初等数论

乐茂华　编著

广东高等教育出版社
·广州·

图书在版编目（CIP）数据

初等数论/乐茂华编著 .—2 版 .—广州：广东高等教育出版社，2002.2
ISBN 7-5361-1781-7

Ⅰ.初… Ⅱ.乐… Ⅲ.初等数论-高等学校-教材
Ⅳ.O156.1

中国版本图书馆 CIP 数据核字（2001）第 057336 号

广东高等教育出版社出版发行
（邮码：510076 电话：（020）87550735
地址：广州市广州大道北广州体院内 20 栋）
中国人民解放军第四二三二工厂印刷
850 毫米×1168 毫米 32 开本 7.75 印张 148 千字
2002 年 2 月第 2 版 2002 年 2 月第 2 次印刷
印数：1001~2600 册
定价：16.00 元

内容提要

本书介绍了整数的整除性、数论函数、同余、同余式、平方剩余、原根与指数、Diophantus 方程等初等数论的基本内容，并且简要地介绍了数论各分支的概况。本书可作为高等师范院校数学系以及其他院校相应专业的初等数论课程的教材，也可作为中学数学教师和数论爱好者的参考书。

前　言

在历史上，人类最早认识的数是整数。因此，研究整数性质的数论是数学中最古老的分支。数论中最经典、最基本的概念、方法和结论构成了初等数论的主要内容。它不但是数论，同时也是所有讨论各类离散结构的数学分支的基础。

本书介绍了初等数论中整数的整除性、数论函数、同余、同余式、平方剩余、原根和指数、Diophantus 方程等基本内容。这些内容可作为师范院校数学系的初等数论课教材，也可供中学数学教师和数论爱好者阅读。另外，本书在第八章和附录中简要地介绍了数论各分支形成和发展的历史以及最新的研究成果，可供对此有兴趣的读者参考。

本书是在作者多年讲授初等数论课程的讲义的基础上修改而成的，并且在内容的编排和结论的证明等方面作了一些创新的尝试。本书的编写得到了湛江师范学院各位领导的关怀和指导，湛江师范学院数学系的领导和老师为本书第一版的出版做了大量的工作，本书的再版得到湛江师范学院“基础数学”重点学科启动经费和重点教改项目经费的资助。作者谨此致以衷心的谢忱。

欢迎对本书的错误和不妥之处提出宝贵意见。

2001 年 7 月于湛江

目　录

第一章　整除性

已知任何两个整数的和、差、积都是整数，但是它们的商则不一定是整数．由此就产生了对整数的整除性的讨论，它是初等数论中最基本的内容．

本章从整除的定义开始，在引入素数与合数的概念之后，直接证明算术基本定理，并用它来讨论最大公因数和最小公倍数的基本性质．同时介绍带余数除法和辗转相除法及其应用．最后讨论 Gauss 函数及其在阶乘的素因数分解中的应用．

§1.1　整　　除

对于整数 a 以及非零整数 b，如果存在整数 q，可使

$$a = bq, \tag{1}$$

则称 b 能整除 a，或者 a 能被 b 整除，记作 $b|a$．相反，如果不存在适合（1）的整数 q，则称 b 不能整除 a，或者 a 不能被 b 整除，记作 $b\nmid a$．

例如，$1|2$，$3|6$，$7|0$，$2\nmid 5$，$12\nmid 30$.

当 $b|a$ 时，b 称为 a 的因数，a 称为 b 的倍数．a 的正

因数也称为a的约数. 通常将2的倍数称为偶数，其他整数称为奇数.

例如，-2是6的因数，-10是5的倍数，3是-12的约数.

定理 1.1.1 对于整数a以及非零整数b，下列整除关系成立：

(ⅰ) $b|0$;

(ⅱ) $1|a$;

(ⅲ) 当$a\neq 0$时，$a|a$;

(ⅳ) 当$b|a$时，$\lambda b|\lambda' a$，其中λ，$\lambda'\in\{-1, 1\}$.

证 当$a=0$时，令$q=0$，此时(1)对于任何整数b都成立，故得(ⅰ). 当$b=1$时，令$q=a$此时(1)显然成立，故得(ⅱ). 同样，当$a\neq 0$且$b=a$时，令$q=1$，则从(1)可知(ⅲ)成立.

当$b|a$时，存在整数q可使(1)成立. 此时，

$$\lambda' a = (\lambda b)(\lambda\lambda' q),$$

其中$\lambda\lambda' q$是整数，因此(ⅳ)成立. 定理证完.

从定理1.1.1之(ⅰ)可知，零是任何非零整数的倍数，又从定理1中的其他结果可知：当$a\neq 0$时，± 1和$\pm a$都是a的因数. 这些因数称为a的平凡因数. a的非平凡因数称为a的真因数，正的真因数也称为真约数.

另外，从定理1之(ⅳ)可知：当b是a的因数时，a必有约数$|b|$. 因此在讨论某个整数的因数时，往往只要考虑它的约数就足够了.

定理 1.1.2 对于非零整数a, b，如果$b|a$则必有$|b|\leqslant$

$|a|$.特别是当 b 是 a 的真因数时，必有 $1<|b|<|a|$.

证　因为 $b|a$，故从（1）可知

$$|a|=|bq|=|b||q|. \tag{2}$$

由于当 $a\neq 0$ 时，(1) 中的 q 是非零整数，所以 $|q|\geqslant 1$，并且从（2）可得 $|b|\leqslant|a|$.

另外，从 $|b|=1$ 以及 $|b|=|a|$，分别可得 $b=\pm 1$ 以及 $b=\pm a$，它们是 a 的所有平凡因数. 因此当 b 是 a 的真因数时，必有 $1<|b|<|a|$. 定理证完.

根据定理 1.1.2 可知，任何非零整数的不同因数的个数是有限的. 由此还可推知：零是唯一能被任何非零整数整除的整数.

定理 1.1.3　如果 a，b，c 是适合 $b|a$ 的整数，则必有

（ⅰ）当 $c|b$ 时，$c|a$；

（ⅱ）当 $c\neq 0$ 时，$bc|ac$；

（ⅲ）当 $c|b$ 且 $c|a$ 时，$b/c|a/c$；

（ⅳ）当 $a\neq 0$ 时，$a/b|a$.

证　由于 $b|a$，故有整数 q 适合（1）. 当 $c|b$ 时，又有整数 q' 适合 $b=cq'$，将此代入（1）立得　$a=c(qq')$. 由此可知 $c|a$，故得（ⅰ）.

当 $c\neq 0$ 时，在（1）的两边同时乘以 c，可得 $ac=(bc)q$. 因为 $bc\neq 0$，故得（ⅱ）.

当 $c|b$ 且 $c|a$ 时，因为 $c\neq 0$，而且 b/c 和 a/c 都是整数，故从（1）可知 $b/c|a/c$，所以（ⅲ）成立.

另外，由于（1）中的整数 $q=a/b\neq 0$，而且 $a=bq=(a/b)b$，所以 $a/b|a$，所以（ⅳ）成立，定理证完.

定理 1.1.4 如果整数 a_1，…，a_n 以及非零整数 b 适合 $b \mid a_i$（$i=1$，…，n），则对于任何整数 k_1，…，k_n，必有 $b \mid k_1a_1+\cdots+k_na_n$.

证 由于 $b \mid a_i$（$i=1$，…，n），故必有整数 q_1，…，q_n，可使 $a_i=bq_i$（$i=1$，…，n）. 此时

$$k_1a_1+\cdots+k_na_n = k_1bq_1+\cdots+k_nbq_n = b(k_1q_1+\cdots+k_nq_n). \tag{3}$$

由于 $k_1q_1+\cdots+k_nq_n$ 是整数，故从(3)可知 $b \mid k_1a_1+\cdots+k_na_n$. 定理得证.

例 1.1.1 已知整数 a，b，c，d，t 满足 $t \mid (10a-b)$ 以及 $t \mid (10c-d)$. 证明：$t \mid ad-bc$.

证 由于

$$ad-bc = c(10a-b)-a(10c-d), \tag{4}$$

所以当 $t \mid (10a-b)$ 且 $t \mid (10c-d)$ 时，根据定理 1.1.4，从 (4) 可知 $t \mid ad-bc$. 证完.

例 1.1.2 设 m，n 是正整数. 证明：$m^2 \mid (m+1)^n+m(m-1)n-1$.

证 设 $f(m,n)=(m+1)^n+m(m-1)n-1$. 由于

$$f(m,n)=\begin{cases} m^2, & \text{当 } n=1 \text{ 时}, \\ 3m^2, & \text{当 } n=2 \text{ 时}, \end{cases}$$

所以当 $n=1$ 或 2 时，显然有 $m^2 \mid f(m,n)$.

当 $n \geqslant 3$ 时，因为

$$f(m,n)=(m^n+\binom{n}{n-1}m^{n-1}+\cdots+\binom{n}{3}m^3+\binom{n}{2}m^2+$$

$$\binom{n}{1}m+\binom{n}{0})+(m^2n-mn)-1=$$

$$m^n+\binom{n}{n-1}m^{n-1}+\cdots+\binom{n}{3}m^3+(\binom{n}{2}+n)m^2, \tag{5}$$

其中 $\binom{n}{i}$（$i=0$，1，…，$n-1$）都是整数，所以根据定理4，从（5）可知此时 $m^2 \mid f(m,n)$．证完．

习题　1.1

1．证明：个位数是偶数的十进制正整数必为偶数．

2．设正整数 a 可表成十进制整数 $a_n\cdots a_1$，证明：当 $3\mid(a_1+\cdots+a_n)$ 时，必有 $3\mid a$．

3．证明：当 n 是奇数时，$1+2+\cdots+n$ 是 n 的倍数．

4．证明：任何奇数的平方减1必为8的倍数．

5．已知整数 a，b，c，d 适合 $(a-c)\mid(ab+cd)$．证明：$(a-c)\mid(ad+bc)$．

6．设 $f(x)$ 是整系数多项式．证明：如果存在偶数 a 和奇数 b，可使 $f(a)$ 和 $f(x)$ 均为奇数，则方程

$$f(x)=0$$

的根都不是整数．

7．设 m，n 是适合 $n>1$ 的正整数．证明：当且仅当 $n-1\mid m$ 时，$(n-1)^2\mid n^m-1$．

8. 已知 n 个整数 $a_1, \cdots, a_n$ 的和等于零，积等于 n. 证明：n 必是 4 的倍数.

§1.2 素数与合数

全体正整数可按因数个数的多少分成以下互不重复的三类：

第一类 仅有平凡因数 ± 1 的正整数称为单位数，显然单位数仅有 1.

第二类 仅有平凡因数的非单位数，称为素数.

第三类 有真因数的正整数，称为合数.

例如，2，3，5，7 都是素数，4，6，8，9 都是合数.

如果素数 p 是整数 a 的因数，则称 p 是 a 的素因数.

例如，2 是 -6 的因数，而且是它的素因数；6 是 18 的因数，但不是它的素因数.

定理 1.2.1 任何大于 1 的正整数必有素因数.

证 设 a 是大于 1 的正整数，已知 a 本身就是 a 的因数，所以 a 必有大于 1 的因数. 设 d 是其中的最小数. 假如 d 不是素数，则因 $d>1$，所以 d 是合数，此时 d 必有真因数 d_1 适合 $1<d_1<d$. 由于 $d_1 \mid d$ 且 $d \mid a$，故必有 $d_1 \mid a$，这就与有关 d 的假设矛盾. 因此 d 必为素数，即 a 必有素因数 d. 证完.

根据定理 1.2.1 的证明过程可直接得出：

推论 1.2.1 如果 a 是大于 1 的正整数，则 a 的大于 1 的最小约数必为素数.

从推论 1.2.1 可知：当 $a>1$ 时，如果 a 不能被任何小于 a 的素数整除，则 a 必为素数，根据这一思路，古希腊数学家 Eratosthenes 提出了一种求不超过某个正整数 a 的所有素数的方法.

例如，当 $a=20$ 时，首先写出 2 到 20 之间的所有正整数

$$\begin{aligned}&2，3，4，5，6，7，8，9，10，\\&11，12，13，14，15，16，17，18，19，20.\end{aligned}\tag{1}$$

已知（1）中最小的正整数 2 是素数. 在（1）中划去 2 以及 2 的所有倍数，得到

$$\begin{aligned}&\not{2}，3，\not{4}，5，\not{6}，7，\not{8}，9，\not{10}，\\&11，\not{12}，13，\not{14}，15，\not{16}，17，\not{18}，19，\not{20}，\end{aligned}\tag{2}$$

此时，（2）中未被划掉的最小正整数 3 必为素数. 再在（2）中划去 3 以及 3 的所有倍数. 重复上述过程直到将（1）中的数全部划掉. 由此可得不超过 20 的素数依次是 2，3，5，7，11，13，17，19.

将不超过 N 的所有素数依次排出的数表称为 N 以内的素数表，它在数论研究中有着重要的作用. 本书的附表一给出了 6000 以内的素数表. 以上给出素数表的方法称为 Eratosthenes 筛法.

另外，从以下定理可知，对于给定的正整数 a，可以用更为简便的方法来判定它是否是素数.

定理 1.2.2　设 a 是大于 1 的正整数. 如果 a 不能被任何适合 $p\leqslant\sqrt{a}$ 的素数 p 整除，则 a 必为素数.

证 从推论 1.2.1 可知，a 的大于 1 的最小约数 p 是素数. 此时

$$a = pq, \tag{3}$$

其中 q 是正整数. 假如 a 是合数，则 p 必为 a 的真因数，并且从 (3) 可知 q 也是 a 的大于 1 的因数. 因此 $q \geqslant p$，并且从 (3) 可知 $p^2 \leqslant a$，即 $p \leqslant \sqrt{a}$. 由此可知合数 a 必定可以被某个适合 $p \leqslant \sqrt{a}$ 的素数 p 整除，故得定理.

例 1.2.1 证明：101 是素数.

证 由于适合 $p \leqslant \sqrt{101}$ 的素数仅有 2，3，5，7，而且它们都不能整除 101，所以 101 是素数. 证完.

根据定理 1.2.2 可以直接得出：

推论 1.2.2 合数 a 的最小素因数 p 满足 $p \leqslant \sqrt{a}$.

由于已知素数是存在的，而且素数的任何方幂都是合数，所以合数的个数是无限的. 以下定理说明素数的个数也是无限的.

定理 1.2.3 素数的个数是无限的.

证 假如素数的个数是有限的，不妨设 p_1，…，p_k 是所有不同的素数. 设 $a = p_1 \cdots p_k + 1$. 因为 $a > 1$，故从定理 1.2.1 可知 a 必有素因数 p. 此时 $p = p_j$ $(1 \leqslant j \leqslant k)$. 由于 $p_j \mid a$ 且 $p_j \mid p_1 \cdots p_k$，故必有 $p_j \mid a - p_1 \cdots p_k$. 由此可得 $p_j \mid 1$ 这一矛盾. 因此素数的个数是无限的. 定理证完.

例 1.2.2 证明：存在无限多个连续合数.

证 设 a 是大于 1 的正整数，p_1，…，p_k 是所有不超过 a 的素数. 根据定理 1.2.1 可知，对于适合 $1 < r \leqslant a$ 的正整数 r，必有适当的 p_j $(1 \leqslant j \leqslant k)$，可使 $p_j \mid r$. 因为 $p_j \mid$

$p_1\cdots p_k$，故有 $p_j \mid p_1\cdots p_k + r$. 由于 $p_1\cdots p_k + r > p_j$ $(j=1, \cdots, k)$，所以 $p_1\cdots p_k + r$ 必为合数. 因此 $a-1$ 个连续正整数

$$p_1\cdots p_k + r, \quad r = 2, \cdots, a, \tag{4}$$

都是合数. 由于从定理 1.2.3 可知素数的个数无限，所以必有无限多个形如 (4) 的连续合数. 证完.

例 1.2.3　证明：对于正整数 n，$2^n - 1$ 是素数的必要条件是 n 必为素数.

证　因为 $2^1 - 1 = 1$，所以若 $2^n - 1$ 是素数，则必有 $n > 1$.

当 n 是合数时，n 有真约数 d 适合 $1 < d < n$. 此时 $n = dq$，其中 q 是大于 1 的正整数. 此时

$$2^n - 1 = 2^{dq} - 1 = (2^d - 1)(2^{d(q-1)} + \cdots + 2^d + 1),$$

其中 $2^d - 1$ 和 $2^{d(q-1)} + \cdots + 2^d + 1$ 都是大于 1 的正整数，所以 $2^n - 1$ 不是素数. 由此可知 $2^n - 1$ 是素数的必要条件是 n 为素数. 定理证完.

习题　1.2

1. 试用 Eratosthenes 筛法求出不超过 100 的全部素数.

2. 证明：10 519 和 17 357 都是合数.

3. 设 p 是合数 a 的最小素因数. 证明：当 $p > \sqrt[3]{a}$ 时，a/p 必为素数.

4. 设 n 是大于 2 的偶数. 证明：n 位十进制正整数 $10\cdots01$ 必为合数.

5. 设 n 是正整数. 证明：n 位十制正整数 $11\cdots1$ 是素数的必要条件是 n 为素数.

6. 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 是 n 次整系数多项式，其中 $n\geqslant1$，$a_0>0$. 证明：存在无限多个整数 b，使得 $f(b)$ 是合数.

7. 设 p_1，…，p_k 是不超过 n 的所有素数. 证明：$p_1\cdots p_k+1$ 的最小素因数大于 n.

8. 证明：存在无限多个形如 $4a-1$ 的素数，其中 a 是正整数.

§1.3 算术基本定理

本节将证明在小学数学中就曾经提到的算术基本定理，它是初等数论中最基本最重要的定理之一.

定理 1.3.1 任何大于 1 的正整数都可表成素数的乘积.

证 设 a 是大于 1 的正整数. 当 a 是素数时，本定理显然成立. 当 a 是合数时，从推论 1.2.2 可知 a 必有素因数 p_1 适合 $p_1<a$. 此时，

$$a=p_1a_1, \tag{1}$$

其中 a_1 是适合 $1<a_1<a$ 的正整数. 如果 a_1 是素数，则从 (1) 可知本定理成立. 如果 a_1 是合数，则必有素数 p_2 以及适合 $1<a_2<a_1$ 的正整数 a_2，可使