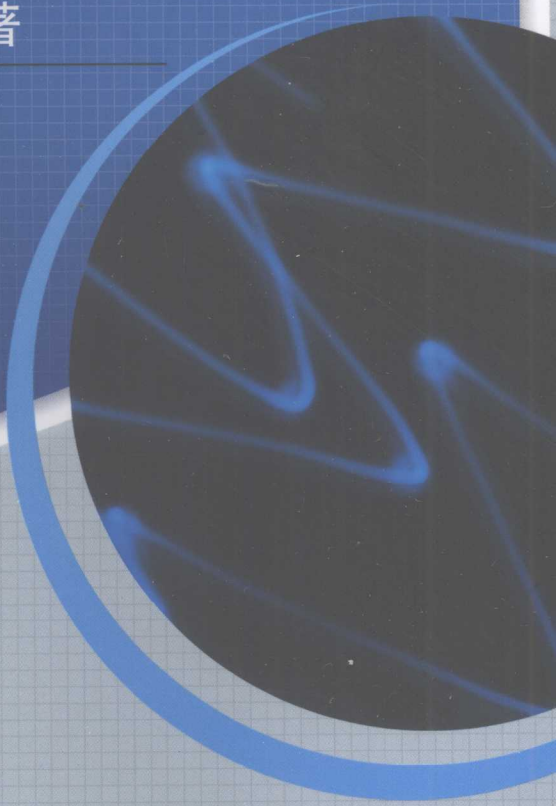
初等数论及其在密码学中的应用与Maple实现

游 林◎著



科学出版社
www.sciencep.com

初等数论及其在密码学中的应用与 Maple 实现

游 林 著

科 学 出 版 社

北 京

内 容 简 介

初等数论是完全以初等的方法研究整数性质的一门很古老的数学分支. 本书介绍了初等数论的基础理论及其在古典密码术与一些公钥密码体制中的应用,同时,还介绍了利用数学软件 Maple 求解初等数论问题. 全书由整除性理论、常用数论函数、同余理论、整数的阶与原根、平方剩余、不定方程理论、初等数论在密码学中的应用等 7 章组成,每章的最后一节介绍如何利用数学软件 Maple 来求解初等数论问题. 同时,在每章的最后都单独配有数量丰富的综合例题、思考题与研究题,以便读者对书中所论述的内容加深理解和掌握,或做进一步的探讨之用.

本书可作为高等院校数学、信息与计算科学等专业的教材或教学参考书,也适用于中学数学老师作为奥林匹克数学竞赛培训或教学的参考教材. 从事密码学、信息安全及通信等专业的工程技术人员也可用本书作为参考资料.

图书在版编目(CIP)数据

初等数论及其在密码学中的应用与 Maple 实现/游林著. —北京:科学出版社,2009

ISBN 978-7-03-025004-9

Ⅰ.初… Ⅱ.游… Ⅲ.①初等数论-应用-密码术②数学-应用软件,Maple Ⅳ.TN918.1 0245

中国版本图书馆 CIP 数据核字(2009)第 118382 号

责任编辑:王志欣 孙 芳 于宏丽/责任校对:陈玉凤

责任印制:赵 博/封面设计:耕者设计工作室

科学出版社 出版

北京东黄城根北街 16 号

邮政编码:100717

http://www.sciencep.com

源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2009 年 7 月第 一 版 开本:B5(720×1000)

2009 年 7 月第一次印刷 印张:14

印数:1—2 500 字数:275 000

定价:40.00 元

(如有印装质量问题,我社负责调换〈路通〉)

前　言

在RSA密码出现之前，可以说，大多数人都认为初等数论完全是纯理论性的数学学科. 但是，自RSA与ElGamal等公钥密码体制出现以后，人们逐渐认识到初等数学的理论知识在密码学、信息安全及通信等领域具有重要的实际应用价值.

本书以全新的方式介绍了整数的整除性、常用数论函数、同余理论、整数的阶与原根、平方剩余及不定方程理论等初等数论的基本内容. 同时，在本书的最后一章介绍了这些初等数论知识在密码学中的一些应用.

本书主要有以下4个方面的特点.

(1) 以极丰富的例子诠释了初等数论问题的若干解题技巧与方法，其中，许多例子都来源于奥林匹克数学竞赛题.

(2) 除各节配有适量习题外，每章还配有一定数量的研究题及思考题，这些研究题与思考题不仅适合相关专业的本科生作为毕业论文的参考选题，而且也适合对初等数论有浓厚兴趣的读者做研究尝试与探讨.

(3) 介绍了初等数论的理论知识在古典密码术及RSA、ElGamal、Rabin等现代公钥密码算法中的应用.

(4) 借助数学软件Maple，给出了若干初等数论问题求解的算法程序.

数论这门古老的科学如今在密码学中发挥着越来越重要的作用，它广泛应用于古典密码术、分组密码、流密码及公钥密码算法或各种密码协议中. 本书在第7章以较简洁的形式介绍了初等数论在Caesar密码、Vigenère密码和Hill密码等比较经典的密码术，以及在RSA、ElGamal、Rabin和MH背包等公钥密码系统中的应用. 其实，从古典密码术到现代密码学的各个分支，处处都显现着初等数论这门基础理论学科的踪影. 此外，初等数论也是与代数学、组合数学、图论、计算机科学、通信等学科密切相关的一门学科.

本书的编写与出版得到杭州电子科技大学出版基金、国家自然科学基金项目(项目编号：60763009)和教育部科学技术研究重点项目(项目编号：207089)的资助，特此致谢.

由于作者水平有限，书中难免存在不妥之处，敬请读者批评指正.

作　者

2009年2月

目　录

第 1 章　整除性理论

本章介绍有关整数的基本概念与性质，主要包括整数的整除性、奇偶性，以及依据整除性而产生的质数与合数、最大公约数与最小公倍数的相关概念与性质. 这里借助自然数集的最小数原理，非常简洁地证明了带余除法、最大公约数及最小公倍数的有关定理.

1.1　整除及带余除法

自然数和它的相反数，以及零均称为整数.

定义 1.1　设 a 与 b 是任意两个整数，且 $b\neq 0$，若存在整数 q 使得 $a=bq$，则称 b 整除 a 或 a 能被 b 整除，记作 $b\mid a$；否则，称 b 不能整除 a 或 a 不能被 b 整除，此时记作 $b\nmid a$.

如果 $b\mid a$，则称 b 是 a 的约数或因数，a 是 b 的倍数. 若 b 是 a 的约数，且 $b\neq\pm 1$，$\pm a$，则称 b 是 a 的真约数或真因数.

定理 1.1　设 a,b,c,m,n 是整数，则有

(1) $a\mid a$.

(2) 如果 $a\mid b$，且 $b\mid a$，则 $a=\pm b$.

(3) 如果 $a\mid b$，且 $b\mid c$，则 $a\mid c$.

(4) 如果 $a\mid b$，且 $a\mid c$，则 $a\mid(mb+nc)$.

定理 1.2(带余除法定理)　对任意两整数 a 与 b，且 $b\neq 0$，存在唯一的一对整数 q 与 r，使得

$$a=qb+r,\quad 0\leqslant r<|b|$$

q 称为 a 被 b 除得到的商，r 称为 a 被 b 除得到的余数.

借助自然数集的最小数原理来证明上述定理.

自然数集的最小数原理　若 S 是广义自然数集的任一非空子集，则存在 $a\in S$，使得 $\forall x\in S$，有 $a\leqslant x$ 成立，此 a 称为 S 的最小数(注：广义自然数集是指包含正整数、零及正无穷大的集合).

定理 1.2 的证明　设 $S=\{a-kb\mid k\in\mathbb{Z},\ a-kb\geqslant 0\}$，则 S 是广义自然数集的非空子集. 于是，存在 S 的最小数 r，即存在 $q\in\mathbb{Z}$，使 $r=a-qb$，亦即 $a=qb+r$. 下面证明 $0\leqslant r<|b|$，且 q 与 r 是唯一的.

若 $r>|b|$，则 $0<r-|b|=a-(q\pm 1)b\in S$，且 $r>r-|b|$，这与 r 是 S 的最小

数矛盾.

若存在两对整数 q_1 与 r_1 及 q_2 与 r_2，使得

$$a = q_1 b + r_1, \quad a = q_2 b + r_2, \quad 0 \leqslant r_1, r_2 < |b|$$

则

$$q_1 b + r_1 = q_2 b + r_2$$

即

$$(q_1 - q_2) b = r_2 - r_1$$

若 $q_1 \neq q_2$，则 $|r_2 - r_1| \geqslant |b|$，这与 $0 \leqslant r_1, r_2 < |b| - 1$ 矛盾，故 $q_1 = q_2$，于是 $r_1 = r_2$.

显然，a 被 b 整除的充分必要条件是其余数为 0.

例 1.1 设 $a = -89, b = 13$，则 $q = -7, r = 2$.

例 1.2 4 个连续的整数之积必为 4 的倍数，为什么？（请读者自证）

例 1.3 任意 1000 个整数中，必有两个整数之差能被 999 整除.

证 设 $a_1, a_2, \cdots, a_{1000}$ 为任意给定的 1000 个整数，由带余除法定理可知，存在 1000 对整数 q_i, r_i，使得

$$a_i = 999 q_i + r_i, \quad 0 \leqslant r_i < 999, \quad i = 1, 2, \cdots, 1000$$

由于每个 r_i 是 0～998 这 999 个整数中的一个，故至少有某两个 r_k 与 r_l 相同，于是，$a_k - a_l = 999(q_k - q_l)$，即有 $999 \mid (a_k - a_l)$.

例 1.4 任意平方数必为 9 的倍数或被 3 除余 1，为什么？（请读者自证）

练 习 1.1

1. 证明对任意整数 n，有 $6 \mid n(n+1)(2n+1)$.

2. 证明对任意整数 x, y，必有

(1) $8 \nmid (x^2 - y^2 - 2)$.

(2) 若 $2 \nmid xy$，则 $x^2 + y^2$ 为非完全平方数.

(3) 若 $3 \nmid xy$，则 $x^2 + y^2$ 为非完全平方数.

3. 如果 $2a + 3b$ 与 $9a + 5b$ 中有一个数能被 17 整除，那么，另一数也一定能被 17 整除.

4. 试将数 232323 用 3 及 23 进制数表示（参见第 1 章综合例题中例 1）.

5. 证明 $7 \mid \overline{a00a}$，其中，$\overline{a00a}$ 表示一个四位数 $a \in \{1, 2, \cdots, 9\}$.

6. 若 a, b 是任意两个整数且 $b \neq 0$，证明存在两个整数 s, t，使得 $a = bs + t$，$|t| \leqslant \frac{|b|}{2}$ 成立，并且当 b 是奇数时，s, t 是唯一的；当 b 是偶数时，有何结论？

1.2　整数的奇偶性

奇数与偶数的定义　能被 2 整除的整数称为偶数；不能被 2 整除的整数称为奇数.

奇数与偶数具有如下基本性质.

(1) 两个整数的和与差具有相同的奇偶性.

(2) 奇数的平方被 4 除余 1，被 8 除也余 1，而偶数的平方能被 4 整除.

(3) 如果若干个整数的乘积是奇数，则每个因数都是奇数；如果若干个整数的乘积是偶数，则至少有一个因数是偶数.

(4) 奇数的平方的十位数字是偶数；若一个平方数的个位数字是零，则十位数字也是零；个位数字是 5，则十位数字是 2；个位数字是 4，则十位数字是偶数；个位数字是 6，则十位数字一定是奇数.

(5) 正整数 n 是完全平方数的充分必要条件是 n 有奇数个正约数；n 不是完全平方数的充分必要条件是 n 有偶数个正约数(约数包括 1 与 n 本身).

以上性质均不难证明，但若运用得当，则能解决许多问题，甚至包括一些看似“无从下手”的难题.

例 1.5　是否存在 10 个正奇数的倒数之和等于 1.

证　若存在 10 个正奇数 $a_1, a_2, \cdots, a_{10}$，其倒数之和为

$$\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_{10}}=1$$

则

$$a_2a_3\cdots a_{10}+a_1a_3\cdots a_{10}+\cdots+a_1a_2\cdots a_9=a_1a_2\cdots a_{10}$$

由于上面的等式左边共 10 个和项，每个和项是奇数之积，故左边是偶数；而右边是奇数之积，故右边为奇数，矛盾.

例 1.6　证明改变一个自然数各位数码的顺序后得到的数与原数之和不能等于 $\underbrace{99\cdots9}_{2009}$.

证　若新数与原数之和为 $\underbrace{99\cdots9}_{2009}$，则原数是一个 2009 位数，设 $a_1, a_2, \cdots, a_{2009}$ 是原数各数位的数字，而 $a_1', a_2', \cdots, a_{2009}'$ 是改变顺序后新数的各数位的数字，则有

$$a_i+a_i'=9,\quad i=1,2,\cdots,2009$$

且

$$a_1+a_2+\cdots+a_{2009}=a_1'+a_2'+\cdots+a_{2009}'$$

于是

$$2(a_1+a_2+\cdots+a_{2009})=9\times2009$$

上式左边是偶数，右边是奇数，矛盾.

例 1.7 设 a,b,c 均为奇数，证明方程 $ax^2+bx+c=0$ 没有有理根.

证 设此方程有有理根，则其判别式必为完全平方数，令

$$b^2-4ac=m^2 \tag{1.2.1}$$

由 a,b,c 均为奇数可得式(1.2.1)左边是奇数，因此，m 也是奇数. 由式(1.2.1)得

$$(b+m)(b-m)=4ac \tag{1.2.2}$$

因 b 与 m 均为奇数，故可设

$$\begin{cases} b+m=2l \\ b-m=2k \end{cases} \tag{1.2.3}$$

代入式(1.2.2)得 $kl=ac$. 因为 a,c 均是奇数，所以，k,l 均是奇数，于是由式(1.2.3)得 $b=k+l$ 是偶数，这与 b 为奇数矛盾，所以方程无有理根.

例 1.8 在广场上有 m(奇数)个学生面向南方排成一行，命令其中 n(偶数)个学生向后转，称作一次“反向运动”. 证明无论做多少次“反向运动”(转向后的学生允许再转动)，都不可能使所有的学生全部面向北方.

证 假设做 k 次“反向运动”后，可使全体学生面向北方，又设各学生“向后转”的次数分别为 $x_1,\cdots,x_m$，而对每个学生来说，从面向南方变为面向北方必须经过奇数次“向后转”，即 $x_1,\cdots,x_m$ 均为奇数，又 m 为奇数，所以，$x_1+x_2+\cdots+x_m$ 是奇数. 另外，每次“反向运动”均是 n 个学生的“向后转”，所以，k 次“反向运动”所做的“向后转”总次数应为 kn，故有 $x_1+x_2+\cdots+x_m=kn$，但该等式左边是奇数，而右边是偶数，矛盾.

由以上可以看到，用到整数奇偶性证明的 4 个例题均采用了反证法.

练 习 1.2

1. 证明空间不可能有这样的多面体存在，它有奇数个面，而每个面都有奇数条边.

2. 4×4 的方格纸上填着 1,9,9,8 4 个数字，如表 1.1 所示，问是否可能在余下的方格内各填入一整数，使得方格纸上的每一行和每一列都构成等差数列.

表 1.1

	9		
1			
			9
		8	

3. 已知多项式 x^3+bx^2+cx+d 的系数均为整数，且 $bd+cd$ 是奇数，证明此多项式不可能分解成两个整系数多项式之积.

4. 将表 1.2 中任何一行或一列做全部变号操作，问可否经过若干次这样的操作使表 1.2 变为表 1.3?

表 1.2

+	+	−
+	+	−
−	−	+

表 1.3

−	−	+
+	−	−
−	−	+

5. 若 a 是奇数，且 $3\nmid a$，求证 $24\mid(a^2-1)$.

6. 设 p,q 是自然数，条件甲：p^3-q^3 是偶数；条件乙：$p+q$ 是偶数. 那么，下面哪个成立？

(1) 甲是乙的充分条件而非必要条件.

(2) 甲是乙的必要条件而非充分条件.

(3) 甲是乙的充分必要条件.

(4) 甲既不是乙的充分条件，也不是乙的必要条件.

7. 设共有 97 人参加某次学术讨论会，已知每人至少和 3 位与会者讨论问题，证明至少有一人起码和 4 人讨论过问题.

1.3　最大公约数与最小公倍数

本节利用带余除法，引入辗转相除法，并由此介绍最大公约数与最小公倍数.

定义 1.2　设 $a_1,a_2,\cdots,a_n$ 是 $n(n\geqslant 2)$ 个整数，若整数 d 是每个 $a_i(i=1,2,\cdots,n)$ 的因数，则称 d 是 $a_1,a_2,\cdots,a_n$ 的一个公因数.

定义 1.3　整数 $a_1,a_2,\cdots,a_n$ 的公因数中的最大者称为它们的最大公因数，记作 $(a_1,a_2,\cdots,a_n)$ 或 $\gcd(a_1,a_2,\cdots,a_n)$.

显然，若 $a_1,a_2,\cdots,a_n$ 中至少有一个非零，比如说 $a_i\neq 0$，则 $(a_1,a_2,\cdots,a_n)\leqslant|a_i|$，因而此时 $a_1,a_2,\cdots,a_n$ 的最大公因数存在.

定义 1.4　如果 $(a_1,a_2,\cdots,a_n)=1$，则称 $a_1,a_2,\cdots,a_n$ 互素(或互质)；如果 $i\neq j$ 时有 $(a_i,a_j)=1$，则称 $a_1,a_2,\cdots,a_n$ 两两互素(或互质). 显然，若后者成立，则前者也成立，反之则不然. 如 $(3,5,10)=1$，但 $(5,10)\neq 1$.

性质定理 1.1　设 $a_1,a_2,\cdots,a_n$ 是 n 个不全为零的整数，则有

(1) $(a_1,a_2,\cdots,a_n)=(a_{i_1},a_{i_2},\cdots,a_{i_n})$，其中，$i_1,i_2,\cdots,i_n$ 是 $1,2,\cdots,n$ 的一个排列.

(2) $(a_1,a_2,\cdots,a_n)=(|a_1|,|a_2|,\cdots,|a_n|)$.

(3) 若 $a_1,a_2,\cdots,a_n$ 中有一个为 1，则它们互素.

(4) 若 $a_{j_1},a_{j_2},\cdots,a_{j_s}$ 是 $a_1,a_2,\cdots,a_n$ 中全不为零的整数，则

$$(a_1,a_2,\cdots,a_n)=(|a_{j_1}|,|a_{j_2}|,\cdots,|a_{j_s}|)$$

以上性质的证明均显而易见.

定理 1.3 如果 $a=bq+r$，则有$(a,b)=(b,r)$.

证 设$(a,b)=d$，$(b,r)=d_1$，则一方面，$d\mid a$ 且$d\mid b$，于是，由 $a=bq+r$ 得 $d\mid r$，从而

$$d \mid d_1 \tag{1.3.1}$$

另一方面，$d_1\mid b$ 且$d_1\mid r$，以及 $a=bq+r$ 得$d_1\mid a$，从而

$$d_1 \mid d \tag{1.3.2}$$

综合式(1.3.1)与式(1.3.2)即得 $d=d_1$.

辗转相除法 设 a,b 是任意两个正整数，多次利用带余除法，可得下列等式：

$$\begin{cases} a = bq_1 + r_1, & 0 < r_1 < b \\ b = r_1q_2 + r_2, & 0 < r_2 < r_1 \\ \quad\vdots & \quad\vdots \\ r_{k-2} = r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1} \\ r_{k-1} = r_kq_{k+1} + r_{k+1}, & r_{k+1} = 0 \end{cases} \tag{1.3.3}$$

由于 b 是有限正整数，且 $b>r_1>r_2>\cdots\geqslant 0$，所以，式(1.3.3)中的正整数 k 是存在的.

辗转相除法式(1.3.3)是我国古代筹算家的一大成就，西方 Euclid(欧几里得)也推得该法则，所以又称为 Euclid 算法.

定理 1.4 设 a,b 是任意给定的两个整数，则由式(1.3.3)可得$(a,b)=r_k$.

证明 反复利用定理 1.3，有

$$(a,b) = (b,r_1) = (r_1,r_2) = \cdots = (r_{k-1},r_k) = (r_k,0) = r_k$$

例 1.9 设 $a=-1895$，$b=1573$，求$(a,b)=?$

解 $(a,b)=(-1895,1573)=(1859,1573)$.

反复利用定理 1.3，如下面的辗转相除计算图(如图 1.1 所示). 再由定理 1.4，即得

$$(a,b) = (1859,1573) = 143.$$

	1859	1573	$1=q_1$
	1573	1430	
$q_2=5$	$286=r_1$	$143=r_2$	$2=q_3$
	286		
	$0=r_3$		

图 1.1

定理 1.5 a 与 b 的任一公约数是(a,b)的约数.

证 设 d 是a 与b 的任一公约数，则由式(1.3.3)知，d 是b 与r_1 的公约数，进而知 d 是r_1 与 r_2 的公约数，如此继续，可得 d 是r_k 的约数.

定理 1.6(Bezout 恒等式[①])　若$(a_1,\cdots,a_n)=d$,则必存在整数 $k_i(i=1,\cdots,n)$,使得

$$k_1a_1+k_2a_2+\cdots+k_na_n=d$$

证　令 $S=\{s\mid s=x_1a_1+x_2a_2+\cdots+x_na_n,x_i\in\mathbb{Z},s>0\}$,则由 $a_1,\cdots,a_n$ 的最大公约数存在知,它们不全为零. 不妨设 $a_1\neq0$. 取 x_1 使 $x_1a_1>0$,再取 $x_2=x_3=\cdots=x_n=0$,则 $s=x_1a_1\in S$,因此,S 是自然数集的非空子集,从而由(自然数集)最小数原理知 S 有最小数,设为 d,则存在 $k_1,\cdots,k_n$,使得 $k_1a_1+k_2a_2+\cdots+k_na_n=d$,且可以证 d 为 $a_1,\cdots,a_n$ 的最大公因数.

首先,证 d 为 $a_1,\cdots,a_n$ 的公约数. 若 $a_1\neq0$,由带余除法定理知,存在 q 与 r 使得 $a_1=dq+r$,其中,$0\leqslant r<d$. 于是,

$$r=a_1-dq=(1-qk_1)a_1-qk_2a_2-\cdots-qk_na_n$$

若 $r\neq0$,则 $r\in S$ 且 $0\leqslant r<d$,这与 d 为 S 的最小元矛盾,从而 $r=0$,即有 $a_1=dq$,亦即 d 为 a_1 的公约数. 同理可证,d 为其他 a_i 的公约数.

其次,若 c 为 $a_1,\cdots,a_n$ 的任一公约数,那么,由 $k_1a_1+k_2a_2+\cdots+k_na_n=d$,得 c 为 d 的约数,从而有 $c\leqslant d$. 因此,由定义知 d 为 $a_1,\cdots,a_n$ 的最大公约数.

Bezout 恒等式又可称为扩展 Euclid 等式,其相应的算法则称为扩展 Euclid 算法(第 1.6 节).

推论 1.1　$(a_1,a_2,\cdots,a_n)=1$ 的充分必要条件是存在 $t_1,t_2,\cdots,t_n\in\mathbb{Z}$,使得

$$t_1a_1+t_2a_2+\cdots+t_na_n=1$$

定理 1.7　设 $a_1,a_2,\cdots,a_n$ 是任意 n 个整数,且$(a_1,a_2)=d_2,(a_2,a_3)=d_3,\cdots,(a_{n-1},a_n)=d_n$,那么,$(a_1,a_2,\cdots,a_n)=d_n$.

证　设$(a_1,a_2,\cdots,a_n)=d$,则 $d\mid a_i(i=1,2,\cdots,n)$,于是,$d\mid d_2$且 $d\mid a_3\Rightarrow d\mid d_3$ 且 $d\mid a_4\Rightarrow\cdots\Rightarrow d\mid d_{n-1}$且 $d\mid a_n\Rightarrow d\mid d_n$.

另外,由$(a_{n-1},a_n)=d_n$ 知,$d_n\mid a_n$且 $d_n\mid d_{n-1}$,又由$(d_{n-2},a_{n-1})=d_{n-1}$得,$d_{n-1}\mid d_{n-2}$且 $d_{n-1}\mid a_{n-1}$. 于是,$d_n\mid a_n,d_n\mid a_{n-1}$且 $d_n\mid d_{n-2}$,依此类推,最后可得 $d_n\mid a_n,d_n\mid a_{n-1},\cdots,d_n\mid a_1$,$d_n$ 是 $a_1,a_2,\cdots,a_n$ 的一个公因数,故有 $d_n\mid d$,从而 $d=d_n$.

性质定理 1.2

(1) 如果$(a,b)=1$,则$(ac,b)=(c,b)$.

(2) 如果$(a,b)=1$,且 $b\mid ac$,则 $b\mid c$.

(3) 如果$(a,c)=1$,且$(c,b)=1$,则$(ab,c)=1$.

(4) 如果 $c(c>0)$ 是 a 与 b 的公约数,则 $\left(\frac{a}{c},\frac{b}{c}\right)=\frac{(a,b)}{c}$,进而有

① Bezout(1730—1783),法国数学家(全名为 Etienne Bezout).

$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$.

以上性质均易证明(请读者自证). 以下讨论最小公倍数.

定义 1.5 设 $a_1,a_2,\cdots,a_n$ 是 $n(n>2)$个全不为零的整数.

(1) 如果 d 是每个 a_i 的倍数,则称 d 是这 n 个数的公倍数.

(2) $a_1,a_2,\cdots,a_n$ 的一切公倍数中的最小正数称为它们的最小公倍数,记为 $[a_1,a_2,\cdots,a_n]$.

由于任意正数均不是 0 的倍数,所以,任意包含 0 的一组整数其最小公倍数均不存在.

性质定理 1.3 设 $a_1,a_2,\cdots,a_n$ 是 n 个全不为零的整数,则有

(1) $0<[a_1,a_2,\cdots,a_n]\leqslant|a_1a_2\cdots a_n|$.

(2) $[a_1,a_2,\cdots,a_n]=[|a_1|,|a_2|,\cdots,|a_n|]$.

(3) $[a_1k,a_2k,\cdots,a_nk]=[a_1,a_2,\cdots,a_n]|k|$.

以上性质请读者自证.

定理 1.8 设 a,b 是任意两个全不为零的整数,则有

(1) 若 m 是 a,b 的任意一公倍数,那么,$[a,b]|m$.

(2) $[a,b](a,b)=ab(ab>0)$.

(3) $\left(\frac{m}{a},\frac{m}{b}\right)=\frac{m}{[a,b]}$.

证 因 m 是 a,b 的公倍数,故有 $k,s\in\mathbb{Z}$,使得

$$m=ak=bs$$

令 $a=(a,b)a_1,b=(a,b)b_1$,则由上式可得

$$a_1k=b_1s,\quad \text{其中},(a_1,b_1)=1$$

于是,由性质定理 1.2 可得 $a_1|s$. 设 $s=a_1t$,则

$$m=bs=ba_1t=\frac{ab}{(a,b)}t \tag{1.3.4}$$

显然,a 与 b 的任意公倍数均具有式(1.3.4)的形式. 因此,当 $t=1$ 时,$m=\frac{ab}{(a,b)}$是 a,b 的最小的正公倍数,即有$[a,b]=\frac{ab}{(a,b)}$,亦即(2)成立.

再由式(1.3.4)得

$$m=[a,b]t \tag{1.3.5}$$

从而(1)成立.

而

$$\left(\frac{m}{a},\frac{m}{b}\right)=\left(\frac{b}{(a,b)}t,\frac{a}{(a,b)}t\right)\qquad\text{(根据式(1.3.4))}$$

$$=(b_1t,a_1t)=(b_1,a_1)t$$

$$= t = \frac{m}{[a,b]} \qquad \text{(根据式(1.3.5))}$$

亦即(3)成立.

类似于定理 1.7,有以下定理.

定理 1.9　设 $a_1,a_2,\cdots,a_n$ 是 n 个全不为零的整数,$[a_1,a_2]=m_2$,$[m_2,a_3]=m_3,\cdots,[m_{n-1},a_n]=m_n$,则有 $[a_1,a_2,\cdots,a_n]=m_n$.

证　设$[a_1,a_2,\cdots,a_n]=m$,则 m 是 $a_1,a_2,\cdots,a_n$ 的倍数,由定理 1.8 知,m 是 m_2 的倍数. 即有 m 是 m_2 与 a_3 的倍数,再由定理 1.8 知,m 是 m_3 的倍数,如此继续,可得 m 是 m_n 的倍数.

另外,由$[m_{n-1},a_n]=m_n$ 知,m_n 是 a_n 与 m_{n-1}的倍数,而 m_{n-1}又是 a_{n-1}与 m_{n-2} 的倍数,于是,m_n 是 a_n,a_{n-1}及 m_{n-2}的倍数,如此继续,可得 m_n 是 $a_n,a_{n-1},\cdots,a_2,a_1$ 的倍数. 因此,由定理 1.8 知,m_n 是 m 的倍数,综上得知 $m_n=m$.

例 1.10　(1) 求$[136,221,391]=?$

(2) 求证 $(a+b)[a,b]=b[a,a+b]$.

解　(1) $[136,221,391]=[[136,221],391]=\left[\frac{136\times221}{17},391\right]=[1768,391]$

$$=\frac{1768\times391}{17}=40664\text{(其中因为(136,221)=17)}$$

(2) $(a+b)[a,b]=(a+b)\frac{ab}{(a,b)}=(a+b)\frac{ab}{(a,a+b)}$(为什么?)

$$=b\,\frac{a(a+b)}{(a,a+b)}=b[a,a+b]$$

例 1.11　设 $a>1,m,n$ 均是正整数,试证$(a^m-1,a^n-1)=a^{(m,n)}-1$.

证法一　设$(m,n)=d$,则 $d\mid m,d\mid n$. 于是,有$(a^d-1)\mid(a^m-1),(a^d-1)\mid(a^n-1)$.

如果 $h(a)$为 a^m-1 与 a^n-1 的任一公因式,而 α 为 $h(a)$任一根,则 $\alpha^m=1$ 且 $\alpha^n=1$;因为$(m,n)=d$,故存在 $s,t\in\mathbb{Z}$,使 $ms+nt=d$,于是

$$\alpha^d=\alpha^{ms+nt}=(\alpha^m)^s(\alpha^n)^t=1$$

这说明 α 也是a^d-1 的根,又 $h(a)$无重根,故 $h(a)\mid a^d-1$,从而

$$(a^m-1,a^n-1)=a^{(m,n)}-1$$

证法二　当 $m=n$ 时,结论显然成立.

设 $m>n$ 且$m=qn+r,0\leqslant r<n$,则有

$$a^m-1=(a^n-1)(a^{m-n}+a^{m-2n}+\cdots+a^{m-qn})+a^r-1$$

于是,由定理 1.3 得

$$(a^m-1,a^n-1)=(a^n-1,a^r-1) \qquad (1.3.6)$$

如果 $r=0$,则

$$(a^m-1,a^n-1)=(a^n-1,0)=a^n-1=a^{(m,n)}-1$$

即结论成立.

若 $r\neq 0$,不妨设

$$\begin{aligned} n&=q_1r+r_1, \quad 0<r_1<r\\ r&=q_2r_1+r_2, \quad 0<r_2<r_1\\ &\vdots\\ r_{k-2}&=q_kr_{k-1}+r_k, 0<r_k<r_{k-1}\\ r_{k-1}&=q_{k+1}r_k \end{aligned}$$

于是,$(m,n)=(n,r)=r_k$ 且类似于式(1.3.6)的推导可得

$$(a^n-1,a^r-1)=(a^r-1,a^{r_1}-1)=\cdots=a^{r_k}-1$$

因此

$$(a^n-1,a^r-1)=(a^r-1,a^{r_1}-1)=\cdots=a^{r_k}-1=a^{(m,n)}-1$$

例 1.12 设 $m>0,n>0$ 且 m 是奇数,试证$(2^m-1,2^n+1)=1$.

证 设$(2^m-1,2^n+1)=d$,则有 $2^m=sd+1$ 及 $2^n=td-1$,于是

$$2^{mn}=(sd+1)^n=kd+1, \quad 2^{mn}=(td-1)^m=ld-1$$

从而$(l-k)d=2$,因此,$d\mid 2$,即有 $d=1$ 或 2. 但 2^m-1 是奇数,所以,$d=1$.

练 习 1.3

1. 对给定正整数 a,b,c,证明

(1) 如果 $a\mid b$,那么,$a\mid bc$.

(2) 如果 $a\mid b$且$a\mid c$,那么,$a^2\mid bc$.

(3) $a\mid b$当且仅当$ac\mid bc$,其中,$c\neq 0$.

2. 对于任意的正整数 a,则三个整数 $a,a+2,a+4$ 中必有一个能被 3 整除.

3. 对于任意的正整数 a,证明 $2\mid a(a+1),3\mid a(a+1)(a+2)$.

4. 对于任意的正整数 n 和任意的整数 a,证明$(a,a+n)\mid n$,因此,$(a,a+1)=1$.

5. 设 n 是正整数,证明$[a^n,b^n]=[a,b]^n$.

6. 证明$[a_1,a_2,\cdots,a_k,a_{k+1},\cdots,a_n]=[[a_1,a_2,\cdots,a_k],[a_{k+1},\cdots,a_n]]$.

7. 设 m 是正整数 $a_1,a_2,\cdots,a_n$ 的正公倍数,证明

(1) $\left(\dfrac{m}{a_1},\dfrac{m}{a_2},\cdots,\dfrac{m}{a_n}\right)=\dfrac{m}{[a_1,\cdots,a_n]}$.

(2) $\left[\dfrac{m}{a_1},\dfrac{m}{a_2},\cdots,\dfrac{m}{a_n}\right]=\dfrac{m}{(a_1,\cdots,a_n)}$.

8. 证明下列结论.

(1) 如果 a 是奇数,那么,$24\mid a(a^2-1)$.

(2) 如果 a,b 都是奇数，那么，$a\mid(a^2-b^2)$.

(3) 对于任意的整数 a，都有 $360\mid a^2(a^2-1)(a^2-4)$.

1.4　质数与合数

可以将整数分成两类：奇数类与偶数类. 当讨论正整数时，也可以将大于 1 的正整数分为两类，对于任何一个正整数 a，它至少有两个正约数，即 1 与 a，称为 a 的当然约数. 有些正整数只有这两个当然约数，如 3,5,7 等，而另一些正整数则还有其他正约数，如 6，还有约数 2 与 3，这类约数称为非当然约数或真约数.

定义 1.6　设 a 是一个大于 1 的正整数，如果 a 只有当然约数，则称 a 为质数或素数；若 a 有真约数，则称 a 为合数.

于是，正整数 $=\{1\}\cup$ 质数集 $\cup$ 合数集.

定理 1.10　设 a 是任一大于 1 的整数，则 a 的最小真因数 q 一定是质数，并且当 a 是合数时，有

$$q\leqslant\sqrt{a}$$

证　如果 q 非质数，则 q 有真约数 p，且 $1<p<q$. 因 q 为 a 的约数，故 p 亦为 a 的真因数，且小于 q，这与 q 为 a 的最小真因数矛盾，因此，q 为质数.

当 a 为合数时，设 $a=qa_1$，因 q 为 a 的最小真因数，故 $a_1\geqslant q$，从而 $a=qa_1\geqslant q^2$，即有

$$q\leqslant\sqrt{a}$$

下面介绍找任一大于 1 的整数内的质数的 Eratosthenes(埃拉托色尼，公元前 276—前 194)筛法.

例 1.13　找出 48 以内的质数.

解　写出 1～48 的所有整数如下：

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

先划去 1，然后依次划去所有满足 $p\leqslant\sqrt{48}<7$ 的素数 p 的倍数，即划去 2,3 及 5 的倍数，留下的数即是 48 以内的所有质数. 该方法称为 Eratosthenes 筛法，简称埃氏筛法.

性质定理 1.4　设 p 是任一质数，则有

(1) 对任一整数 a，有 $(a,p)=1$ 或 $p\mid a$.

(2) 如果 $p\mid ab$，则 $p\mid a$ 或 $p\mid b$.

(3) 如果 $p\mid a_1a_2\cdots a_n$ 则存在 i，使 $p\mid a_i$.