立.

综上证得所需要的结论.

习 题 一

1. 证明定理 1.
2. 证明：若 $m - p \mid mn + pq$，则 $m - p \mid mq + np$.
3. 证明：任意给定的连续 39 个自然数，其中至少存在一个自然数，使得这个自然数的数字和能被 11 整除.
4. 设 p 是 n 的最小素约数，$n = pn_1, n_1 > 1$，证明：若 $p > \sqrt[3]{n}$，则 n_1 是素数.
5. 证明：存在无穷多个自然数 n，使得 n 不能表示为

$$a^2 + p(a > 0 \text{ 是整数}, p \text{ 为素数})$$

的形式.

第二节　带余数除法

在本节中，我们要介绍带余数除法及其简单应用.

定理 1(带余数除法)　设 a 与 b 是两个整数，$b \neq 0$，则存在唯一的两个整数 q 和 r，使得

$$a = bq + r, 0 \leqslant r < |b|. \tag{1}$$

证明　存在性　若 $b \mid a, a = bq, q \in \mathbf{Z}$，可取 $r = 0$. 若 $b \nmid a$，考虑集合

$$A = \{a + kb; k \in \mathbf{Z}\},$$

其中 $\mathbf{Z}$ 表示所有整数的集合，以后，仍使用此记号，并以 $\mathbf{N}$ 表示所有正整数的集合.

在集合 A 中有无限多个正整数，设最小的正整数是 $r = a + k_0 b$，则必有

$$0 < r < |b|, \tag{2}$$

否则就有 $r \geqslant |b|$. 因为 $b \nmid a$，所以 $r \neq |b|$. 于是 $r > |b|$，即 $a + k_0 b > |b|$，$a + k_0 b - |b| > 0$，这样，在集合 A 中，又有正整数 $a + k_0 b - |b| < r$，这与 r 的最小性矛盾. 所以式(2)必定成立. 取 $q = -k_0$ 知式(1)成立. 存在性得证.

唯一性　假设有两对整数 q', r' 与 q'', r'' 都使得式(1)成立，即

$$a = q''b + r'' = q'b + r', 0 \leqslant r', r'' < |b|,$$

则

$$(q'' - q')b = r' - r'', |r' - r''| < |b|, \tag{3}$$

因此 $r' - r'' = 0$，$r' = r''$，再由式(3)得出 $q' = q''$，唯一性得证. 证毕.

定义 1　称式(1)中的 q 是 a 被 b 除的商，r 是 a 被 b 除的余数.

由定理 1 可知，对于给定的整数 b，可以按照被 b 除的余数将所有的整数分成 b 类. 在同一类中的数被 b 除的余数相同. 这就使得许多关于全体整数的问题可以归化为对有限个整数类的研究.

以后在本书中，除特别声明外，在谈到带余数除法时总是假定 b 是正整数.

例 1　设 a, b, x, y 是整数，k 和 m 是正整数，并且

$$a = a_1 m + r_1, 0 \leqslant r_1 < m,$$

$$b = b_1 m + r_2, 0 \leqslant r_2 < m,$$

则 $ax + by$ 和 ab 被 m 除的余数分别与 $r_1 x + r_2 y$ 和 $r_1 r_2$ 被 m 除的

余数相同.特别地,a^k 与 $r_1{}^k$ 被 m 除的余数相同.

解　由

$$\begin{aligned} ax + by &= (a_1m + r_1)x + (b_1m + r_2)y \\ &= (a_1x + b_1y)m + r_1x + r_2y \end{aligned}$$

可知,若 $r_1x + r_2y$ 被 m 除的余数是 r,即

$$r_1x + r_2y = qm + r, 0 \leqslant r < m,$$

则

$$ax + by = (a_1x + b_1y + q)m + r, 0 \leqslant r < m,$$

即 $ax + by$ 被 m 除的余数也是 r.

同样方法可以证明其余结论.

例 2　设 $a_1, a_2, \cdots, a_n$ 为不全为零的整数,以 y_0 表示集合

$$A = \{y \mid y = a_1x_1 + \cdots + a_nx_n, x_i \in \mathbf{Z}, 1 \leqslant i \leqslant n\}$$

中的最小正数,则对于任何 $y \in A$, $y_0 \mid y$.特别地, $y_0 \mid a_i, 1 \leqslant i \leqslant n$.

解　设 $y_0 = a_1x_1' + \cdots + a_nx_n'$,对任意的 $y = a_1x_1 + \cdots + a_nx_n \in A$,由定理 1,存在 $q, r_0 \in \mathbf{Z}$,使得

$$y = qy_0 + r_0, 0 \leqslant r_0 < y_0.$$

因此

$$r_0 = y - qy_0 = a_1(x_1 - qx_1') + \cdots + a_n(x_n - qx_n') \in A.$$

如果 $r_0 \neq 0$,那么,因为 $0 < r_0 < y_0$,所以 r_0 是 A 中比 y_0 还小的正数,这与 y_0 的定义矛盾.所以 $r_0 = 0$,即 $y_0 \mid y$.

显然 $a_i \in A (1 \leqslant i \leqslant n)$,所以 y_0 整除每个 $a_i (1 \leqslant i \leqslant n)$.

例 3　任意给出的五个整数中,必有三个数之和被 3 整除.

解　设这五个数是 $a_i, i = 1,2,3,4,5$,记

$$a_i = 3q_i + r_i, 0 \leqslant r_i < 3, i = 1,2,3,4,5.$$

分别考虑以下两种情形: