

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

(O-3595.0101)

初等数论及其在密码学中的 应用与Maple实现

科学出版社

联系电话：010-64006909

E-mail:gcjs@mail.sciencep.com

销售分类建议：数学

ISBN 978-7-03-025004-9



9 787030 250049 >

定价：40.00 元

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论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

前言

第 1 章 整除性理论	1
1.1 整除及带余除法	1
1.2 整数的奇偶性	3
1.3 最大公约数与最小公倍数	5
1.4 质数与合数	11
1.5 整数的分解——算术基本定理	14
1.6 利用 Maple 求解整除性问题	19
第 1 章综合例题	22
思考题、研究题一	27
第 2 章 常用数论函数	30
2.1 Gauss 函数 $[x]$	30
2.2 Euler 函数	39
2.3 积性函数	48
2.4 利用 Maple 求常用数论函数的值	56
第 2 章综合例题	59
思考题、研究题二	65
第 3 章 同余理论	68
3.1 同余的定义及性质	68
3.2 同余类与剩余类	73
3.3 同余理论中的几个著名定理	79
3.4 一次同余方程	87
3.5 一次同余方程组与孙子定理	92
3.6 素数模的高次同余方程	98
3.7 利用 Maple 计算同余式与求解同余方程	102
第 3 章综合例题	105
思考题、研究题三	110
第 4 章 整数的阶与原根	112
4.1 整数的阶及其性质	112
4.2 原根的存在条件	115

4.3	原根的个数及求法	119
4.4	指数及 k 次剩余	121
4.5	利用 Maple 计算关于整数模的阶与原根	124
	第 4 章综合例题	126
	思考题、研究题四	130
第 5 章	平方剩余	132
5.1	二次剩余	132
5.2	Legendre 符号	135
5.3	Jacobi 符号	142
5.4	利用 Maple 计算 Legendre 符号与 Jacobi 符号	146
	第 5 章综合例题	149
	思考题、研究题五	156
第 6 章	不定方程理论	158
6.1	一次不定方程	158
6.2	整数的平方和表示	161
6.3	整数表示为多个整数的平方和	166
6.4	勾股不定方程 $x^2 + y^2 = z^2$	169
6.5	Fermat 最后定理简介	173
6.6	用 Maple 解不定方程	175
	第 6 章综合例题	180
	思考题、研究题六	184
第 7 章	初等数论在密码学中的应用	186
7.1	古典密码术	186
7.2	RSA 公钥密码体制	189
7.3	ElGamal 公钥密码系统	195
7.4	MH 背包公钥密码系统	202
7.5	Rabin 公钥加密系统	205
	第 7 章综合例题	209
	思考题、研究题七	216
参考文献	218

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 $b|a$;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 $b|a$,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) $a|a$.
- (2) 如果 $a|b$,且 $b|a$,则 $a = \pm b$.
- (3) 如果 $a|b$,且 $b|c$,则 $a|c$.
- (4) 如果 $a|b$,且 $a|c$,则 $a|(mb+nc)$.

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

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

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 $a \leq x$ 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 $S = \{a - kb | k \in \mathbb{Z}, a - kb \geq 0\}$,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 $0 \leq r < |b|$,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

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

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 $|r_2 - r_1| \geq |b|$, 这与 $0 \leq r_1, r_2 < |b| - 1$ 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 $a_1, a_2, \dots, a_{1000}$ 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

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

由于每个 r_i 是 $0 \sim 998$ 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 $a \in \{1, 2, \dots, 9\}$.
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 $a = bs + t$, $|t| \leq \frac{|b|}{2}$ 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, \dots, a_{10} , 其倒数之和为

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

则

$$a_2 a_3 \cdots a_{10} + a_1 a_3 \cdots a_{10} + \dots + a_1 a_2 \cdots a_9 = a_1 a_2 \cdots a_{10}$$

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 $\underbrace{99 \cdots 9}_{2009}$.

证 若新数与原数之和为 $\underbrace{99 \cdots 9}_{2009}$, 则原数是一个 2009 位数, 设 $a_1, a_2, \dots, a_{2009}$ 是原数各数位的数字, 而 $a'_1, a'_2, \dots, a'_{2009}$ 是改变顺序后新数的各数位的数字, 则有

$$a_i + a'_i = 9, \quad i = 1, 2, \dots, 2009$$

且

$$a_1 + a_2 + \dots + a_{2009} = a'_1 + a'_2 + \dots + a'_{2009}$$

于是

$$2(a_1 + a_2 + \dots + a_{2009}) = 9 \times 2009$$

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

$$b^2 - 4ac = m^2 \quad (1.2.1)$$

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

$$(b+m)(b-m) = 4ac \quad (1.2.2)$$

因 b 与 m 均为奇数,故可设

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

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, \dots, 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, \dots, x_m 均为奇数,又 m 为奇数,所以, $x_1 + x_2 + \dots + x_m$ 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 $x_1 + x_2 + \dots + x_m = kn$, 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, \dots, a_n 是 $n (n \geq 2)$ 个整数, 若整数 d 是每个 $a_i (i = 1, 2, \dots, n)$ 的因数, 则称 d 是 a_1, a_2, \dots, a_n 的一个公因数.

定义 1.3 整数 a_1, a_2, \dots, 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, \dots, a_n) 或 $\gcd(a_1, a_2, \dots, a_n)$.

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

定义 1.4 如果 $(a_1, a_2, \dots, a_n) = 1$, 则称 a_1, a_2, \dots, 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, \dots, 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, \dots, a_n 是 n 个不全为零的整数, 则有

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

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

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

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

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

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, $d|a$ 且 $d|b$, 于是, 由 $a=bq+r$ 得 $d|r$, 从而

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

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

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

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:

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

由于 b 是有限正整数, 且 $b > r_1 > r_2 > \dots \geq 0$, 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

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

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 $(a_1, \dots, a_n) = d$, 则必存在整数 $k_i (i=1, \dots, n)$, 使得

$$k_1 a_1 + k_2 a_2 + \dots + k_n a_n = d$$

证 令 $S = \{s \mid s = x_1 a_1 + x_2 a_2 + \dots + x_n a_n, x_i \in \mathbb{Z}, s > 0\}$, 则由 a_1, \dots, a_n 的最大公约数存在知, 它们不全为零. 不妨设 $a_1 \neq 0$. 取 x_1 使 $x_1 a_1 > 0$, 再取 $x_2 = x_3 = \dots = x_n = 0$, 则 $s = x_1 a_1 \in S$, 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, \dots, k_n , 使得 $k_1 a_1 + k_2 a_2 + \dots + k_n a_n = d$, 且可以证 d 为 a_1, \dots, a_n 的最大公因数.

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

$$r = a_1 - dq = (1 - qk_1)a_1 - qk_2 a_2 - \dots - qk_n a_n$$

若 $r \neq 0$, 则 $r \in S$ 且 $0 \leq r < d$, 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, \dots, a_n 的任一公约数, 那么, 由 $k_1 a_1 + k_2 a_2 + \dots + k_n a_n = d$, 得 c 为 d 的约数, 从而有 $c \leq d$. 因此, 由定义知 d 为 a_1, \dots, 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 $(a_1, a_2, \dots, a_n) = 1$ 的充分必要条件是存在 $t_1, t_2, \dots, t_n \in \mathbb{Z}$, 使得

$$t_1 a_1 + t_2 a_2 + \dots + t_n a_n = 1$$

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

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

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, \dots, a_n 是 n 个全不为零的整数, 则有

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

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

$$(3) [a_1 k, a_2 k, \dots, a_n k] = [a_1, a_2, \dots, a_n] |k|.$$

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, $[a, b] | m$.

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

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

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

$$a_1 k = b_1 s, \quad \text{其中, } (a_1, b_1) = 1$$

于是, 由性质定理 1.2 可得 $a_1 | s$. 设 $s = a_1 t$, 则

$$m = bs = b a_1 t = \frac{ab}{(a, b)} t \quad (1.3.4)$$

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

$$m = [a, b] t \quad (1.3.5)$$

从而 (1) 成立.

而

$$\begin{aligned} \left(\frac{m}{a}, \frac{m}{b}\right) &= \left(\frac{b}{(a, b)} t, \frac{a}{(a, b)} t\right) && \text{(根据式(1.3.4))} \\ &= (b_1 t, a_1 t) = (b_1, a_1) t \end{aligned}$$

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

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

证 设 $[a_1, a_2, \dots, a_n] = m$, 则 m 是 a_1, a_2, \dots, 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 $a_n, a_{n-1}, \dots, a_2, a_1$ 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) $[136, 221, 391] = [[136, 221], 391] = \left[\frac{136 \times 221}{17}, 391 \right] = [1768, 391]$
 $= \frac{1768 \times 391}{17} = 40664$ (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 $d | m, d | n$. 于是, 有 $(a^d - 1) | (a^m - 1), (a^d - 1) | (a^n - 1)$.

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 $h(a) | a^d - 1$, 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 $m = qn + r, 0 \leq r < n$, 则有

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

于是, 由定理 1.3 得

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

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

$$\begin{aligned} n &= q_1 r + r_1, & 0 < r_1 < r \\ r &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ & \vdots \\ r_{k-2} &= q_k r_{k-1} + r_k, & 0 < r_k < r_{k-1} \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

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, $d | 2$, 即有 $d = 1$ 或 2 . 但 $2^m - 1$ 是奇数, 所以, $d = 1$.

练习 1.3

- 对给定正整数 a, b, c , 证明
 - 如果 $a | b$, 那么, $a | bc$.
 - 如果 $a | b$ 且 $a | c$, 那么, $a^2 | bc$.
 - $a | b$ 当且仅当 $ac | bc$, 其中, $c \neq 0$.
- 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.
- 对于任意的正整数 a , 证明 $2 | a(a+1), 3 | a(a+1)(a+2)$.
- 对于任意的正整数 n 和任意的整数 a , 证明 $(a, a+n) | n$, 因此, $(a, a+1) = 1$.
- 设 n 是正整数, 证明 $[a^n, b^n] = [a, b]^n$.
- 证明 $[a_1, a_2, \dots, a_k, a_{k+1}, \dots, a_n] = [[a_1, a_2, \dots, a_k], [a_{k+1}, \dots, a_n]]$.
- 设 m 是正整数 a_1, a_2, \dots, a_n 的正公倍数, 证明
 - $\left(\frac{m}{a_1}, \frac{m}{a_2}, \dots, \frac{m}{a_n}\right) = \frac{m}{[a_1, \dots, a_n]}$.
 - $\left[\frac{m}{a_1}, \frac{m}{a_2}, \dots, \frac{m}{a_n}\right] = \frac{m}{(a_1, \dots, a_n)}$.
- 证明下列结论.
 - 如果 a 是奇数, 那么, $24 | a(a^2 - 1)$.

- (2) 如果 a, b 都是奇数, 那么, $a | (a^2 - b^2)$.
 (3) 对于任意的整数 a , 都有 $360 | a^2(a^2 - 1)(a^2 - 4)$.

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

$$q \leq \sqrt{a}$$

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 $a_1 \geq q$, 从而 $a = qa_1 \geq q^2$, 即有

$$q \leq \sqrt{a}$$

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 $p \leq \sqrt{48} < 7$ 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 $p | a$.
- (2) 如果 $p | ab$, 则 $p | a$ 或 $p | b$.
- (3) 如果 $p | a_1 a_2 \cdots a_n$ 则存在 i , 使 $p | a_i$.

证 (1) 因为 $(a, p) | p$, 而 p 为质数, 于是, $(a, p) = 1$ 或 p , 若 $(a, p) = p$, 即有 $p | a$.

(2) 如果 $p \nmid a$, 则由(1)知 $(a, p) = 1$, 由已知 $p | ab$, 于是, 由性质定理 1.2 知 $p | b$.

(3) 此条是(2)的推广.

例 1.14 如果 m 是合数, 试证 $n_m = \underbrace{1 \cdots 1}_m$ 也是合数.

证 设 $m = ab$, 那么

$$10^m - 1 = (10^a)^b - 1 = (10^a - 1)(10^{a(b-1)} + \cdots + 10^a + 1)$$

即

$$9 \cdot \underbrace{1 \cdots 1}_m = 9 \cdot \underbrace{1 \cdots 1}_a \cdot (10^{a(b-1)} + \cdots + 10^a + 1)$$

所以, $\underbrace{1 \cdots 1}_a$ 是 n_m 的因数.

例 1.15 设 p, q 为自然数, 满足 $\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{1334} + \frac{1}{1335}$, 证明 $2003 | p$.

$$\begin{aligned} \text{证 } \frac{p}{q} &= 1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{1334} + \frac{1}{1335} \\ &= \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{1335}\right) - 2\left(\frac{1}{2} + \frac{1}{4} + \frac{1}{1334}\right) \\ &= \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{1335}\right) - \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{667}\right) \\ &= \frac{1}{668} + \frac{1}{669} + \cdots + \frac{1}{1334} + \frac{1}{1335} \\ &= \left(\frac{1}{668} + \frac{1}{1335}\right) + \left(\frac{1}{669} + \frac{1}{1334}\right) + \cdots + \left(\frac{1}{1001} + \frac{1}{1002}\right) \\ &= \frac{2003}{668 \times 1335} + \frac{2003}{669 \times 1334} + \cdots + \frac{2003}{1001 \times 1002} \end{aligned}$$

于是可得

$$1335! \cdot p = 2003 \cdot q \cdot t$$

其中, $t = 1335! \times \left(\frac{1}{668 \times 1335} + \frac{1}{669 \times 1334} + \cdots + \frac{1}{1001 \times 1002}\right)$ 为整数, 从而有

$$2003 | 1335! \cdot p$$

由于 2003 为质数, 且 $(2003, 1335!) = 1$, 依据性质定理 1.2 有 $2003 | p$.

例 1.16 设 $n > 2$, 证明在 n 与 $n!$ 之间一定有一个素数.

证 设 p_1, p_2, \cdots, p_k 是所有不超过 n 的素数. 令 $a = p_1 p_2 \cdots p_k - 1$, p 为 a 的一个素因数, 则显然 $p \neq p_i (i = 1, 2, \cdots, k)$, 且 $p > n$. 因若 $p \leq n$, 那么, p 是不超过 n 的素数, 矛盾.

例 1.17 如果一个自然数是素数,而且它的数字的位置经过任意交换后仍然是素数,则称这个数为绝对素数,证明绝对素数不能有多于三个不同的数字(此题为十八届全苏数学奥林匹克竞赛题).

分析 这实际上是一个数字问题,处理数字问题的一个重要手段是借助十进制的数字表示方法.这种绝对素数两位数的有 13,17,37,79.显然,绝对素数中不能含数字 2,4,5,6,8,0,即一个绝对素数如含有 4 个不同的数字,则这 4 个不同的数字一定是 1,3,7,9.

证 设 $p_1 = \overline{a_1 \cdots a_i 1379} = q + 1379$ (其中, $q = \overline{a_1 \cdots a_i} \cdot 10^4$) 是一个含有 4 个不同数字的绝对素数,则由绝对素数的定义知

$$p_2 = q + 3179, \quad p_3 = q + 9137$$

$$p_4 = q + 1379, \quad p_5 = q + 3197$$

$$p_6 = q + 7913, \quad p_7 = q + 7139$$

全是素数.经过验证知,这 7 个数中每两个数的差均不能被 7 整除,这说明 p_1, p_2, \dots, p_7 被 7 除的余数各不相同,从而必有一个余数为零,即能被 7 整除,因此,该数非素数,矛盾,故绝对素数不能有多于三个不同的数字.

定理 1.11 质数有无穷多个.

证 设 n 是任一大于 2 的数,而 p 是 $n! - 1$ 的最小正约数,则由定理 1.10 知 p 是质数.如果 $p \leq n$,则 $p | n!$,于是, $p | (n! - 1 - n!)$,即 $p | 1$,矛盾.因此, $p > n$,这说明对于任意给定的大于 2 的数 n ,均存在大于 n 的素数,从而素数有无穷多个.

例 1.18 证明形如 $4n+3$ 的素数有无限多个.

证 若形如 $4n+3$ 的素数只有 k 个,即 p_1, p_2, \dots, p_k .令 $a = 4p_1 p_2 \cdots p_k - 1 = 4(p_1 p_2 \cdots p_k - 1) + 3$.显然, a 的素因数不能为 $p_i (i=1, 2, \dots, k)$.而由 a 为奇数知, a 的素因数只能为 $4n+1$ 或 $4n+3$ 的形式.若 a 的素因数全为 $4n+1$ 的形式,则由 $(4l+1)(4m+1) = 4(4lm+l+m) + 1$ 知, a 为形如 $4n+1$ 的数,矛盾.所以, a 有形如 $4n+3$ 的素数且不等于 $p_i (i=1, 2, \dots, k)$,矛盾.因此,形如 $4n+3$ 的素数有无穷多个.

练习 1.4

1. 证明奇素数可表示为两个自然数的平方差.
2. 设 n 是大于 2 的整数,如果 $2^n + 1$ 和 $2^n - 1$ 中有一个是素数,那么,另一数必为合数.
3. 试证形如 $3n+2$ 的质数有无穷多个.
4. 试证正整数 $10 \cdots 01$ 是合数.

5. 设 p 和 $p^n + 1$ 均为素数, 证明 $p = 2$ 且 n 为 2 的方幂.

6. 利用 Maple 软件, 回答以下问题.

(1) 第 2^{23} 个素数是多少?

(2) 正整数 $2 \cdots 2 - 1$ 是不是素数?

(3) 不超过 10^{10} 的素数有多少个?

1.5 整数的分解——算术基本定理

任一大于 1 的整数 a 或者是素数, 或者是合数, 如果 a 是一个合数, 设 p_1 是 a 的大于 1 的最小正约数, 则 p_1 是一个素数, 且存在正整数 q_1 , 使 $a = p_1 q_1$ ($1 < q_1 < a$). 如果 q_1 是一个素数, 则 a 就表示成了两个素数之积, 如果 q_1 非素数, 则 q_1 有素因数 p_2 , 于是 $a = p_1 p_2 a_2$. 如果 a_2 是素数, 则就表示成三个素数之积, 否则 a_2 有素因数 p_3 . 如此继续下去, 可知 a 一定可以表示成若干个素数之积.

算术基本定理 设 a 是任一大于 1 的整数, 则 a 能表示成若干个素数的积, 即

$$a = p_1 p_2 \cdots p_n, \quad p_1 \leq p_2 \leq \cdots \leq p_n \quad (1.5.1)$$

其中, p_1, p_2, \dots, p_n 是素数, 且表达式 (1.5.1) 是唯一的.

证 由上面的讨论可知, 表达式 (1.5.1) 一定存在. 下面再用第二数学归纳法证明.

存在性 当 $a = 2$ 时, 2 是一个素数, 所以, $q = 2$ 已是式 (1.5.1) 的形式.

当 $a > 2$ 时, 假设存在性对于大于 1、小于 a 的整数均成立, 现证 a 也可以表示成式 (1.5.1) 的形式.

设 p_1 是 a 的大于 1 的最小正约数, 则由定理 1.10 知 p_1 是素数, 且存在正整数 a_1 , 使得 $a = p_1 a_1$, 其中, $1 \leq a_1 < a$. 如果 $a_1 = 1$, 则 $a = p_1$ 是式 (1.5.1) 的形式; 如果 $a_1 > 1$, 那么由归纳假设知, a_1 可以表示成式 (1.5.1) 的形式. 不妨设 $a_1 = p_2 p_3 \cdots p_n$, 且 $p_2 \leq p_3 \leq \cdots \leq p_n$. 由于 p_1 为 a 的最小正约数, 故 $p_1 \leq p_2$, 因而有 $p_1 \leq p_2 \leq \cdots \leq p_n$, 即式 (1.5.1) 完全成立.

唯一性 如果 a 还可表示成

$$a = q_1 q_2 \cdots q_m$$

其中, q_1, q_2, \dots, q_m 为素数. 则有

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \quad (1.5.2)$$

于是, $p_1 \mid q_1 q_2 \cdots q_m$ 且 $q_1 \mid p_1 p_2 \cdots p_n$. 由性质定理 1.4 知, 存在 q_k, p_l 使得

$$p_1 \mid q_k \text{ 且 } q_1 \mid p_l$$

而 q_k 及 p_l 均为素数, 故 $p_1 = q_k, q_1 = p_l$, 于是

$$q_1 = p_l \geq p_1 = q_k \geq q_1$$

因此有 $p_1 = q_1$, 由式(1.5.2)可得

$$p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m$$

同理可得, $p_2 = q_2, \dots, p_n = q_m$, 且 $n = m$.

说明 也可通过对式(1.5.2)中的 n 利用归纳法证明 $m = n, p_i = q_i (i = 1, 2, \dots, n)$.

算术基本定理也可以称为整数的唯一分解定理. 式(1.5.2)中的素数 p_i 可能有相同的, 将相同的素因数合写成方幂的形式, 则有 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \alpha_i > 0 (i = 1, 2, \dots, k)$, 其中, $p_i < p_j (i < j)$ 是素数.

推论 1.2 任一大于 1 的整数 a 均可唯一地分解成

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \alpha_i > 0 \quad (i = 1, 2, \dots, k) \quad (1.5.3)$$

其中, $p_i < p_j (i < j)$ 是素数.

式(1.5.3)称为 a 的标准素因数分解式.

推论 1.3 设大于 1 的整数 a 的标准分解式如式(1.5.3), d 为正整数, 则

$$d | a \Leftrightarrow d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}, \quad 0 \leq \beta_i \leq \alpha_i, \quad i = 1, 2, \dots, t$$

证 充分性显然.

必要性 若 p 为 d 的任一素因数, 则由 $d | a$ 知 $p | a$, 即 p 亦是 a 的素因数, 因此, p 必为某个 p_i , 可设 d 的标准分解式为

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}, \quad \beta_i > 0, \quad i = 1, 2, \dots, t$$

下面证明 $\beta_i \leq \alpha_i (1 \leq i \leq t)$.

如果 $\beta_1 > \alpha_1$, 则由 $p_1^{\beta_1} | d$ 及 $d | a$ 得, $p_1^{\beta_1} | p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, 即有

$$p_1^{\beta_1 - \alpha_1} | p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

从而

$$p_1 | p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

由性质定理 1.4 推得, p_1 必与 p_2, p_3, \dots, p_t 之中某个数相同, 矛盾, 故 $\beta_1 \leq \alpha_1$.

同理可证 $\beta_i \leq \alpha_i (2 \leq i \leq t)$.

推论 1.4 设 a 与 b 是任意两个正整数, 其标准分解式为

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_i \geq 0 \quad (i = 1, 2, \dots, s)$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}, \quad \beta_i \geq 0 \quad (i = 1, 2, \dots, s)$$

则

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}, \quad \text{其中, } \gamma_i = \min(\alpha_i, \beta_i) \quad (1.5.4)$$

$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}, \quad \text{其中, } \delta_i = \max(\alpha_i, \beta_i) \quad (1.5.5)$$

及

$$(a, b)[a, b] = ab$$

推论 1.4 可由推论 1.2 证得,请读者给出详细论证.

推论 1.5 如果 $(a, b) = 1$ 且 $ab = c^k$, 则

$$a = u^k, \quad b = v^k \text{ 且 } u = (a, c), \quad v = (b, c)$$

证 设 $c = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ 为 c 的标准分解式, 则有

$$c^k = p_1^{k\alpha_1} p_2^{k\alpha_2} \cdots p_s^{k\alpha_s}$$

由推论 1.3 可得

$$a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

$$b = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$$

由条件 $ab = c^k$ 知, $\beta_i + \gamma_i = k\alpha_i (1 \leq i \leq s)$. 再由 $(a, b) = 1$ 知, $\min(\alpha_i, \beta_i) = 0 (1 \leq i \leq s)$, 因此

$$\begin{cases} \beta_i = 0 \\ \gamma_i = k\alpha_i \end{cases} \quad \text{或} \quad \begin{cases} \gamma_i = 0 \\ \beta_i = k\alpha_i \end{cases}$$

从而 a 是 $p_1^{k\alpha_1} p_2^{k\alpha_2} \cdots p_s^{k\alpha_s}$ 中若干个的乘积, b 则是其余若干个的乘积, 所以, a 与 b 均是某整数的 k 次幂.

设 $a = u^k, b = v^k$, 则由 $ab = c^k$ 及 $ab = (uv)^k$ 得 $c = uv$, 于是

$$(a, c) = (a, uv) = (u^k, uv) = u(u^{k-1}, v)$$

另外, 由 $(a, b) = 1$ 知, $(u^k, v^k) = 1$, 即有 $(u, v) = 1$, 则 $(u^{k-1}, v) = 1$, 从而

$$(a, c) = u(u^{k-1}, v) = u$$

同理可证 $(b, c) = v$.

设 a 是正整数, 用 $T(a)$ 表示 a 的所有正约数的个数, 称为 a 的约数函数; 用 $S(a)$ 表示 a 的所有正约数的和, 称为 a 的约数和函数; 用 $P(a)$ 表示 a 的所有正约数的积, 称为 a 的约数积函数.

定理 1.12 设 a 是一大于 1 的整数, 且 a 的标准素因数分解为

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

其中, $\alpha_i \geq 0 (i = 1, 2, \dots, t)$, 且 p_1, p_2, \dots, p_t 互不相同, 则有

$$(1) T(a) = \prod_{i=1}^t (\alpha_i + 1).$$

$$(2) S(a) = \prod_{i=1}^t \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

$$(3) P(a) = a^{\frac{1}{2}T(a)}.$$

证 由推论 1.3 得, a 的任一正约数 d 形如

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}, \quad 0 \leq \beta_i \leq \alpha_i,$$

$$(1) a \text{ 的正约数的个数为 } \binom{\alpha_1+1}{1} \cdots \binom{\alpha_t+1}{1}, \text{ 即}$$

$$T(a) = (\alpha_1 + 1) \cdots (\alpha_t + 1) = \prod_{i=1}^t (\alpha_i + 1)$$

(2) a 的所有正约数之和为

$$\begin{aligned} S(a) &= \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_t=0}^{\alpha_t} p_1^{\beta_1} \cdots p_t^{\beta_t} = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \right) \cdots \left(\sum_{\beta_t=0}^{\alpha_t} p_t^{\beta_t} \right) \\ &= \frac{p_1^{\alpha_1+1}}{p_1-1} \cdots \frac{p_t^{\alpha_t+1}}{p_t-1} = \prod_{i=1}^t \frac{p_i^{\alpha_i+1}}{p_i-1} \end{aligned}$$

(3) 设 $a_1, \dots, a_{T(a)}$ 是 a 的所有正约数, 则 $\frac{a}{a_1}, \dots, \frac{a}{a_{T(a)}}$ 亦是 a 的所有正约数, 因此

$$P(a)^2 = (a_1 \cdots a_{T(a)}) \left(\frac{a}{a_1} \cdots \frac{a}{a_{T(a)}} \right) = a^{T(a)}$$

即有 $P(a) = a^{\frac{1}{2}T(a)}$.

例 1.19 设 $a=860$, 求 $T(a)$, $S(a)$ 及 $P(a)$.

解 因为 a 的标准素因数分解为 $860=2^2 \times 5^1 \times 43^1$, 所以有

$$\begin{aligned} T(860) &= (2+1)(1+1)(1+1) = 12 \\ S(860) &= \frac{2^{2+1}-1}{2-1} \frac{5^{1+1}-1}{5-1} \frac{43^{1+1}-1}{43-1} = 7 \times 6 \times 44 = 1848 \\ P(860) &= 860^6 \end{aligned}$$

例 1.20 设 a 为任一正整数, 求 $\sum_{d|a} \frac{1}{d}$ 及当 $a=860$ 时的值.

解 由于当 d 取遍 a 的正约数时, a/d 亦取遍 a 的正约数, 所以有

$$\sum_{d|a} \frac{1}{d} = \sum_{d|a} \frac{1}{a/d} = \sum_{d|a} \frac{d}{a} = \frac{1}{a} \sum_{d|a} d = \frac{1}{a} S(a)$$

当 $a=860$ 时,

$$\sum_{d|a} \frac{1}{d} = \frac{1}{a} S(a) = \frac{1}{860} \times 1848 = \frac{462}{215}$$

例 1.21 求证满足 $2^5 a^b = 25ab$ 的 $0 \sim 9$ 的数码 a 与 b 为多少?

证 因为 $0 \leq a, b \leq 9$, 故 $2500 \leq 2^5 a^b < 2600$, 则

$$78 \leq a^b < 82$$

从而只有

$$a = 9, b = 2$$

例 1.22 试证当 $a > 2$ 时, 有 $S(a) < a\sqrt{a}$.

证 分三步来证明此题.

(1) 若 $a=2^k, k \geq 2$, 则有

$$S(a) = \frac{2^{k+1} - 1}{2 - 1} = 2^{k+1} - 1 < 2^{k+1} = a \cdot 2 \leq a \cdot 2^{\frac{k}{2}} = a\sqrt{a}$$

(2) 若 $a = p^k$, p 为奇素数, 则有

$$S(a) = \frac{p^{k+1} - 1}{p - 1} = \frac{p^k - 1}{1 - \frac{1}{p}} < \frac{a}{1 - \frac{1}{p}} \leq \frac{a}{1 - \frac{1}{3}} = \frac{3}{2}a < a\sqrt{3}$$

(3) 若 $a = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, 则当 $\alpha_0 > 1$ 时, 有

$$\begin{aligned} S(a) &= S(2^{\alpha_0})S(p_1^{\alpha_1}) \cdots S(p_t^{\alpha_t}) < 2^{\alpha_0} \sqrt{2^{\alpha_0}} \cdot p_1^{\alpha_1} \sqrt{p_1^{\alpha_1}} \cdots p_t^{\alpha_t} \sqrt{p_t^{\alpha_t}} \\ &= (2^{\alpha_0} p_1^{\alpha_1} \cdots p_t^{\alpha_t}) \cdot \sqrt{2^{\alpha_0} p_1^{\alpha_1} \cdots p_t^{\alpha_t}} = a\sqrt{a} \end{aligned}$$

当 $\alpha_0 = 1$ 时, 由于

$$\begin{aligned} S(2p_1^{\alpha_1}) &= S(2)S(p_1^{\alpha_1}) = 3S(p_1^{\alpha_1}) < 3 \cdot \frac{3}{2} p_1^{\alpha_1} = 2p_1^{\alpha_1} \cdot \frac{9}{4} < 2p_1^{\alpha_1} \sqrt{6} \\ &\leq 2p_1^{\alpha_1} \sqrt{2p_1^{\alpha_1}} \end{aligned}$$

所以有

$$\begin{aligned} S(a) &= S(2p_1^{\alpha_1})S(p_2^{\alpha_2}) \cdots S(p_t^{\alpha_t}) < 2p_1^{\alpha_1} \sqrt{2p_1^{\alpha_1}} \cdot p_2^{\alpha_2} \sqrt{p_2^{\alpha_2}} \cdots p_t^{\alpha_t} \sqrt{p_t^{\alpha_t}} \\ &= 2^{\alpha_0} p_1^{\alpha_1} \cdots p_t^{\alpha_t} \sqrt{2^{\alpha_0} p_1^{\alpha_1} \cdots p_t^{\alpha_t}} = a\sqrt{a} \end{aligned}$$

注 这里用到了约数和函数的一个性质: 当 $(a, b) = 1$ 时, $S(ab) = S(a)S(b)$. (请读者自证)

练习 1.5

1. 分别求 2160 及 $\underbrace{99 \cdots 99}_{12}$ 的标准分解式.
2. 设 $a = 2160$, 求 $T(a)$, $S(a)$ 及 $P(a)$.
3. 利用 Maple 函数求 8203513468500 的标准分解式.
4. 设 a, b, c 是任意整数, 则有
 - (1) $\max(\min(a, b), \min(a, c)) = \min(a, \max(b, c))$.
 - (2) $[(a, b), (a, c)] = (a, [b, c])$.
5. 证明正整数 n 是素数的充分必要条件是 $S(n) = n + 1$.
6. 求满足条件 $T(a) = 6$ 的最小正整数 a .
7. 求所有正约数的积等于 64 的一切正整数.
8. 一个正整数 a 称为完全数, 如果有 $S(a) = 2a$, 请解答以下问题.
 - (1) 找出两个完全数.
 - (2) 若 $2^k - 1$ 是素数, 则 $2^{k-1}(2^k - 1)$ 是完全数; 若 a 是偶完全数, 则 $a = 2^n(2^{n+1} - 1)$, 且 $2^{n+1} - 1$ 是素数.

(3) 正整数 a 是完全数的充分必要条件是 $\sum_{d|a} \frac{1}{d} = 2$.

1.6 利用 Maple 求解整除性问题

利用 Maple 实现带余除法,有 4 个 Maple 函数^①: $\text{irem}(a,b)$, $\text{irem}(a,b,'q')$, $\text{iquo}(a,b)$, $\text{iquo}(a,b,'r')$. 它们分别表示求 b 除 a 的余数, b 除 a 的余数与商, b 除 a 的商, b 除 a 的商与余数,如下所示:

```
>irem(23,5);
3
>irem(23,5,'q');
3
>q;
4
>iquo(23,5);
4
>iquo(23,5,'r');
4
>r;
3
```

Maple 中有两个求最大公约数及最小公倍数的 Maple 函数,分别是 $\text{igcd}(x_1, x_2, \dots)$ 和 $\text{ilcm}(x_1, x_2, \dots)$, 其中, x_1, x_2, \dots 是整数. 如下所示:

```
>igcd(135,220,395);
5
>ilcm(136,221,390);
26520
```

如果要求出两个整数 a, b 的最大公约数 d , 并求出相应的 s, t , 使 $as + bt = d$, 则使用 Maple 函数 $\text{igcdex}(a, b, 's', 't')$, 此函数又可称为扩展 Euclid 函数或算法. 如下所示:

```
>igcdex(135,220,'s','t');
5
>s,t;
-13,8
```

即 5 是 135 与 220 的最大公约数, 且 $5 = -13 \times 135 + 8 \times 220$.

如果要判断整数 x_1, x_2, \dots 是否互素, 可利用 Maple 函数 $\text{evalb}(\text{igcd}(x_1,$

^① 本书将 Maple 数学软件里的单个模块函数均称为 Maple 函数.

$x_2, \dots) = 1$). 当运算值为“true”时, 说明这些整数是互素的; 当运算值为“false”时, 就说明这些整数是不互素的. 如下所示:

```
>evalb(igcd(135, 220, 395) = 1);
false
>evalb(igcd(135, 221, 395) = 1);
true
```

一般来讲, 要判断一个较大的正整数是不是素数, 只靠纸与笔去推算是一件很困难的事, 如果运用 Maple 函数, 则可以说是小事一桩. 在 Maple 中, 判断一个正整数 n 是不是素数的 Maple 函数有两个: `isprime(n)` 与 `type(n , prime)`. 如下所示:

```
>isprime(8191);
true
>type(8191, prime);
true
```

找出第 n 个素数的 Maple 函数是 `ithprime(n)`. 求出不超过某一正实数 x 的素数个数的 Maple 函数是 `pi(n)` 或 `nops(select('isprime', [$2.. n]))`. 如下所示:

```
>ithprime(2008);
17467
>pi(2008);
304
>nops( select( 'isprime', [MYM2..2008] ));
304 (* 即不超过 2008 的素数共有 304 个 *)
>pi(10^9);
50847534 (* 不超过 10^9 的素数共有 50847534 个 *)
```

用于进行整数素因子分解的 Maple 函数是 `ifactors(n)`, 如下所示:

```
>ifactors(2434500);
[1, [[2, 2], [3, 2], [5, 3], [541, 1]]]
>ifactors(1690575565024346828676664200680);
[1, [[ 2, 3 ], [ 5, 1 ], [ 17, 2 ], [ 12093120399163, 1 ],
[12093120399131, 1]]]
```

即 2434500 与 1690575565024346828676664200680 的标准分解式为

$$2434500 = 2^2 \times 3^2 \times 5^3 \times 541$$

与

$$\begin{aligned} &1690575565024346828/676664200680 \\ &= 2^3 \times 5 \times 17^2 \times 12093120399163 \times 12093120399131 \end{aligned}$$

求一个正整数 n 的所有正素因子集合的 Maple 函数是 `factorset(n)`, 但在使用时必须先调用软件包“numtheory”. 如下所示:

```
>with(numtheory):
>factorset(34562);
{2, 11, 1571}
```

如要求一个正整数 n 的所有正约数的集合, 则用 $\text{divisors}(n)$, 如下所示:

```
>with(numtheory):
divisors(34562);
{1, 2, 11, 22, 1571, 3142, 17281, 34562}
```

求一个正整数 n 的所有正约数的个数 $T(n)$ 用 Maple 函数 $\text{tau}(n)$, 求 n 的所有正约数的和及积, 则可简单用 Maple 程序实现, 如下所示:

```
>with(numtheory):
>L:=divisors(n);
S(n):=add(i, i=L);
P(n):=mul(i, i=L);
```

如

```
>with(numtheory):
L:=divisors(34562);
S(34562):=add(i, i=L);
P(34562):=mul(i, i=L);
L:= {1, 2, 11, 22, 1571, 3142, 17281, 34562}
S(34562):= 56592
P(34562):= 1426906326330040336
```

Maple 中有一个直接求 n 的所有正约数的和的函数 $\text{sigma}(n)$, 用此函数更方便.

```
>with(numtheory):
sigma(34562);
56592
```

哥德巴赫猜想(Goldbach's conjecture)说, 每个大于 2 的偶数均可表示成两个奇素数之和. 利用 Maple 编程, 可对哥德巴赫猜想进行验证, 如 Maple 程序算法.

```
>with(numtheory):
GoldbConjVer:=proc(n::posint)
local i;
for i from 3 by 2 while i<n do
if isprime(i)=true and isprime(n-i)=true
printf("%d = %d + %d\n", n, i, n-i);
break;
fi;
od;
```

```
end:
```

可对任意大于 2 的偶数进行验证此猜想. 如下所示:

```
> GoldbConjVer(100): GoldbConjVer(1000): GoldbConjVer(200888): GoldbConjVer(100000);
```

```
100 = 3 + 97
```

```
1000 = 3 + 997
```

```
200888 = 7 + 200881
```

```
100000 = 11 + 99989
```

孪生素数是指差为 2 的任意两个素数. 孪生素数的猜想是指存在无穷多组孪生素数. 利用 Maple 编程可找出不超过任意一个确定的自然数的孪生素数. 下面的程序函数 TwinPrime() 就可给出所有不超过自然数 n 的孪生素数.

```
>with(numtheory):
TwinPrime:=proc(n::posint)
local i;
for i from 3 by 2 while i+1<n do
if isprime(i)=true and isprime(i+2)=true
then print(i,i+2);
fi;
od;
end:
```

例如, 可得到不超过 100 的孪生素数有以下 8 组:

```
>TwinPrime(100);
3,5
5,7
11,13
17,19
29,31
41,43
59,61
71,73
```

第 1 章综合例题

例 1 设 g 是大于 1 的整数, 那么, 任意正整数 a 可以唯一地表示成

$$a = c_n g^n + \cdots + c_1 g + c_0 \quad (1.1)$$

其中, $n \geq 0$, c_i 是整数, 且 $0 \leq c_i < g$.

证(用第二归纳法) 当 $a=1$ 时, $n=0$, $c_0=1$, 式(1.1)成立.

归纳假设式(1.1)对于小于 a 的正整数成立,下面证式(1.1)对 a 成立.

由于 $g > 1$,所以, a 必定属于某区间 $[g^n, g^{n+1})$ (n 为某一非负整数),即有

$$g^n \leq a < g^{n+1}$$

利用带余除法有

$$a = c_n g^n + r, \quad 0 \leq r < g^n$$

显然, $0 < c_n < g$ 且 $r < a$.

若 $r=0$,则 $a=c_n g^n+0g^{n-1}+\cdots+0g+0$ 为式(1.1)的形式,若 $r \neq 0$,则由归纳假设

$$r = c_k g^k + \cdots + c_1 g + c_0, \quad k < n, \quad 0 \leq c_i < g$$

于是

$$a = c_n g^n + \cdots + c_1 g + c_0$$

为式(1.1)的形式.

把 $(c_n c_{n-1} \cdots c_1 c_0)_g$ 叫作 a 的 g 进制数, g 称为 a 的底.如 $a=3712$,取 $g=10$,则有

$$3712 = 3 \times 10^3 + 7 \times 10^2 + 10 + 2 = (3712)_{10}$$

取 $g=2$,则有

$$3712 = (11101000000)_2$$

取 $g=16$,则有

$$3712 = (A80)_{16}, \text{ 其中, } A = 14$$

例2 设自然数 a_1, a_2, \cdots, a_n 是 $1, 2, \cdots, n$ 的某种排列,如果 n 是奇数,则

$$(a_1 - 1)(a_2 - 2) \cdots (a_n - n)$$

是偶数.

证 由已知有

$$(a_1 - 1) + (a_2 - 2) + \cdots + (a_n - n) = 0 \quad (1.2)$$

而 n 为奇数,故 $(a_1 - 1), (a_2 - 2), \cdots, (a_n - n)$ 是奇数个整数,若它们全为奇数,则

$$(a_1 - 1) + (a_2 - 2) + \cdots + (a_n - n)$$

是奇数个奇数相加,其和应是奇数,这与式(1.2)矛盾,故

$$(a_1 - 1), (a_2 - 2), \cdots, (a_n - n)$$

中有偶数,于是, $(a_1 - 1)(a_2 - 2) \cdots (a_n - n)$ 是偶数.

例3 设 $f(x)$ 是一个整系数多项式,并且有一个偶数 α 和奇数 β 使得 $f(\alpha)$ 和 $f(\beta)$ 都是奇数,求证方程 $f(x)=0$ 没有整数根.

证(反证法) 设 $f(x)=a_0 x^n+a_1 x^{n-1}+\cdots+a_{n-1} x+a_n$,且 $f(x)=0$ 有一个整数根 γ ,于是有

$$f(\alpha) = f(\alpha) - f(\gamma) = a_0(\alpha^n - \gamma^n) + a_1(\alpha^{n-1} - \gamma^{n-1}) + \cdots + a_{n-1}(\alpha - \gamma)$$

$$f(\beta) = f(\beta) - f(\gamma) = a_0(\beta^n - \gamma^n) + a_1(\beta^{n-1} - \gamma^{n-1}) + \cdots + a_{n-1}(\beta - \gamma)$$

即有

$$f(\alpha) = (\alpha - \gamma)a, \quad f(\beta) = (\beta - \gamma)b, a, b \text{ 为整数}$$

于是得

$$f(\alpha)f(\beta) = (\alpha - \gamma)(\beta - \gamma)ab \quad (1.3)$$

由题设知, $f(\alpha)$ 与 $f(\beta)$ 均为奇数. 而 α 为偶数, β 为奇数, 因此, 式(1.3)的右边为偶数, 而左边为奇数, 矛盾. 所以, $f(x)=0$ 不能有整数解.

例 4 证明不论 n 是什么整数, 方程 $x^2 - 16nx + 7^5 = 0$ 均无整数解.

证 设 x_1, x_2 是方程 $x^2 - 16nx + 7^5 = 0$ 的一对整数解, 则由根与系数的关系得

$$x_1 + x_2 = 16n \quad (1.4)$$

$$x_1 \cdot x_2 = 7^5 \quad (1.5)$$

于是, 可设 $x_1 = 7^k, x_2 = 7^l$, 且 $l+k=5$. 不妨设 $k < l$, 则

(1) 若 $k=0, l=5$ 时, 由式(1.4)有, $1+7^5 = 16n$, 即 $8(7^4 - 7^3 + 7^2 - 7 + 1) = 16n$, 不可.

(2) 若 $k=1, l=4$ 时, 由式(1.4)有, $7+7^4 = 16n$, 即 $7 \times 8 \times (7^2 - 7 + 1) = 16n$, 不可.

(3) 若 $k=2, l=3$ 时, 由式(1.4)有, $(7^3 + 7^2) = 16n$, 即 $7^2 \times 8 = 16n$, 不可.

综上所述, 原方程无整数解.

例 5 已知圆 $x^2 + y^2 = r^2$ (r 为奇数), 交 x 轴于 $A(r, 0)$ 与 $B(-r, 0)$, 交 y 轴于 $C(0, -r), D(0, r)$. (u, v) 是圆周上一点, $u = p^m, v = q^n$ (p, q 均为素数, $m, n \in \mathbb{N}$), $u > v$, 且 u, v 在 x 轴与 y 轴上的射影分别是 M 与 N , 证明 $|AM|, |BM|, |CN|, |DN|$ 分别为 $1, 9, 8, 2$.

证 因为 $u^2 + v^2 = r^2$, 而 r 是奇数, 故 u, v 必为一奇一偶, 设 u 为偶数, 依题意得 $u = 2^m$. 由 $u^2 + v^2 = r^2$, 即 $(r+u)(r-u) = v^2, v = q^n, r+u = q^\alpha, r-u = q^\beta, \alpha > \beta$, 于是, $2u = q^\beta(q^{\alpha-\beta} - 1), q^\beta | 2u$, 即 $q^\beta | 2^{m+1}$.

由 v 为奇数知, q 为奇素数, 从而有 $\beta=0$, 因此

$$r = u + 1 = 2^m + 1, \quad q^{2n} = r + u = (2^m + 1) + 2^m = 2^{m+1} + 1$$

即有

$$(q^n + 1)(q^n - 1) = 2^{m+1} \quad (1.6)$$

不妨设 $q^n + 1 = 2^s, q^n - 1 = 2^t, s > t$ 则有

$$q^n = 2^{s-1} + 2^{t-1}$$

而 q 为奇素数, 必有 $t-1=0$, 即 $t=1$. 于是, 由 $q^n - 1 = 2^t$ 得 $q^n = 2^t + 1 = 3$, 即 $v = 3$, 因而 $n=1, q=3$. 代入式(1.6)得, $m=2, u=4, r=5$.

$$|AM| = r - u = 1, \quad |BM| = r + u = 9$$

$$|CN| = r + v = 8, \quad |DN| = r - v = 2$$

注 此题用 6.4 节的高高不定方程解的一般形式证明要简单些.

例 6 桌上有 7 只茶杯, 杯口全部朝上, 每次“运动”是指将其中 4 只茶杯同时翻转, 问能否经过若干次运动使杯口全部朝下? 为什么?

解 不能, 论证如下.

记杯口朝上、朝下分别为 +1, -1, 7 只茶杯状态对应的 7 个数 (+1 或 -1) 的乘积记为 p , 每次“运动”, 4 只茶杯同时翻转, 即将 p 的 4 个因数同时乘以 -1. 由 $(-1)^4 p = p$ 知, 无论“运动”多少次, p 的值总与初始值一样, 而要杯口全部朝下, 必须 $p = -1$, 这不可能.

例 7 证明 $n^3 + \frac{3}{2}n^2 + \frac{1}{2}n - 1$ 对任何自然数均是整数, 且用 3 除余数为 2.

证 因为 $n^3 + \frac{3}{2}n^2 + \frac{1}{2}n - 1 = \frac{n(n+1)(2n+1)}{2} - 1$, 而 $2 | n(n+1)$, 所以, $n^3 + \frac{3}{2}n^2 + \frac{1}{2}n - 1$ 是整数. 又

$$\begin{aligned} n^3 + \frac{3}{2}n^2 + \frac{1}{2}n - 1 &= \frac{n(n+1)((n+2) + (n-1))}{2} - 1 \\ &= \frac{n(n+1)(n+2)}{2} + \frac{(n-1)n(n+1)}{2} - 3 + 2 \end{aligned}$$

由于任意三个连续整数之积能被 $3!$ 整除, 故由上式知 $n^3 + \frac{3}{2}n^2 + \frac{1}{2}n - 1$ 用 3 除余数为 2.

例 8 证明 $7 | (3333^{4444} + 4444^{3333})$.

证 因为 $3333 = 7 \times 476 + 1$ 及 $4444 = 7 \times 635 - 1$, 所以

$$\begin{aligned} 3333^{4444} + 4444^{3333} &= (7 \times 476 + 1)^{4444} + (7 \times 635 - 1)^{3333} \\ &= 7q + 1^{4444} + (-1)^{3333} = 7q \end{aligned}$$

其中, q 为整数, 得 $7 | (3333^{4444} + 4444^{3333})$.

例 9 给定如下三角形的数表:

$$\begin{array}{ccccccc} 0 & 1 & 2 & \cdots & 1998 & 1999 & \\ & \swarrow & \searrow & & \swarrow & \searrow & \\ & 1 & 3 & \cdots & & 3997 & \\ & & & & & & \\ & & & & & & \end{array}$$

其中, 每一行 (除最上面一行外) 的每个数等于前一行邻近两数的和. 证明最低行的一个数能被 1999 整除.

证 设最上面一行有 n 个数 a_1, a_2, \dots, a_n , 则易知其最下面的一个数 (数表的第 n 行) 是

$$a_1 + a_2 \binom{n-1}{1} + \cdots + a_{i+1} \binom{n-1}{i} + \cdots + a_{n-1} \binom{n-1}{n-2} + a_n$$

则原三角形表最下面的一个数是

$$S = 0 + 1 \binom{1999}{1} + 2 \binom{1999}{2} + \cdots + 1998 \binom{1999}{1998} + 1999$$

由于对每个满足 $1 \leq i < 1999$ 的整数 i , 有 $\binom{1999}{i} = \frac{1999}{i} \binom{1998}{i-1}$, 且由 1999 是素数知 $i \mid \binom{1998}{i-1}$, 因此, $1999 \mid S$.

例 10 设有整系数多项式

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x^1 + a_n, \quad a_0 \neq 0$$

证明一定存在无穷多个整数 k , 使 $f(k)$ 为合数或相差一个负号.

证 (1) 若对任何整数 k , $f(k)$ 均为合数或 -1 乘一合数, 则结论已成立.

(2) 若存在某整数 k_0 使 $f(k_0) = p$ 或 $-p$, 其中, p 为素数, 则对任何整数 l 有

$$\begin{aligned} f(k_0 + lp) &= a_0 (k_0 + lp)^n + a_1 (k_0 + lp)^{n-1} + \cdots + a_{n-1} (k_0 + lp)^1 + a_n \\ &= f(k_0) + p \cdot q(l) = p(q(l) \pm 1) \end{aligned}$$

其中, $q(l)$ 为与 l 有关的整数. 因此, 有无穷多个整数 l , 使 $f(k_0 + lp)$ 为合数或相差一个负号, 即有无穷多个整数 k , 使 $f(k)$ ($k = k_0 + lp$) 为合数或相差一个负号.

例 11 证明若 $a+b \neq 0$, $(a, b) = 1$, p 是奇素数, 则

$$\left(a + b, \frac{a^p + b^p}{a + b}\right) = 1 \text{ 或 } p$$

证 设 $\left(a + b, \frac{a^p + b^p}{a + b}\right) = d$ 及 $a + b = kd$, $\frac{a^p + b^p}{a + b} = ld$, 其中, $(k, l) = 1$, 则有

$$a^p + b^p = ld(a + b) = kld^2$$

另外

$$\begin{aligned} a^p + b^p &= a^p + (kd - a)^p \\ &= a^p + (kd)^p - \binom{p}{1}(kd)^{p-1} + \cdots + \binom{p}{p-1}(kd)(-a)^{p-1} + (-a)^p \end{aligned}$$

因为 $(-a)^p = -a^p$, 所以有

$$ld = (kd)^{p-1} - \binom{p}{1}(kd)^{p-2} + \cdots + \binom{p}{p-1}(-a)^{p-1}$$

于是

$$d \mid \binom{p}{p-1}(-a)^{p-1}, \text{ 即 } d \mid pa^{p-1}$$

如果 $(d, a) = d_1$, 则 $d_1 \mid d$, 于是 $d_1 \mid (a + b)$, 因而 $d_1 \mid (a, a + b)$. 而 $(a, a + b) =$

$(a, b) = 1$, 故 $d_1 = 1$, 即有 $(d, a) = 1$, 从而由 $d | pa^{p-1}$ 得 $d | p$, 所以 $d = 1$ 或 p .

例 12 设 3^{10000} 的各位数字和为 A , A 的各位数字和为 B , B 的各位数字和为 C , 求 C 等于多少?

解 首先注意到一条事实: 一个整数能被 9 整除的充分必要条件是其个位数字之和能被 9 整除. 由于 $9 | 3^{10000}$, 所以, $9 | A, 9 | B$ 及 $9 | C$. 另外, $3^{10000} = 9^{5000} < 10^{5000}$, 故 $A < 5001 \times 9 = 45009$, 即有 $B \leq 5 \times 9 = 45$, 于是, $C < 2 \times 9 = 18$, 从而由 $9 | C$ 知 $C = 9$.

例 13 已知 $695xy155$ 是 99 的倍数, 求 x 与 y (其中 x 与 y 为 $0 \sim 9$ 的数).

解 由 $99 | 695xy155$ 可得 $9 | 695xy155, 11 | 695xy155$, 于是有

$$\begin{cases} 6 + 9 + 5 + x + y + 1 + 5 + 5 = 9k \\ (5 + 1 + x + 9) - (5 + y + 5 + 6) = 11t \end{cases}$$

即

$$\begin{cases} x + y = 9k - 31 \\ x - y = 11t + 1 \end{cases} \quad (1.7)$$

则由 $0 \leq x, y \leq 9$ 得

$$0 \leq 9k - 31 \leq 18 \quad \text{及} \quad -9 \leq 11t + 1 \leq 9$$

即有

$$\frac{31}{9} \leq k \leq \frac{49}{9} \quad \text{及} \quad -\frac{10}{11} \leq t \leq \frac{8}{11}$$

从而 $k = 4$ 或 5 及 $t = 0$.

再由式(1.7)得

$$\begin{cases} x + y = 9 \times 4 - 31 = 5 \\ x - y = 1 \end{cases} \quad \text{或} \quad \begin{cases} x + y = 9 \times 5 - 31 = 14 \\ x - y = 1 \end{cases}$$

即有

$$\begin{cases} x = 3 \\ y = 2 \end{cases} \quad \text{或} \quad \begin{cases} x = \frac{15}{2} \\ y = \frac{13}{2} \end{cases} \quad (\text{舍去})$$

因而

$$\begin{cases} x = 3 \\ y = 2 \end{cases}$$

思考题、研究题一

1. 如 $a_1 b_2 - a_2 b_1 = \pm 1$, 那么, 分数 $\frac{a_1 + a_2}{b_1 + b_2}$ 是不可约分数.

2. 将与 105 互素的所有正整数从小到大排列成数列, 试求出这个数列的第 1000 项(该题为 1994 年全国高中数学联合竞赛考题)(注: 将 105 改为 165 或 195 如何?).

3. 求一切实数 p , 使得三次方程 $5x^3 - 5(p+1)x^2 + (71p-1)x + 1 = 66p$ 的三个根均为自然数.

4. 如果一个矩形的长和宽均为奇数, 问在其内部是否存在这样的点, 它到 4 个顶点的距离均为正整数.

5. 设 a, b 均为自然数, 且 $a^2 + b^2 = q(a+b) + r$, 试求出所有使 $q^2 + r + 1 = 1979$ 成立的 a, b (注: 该题为第 20 届国际数学奥林匹克竞赛试题, 若将 1979 改为 1999 或 2009 如何?).

6. 设 n 是大于 1 的自然数, 证明 $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ 不是整数(提示: 反证法).

7. 若 p 是一个素数, 那么, $2^p + 3^p$ 不能表示为 n^k 的形式, 其中, n 和 k 均为自然数且 $k > 1$ (该题为 1981 年德国竞赛题).

8. 试证有无穷多个自然数 a 具有下列性质: 不存在一个自然数 n , 使得 $n^4 + a$ 是素数(注: 该题为第 11 届国际数学奥林匹克竞赛试题).

9. 求 $\binom{2n}{1}, \binom{2n}{3}, \binom{2n}{5}, \dots, \binom{2n}{2n-1}$ 的最大公因数.

10. m 个盒子, 每个盒子中有一些球, 设 $n < m$ 为一已知自然数, 施行下面的“运算”: 从这些盒子中取 n 个球后, 再在指定的盒子中放入一个球. 证明若 $(m, n) = 1$, 则可以在施行有限次“运算”后, 使所有的盒子中含有相等数目的球.

11. 证明存在无穷多个合数 n , 使对任意整数 a 有 $n | (a^{n-1} - a)$.

12. (1) 把 4444^{4444} 写成十进制数时, 它的各位数码之和是 A , 而 A 的各位数码之和是 B , 求 B 的各位数码之和 C .

(2) 设 α 与 β 是两个 $1 \sim 9$ 的整数, 类似(1)的情况, 研究 $(\alpha \cdots \alpha)^{\alpha \cdots \alpha}$ 及 $(\beta \cdots \beta)^{\alpha \cdots \alpha}$ 的第三次的各位数码之和.

13. 证明不存在这样的整系数多项式(非常数) $f(n)$, 使得对任意自然数 n , $f(n)$ 均是素数. 另问, 是否存在整系数的非零次多项式 $g(n)$, 使对任意自然数 n , 其值 $g(n)$ 均为合数?

14. 设 a, b, c, d 是正整数, 且 $ad = b^2 + bc + c^2$, 证明 $a^2 + b^2 + c^2 + d^2$ 是合数(该题是 2007 年波兰奥林匹克数学竞赛题).

15. 设 n 是奇完全数, 则它可表示成

$$n = p^\alpha q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_t^{2\beta_t}$$

其中, p, q_1, \dots, q_t 是互不相同的质数, $t \geq 2$, α, p 关于模 4 同余 1, 每个 β_i 是非负

整数.

16. 设 a, b 是正整数且满足 $(4ab-1) \mid (4a^2-1)^2$, 证明 $a=b$ (该题是 2007 年第 48 届国际奥林匹克数学竞赛题).

第 2 章 常用数论函数

定义域为整数集的实(复)值函数或定义域为实(复)数集的其值为整数的函数称为数论函数或算术函数. 数论理论中有许多自变量取整数的函数或其值为整数的函数, 如 n^a , $\lg 2n$, $n!$, 数列 a_n 等函数, 还有一些特殊的这类函数, 它们在数论研究中有着重要的作用. 本章将介绍 Gauss 函数, Euler 函数, Möbius 函数及 Möbius 反演公式.

2.1 Gauss 函数 $[x]$

定义 2.1 对任意的 $x \in \mathbb{R}$, 规定 $[x]$ 为不大于 x 的最大整数, 则 $[x]$ 是定义域为 \mathbb{R} 的一个函数, 称为 Gauss 函数.

如 $[-3.14] = -4$, $[-0.14] = -1$, $[-3] = -3$, $[3.14] = 3$.

由 Gauss 函数的定义可知, 对任意实数 a , 均有 $a = [a] + a'$, 其中, $0 \leq a' < 1$. 将 a' 称为 a 的小数部分, 记作 $\{a\}$, 于是 $a = [a] + \{a\}$.

Gauss 函数的性质定理 设 x, y 为实数, 则有

(1) $[x] \leq x < [x] + 1$.

(2) 当 $x \leq y$ 时, $[x] \leq [y]$.

(3) $[n+x] = n + [x]$, 其中, $n \in \mathbb{Z}$.

(4) $[x] + [y] \leq [x+y] \leq [x] + [y] + 1$.

(5) 若 $[x] = [y]$, 则 $|x-y| < 1$.

(6) $[x] = \begin{cases} -[x]-1, & x \text{ 非整数} \\ -[x], & x \text{ 为整数} \end{cases}$.

(7) 若 $x \geq 0, y \geq 0$, 则 $[xy] \geq [x][y]$.

(8) 若 n 为正整数, 则 $\left[\frac{[x]}{n} \right] = \left[\frac{x}{n} \right]$.

(9) 若 x 为正实数, n 为正整数, 则在不超过 x 的正整数中, n 的倍数共有 $\left[\frac{x}{n} \right]$ 个.

(10) 设 p 为素数, 在 $n!$ 中所含 p 的最高乘方次数记为 $p(n!)$, 则

$$p(n!) = \sum_{k=1}^m \left[\frac{n}{p^k} \right], \text{ 其中, } p^m \leq n < p^{m+1}$$

证 (3) 由(1)有, $[x] \leq x < [x] + 1$, 则 $n + [x] \leq n + x < n + [x] + 1$, 从而有

$$[n + [x]] \leq [n + x] < n + [x] + 1$$

即有

$$n + [x] \leq [n + x] < n + [x] + 1$$

因此

$$[n + x] = n + [x]$$

(4) 设 $x = [x] + \alpha, y = [y] + \beta$, 其中, $0 \leq \alpha, \beta < 1$, 则有

$$x + y = [x] + [y] + \alpha + \beta$$

因为 $0 \leq \alpha + \beta < 2$, 故 $[\alpha + \beta] = 0$ 或 1 , 从而由(3)知

$$[x + y] = [x] + [y] + [\alpha + \beta] = [x] + [y] \text{ 或 } [x] + [y] + 1$$

即有

$$[x] + [y] \leq [x + y] \leq [x] + [y] + 1$$

(8) 令 $\left[\frac{x}{n}\right] = a$, 则有

$$a \leq \frac{x}{n} < a + 1$$

即有

$$\begin{aligned} an &\leq x < na + n \\ an &\leq [x] < na + n \end{aligned}$$

亦即

$$a \leq \frac{[x]}{n} < a + 1$$

从而

$$a \leq \left[\frac{[x]}{n}\right] < a + 1$$

故有

$$\left[\frac{[x]}{n}\right] = a$$

(9) 因为 $\left[\frac{x}{n}\right] \leq \frac{x}{n} < \left[\frac{x}{n}\right] + 1$, 即有

$$\left[\frac{x}{n}\right]n \leq x < \left(\left[\frac{x}{n}\right] + 1\right) \cdot n$$

所以, 不超过 x 的正整数中, n 的倍数的数有 $n, 2n, \dots, \left[\frac{x}{n}\right] \cdot n$, 总共为 $\left[\frac{x}{n}\right]$ 个.

(10) 因 p 为质数, 若 $p \mid n!$, 则 p 一定能够整除 $1, 2, \dots, n$ 中某数, 而 $1, 2, \dots, n$ 中有 $\left[\frac{n}{p}\right]$ 个 p 的倍数

$$p, 2p, \dots, \left[\frac{n}{p}\right] \cdot p$$

于是, $n!$ 中 p 的最高乘方次数就是乘积

$$p \cdot 2p \cdots \left[\frac{n}{p} \right] \cdot p = \left[\frac{n}{p} \right]! \cdot p^{\left[\frac{n}{p} \right]}$$

中 p 的最高乘方次数, 因此

$$p(n!) = \left[\frac{n}{p} \right] + p \left(\left[\frac{n}{p} \right]! \right) \quad (2.1.1)$$

同理可得

$$p \left(\left[\frac{n}{p} \right]! \right) = \left[\frac{\left[\frac{n}{p} \right]}{p} \right] + p \left(\left[\frac{\left[\frac{n}{p} \right]}{p} \right]! \right) = \left[\frac{n}{p^2} \right] + p \left(\left[\frac{n}{p^2} \right]! \right)$$

则

$$p(n!) = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + p \left(\left[\frac{n}{p^2} \right]! \right) \quad (2.1.2)$$

由于 $p^{m+1} > n$, 故 $\left[\frac{n}{p^{m+1}} \right] = 0$. 将式(2.1.1)结果多次应用于式(2.1.2), 最后即可得

$$p(n!) = \sum_{k=1}^m \left[\frac{n}{p^k} \right]$$

该结论又称为 Legendre 定理.

Hermite 恒等式定理 设 x 是任意实数, n 是正整数, 那么有

$$\lceil nx \rceil = \lceil x \rceil + \left\lceil x + \frac{1}{n} \right\rceil + \left\lceil x + \frac{2}{n} \right\rceil + \cdots + \left\lceil x + \frac{n-1}{n} \right\rceil$$

证法一 令 $f(x) = \lceil nx \rceil - \lceil x \rceil - \left\lceil x + \frac{1}{n} \right\rceil - \left\lceil x + \frac{2}{n} \right\rceil - \cdots - \left\lceil x + \frac{n-1}{n} \right\rceil$, 则

$$\begin{aligned} f\left(x + \frac{1}{n}\right) &= \lceil nx + 1 \rceil - \left\lceil x + \frac{1}{n} \right\rceil - \left\lceil x + \frac{2}{n} \right\rceil - \cdots - \left\lceil x + \frac{n-1}{n} \right\rceil - \lceil x + 1 \rceil \\ &= \lceil nx \rceil - \lceil x \rceil - \left\lceil x + \frac{1}{n} \right\rceil - \left\lceil x + \frac{2}{n} \right\rceil - \cdots - \left\lceil x + \frac{n-1}{n} \right\rceil = f(x) \end{aligned}$$

当 $0 \leq x \leq \frac{1}{n}$ 时, $f(x) = 0$. 当 $\frac{1}{n} \leq x \leq \frac{2}{n}$ 时, $f(x) = f\left(x - \frac{1}{n}\right) = 0$.

如此继续可推得, 当 $\frac{k}{n} \leq x \leq \frac{k+1}{n}$ 时, $f(x) = f\left(x - \frac{1}{n}\right) = 0$, 其中, k 为任何非负的整数. 因此, 当 x 为非负实数时, 有 $f(x) = 0$.

当 $-\frac{1}{n} \leq x < 0$ 时, 有

$$\lceil nx \rceil = -1, \quad \lceil x \rceil = -1, \quad \left\lceil x + \frac{i}{n} \right\rceil = 0, \quad 1 \leq i \leq n-1$$

所以

$$\begin{aligned} f(x) &= [nx] - [x] - \left[x + \frac{1}{n}\right] - \left[x + \frac{2}{n}\right] - \cdots - \left[x + \frac{n-1}{n}\right] \\ &= -1 - (-1) - 0 - 0 - \cdots - 0 = 0 \end{aligned}$$

当 $-\frac{2}{n} \leq x < -\frac{1}{n}$ 时, 有 $f(x) = f\left(x + \frac{1}{n}\right) = 0$.

如此继续可推得, 当 $-\frac{k+1}{n} \leq x < -\frac{k}{n}$ 时, 有 $f(x) = f\left(x + \frac{1}{n}\right) = 0$. 其中, k 为任何非负整数, 因此, 当 x 为负实数时有 $f(x) = 0$. 因此, 当 x 为实数时有 $f(x) = 0$, 即

$$[nx] = [x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right]$$

证法二 由带余除法, 可设

$$[nx] = nq + r, \quad 0 \leq r < n$$

于是

$$nq + r \leq nx < nq + r + 1$$

即

$$q + \frac{r}{n} \leq x < q + \frac{r+1}{n}$$

从而

$$q + \frac{r+i}{n} \leq x + \frac{i}{n} < q + \frac{r+i+1}{n}$$

则

$$\left[x + \frac{i}{n}\right] = \begin{cases} q, & 0 \leq i \leq n-r-1 \\ q+1, & n-r \leq i \leq n-1 \end{cases}$$

因此

$$\begin{aligned} & [x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right] \\ &= \sum_{i=0}^{n-r-1} \left[x + \frac{i}{n}\right] + \sum_{i=n-r}^{n-1} \left[x + \frac{i}{n}\right] = q(n-r) + (q+1)r \\ &= nq + r = [nx] \end{aligned}$$

例 2.1 求 1842~1997 的整数中 7 的倍数的个数.

解 因为 $\left[\frac{1842}{7}\right] = 263$ 及 $\left[\frac{1997}{7}\right] = 285$, 所以, 个数为 $285 - 263 = 22$.

例 2.2 求 35! 的素因数分解式.

解 不超过 35 的素数有下列 11 个:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$$

因为

$$\begin{aligned}
 2(35!) &= \left[\frac{35}{2} \right] + \left[\frac{35}{2^2} \right] + \left[\frac{35}{2^3} \right] + \left[\frac{35}{2^4} \right] + \left[\frac{35}{2^5} \right] + \dots \\
 &= 17 + 8 + 4 + 2 + 1 + 0 \\
 &= 32
 \end{aligned}$$

$$\begin{aligned}
 3(35!) &= \left[\frac{35}{3} \right] + \left[\frac{35}{3^2} \right] + \left[\frac{35}{3^3} \right] + \left[\frac{35}{3^4} \right] + \dots \\
 &= 11 + 3 + 1 + 0 \\
 &= 15
 \end{aligned}$$

$$\begin{aligned}
 5(35!) &= \left[\frac{35}{5} \right] + \left[\frac{35}{5^2} \right] + \left[\frac{35}{5^3} \right] + \dots \\
 &= 7 + 1 + 0 \\
 &= 8
 \end{aligned}$$

$$\begin{aligned}
 7(35!) &= \left[\frac{35}{7} \right] + \left[\frac{35}{7^2} \right] + \dots \\
 &= 5 + 0 \\
 &= 5
 \end{aligned}$$

$$\begin{aligned}
 11(35!) &= \left[\frac{35}{11} \right] + \left[\frac{35}{11^2} \right] + \dots \\
 &= 3 + 0 \\
 &= 3
 \end{aligned}$$

$$\begin{aligned}
 13(35!) &= \left[\frac{35}{13} \right] + \left[\frac{35}{13^2} \right] + \dots \\
 &= 2 + 0 \\
 &= 2
 \end{aligned}$$

$$\begin{aligned}
 17(35!) &= \left[\frac{35}{17} \right] + \left[\frac{35}{17^2} \right] + \dots \\
 &= 2 + 0 \\
 &= 2
 \end{aligned}$$

$$\begin{aligned}
 19(35!) &= \left[\frac{35}{19} \right] + \left[\frac{35}{19^2} \right] + \dots \\
 &= 1 + 0 \\
 &= 1
 \end{aligned}$$

$$23(35!) = 29(35!) = 31(35!) = 1$$

所以, $35!$ 的素因数分解式为

$$35! = 2^{32} \times 3^{15} \times 5^8 \times 7^5 \times 11^3 \times 13^2 \times 17^2 \times 19 \times 23 \times 29 \times 31$$

例 2.3 求 $2000!$ 中末尾零的个数.

解 由于末尾的每个零有一个素因子 2 及一个素因子 5 产生,因此, $2000!$ 的素因数分解式中, 5 与 2 的幂次的最小者即是 $2000!$ 的末尾零的个数, 而显然 $2000!$ 的素因数标准分解中 5 的幂次不大于 2 的幂次, 所以, $2000!$ 的末尾零的个数等于 $5(2000!)$. 由于

$$\begin{aligned} 5(2000!) &= \left[\frac{2000}{5} \right] + \left[\frac{2000}{5^2} \right] + \left[\frac{2000}{5^3} \right] + \left[\frac{2000}{5^4} \right] + \left[\frac{2000}{5^5} \right] + \cdots \\ &= 400 + 80 + 16 + 3 + 0 = 499 \end{aligned}$$

因此, $2000!$ 的末尾零的个数为 499.

例 2.4 证明 $\sum_{k=0}^{\infty} \left[\frac{x+2^k}{2^{k+1}} \right] = [x]$ (第 10 届国际数学奥林匹克竞赛题).

证 由 Hermite 恒等式 $(n \rightarrow 2, x \rightarrow \frac{x}{2^{n+1}})$, 有

$$\left[\frac{x+2^k}{2^{k+1}} \right] = \left[\frac{x}{2^{k+1}} + \frac{1}{2} \right] = \left[\frac{x}{2^k} \right] - \left[\frac{x}{2^{k+1}} \right]$$

于是

$$\sum_{k=0}^{\infty} \left[\frac{x+2^k}{2^{k+1}} \right] = \left([x] - \left[\frac{x}{2} \right] \right) + \left(\left[\frac{x}{2} \right] - \left[\frac{x}{2^2} \right] \right) + \cdots = [x]$$

例 2.5 已知 $a, b, c \in \mathbb{R}^+$, $a+b+c=1$, 记 $M = \sqrt{3a+1} + \sqrt{3b+1} + \sqrt{3c+1}$, 求 $[M] = ?$

解 由 $a, b, c \in (0, 1)$ 知, $a^2 < a, b^2 < b, c^2 < c$, 则

$$\begin{aligned} M &> \sqrt{a^2+2a+1} + \sqrt{b^2+2b+1} + \sqrt{c^2+2c+1} \\ &= (a+1) + (b+1) + (c+1) = 4 \end{aligned}$$

另一方面

$$\begin{aligned} M &= \sqrt{(3a+1) \times 1} + \sqrt{(3b+1) \times 1} + \sqrt{(3c+1) \times 1} \\ &< \frac{(3a+1)+1}{2} + \frac{(3b+1)+1}{2} + \frac{(3c+1)+1}{2} \\ &= 3 + \frac{3}{2}(a+b+c) = 4.5 \end{aligned}$$

所以, $[M] = 4$.

例 2.6 设 $[(5\sqrt{2}+7)^{2n+1}] = A, \{(5\sqrt{2}+7)^{2n+1}\} = B$, 则 $(A+B)B = 1$.

证 由题意知, $(5\sqrt{2}+7)^{2n+1} = A+B$. 由于

$$(5\sqrt{2}+7)^{2n+1} (5\sqrt{2}-7)^{2n+1} = 1$$

所以

$$(5\sqrt{2}-7)^{2n+1} = \frac{1}{A+B}$$

显然, $(5\sqrt{2}+7)^{2n+1} - (5\sqrt{2}-7)^{2n+1}$ 为整数, 即

$$(A+B) - \frac{1}{A+B}$$

为整数. 而 A 为整数, 故

$$B - \frac{1}{A+B}$$

为整数. 但是, 有 $0 < B < 1$, 及 $0 < \frac{1}{A+B} < 1$, 从而

$$B - \frac{1}{A+B} = 0$$

即

$$B = \frac{1}{A+B}$$

亦即

$$(A+B)B = 1$$

例 2.7 计算 $[\sqrt{1}] + [\sqrt{2}] + [\sqrt{3}] + \cdots + [\sqrt{n^2-1}]$.

解 因为

$$\begin{aligned} [\sqrt{1^2}] &= [\sqrt{1^2+1}] = [\sqrt{(1+1)^2-1}] = 1 \\ [\sqrt{2^2}] &= [\sqrt{2^2+1}] = \cdots = [\sqrt{(2+1)^2-1}] = 2 \\ [\sqrt{3^2}] &= [\sqrt{3^2+1}] = \cdots = [\sqrt{(3+1)^2-1}] = 3 \\ &\vdots \\ [\sqrt{k^2}] &= [\sqrt{k^2+1}] = \cdots = [\sqrt{(k+1)^2-1}] = k \end{aligned}$$

所以

$$\begin{aligned} &[\sqrt{1}] + [\sqrt{2}] + [\sqrt{3}] + \cdots + [\sqrt{n^2-1}] \\ &= 1 \times 3 + 2 \times 5 + 3 \times 7 + \cdots + (n-1) \times (2(n-1)+1) \\ &= \sum_{k=1}^{n-1} k(2k+1) = 2 \sum_{k=1}^{n-1} k^2 + \sum_{k=1}^{n-1} k \\ &= 2 \frac{(n-1)n(2n-1)}{6} + \frac{n(n-1)}{2} = \frac{(n-1)n(4n+1)}{6} \end{aligned}$$

例 2.7 求和的关键在于分组, 使每一组中各项均有相同的值, 此解法称为分组凑整求和法.

例 2.8 证明: $[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+2}]$, $n \in \mathbb{N}$.

证 因为对任何正整数 a, b , 由 $a^2 + b^2 + 2ab \leq 2(a^2 + b^2)$ 可得, $\frac{a+b}{2} \leq$

$\sqrt{\frac{a^2+b^2}{2}}$, 则有

$$\frac{\sqrt{n} + \sqrt{n+1}}{2} \leq \frac{\sqrt{n+(n+1)}}{2} = \sqrt{n + \frac{1}{2}}$$

亦即

$$\sqrt{n} + \sqrt{n+1} \leq \sqrt{4n+2}$$

从而

$$[\sqrt{n} + \sqrt{n+1}] \leq [\sqrt{4n+2}]$$

另外, 若 $[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+2}]$ 不恒成立, 则存在某个自然数 m , 使得

$$[\sqrt{m} + \sqrt{m+1}] < [\sqrt{4m+2}]$$

令 $a = [\sqrt{4m+2}]$, 则

$$\sqrt{m} + \sqrt{m+1} < a \leq \sqrt{4m+2}$$

即有

$$2m+1 + 2\sqrt{m(m+1)} < a^2 \leq 4m+2$$

亦即有

$$2\sqrt{m(m+1)} < a^2 - 2m - 1 \leq 2m+1$$

各项平方后有

$$4m(m+1) < (a^2 - 2m - 1)^2 \leq 4m(m+1) + 1$$

由于上式两端为相邻整数, 故有

$$(a^2 - 2m - 1)^2 = 4m(m+1) + 1 = (2m+1)^2$$

即得

$$a^2 - 2m - 1 = 2m+1$$

亦即

$$a^2 = 4m+2$$

但是, 形如 $4k+2 (k \in \mathbb{Z})$ 的整数不可能为一平方数, 矛盾, 所以, $[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+2}]$ 对所有 $n \in \mathbb{N}$ 成立.

例 2.8 采用的是不等式证明法, 后部不等式的证明运用了反证法.

例 2.9 平面上坐标为整数的点称为整点或格点. 设 $y=f(x) (a < x \leq b)$ 是非负连续函数, 证明

(1) 区域 $a < x \leq b, 0 < y \leq f(x)$ 上的整点的个数是 $M = \sum_{a < n \leq b} [f(n)]$.

(2) $[a] - [b] < M - \sum_{a < n \leq b} f(n) \leq 0$.

证 (1) 显然上述区域上的整点是竖直线段 $x=n (a < n \leq b$ 且 n 取整数) 与水

平线段 $y=m$ (m 为整数且 $1 \leq m \leq [f([b])]$) 的交点, 对于固定的 n , 在 $x=n$ 上有 $[f(n)]$ 个这样的交点, 因此

$$M = \sum_{a < n \leq b} [f(n)]$$

即(1)成立.

(2) 因为 $[f(n)] = f(n) - \{f(n)\}$, 所以有

$$M - \sum_{a < n \leq b} f(n) = - \sum_{a < n \leq b} \{f(n)\} \leq 0$$

又因为 $\{f(n)\} < 1$, 故有 $M - \sum_{a < n \leq b} f(n) > - \sum_{a < n \leq b} 1$. 由于满足 $a < n \leq b$ 的整数 n 共有 $[b] - [a]$ 个 (大于 a 的最小整数是 $[a] + 1$, 小于 b 的最大整数是 $[b]$), 因此有

$$M - \sum_{a < n \leq b} f(n) > - ([b] - [a])$$

即

$$[a] - [b] < M - \sum_{a < n \leq b} f(n) \leq 0$$

亦即(2)成立.

练习 2.1

1. 设 a, b 是整数, $a \geq 1, b = qa + r, 0 \leq r < a$, 证明: $q = \left[\frac{b}{a} \right], r = a \left\{ \frac{b}{a} \right\}$.

2. 讨论对于任意实数 x, y , 不等式 $[xy] \geq [x][y]$ 是否成立, 为什么? 对怎样的 x 与 y , 该不等式不成立?

3. 证明下列结论.

(1) $\forall \alpha, \beta \in \mathbb{R}$, 有 $[2\alpha] + [2\beta] \geq [\alpha] + [\beta] + [\alpha + \beta]$, 但不一定有 $[3\alpha] + [3\beta] \geq [\alpha] + [\beta] + [2\alpha + 2\beta]$ 成立, 为什么?

(2) 设 m, n 是正整数, 则 $\forall \alpha, \beta \in \mathbb{R}$, 有

$$[(m+n)\alpha] + [(m+n)\beta] \geq [m\alpha] + [m\beta] + [n\alpha + n\beta]$$

成立的充分必要条件是 $m = n$.

4. 试说明对怎样的实数 x , 下面的等式成立.

$$(1) [x+1] = 1+x. \quad (2) [x] + [x] = [2x]. \quad (3) [nx] = 11.$$

$$(4) [11x] = 9. \quad (5) \left[x + \frac{1}{2} \right] + \left[x - \frac{1}{2} \right] = [2x].$$

5. 求 $21(2001!) = ?$

6. 求 $368 \sim 863$ 的整数中 13 的倍数的个数.

7. $(2000!)^2$ 的末尾有多少个连续的零?

8. 利用 Gauss 函数证明, 若 m, n 均为正整数, 则

$$(1) \frac{(n_1 + n_2 + \cdots + n_k)!}{n_1! n_2! \cdots n_k!} \text{是整数.}$$

$$(2) \frac{(2m)! (2n)!}{m! n! (m+n)!} \text{是整数.}$$

9. 设 m 是正整数, 证明

$$(1) [\sqrt{m} + \sqrt{m+1}] = [\sqrt{m} + \sqrt{m+2}].$$

$$(2) [\sqrt{m} + \sqrt{m+1}] = [\sqrt{4m+1}] = [\sqrt{4m+2}] = [\sqrt{4m+3}].$$

10. 求证

$$\left[\sqrt[3]{1 + \sqrt[3]{2 + \sqrt[3]{3 + \cdots + \sqrt[3]{2008}}} \right] = 1$$

11. 求由直线 $9x - 15y + 5 = 0$, $x = 0$ 及横坐标轴围成的三角形的内部与边上的格点数.

12. 求证 $[(2 + \sqrt{3})^n]$ 是奇数, 其中, $n \in \mathbb{N}$.

13. 求证 $\left[\frac{n}{k} \right] + \left[\frac{n+1}{k} \right] + \cdots + \left[\frac{n+k-1}{k} \right] = n$, 其中, $n, k \in \mathbb{N}$.

14. 设 a, b 是两个互质的正整数. 证明

(1) 在以坐标 $(0, 0), (0, b), (a, 0), (a, b)$ 为顶点的矩形内部有 $(a-1)(b-1)$ 个整点.

$$(2) \sum_{t=1}^{a-1} \left[\frac{bt}{a} \right] = \frac{1}{2}(a-1)(b-1).$$

15. 求 $\left[\frac{23 \times 1}{101} \right] + \left[\frac{23 \times 2}{101} \right] + \left[\frac{23 \times 3}{101} \right] + \cdots + \left[\frac{23 \times 99}{101} \right] + \left[\frac{23 \times 100}{101} \right]$ 的值.

2.2 Euler 函数

定义 2.2 对任意正整数 n , 规定 $\varphi(n)$ 为不超过 n 且与 n 互质的正整数的个数, 则 $\varphi(n)$ 是定义域为 \mathbb{N} 的函数, 称为 Euler 函数.

如 $\varphi(1) = 1, \varphi(2) = 1, \varphi(4) = 1, \varphi(10) = 4$.

Euler 函数的基本性质定理 (1) 若 p 是素数, 则 $\varphi(p) = p - 1$; 反之亦成立. 即若 p 为合数, 则有 $\varphi(p) \leq p - 2$.

(2) 不超过 n 且与 n 互质的所有正整数的和为 $\frac{1}{2}n\varphi(n)$.

(3) 若 p 是素数, 则 $\varphi(p^k) = p^{k-1}(p-1)$.

(4) 若 $m = m_1 m_2$, 且 $(m_1, m_2) = 1$, 则 $\varphi(m) = \varphi(m_1)\varphi(m_2)$.

(5) 若 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ 是 n 的质数分解, 则

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right)$$

$$= n \prod_{i=1}^t \left(1 - \frac{1}{p_i}\right) \quad \text{或} \quad n \prod_{p|n} \left(1 - \frac{1}{p}\right) \quad (p \text{ 为素数})$$

$$(6) \varphi(2n) = \begin{cases} \varphi(n), & n \text{ 为奇数} \\ 2\varphi(n), & n \text{ 为偶数} \end{cases}$$

(7) 设 d 为 n 的正约数, 则不大于 n 且与 n 有最大公因数 d 的正整数个数为 $\varphi\left(\frac{n}{d}\right)$.

(8) 自然数 n 的所有正约数的 Euler 函数值的和等于 n , 即有

$$\sum_{d|n} \varphi(d) = n \quad \text{或} \quad \sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$$

(9) 若 $a|b$, 则 $\varphi(a)|\varphi(b)$.

证 (1) 显然成立.

(2) 若 $a_1, a_2, \dots, a_{\varphi(n)}$ 是不超过 n 且与 n 互质的所有正整数, 则

$$(n - a_1), (n - a_2), \dots, (n - a_{\varphi(n)})$$

亦是不超过 n 且与 n 互质的所有正整数, 因此必有

$$a_1 + a_2 + \dots + a_{\varphi(n)} = (n - a_1) + (n - a_2) + \dots + (n - a_{\varphi(n)})$$

于是

$$2(a_1 + a_2 + \dots + a_{\varphi(n)}) = \varphi(n) \cdot n$$

即(2)成立.

(3) 因为不超过 p^k 且与 p^k 不互素, 即与 p 不互素的所有正整数为 $p, 2p, \dots, p^{k-1}p$, 共为 p^{k-1} 个整数, 故不超过 p^k 且与 p^k 互素的所有正整数的个数为 $p^k - p^{k-1}$, 即

$$\varphi(p^k) = p^{k-1}(p - 1)$$

(4) 运用概率知识来证明该结论.

记 $\Omega = \{1, 2, \dots, m\}$; $E = \{x \in \Omega | (x, m) = 1\}$; $E_i = \{x \in \Omega | (x, m_i) = 1\}$, $i = 1, 2$, 则

$$|\Omega| = m, \quad |E| = \varphi(m), \quad |E_1| = m_1 \varphi(m_1), \quad |E_2| = m_2 \varphi(m_2)$$

设事件 A 为从 Ω 中随机取一数, 该数属于 E ; 事件 A_i 为从 Ω 中随机取一数, 该数属于 E_i ($i=1, 2$). 因为任意的 $x \in \Omega$, 有 $(x, m) = 1$ 当且仅当且 $(x, m_1) = 1$, $(x, m_2) = 1$, 即事件 A 发生当且仅当事件 A_1 与事件 A_2 同时发生. 由于 $(m_1, m_2) = 1$, 故 A_1 与 A_2 是相互独立的, 从而

$$P(A) = P(A_1 \cap A_2) = P(A_1)P(A_2)$$

但是

$$P(A) = \frac{|E|}{|\Omega|} = \frac{\varphi(m)}{m}$$

$$P(A_1) = \frac{|E_1|}{|\Omega|} = \frac{m_2 \varphi(m_1)}{m} = \frac{\varphi(m_1)}{m_1}$$

$$P(A_2) = \frac{|E_2|}{|\Omega|} = \frac{m_1 \varphi(m_2)}{m} = \frac{\varphi(m_2)}{m_2}$$

所以

$$\frac{\varphi(m)}{m} = \frac{\varphi(m_1)}{m_1} \cdot \frac{\varphi(m_2)}{m_2}$$

即

$$\varphi(m) = \varphi(m_1)\varphi(m_2)$$

(5) 由(3)有, $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i-1}(p_i-1) = p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right)$, $i=1, 2, \dots, t$, 从而由(4)得

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_t^{\alpha_t}) \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_t^{\alpha_t} \left(1 - \frac{1}{p_t}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right) \\ &= n \prod_{i=1}^t \left(1 - \frac{1}{p_i}\right) \quad (p_i \text{ 为 } n \text{ 的全部不同的素因子}) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \quad (p \text{ 为素数}) \end{aligned}$$

(6) 当 n 为奇数时, $(2, n) = 1$. 由(3)有

$$\varphi(2n) = \varphi(2)\varphi(n) = 1 \cdot \varphi(n) = \varphi(n)$$

当 n 为偶数时, 对任何素数 p , $p|2n$ 当且仅当 $p|n$, 从而由(4)有

$$\varphi(2n) = (2n) \cdot \prod_{p|2n} \left(1 - \frac{1}{p}\right) = 2 \cdot \left(n \prod_{p|n} \left(1 - \frac{1}{p}\right)\right) = 2\varphi(n)$$

即(6)成立.

(7) 若 x 为任一不大于 n 且与 n 有最大公因数 d 的正整数, 则 x 必为 d 的倍数. 设 $x = dx_1$, 那么, $(x_1, n/d) = 1$. 由 $x \leq n$ 知 $x_1 \leq n/d$, 因此, x 可能的个数为 $\varphi(n/d)$.

(8) 证法一 由(7)可知: 对 n 的任一公约数 d , $\{1, 2, \dots, n\}$ 中与 n 有最大公因数 d 的数的个数为 $\varphi(n/d)$. 于是, 可按 n 的约数将集合 $\{1, 2, \dots, n\}$ 分类. 若 d_1, d_2, \dots, d_t 是 n 的全部约数(正的), 记 $S_{d_i} = \{x \in \{1, 2, \dots, n\} \mid (x, n) = d_i\}$, 则 S_{d_i} ($i=1, 2, \dots, t$) 两两不相交, 且显然

$$\{1, 2, \dots, n\} = \bigcup_{i=1}^t S_{d_i}$$

于是

$$n = \sum_{i=1}^t |S_{d_i}| = \sum_{i=1}^t \varphi(n/d_i) = \sum_{d|n} \varphi(n/d)$$

由于 $n/d_1, n/d_2, \dots, n/d_t$ 亦是 n 的全部正约数, 所以有 $\sum_{i=1}^t \varphi(n/d_i) = \sum_{i=1}^t \varphi(d_i)$, 从而

$$n = \sum_{i=1}^t \varphi(d_i) = \sum_{d|n} \varphi(d)$$

证法二 设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ 是 n 的素因数分解式, 则 n 的任一正约数 d 为 $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$, $0 \leq \beta_i \leq \alpha_i, i = 1, 2, \dots, t$, 于是由(4)得

$$\begin{aligned} \sum_{d|n} \varphi(d) &= \sum_{\substack{\beta_i=0 \\ i=1,2,\dots,t}}^{\alpha_i} \varphi(p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}) \\ &= \sum_{\substack{\beta_i=0 \\ i=1,2,\dots,t}}^{\alpha_i} \left(\prod_{i=1}^t \varphi(p_i^{\beta_i}) \right) = \prod_{i=1}^t \left(\sum_{\beta_i=0}^{\alpha_i} \varphi(p_i^{\beta_i}) \right) \quad (2.2.1) \end{aligned}$$

由(3)可得, $\sum_{\beta_i=0}^{\alpha_i} \varphi(p_i^{\beta_i}) = \sum_{\beta_i=0}^{\alpha_i} (p_i^{\beta_i} - p_i^{\beta_i-1}) = p_i^{\alpha_i}$. 代入式(2.2.1)得

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^t (p_i^{\alpha_i}) = n$$

(9) 利用(5)易得.

对于任意的两个正整数 m 与 n , 若 $(m, n) = 1$, 有性质 $\varphi(mn) = \varphi(m)\varphi(n)$. 而当 $(m, n) = d > 1$, 则有下述定理.

定理 2.1 若 $(m, n) = d$, 则有

$$\varphi(mn) = \frac{d}{\varphi(d)} \varphi(m)\varphi(n)$$

证法一 由性质(4)有

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn} \left(1 - \frac{1}{p}\right)$$

由于 mn 的素因子包括 m 与 n 的共同的素因子(即 d 的素因子)及 m 与 n 的不同的素因子, 因此

$$\prod_{p|mn} \left(1 - \frac{1}{p}\right) = \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|d} \left(1 - \frac{1}{p}\right)} = \frac{\varphi(m)}{m} \cdot \frac{\varphi(n)}{\varphi(d)}$$

即有

$$\varphi(mn) = \frac{d}{\varphi(d)}\varphi(m)\varphi(n)$$

证法二 用概率知识证明.

首先设 $d=1$. 记 $\Omega = \{1, 2, \dots, mn\}$, $E = \{x \in \Omega \mid (x, mn) = 1\}$, $E_1 = \{x \in \Omega \mid (x, m) = 1\}$, $E_2 = \{x \in \Omega \mid (x, n) = 1\}$, 则 $|\Omega| = mn$, $|E| = \varphi(mn)$, $|E_1| = n\varphi(m)$, $|E_2| = m\varphi(n)$.

设事件 A 为从 Ω 中随机取一数, 该数属于 E ; 设事件 $A_i (i=1, 2)$ 为从 Ω 中随机取一数, 该数属于 $E_i (i=1, 2)$.

(1) 因为 $\forall x \in \Omega$ 有 $(x, mn) = 1$, 当且仅当 $(x, m) = 1$ 且 $(x, n) = 1$, 即“事件 A 发生”当且仅当“事件 A_1 与事件 A_2 同时发生”. 如果 $(m, n) = 1$, 则事件 A_1 与事件 A_2 相互独立, 从而由独立事件概型的乘法定理知

$$P(A) = P(A_1 A_2) = P(A_1)P(A_2)$$

又因为

$$\begin{aligned} P(A) &= \frac{|E|}{|\Omega|} = \frac{\varphi(mn)}{mn} \\ P(A_1) &= \frac{|E_1|}{|\Omega|} = \frac{n\varphi(m)}{mn} = \frac{\varphi(m)}{m} \\ P(A_2) &= \frac{|E_2|}{|\Omega|} = \frac{m\varphi(n)}{mn} = \frac{\varphi(n)}{n} \end{aligned}$$

所以

$$\frac{\varphi(mn)}{mn} = \frac{\varphi(m)}{m} \cdot \frac{\varphi(n)}{n}$$

即 $\varphi(mn) = \varphi(m)\varphi(n)$.

(2) 如果 $(m, n) = d (d > 1)$, 即事件 A_1 与事件 A_2 不相互独立, 则由事件的条件概型公式知

$$P(A) = P(A_1) \cdot P(A_2 | A_1)$$

然后计算出 $P(A_2 | A_1) = \frac{d\varphi(n)}{\varphi(d)n}$, 则

$$\frac{\varphi(mn)}{mn} = \frac{\varphi(m)}{m} \cdot \frac{d\varphi(n)}{\varphi(d)n}$$

即 $\varphi(mn) = \frac{d}{\varphi(d)} \cdot \varphi(m)\varphi(n)$.

下面介绍 Euler 函数的若干应用.

例 2.10 证明素数有无穷多个.

证 设素数只有有限个 p_1, p_2, \dots, p_n . 令 $a = p_1 p_2 \cdots p_n$, 则在 $1 \sim a$ 的所有正整数中, 与 a 互素的只有一个, 即 1. 因此, $\varphi(a) = 1$, 但

$$\begin{aligned}\varphi(a) &= \varphi(p_1 p_2 \cdots p_n) = \varphi(p_1) \varphi(p_2) \cdots \varphi(p_n) \\ &= (p_1 - 1)(p_2 - 1) \cdots (p_n - 1) > 1\end{aligned}$$

矛盾. 所以, 素数有无穷多个.

例 2.11 将与 105 互素的所有正整数从小到大排列成数列, 试求出这个数列的第 1000 项(该题为 1994 年全国高中数学联赛题).

解 设此数列为 $\{a_n\}$. 求 $a_{1000} = ?$

1~105 的所有正整数中共有 $\varphi(105) = \varphi(3)\varphi(5)\varphi(7) = 48$ 个与 105 互素, 它们从小到大的排列是

$$a_1 = 1, a_2 = 2, a_3 = 4, a_4 = 8, a_5 = 11, \cdots, a_{48} = 104$$

对于任一 $a_n (n \geq 1)$, 由带余除法存在唯一的 q 与 r , 使

$$a_n = 105q + r, \quad \text{其中, } q \geq 0, \quad 0 \leq r < 105$$

由 $(a_n, 105) = 1$ 推得 $(r, 105) = 1$, 即 $r \in \{a_1, a_2, \cdots, a_{48}\}$.

反之, 对于任意固定非负整数 q 与 $r \in \{a_1, a_2, \cdots, a_{48}\}$ 有, $(105q + r, 105) = 1$, 于是

$$105q + r \in \{a_n\}$$

从而存在正整数 n , 使 $a_n = 105q + r$. 因此, $\{a_n\}$ 是仅由形如 $105q + a_i (i = 1, 2, \cdots, 48)$ 的数从小到大排列而成的.

因 $1000 = 48 \times 20 + 40$, 故 $a_{1000} = 105 \times 20 + a_{40}$. 再由 $a_{48} = 104$, 易求得 $a_{40} = 86$. 所以

$$a_{1000} = 105 \times 20 + 86 = 2186$$

例 2.12 设 n 与 a 均为整数, $n > 1$, 且 $(a, n) = 1$. $a_1, a_2, \cdots, a_{\varphi(n)}$ 表示不超过 n 且与 n 互素的 $\varphi(n)$ 个整数, 则

$$\sum_{i=1}^{\varphi(n)} \left\{ \frac{a a_i}{n} \right\} = \frac{1}{2} \varphi(n)$$

证 由 $(a, n) = 1$ 知 $(a a_i, n) = 1$, 利用带余除法可设 $a a_i = q_i n + r_i$, 其中, $1 \leq r_i \leq n-1$, 于是

$$\left\{ \frac{a a_i}{n} \right\} = \frac{r_i}{n}$$

且由 $(a a_i, n) = 1$ 得 $(r_i, n) = 1, i = 1, 2, \cdots, \varphi(n)$, 所以, $r_1, r_2, \cdots, r_{\varphi(n)}$ 是所有不超过 n 且与 n 互素的正整数, 从而 $n - r_1, n - r_2, \cdots, n - r_{\varphi(n)}$ 亦是所有不超过 n 且与 n 互素的正整数, 所以

$$\sum_{i=1}^{\varphi(n)} \left\{ \frac{a a_i}{n} \right\} = \sum_{i=1}^{\varphi(n)} \left\{ \frac{r_i}{n} \right\} = \frac{1}{n} \sum_{i=1}^{\varphi(n)} r_i = \frac{1}{n} \sum_{i=1}^{\varphi(n)} (n - r_i) = \varphi(n) - \frac{1}{n} \sum_{i=1}^{\varphi(n)} r_i$$

亦即

$$\frac{1}{n} \sum_{i=1}^{\varphi(n)} r_i = \varphi(n) - \frac{1}{n} \sum_{i=1}^{\varphi(n)} r_i$$

故

$$\sum_{i=1}^{\varphi(n)} \left\{ \frac{a a_i}{n} \right\} = \frac{1}{n} \sum_{i=1}^{\varphi(n)} r_i = \frac{1}{2} \varphi(n)$$

利用例 2.12, 可以很容易地证明

$$\sum_{i=1}^{\varphi(n)} \left[\frac{a a_i}{n} \right] = \frac{(a-1)\varphi(n)}{2}$$

这是因为

$$\begin{aligned} \sum_{i=1}^{\varphi(n)} \left[\frac{a a_i}{n} \right] &= \sum_{i=1}^{\varphi(n)} \left(\frac{a a_i}{n} - \left\{ \frac{a a_i}{n} \right\} \right) = \sum_{i=1}^{\varphi(n)} \frac{a a_i}{n} - \sum_{i=1}^{\varphi(n)} \left\{ \frac{a a_i}{n} \right\} \\ &= \frac{a}{n} \sum_{i=1}^{\varphi(n)} a_i - \frac{1}{2} \varphi(n) = \frac{a}{n} \cdot \frac{1}{2} n \varphi(n) - \frac{1}{2} \varphi(n) = \frac{(a-1)\varphi(n)}{2} \end{aligned}$$

上式中倒数第二个等号利用了性质定理(2).

读者可类似证明下列结论.

设 $a, b, n (n > 1)$ 是正整数, 且 $(a, n) = 1$, 则有

$$(1) \sum_{k=0}^{n-1} \left\{ \frac{ak+b}{n} \right\} = \frac{1}{2}(n-1).$$

$$(2) \sum_{k=1}^{n-1} \left[\frac{ak}{n} \right] = \frac{1}{2}(a-1)(n-1).$$

例 2.13 设 $\varphi(n) = \frac{1}{3}n$, 求 $n = ?$

解 设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ 是 n 的素因数分解, 且 $p_1 < p_2 < \cdots < p_t$, 则由 $\varphi(n) = \frac{1}{3}n$ 得等式

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right) = \frac{1}{3} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

即有

$$3(p_1 - 1) \cdots (p_t - 1) = p_1 p_2 \cdots p_t \quad (2.2.2)$$

因为 $p_1 < p_2 < \cdots < p_t$, 且 $p_t | 3(p_1 - 1) \cdots (p_t - 1)$ 及 p_t 为素数, 知 $p_t \geq 3$, 从而 $t = 1, 2$. 如果 $t = 1$, 则 $n = 3^{\alpha_1}$. 由式(2.2.2)得 $3(3-1) = 3$, 矛盾, 故 $t = 2$. 从而 $p_1 = 2, p_2 = 3$. 此时, $n = 2^{\alpha_1} 3^{\alpha_2}$ 且式(2.2.2)成立, 即 $\varphi(n) = \frac{1}{3}n$ 成立. 所以

$$n = 2^{\alpha_1} 3^{\alpha_2}$$

其中, α_1, α_2 是大于 0 的整数.

例 2.14 证明若 n 是合数, 则 $\varphi(n) \leq n\sqrt{n}$.

证 分三种情况来证明.

(1) 若 $n = p^\alpha, \alpha > 1, p$ 为素数, 则有

$$\begin{aligned} \varphi(n) &= \varphi(p^a) = p^a - p^{a-1} = p^a - p^{\frac{a}{2}} \cdot p^{\frac{a}{2}-1} \leq p^a - p^{\frac{a}{2}} = n - \sqrt{n} \\ (2) \text{ 若 } n &= p^a q, a \geq 1, q \text{ 与 } p \text{ 为互异素数, 则} \\ \varphi(n) &= \varphi(p^a)\varphi(q) = (p^a - p^{a-1})(q-1) = p^a q - (p^{a-1}q + p^a - p^{a-1}) \end{aligned} \tag{2.2.3}$$

由于

$$p^{a-1}q + p^a - p^{a-1} \geq 2(p^{a-1}q)^{\frac{1}{2}}(p^a)^{\frac{1}{2}} - p^{a-1} = 2p^{a-\frac{1}{2}}q^{\frac{1}{2}} - p^{a-1} > p^{\frac{a}{2}}q^{\frac{1}{2}}$$

因此由式(2.2.3)得

$$\varphi(n) < p^a q - p^{\frac{a}{2}}q^{\frac{1}{2}} = n - \sqrt{n}$$

(3) 若 $n = p^a q, a \geq 1, (p, q) = 1, p$ 为素数, q 为合数, 则依据第二数学归纳法, q 是比 n 小的合数, 因而 $\varphi(q) \leq q - q^{\frac{1}{2}}$, 所以

$$\begin{aligned} \varphi(n) &= (p^a - p^{a-1})\varphi(q) \leq (p^a - p^{a-1})(q - q^{\frac{1}{2}}) \\ &= p^a q - (p^{a-1}q + p^a q^{\frac{1}{2}} - p^{a-1}q^{\frac{1}{2}}) \\ &= p^a q - p^{\frac{a}{2}}q^{\frac{1}{2}}(p^{\frac{a}{2}-1}q^{\frac{1}{2}} + p^{\frac{a}{2}} - p^{\frac{a}{2}-1}) \\ &< p^a q - p^{\frac{a}{2}}q^{\frac{1}{2}} = n - \sqrt{n} \end{aligned}$$

在例 2.14 的证明过程中, 可以看出, 如果 n 是一个不等于某素数平方的合数, 则等号不成立, 即有 $\varphi(n) < n - \sqrt{n}$.

对于给定的正整数 n 与 m , 等式 $\varphi(nm) = \varphi(n) + \varphi(m)$ 不一定成立, 如 $m = n = 1, 1 \neq 2; m = 2, n = 3$ 时, $2 \neq 3$; 那么, 有哪些整数对 m 与 n 使该等式成立? 下面来求出这些整数对.

例 2.15 求方程 $\varphi(xy) = \varphi(x) + \varphi(y)$ 的正整数解.

解 由定理 2.1 可知, $\varphi(xy) = \frac{d}{\varphi(d)}\varphi(x)\varphi(y)$, 其中, d 为 x 与 y 的公约数, 则方程 $\varphi(xy) = \varphi(x) + \varphi(y)$ 变为 $d\varphi(x)\varphi(y) = \varphi(x)\varphi(d) + \varphi(y)\varphi(d)$, 即有

$$d = \frac{\varphi(d)}{\varphi(y)} + \frac{\varphi(d)}{\varphi(x)}$$

亦即

$$d = \frac{1}{\frac{\varphi(y)}{\varphi(d)}} + \frac{1}{\frac{\varphi(x)}{\varphi(d)}} \tag{2.2.4}$$

由性质定理(9)知 $\varphi(x)/\varphi(d)$ 及 $\varphi(y)/\varphi(d)$ 均为整数, 所以, 要使式(2.2.4)成立, 只有

$$\varphi(x)/\varphi(d) = \varphi(y)/\varphi(d) = 1 \text{ 或 } 2$$

此时, $d = 2$ 或 1 .

(1) 若 $\varphi(x)/\varphi(d) = \varphi(y)/\varphi(d) = 1$, 即 $d = 2$, 则

$$\varphi(x) = \varphi(y) = \varphi(d) = \varphi(2) = 1$$

从而 $x=y=2$.

(2) 若 $\varphi(x)/\varphi(d) = \varphi(y)/\varphi(d) = 2$, 即 $d=1$, 则 $\varphi(x) = \varphi(y) = 2$. 由于使 $\varphi(x)=2$ 的正整数只有 $x=3, 4$ 或 6 , 从而由 $d=1$ 知, $x=3, y=4$ 或 $x=4, y=3$. 综上知, 原方程的解为三对

$$\begin{cases} x=2 \\ y=2 \end{cases}, \quad \begin{cases} x=3 \\ y=4 \end{cases}, \quad \begin{cases} x=4 \\ y=3 \end{cases}$$

下面再来看一个与 Euler 方程函数有关的数论方程.

例 2.16 设 k 是任一给定的正整数, 求证方程 $\varphi(x+k) - \varphi(x) = 0$ 有正整数解.

分析 对任意给定的正整数 k , 取 $x=mk$, 则方程 $\varphi(x+k) - \varphi(x) = 0$ 变为

$$\varphi((m+1)k) - \varphi(mk) = 0$$

如果 $(m+1)$ 与 k 互素, 则得方程

$$\varphi(m+1)\varphi(k) - \varphi(mk) = 0$$

如果 $(m+1)$ 是素数, 则得方程

$$m\varphi(k) - \varphi(mk) = 0 \tag{2.2.5}$$

如果 mk 与 k 有相同的素因数, 那么, 利用性质定理(5)可证式(2.2.5)成立(请读者自证). 因此, 可得如下证明.

证 取 $x=(p-1)k$, 其中, p 是使 $p \nmid k$ 成立的最小素数, 则 $(p-1)$ 与 k 有相同的素因数(否则有 $(p-1)$ 的素因数 q 使 $q \nmid k$, 这与 p 的最小性矛盾). 于是, 由上面的分析得

$$\varphi((p-1)k) = (p-1)\varphi(k)$$

即

$$\varphi((p-1)k) = \varphi(p)\varphi(k)$$

再由性质定理(4)得

$$\varphi((p-1)k) = \varphi(pk)$$

亦即

$$\varphi(x) = \varphi(x+k)$$

这说明 $x=(p-1)k$ 是方程 $\varphi(x) - \varphi(x+k) = 0$ 的正整数解.

显然, 例 2.16 的证明中给出的解不一定是该方程的唯一解, 如 $k=1$ 时, 取 $x=1$ 或 3 均有 $\varphi(1+1) = \varphi(1)$, $\varphi(3+1) = \varphi(3)$; 如 $k=5$, 则取 $x=5$ 及 $x=15$ 均是该方程的解. 于是提出如下问题.

问题 1 对固定的正整数 k , 方程 $\varphi(x) - \varphi(x+k) = 0$ 的最小正整数解是什么?

问题 2 对固定的正整数 k , 方程 $\varphi(x) - \varphi(x+k) = 0$ 的全部正整数解是什

么? 以上问题可针对某些特殊的正整数 k 进行讨论.

练 习 2.2

1. 求下列数论方程的所有正整数解.

$$(1) \varphi(x) = \varphi(2x), \quad (2) \varphi(3x) = \varphi(4x).$$

$$(3) \varphi(3x) = 2\varphi(x), \quad (4) \varphi(x+y) = \varphi(x) + \varphi(y).$$

2. 证明分母不大于 n 的既约真分数的个数等于 $\varphi(2) + \varphi(3) + \cdots + \varphi(n)$.

3. 对给定的正整数 k , 求解下列数论方程.

$$(1) \varphi(x) = 8k + 4, \quad (2) \varphi(x) = 6k + 3.$$

4. 你能找出方程 $\varphi(\varphi(x)) = \varphi(x)$ 的几个正整数解?

5. 设 n 与 m 是大于 1 的任意两正整数.

(1) 求所有不超过 n 且与 n 互素的正整数之和 S_n .

(2) 求所有不超过 n 且与 m 互素的正整数之和 $S_{n,m}$.

(3) 如果 $S_n = S_m$, 证明 $n = m$.

2.3 积性函数

2.2 节讨论的 Euler 函数有这样一个性质: 若 $(n, m) = 1$, 则 $\varphi(mn) = \varphi(m)\varphi(n)$. 具有这一性质的数论函数在计算其值或证明有关结论时, 利用整数的素数分解, 可达到“大事化小”、“繁事化简”的效果. 因此, 具有这一性质特征的数论函数很值得作进一步的学习研究.

定义 2.3 设 $f(x)$ 是定义域为正整数集的一个不恒等于零的数论函数, 若 $f(x)$ 满足: 对任意 n, m 为正整数, $(n, m) = 1$, 有

$$f(nm) = f(n)f(m) \quad (2.3.1)$$

则称 $f(x)$ 是一个积性函数.

Euler 函数是积性函数. $f(x) = x^\alpha (x \in \mathbb{N})$ 是积性函数 (α 是任一实数). 同样, $f(x) = a^{\ln x} (x \in \mathbb{N}, a > 0)$ 也是积性函数.

显然, Gauss 函数不一定是积性函数(为什么?). Gauss 函数在什么情况下成为积性函数?

下面再看几个重要的积性函数.

例 2.17 设 n 是任一正整数, 分别用 $T(n)$, $S(n)$ 及 $P(n)$ 表示 n 的所有正约数的个数、 n 的所有正约数之和及 n 的所有正约数之积, 则 $T(n)$, $S(n)$ 是积性函数, 而 $P(n)$ 是非积性函数.

已经证明了如下结果(定理 1.12).

$$(1) T(n) = \prod_{i=1}^t (\alpha_i + 1).$$

$$(2) S(n) = \prod_{i=1}^t \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right).$$

(3) $P(n) = n^{\frac{1}{2}T(n)}$. 若 d 是 n 的任一正约数, 则显然 d 具有如下形式:

$$d = p_1^{d_1} p_2^{d_2} \cdots p_t^{d_t}, \quad 0 \leq d_i \leq \alpha_i, \quad i = 1, 2, \dots, t$$

请读者自行用式(2.3.1)证明式(3).

以下证明 $T(n)$ 及 $S(n)$ 是积性函数.

若 a 与 b 是互素的两整数, 且

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

与

$$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

是它们的素因数分解, 则

$$ab = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

是 ab 的素因数分解.

于是, 由式(1)知

$$T(ab) = (\alpha_1 + 1) \cdots (\alpha_t + 1) (\beta_1 + 1) \cdots (\beta_s + 1) = T(a)T(b)$$

依定义, $T(n)$ 是积性函数.

又由式(2)知

$$S(ab) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_t^{\alpha_t+1} - 1}{p_t - 1} \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{\beta_s+1} - 1}{q_s - 1} = S(a)S(b)$$

这说明 $S(n)$ 亦是积性函数.

而对 $P(n)$, 取 $a=2, b=3$, 则 $(a, b)=1$, 且

$$P(a) = P(2) = 2, \quad P(b) = P(3) = 3$$

$$P(ab) = P(6) = 1 \times 2 \times 3 \times 6 = 36 \neq P(a)P(b)$$

因此, $P(n)$ 是非积性函数. 但是, 有 $P(nm) = P(n)^{T(m)} \cdot P(m)^{T(n)}$, 其中, $(n, m)=1$.

例 2.18 定义 $f(n)$ 为正整数 n 的所有互不相同的素因数之积, 则易证 $f(n)$ 是积性函数.

若 $g(n)$ 表示 n 的所有互不相同的素因数之和, 则 $g(n)$ 是否为积性函数? 为什么?

例 2.19 设 n 为任一正整数, 定义 $\mu(n)$ 如下:

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & n \text{ 被一个素数的平方整除} \\ (-1)^r, & n \text{ 是 } r \text{ 个不同素数的乘积} \end{cases}$$

易知 $\mu(n)$ 是一个定义在正整数集上的数论函数, 此函数称为 Möbius 函数, 或称默比乌斯函数. 下面证明 Möbius 函数是积性函数.

证 设 a, b 是任意两互素的正整数, 以下分三种情况来证明 $\mu(ab) = \mu(a)\mu(b)$.

(1) 若 $ab=1$, 则 $a=b=1$, 此时

$$\mu(ab) = 1 = 1 \times 1 = \mu(a)\mu(b)$$

(2) 若 ab 至少被某一素数 p 的平方整除, 即 $p^2 | ab$, 则由 $(a, b)=1$ 知, $p^2 | a$ 或 $p^2 | b$. 于是, 此时有 $\mu(ab)=0$ 及 $\mu(a)=0$ ($p^2 | a$ 时), 或 $\mu(b)=0$ ($p^2 | b$ 时), 从而

$$\mu(ab) = 0 = \mu(a)\mu(b)$$

(3) 若 ab 是 r 个不同素数 p_1, p_2, \dots, p_r 的乘积, 则 a 必是 p_1, p_2, \dots, p_r 中某 t 个不同素数的乘积, 而 b 必是 p_1, p_2, \dots, p_r 中其余 $r-t$ 个不同素数的乘积, 于是

$$\mu(ab) = (-1)^r = (-1)^t (-1)^{r-t} = \mu(a)\mu(b)$$

综上知, 当 $(a, b)=1$ 时, 有 $\mu(ab) = \mu(a)\mu(b)$.

下面给出一个积性函数的充分必要条件.

定理 2.2 设 $f(n)$ 是一个不恒为零的数论函数, 则 $f(n)$ 是积性函数的充分必要条件是以下两条成立.

(1) $f(1)=1$.

(2) 任一正整数 n 的素因数分解 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ 有

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_t^{\alpha_t})$$

证明 必要性 由 $f(n)$ 不恒为零知, 必存在某一正整数 n_0 , 使 $f(n_0) \neq 0$, 则由 $(1, n_0)=1$ 得

$$f(n_0) = f(1 \cdot n_0) = f(1)f(n_0)$$

即有 $f(1)=1$, 亦即定理 2.2 中(1)成立. 定理 2.2 中(2)的证明显然.

充分性 设 $(a, b)=1$ (a, b 均大于 1), 且

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

与

$$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

分别是 a 与 b 的素因数分解, 则由 $(a, b)=1$ 知

$$ab = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

是 ab 的素因数分解. 于是, 由定理 2.2 中(2)得

$$f(ab) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_r^{\alpha_r}) f(q_1^{\beta_1}) f(q_2^{\beta_2}) \cdots f(q_s^{\beta_s}) = f(a)f(b)$$

若 $(a, b)=1$ 且 $a=1$ ($b=1$ 也类似), 则由定理 2.2 中(1)有 $f(a)=1$, 此时仍有 $f(ab) = f(a)f(b)$, 即 $f(n)$ 满足式(2.3.1). 因此, $f(n)$ 是积性函数.

定理 2.3 若 $f(n)$ 是积性函数, 则函数

$$F(n) = \sum_{d|n} f(d)$$

是积性函数,这里, $\sum_{d|n} f(d)$ 表示对 n 的所有正约数求和.

证 $n=1$ 时,由定理 2.2 可得, $F(1) = \sum_{d|1} f(d) = f(1) = 1$.

设 $n \neq 1$ 且 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ 是 n 的素因数分解,则若 $d|n$,

$$d = p_1^{l_1} p_2^{l_2} \cdots p_t^{l_t}, \quad 0 \leq l_i \leq \alpha_i, \quad i = 1, 2, \dots, t$$

从而

$$\begin{aligned} F(n) &= \sum_{d|n} f(d) = \sum_{l_1=0}^{\alpha_1} \cdots \sum_{l_t=0}^{\alpha_t} f(p_1^{l_1} \cdots p_t^{l_t}) \\ &= \sum_{l_1=0}^{\alpha_1} \cdots \sum_{l_t=0}^{\alpha_t} f(p_1^{l_1}) \cdots f(p_t^{l_t}) \quad (\text{由定理 2.2}) \\ &= \left(\sum_{l_1=0}^{\alpha_1} f(p_1^{l_1}) \right) \cdots \left(\sum_{l_t=0}^{\alpha_t} f(p_t^{l_t}) \right) \\ &= \sum_{d_1|p_1^{\alpha_1}} f(d_1) \cdots \sum_{d_t|p_t^{\alpha_t}} f(d_t) \\ &= F(p_1^{\alpha_1}) \cdots F(p_t^{\alpha_t}) \end{aligned}$$

因此,根据定理 2.2 知, $F(n) = \sum_{d|n} f(d)$ 是积性函数.

由定理 2.3 知, $\sum_{d|n} 1$, $\sum_{d|n} d$ 及 $\sum_{d|n} \varphi(d)$ ($f(n)$ 分别取 $1, n$ 及 $\varphi(n)$) 均是积性函数,且由定理 2.3 的证明可得

$$\begin{aligned} T(n) &= T(p_1^{\alpha_1}) T(p_2^{\alpha_2}) \cdots T(p_t^{\alpha_t}) \\ &= \sum_{d|n} 1 = \left(\sum_{d_1|p_1^{\alpha_1}} 1 \right) \cdots \left(\sum_{d_t|p_t^{\alpha_t}} 1 \right) \\ &= (\alpha_1 + 1) \cdots (\alpha_t + 1) \\ S(n) &= S(p_1^{\alpha_1}) \cdots S(p_t^{\alpha_t}) \\ &= \sum_{d|n} d = \left(\sum_{d_1|p_1^{\alpha_1}} d_1 \right) \cdots \left(\sum_{d_t|p_t^{\alpha_t}} d_t \right) \\ &= \left(\sum_{l_1=0}^{\alpha_1} p_1^{l_1} \right) \cdots \left(\sum_{l_t=0}^{\alpha_t} p_t^{l_t} \right) \\ &= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_t^{\alpha_t+1} - 1}{p_t - 1} \\ &= \prod_{i=1}^t \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \end{aligned}$$

当 $F(n) = \sum_{d|n} \varphi(d)$ 时,有

$$\begin{aligned} F(n) &= F(p_1^{\alpha_1}) \cdots F(p_i^{\alpha_i}) = \left(\sum_{d_1 | p_1^{\alpha_1}} \varphi(d_1) \right) \cdots \left(\sum_{d_i | p_i^{\alpha_i}} \varphi(d_i) \right) \\ &= \left(\sum_{l_1=0}^{\alpha_1} \varphi(p_1^{l_1}) \right) \cdots \left(\sum_{l_i=0}^{\alpha_i} \varphi(p_i^{l_i}) \right) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} = n \end{aligned}$$

这里, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}$ 为素因数分解.

即利用积性函数的性质从另一角度证明了定理 1.12 中的式(1),(2)及 Euler 函数的性质定理(8).

容易证明,两个积性函数的积仍是积性函数(请读者自证).因此,若 $f(n)$ 是积性函数,则 $\mu(n)f(n)$ 是积性函数,从而由定理 2.3 可得下面的定理 2.4.

定理 2.4 若 $f(n)$ 是积性函数,则数论函数

$$G(n) = \sum_{d|n} \mu(d) f(d)$$

是积性函数.

例 2.20 设 λ 是任一实数, $n (> 1)$ 的素因数分解为 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}$, 则有

$$\sum_{d|n} \frac{\mu(d)}{d^\lambda} = \left(1 - \frac{1}{p_1^\lambda}\right) \cdots \left(1 - \frac{1}{p_i^\lambda}\right)$$

证 因 $\frac{1}{n^\lambda}$ 是积性函数,由定理 2.4 知 $\sum_{d|n} \mu(d) \frac{1}{d^\lambda}$ 是积性函数.于是,由定理

2.2 第(2)条得

$$\begin{aligned} \sum_{d|n} \frac{\mu(d)}{d^\lambda} &= \left[\sum_{d_1 | p_1^{\alpha_1}} \frac{\mu(d_1)}{d_1^\lambda} \right] \cdots \left[\sum_{d_i | p_i^{\alpha_i}} \frac{\mu(d_i)}{d_i^\lambda} \right] \\ &= \left(\frac{\mu(1)}{1} + \frac{\mu(p_1)}{p_1^\lambda} + \cdots + \frac{\mu(p_1^{\alpha_1})}{(p_1^{\alpha_1})^\lambda} \right) \cdots \left(\frac{\mu(1)}{1} + \frac{\mu(p_i)}{p_i^\lambda} + \cdots + \frac{\mu(p_i^{\alpha_i})}{(p_i^{\alpha_i})^\lambda} \right) \end{aligned} \quad (2.3.2)$$

由 Möbius 函数 $\mu(n)$ 的定义可知

$$\mu(1) = 1, \quad \mu(p_i) = -1, \quad \mu(p_i^l) = 0 \quad (l \geq 2)$$

将此代入式(2.3.2)得

$$\sum_{d|n} \frac{\mu(d)}{d^\lambda} = \left(1 - \frac{1}{p_1^\lambda}\right) \cdots \left(1 - \frac{1}{p_i^\lambda}\right)$$

例 2.21 设 $f(n)$ 与 $g(n)$ 是两个数论函数,则 $h(n) = \sum_{d|n} f(d)g(n/d)$ 是数论函数,且当 $f(n)$ 与 $g(n)$ 是积性函数时,证明 $h(n)$ 亦是积性函数.

证明请读者依据定理 2.2 完成.

通常称 $h(n) = \sum_{d|n} f(d)g(n/d)$ 为 $f(n)$ 与 $g(n)$ 的 Dirichlet 卷积,并记为

$$h(n) = f(n) * g(n)$$

下面要引入组合数学中一个著名的反演公式——Möbius 反演公式,为此先证明一个引理.

引理 2.1 对任意正整数 n , 有

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases} \quad (2.3.3)$$

证 当 $n=1$ 时, 显然成立.

当 $n>1$ 时, 设 $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ 是 n 的素因数分解. 由定理 2.2 得

$$\begin{aligned} \sum_{d|n} u(d) &= \sum_{d|p_1^{\alpha_1}} u(d) \cdots \sum_{d|p_t^{\alpha_t}} u(d) \\ &= (\mu(1) + \mu(p_1) + \mu(p_1^2) + \cdots + \mu(p_1^{\alpha_1})) \cdots (\mu(1) + \mu(p_t) \\ &\quad + \mu(p_t^2) + \cdots + \mu(p_t^{\alpha_t})) \\ &= (1 + (-1)^1 + 0 + \cdots + 0) \cdots (1 + (-1)^1 + 0 + \cdots + 0) = 0 \end{aligned}$$

定理 2.5 (Möbius 反演定理) 设 $f(n)$ 与 $g(n)$ 是两个定义域为正整数集的数论函数, 若对任意正整数 n 有

$$f(n) = \sum_{d|n} g(d) \quad (2.3.4)$$

那么

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) \quad (2.3.5)$$

反之, 由式(2.3.5)可推出式(2.3.4).

$$\begin{aligned} \text{证} \quad \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) &= \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \sum_{d_1 | \left(\frac{n}{d}\right)} g(d_1) = \sum_{d_1 | n} \sum_{d_1 | \left(\frac{n}{d}\right)} \mu(d) g(d_1) \\ &= \sum_{d_1 | n} \sum_{d_1 | \left(\frac{n}{d}\right)} \mu(d) g(d_1) \text{ (调换 } d \text{ 与 } d_1 \text{ 的位置不影响求和值)} \\ &= \sum_{d_1 | n} g(d_1) \sum_{d | \left(\frac{n}{d_1}\right)} \mu(d) \\ &= g(n) \end{aligned}$$

即式(2.3.5)成立.

最后一等式是由式(2.3.3), 当 $d_1 = n$ 时, $\sum_{d | (n/d_1)} \mu(d) = 1$, 当 $d_1 < n$ 时,

$\sum_{d | (n/d_1)} \mu(d) = 0$ 得到.

反之, 如式(2.3.5)成立, 则有

$$\begin{aligned}
 \sum_{d|n} g(d) &= \sum_{d|n} g\left(\frac{n}{d}\right) = \sum_{d|n} \left[\sum_{d_1 | \left(\frac{n}{d}\right)} \mu\left(\frac{d}{d_1}\right) f(d_1) \right] \quad (\text{由式(2.3.5)得}) \\
 &= \sum_{d|n} \sum_{d_1 | \left(\frac{n}{d}\right)} \mu\left(\frac{d}{d_1}\right) f(d_1) = \sum_{d_1|n} \left[\sum_{d|(n/d_1)} \mu\left(\frac{d}{d_1}\right) \right] f(d_1) \\
 &= \sum_{d_1|n} \sum_{d|(n/d_1)} \mu(d) f(d_1) = \sum_{d_1|n} \left(\sum_{d|(n/d_1)} \mu(d) \right) f(d_1) \\
 &= f(n) \quad (\text{由式(2.3.3)得})
 \end{aligned}$$

将式(2.3.4)及式(2.3.5)称为 Möbius 反演公式.

例 2.22 证明对 Euler 函数 $\varphi(n)$, 有

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

证 由 Euler 函数的性质定理有

$$n = \sum_{d|n} \varphi(d)$$

于是, 由 Möbius 反演定理得

$$\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$$

用 $\frac{n}{d}$ 代 d , 和式值不变, 即有

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \cdot \sum_{d|n} \frac{\mu(d)}{d}$$

关于积性函数, 还有下面一条重要性质.

定理 2.6 若 $f(n)$ 是积性函数, 则对任何正整数 a 与 b 有

$$f(a)f(b) = f((a,b)) \cdot f([a,b]) \quad (2.3.6)$$

其中, (a,b) 与 $[a,b]$ 分别表示 a 与 b 的最大公约数与最小公倍数. 反之, 若 $f(1) = 1$ 且式(2.3.6)成立, 则 $f(n)$ 是积性函数.

证 设 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$, 其中, $\alpha_i \geq 0, \beta_i \geq 0, i = 1, 2, \dots, t, p_1, p_2, \dots, p_t$ 是互异素数. 由定理 2.2 得

$$\begin{aligned}
 f(a)f(b) &= (f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_t^{\alpha_t})) (f(p_1^{\beta_1})f(p_2^{\beta_2})\cdots f(p_t^{\beta_t})) \\
 &= (f(p_1^{\alpha_1})f(p_1^{\beta_1})) \cdots (f(p_t^{\alpha_t})f(p_t^{\beta_t})) \quad (2.3.7)
 \end{aligned}$$

另外

$$\begin{aligned}
 (a,b) &= p_1^{\min(\alpha_1, \beta_1)} \cdots p_t^{\min(\alpha_t, \beta_t)} \\
 [a,b] &= p_1^{\max(\alpha_1, \beta_1)} \cdots p_t^{\max(\alpha_t, \beta_t)}
 \end{aligned}$$

所以, 由定理 2.2 有

$$\begin{aligned} f((a,b)) \cdot f([a,b]) &= f(p_1^{\min(\alpha_1, \beta_1)}) \cdots f(p_i^{\min(\alpha_i, \beta_i)}) \cdot f(p_1^{\max(\alpha_1, \beta_1)}) \cdots f(p_i^{\max(\alpha_i, \beta_i)}) \\ &= (f(p_1^{\min(\alpha_1, \beta_1)}) \cdot f(p_1^{\max(\alpha_1, \beta_1)})) \cdots (f(p_i^{\min(\alpha_i, \beta_i)}) \cdot f(p_i^{\max(\alpha_i, \beta_i)})) \end{aligned} \quad (2.3.8)$$

因为对任意 $i=1, 2, \dots, n$, 有

$$f(p_i^{\alpha_i}) \cdot f(p_i^{\beta_i}) = f(p_i^{\min(\alpha_i, \beta_i)}) \cdot f(p_i^{\max(\alpha_i, \beta_i)})$$

所以, 比较式(2.3.7)与式(2.3.8)即得

$$f(a)f(b) = f((a,b)) \cdot f([a,b])$$

即式(2.3.6)成立.

反之, 若 $f(1)=1$ 且式(2.3.6)成立, 则当 $(a,b)=1$ 时, $[a,b]=ab$. 于是

$$f((a,b)) = f(1) = 1, \quad f([a,b]) = f(ab)$$

从而由式(2.3.6)得

$$f(ab) = f(a)f(b)$$

依定义 $f(n)$ 是积性函数.

设 $f(n)$ 是一个数论函数, 若对任意两个正整数 a 与 b 均有

$$f(ab) = f(a)f(b)$$

则称 $f(n)$ 是完全积性函数. 请读者讨论完全积性函数的有关性质, 并给出与定理 2.2 类似的完全积性函数的一个充分必要条件.

练习 2.3

1. 除本节出现的积性函数外, 举出两三个积性函数的例子.

2. 设 $f(n)$ 及 $g(n)$ 是积性函数, 请判断下列数论函数是否是积性函数. 如是, 请给出证明.

(1) $|f(n)|$. (2) $f(n^k)$ (k 是给定的正整数).

(3) $nf(n)$. (4) $af(n)$ (a 是一固定正整数).

(5) $f(n)+g(n)$. (6) $f^a(n) \cdot g^b(n)$ (a 与 b 是给定的两正整数).

(7) $f(g(n))$. (8) 若 $f(n)$ 有反函数 $f^{-1}(n)$, 则 $f^{-1}(n)$ 是否是积性函数?

(9) 对给定的正整数 $k > 0$, $F(n) = \begin{cases} 0, & (n,k) \neq 1 \\ f(n), & (n,k) = 1 \end{cases}$

3. 设 n 是给定的正整数, 求 $\sum_{d|n} \frac{1}{d}$.

4. 设 $f(n)$ 是积性函数. 如果 $F(n) = \sum_{d|n} f(d)$ 是积性函数, 证明 $f(n)$ 是积性函数, 且当 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}$ 为 n 的素因数分解时, 有

$$f(n) = \prod_{i=1}^l (F(p_i^{\alpha_i}) - F(p_i^{\alpha_i-1})).$$

5. 设 k 是给定的正整数, 证明数论函数

$$f_k(n) = \begin{cases} 1, & n \text{ 不含大于 } 1 \text{ 的 } k \text{ 次方因数} \\ 0, & \text{其他} \end{cases}$$

是积性函数, 且仅当 $k=1$ 时是完全积性函数.

6. 计算下列各式的值(n 为给定正整数).

(1) $\sum_{d|n} \mu(d)s(d)$ ($s(d)$ 为 d 的约数和函数).

(2) $\sum_{d|n} \mu(d)\varphi(d)$ ($\varphi(d)$ 为 Euler 函数).

(3) $\sum_{d|n} \mu(d)d^\lambda$ (λ 为任一给定的整数).

(4) $\sum_{d|n} \mu(n)/d^\lambda$ (λ 为任一给定的整数).

7. 利用上题证明

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p \in P} \left(1 - \frac{1}{p^s}\right)$$

$s > 1, P$ 表示全体素数集.

2.4 利用 Maple 求常用数论函数的值

在 Maple 中, 相应于 Gauss 函数 $[-]$ 的 Maple 函数是 $\text{floor}(n)$, 即 $\text{floor}(x) = [x]$. 如下所示:

```
> floor(2.6); floor(-2.6);
      2
      -3
```

其他还有一些相关的 Maple 函数, 如 $\text{ceil}(x)$ 、 $\text{round}(x)$ 、 $\text{trunc}(x)$ 、 $\text{frac}(x)$, 它们分别表示求大于或等于实数 x 的最小整数、接近于实数 x 的整数、最大于或等于实数 x 的最小整数(当 $x \geq 0$ 时)或 $\text{trunc}(x) = -\text{trunc}(-x)$ (当 $x \geq 0$ 时)、实数 x 的小数部分(即 $\text{frac}(x) = x - \text{trunc}(x)$). 利用简单的 Maple 编程, 可求证练习 2.1 中第 10 题, 其程序为

```
> S := proc(n::posint)
    local i, t, l;
    t[n] := r(1/3);
    for i from n by -1 to 2 do
        t[i-1] := (i-1+t[i])^(1/3);
    end do;
    print(floor(evalf(t[1])));
end;
```

```
>S(2008);
```

1

类似可用一个简单的 Maple 程序来完成练习 2.1 中第 15 题的求值.

在 Maple 中函数, 对应于 Euler 函数 $\varphi(-)$ 及 Möbius 函数 $\mu(-)$ 的 Maple 函数分别是 $\text{phi}(n)$ 与 $\text{möbius}(n)$, 如下所示:

```
>with(numtheory):
  phi(2008);
  möbius(2003);

1000
- 1
```

对于具体的正整数 n , 也可以用 Maple 编程来验证引理 2.1 成立, 如下所示:

```
>with(numtheory):
  MöbiusSum:= proc(n::posint)
  local s,d,L;
  L:= divisors(n);
  s:= add(möbius(d),d=L);
  end;
```

如

```
>seq(MöbiusSum(n),n=1..30);
1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
```

下面的 Maple 程序 $\text{TriPhi}()$ 是求不超过自然数 n 的满足条件

$$\varphi(k) = \varphi(k+1) = \varphi(k+2) \quad (2.4.1)$$

的所有正整数 k 的一个算法.

```
>TriPhi:= proc(n::posint)
  local k,a,b,c;
  for k from 1 by 1 while k<n do
  a:= phi(k);
  b:= phi(k+1);
  c:= phi(k+2);
  if a=b and b=c then printf("% d ",k);
  fi;
  od;
end:
```

用此算法, 可求得在不超过 10^8 的所有正整数中, 只有 5186 这个数满足条件式(2.4.1).

```
>TriPhi(100000000);
```

5186

对任意给定的正整数 n , 设要求满足 $\varphi(x) = n$ 的正整数解, 则由于不等式 $\varphi(n^2) \geq n$ 对任何正整数 n 均成立, 且等式仅当 $n=2$ 时成立, 所以, 可用下列 Maple 程序算法 SolvePhi() 来求解此方程.

```
>with(numtheory):
SolvePhi:=proc(n::posint)
local k,t;
for k from 1 by 1 while k<=n do
t:=phi(k);
if t=n then printf("%d",k);
fi;
od;
end;
```

如当 $n=1000$ 时, 方程 $\varphi(x)=1000$ 共有 11 个解.

```
>SolvePhi(1000);
```

1111 1255 1375 1875 2008 2222 2500 2510 2750 3012 3750

Mertens 函数 (Mertens function) $M(n)$ 定义为

$$M(n) = \sum_{i=1}^n \mu(i)$$

Mertens 猜想是指不等式

$$|M(n)| = \left| \sum_{i=1}^n \mu(i) \right| \leq \sqrt{n}$$

对任意正整数 n 成立.

利用下面的 Maple 程序算法 MertensConj(), 可验证对任意给定的正整数 n , Mertens 猜想是否成立.

```
>with(numtheory):
MertensConj:=proc(n::posint)
local k,s,r,S;
s:=evalf(sqrt(n));
r:=add(möbius(k),k=1..n);
S:=abs(r);
if S<=s then printf("The Mertens conjecture is true for n= %d!",n)
else printf("The Mertens conjecture is false for n= %d!",n)
fi;
end;
```

例如

```
>MertensConj(1000000);
```

The Mertens conjecture is true for n=1000000 !

第2章综合例题

例1 证明若 p 是大于1的奇质数, 则 $[(3+\sqrt{11})^p]-2 \cdot 3^p$ 是 $11p$ 的倍数.

证 因 $(3+\sqrt{11})^p+(3-\sqrt{11})^p$ 为整数, 且由 $0 < (3-\sqrt{11})^p < 1$ 知, 该整数是不超过 $(3+\sqrt{11})^p$ 的最大整数, 即 $[(3+\sqrt{11})^p] = (3+\sqrt{11})^p + (3-\sqrt{11})^p$, 从而

$$[(3+\sqrt{11})^p] = 2 \left(3^p + \binom{p}{2} \cdot 3^{p-2} \cdot 11 + \binom{p}{4} \cdot 3^{p-4} \cdot 11^2 + \cdots + \binom{p}{p-1} \cdot 3^1 \cdot 11^{\frac{p-1}{2}} \right)$$

于是, 由上式即可知 $[(3+\sqrt{11})^p]-2 \cdot 3^p$ 是 $11p$ 的倍数.

例2 设 $f(n) = n + [\sqrt{n}]$. 证明对任意给定正整数 m , 序列

$$m, f(m), f(f(m)), f(f(f(m))), \cdots$$

中至少包含一个整数的平方.

证 设 $m = a^2 + r$, $0 \leq r \leq 2a$, 则

$$[\sqrt{m}] = a, \quad f(m) = a^2 + a + r = (a+1)^2 + (r-a-1)$$

若 $r=0$, 则 m 已是平方数.

设 $r \neq 0$, 记 $A = \{k^2 + s \mid k, s \in \mathbb{N}, 0 < s \leq k\}$, $B = \{k^2 + s \mid k, s \in \mathbb{N}, k < s \leq 2k\}$

如果 $m \in B$, 则存在正整数 k 与 s , 使 $m = k^2 + s$, $k < s \leq 2k$. 于是

$$f(m) = k^2 + s + k = (k+1)^2 + (s-k-1), \quad 0 \leq s-k-1 \leq k-1$$

因此, $f(m)$ 或为平方数(当 $s-k-1=0$ 时)或 $f(m) \in A$. 所以, 只须讨论 $m \in A$ 的情况.

此时, 存在 k 与 s , 使 $m = k^2 + s$ 且 $0 < s \leq k$, 于是

$$f(m) = m + k$$

$$f(f(m)) = f(m+k) = m + 2k = k^2 + s + 2k = (k+1)^2 + s - 1$$

由 $0 \leq s-1 \leq k-1$ 得知, $f(f(m))$ 或为平方数(当 $s-1=0$ 时)或 $f(f(m)) \in A$.

若 $f(f(m)) \in A$, 则

$$\begin{aligned} f(f(f(m))) &= m + 2k + [\sqrt{m+2k}] \\ &= m + 2k + [\sqrt{k^2 + s + 2k}] \\ &= m + 3k + 1 \end{aligned}$$

$$\begin{aligned} f(f(f(f(m)))) &= m + 3k + 1 + [\sqrt{m+3k+1}] \\ &= m + 3k + 1 + k + 1 \\ &= (k+2)^2 + s - 2 \end{aligned}$$

如此继续,可知或存在某正整数 l 使 $f(\cdots(f(m))\cdots)$ 为平方数,或有数列

$$f(f(m)), f(f(f(m))), f(f(f(f(m))))\cdots$$

该数列每项与某平方数的差构成数列 $s-1, s-2, s-3, \cdots$. 由于对于给定的正整数 m, s 是一固定的正整数,所以,以上差数序列必终止于有限项,即存在某正整数 t (偶数),使 $f(\cdots(f(m))\cdots)$ (t 个 f) 是平方数.

综上所述,即证得序列

$$m, f(m), f(f(m)), f(f(f(m))), \cdots$$

中至少包含一个整数的平方.

例 3 设 x 是一个正实数, n 是一个正整数,证明

$$[nx] \geq \frac{[x]}{1} + \frac{[2x]}{2} + \frac{[3x]}{3} + \cdots + \frac{[nx]}{n}$$

(该题为美国第 10 届数学奥林匹克试题)

证 若设 $x_n = \sum_{k=1}^n \frac{[kx]}{k}$, 则 $x_{n+1} = x_n + \frac{[(n+1)x]}{n+1}$. 序列 $\{x_n\}$ 有明确的递推关系,可考虑用归纳法证明.

当 $n=1$ 时,结论显然成立.

假设结论对 $n \leq k-1$ 时成立,即 $x_i \leq [ix], i=1, 2, \cdots, k-1$. 由 $x_t = x_{t-1} + \frac{[tx]}{t}$ 得

$$tx_t = tx_{t-1} + [tx] = (t-1)x_{t-1} + x_{t-1} + [tx]$$

即 $tx_t - (t-1)x_{t-1} = x_{t-1} + [tx]$. 于是

$$\sum_{t=2}^k (tx_t - (t-1)x_{t-1}) = \sum_{t=2}^k (x_{t-1} + [tx])$$

亦即

$$kx_k - x_1 = (x_{k-1} + x_{k-2} + \cdots + x_1) + ([kx] + [(k-1)x] + \cdots + [2x])$$

$$kx_k = (x_{k-1} + x_{k-2} + \cdots + x_1 + x_1) + ([kx] + [(k-1)x] + \cdots + [2x])$$

由归纳假设及 Gauss 函数性质定理(4),可得

$$\begin{aligned} kx_k &\leq ([kx] + [(k-1)x] + \cdots + [x]) + ([kx] + [(k-1)x] + \cdots + [2x] + [x]) \\ &= [kx] + ([kx] + [(k-1)x] + [x]) + ([kx] + [(k-2)x] + [2x]) + \cdots \\ &\quad + ([2x] + [(k-2)x]) + ([x] + [(k-1)x]) \\ &\leq [kx] + [kx] + \cdots + [kx] + [kx] = k \cdot [kx] \end{aligned}$$

因此, $x_k \leq [kx]$. 由第二归纳法原理,本题结论对任何正整数 n 成立.

例 4 设有 n 个自然数 $a_1 < a_2 < \cdots < a_n \leq 2n$, 且它们中任意两个数的最小公倍数均大于 $2n$, 求证 $a_1 > \lceil \frac{2n}{3} \rceil$.

证 由题设知 $\{a_1, a_2, \cdots, a_n\}$ 中任一数均非另一数的倍数,因此可设

$$a_i = 2^{\alpha_i} q_i, \quad i = 1, 2, \dots, n$$

其中, α_i 为非负整数, q_i 为奇数, 且 $i \neq j$ 时, 有 $q_i \neq q_j$.

因 $\alpha_i \leq 2n$, 故 $q_i \leq 2n-1$, 从而有

$$\{q_1, q_2, q_3, \dots, q_n\} = \{1, 2, \dots, 2n-1\}$$

如果 $a_1 \leq \left[\frac{2n}{3}\right]$, 即 $2^{\alpha_1} q_1 \leq \left[\frac{2n}{3}\right] \leq \frac{2n}{3}$, $2^{\alpha_1} \cdot 3q_1 \leq 2n$, $3q_1 \leq 2n$.

因 $3q_1$ 为奇数, 故存在某 j 使 $3q_1 = q_j$. 由于 $a_j = 2^{\alpha_j} q_j$, 故

$$[a_1, a_j] = [2^{\alpha_1} q_1, 2^{\alpha_j} q_j] = [2^{\alpha_1} q_1, 2^{\alpha_j} 3q_1] = 2^{\alpha_1} \cdot 3q_1 \text{ 或 } 2^{\alpha_j} \cdot 3q_1$$

因 $2^{\alpha_1} \cdot 3q_1$ 及 $2^{\alpha_j} \cdot 3q_1 = a_j$ 均不超过 $2n$, 这与题设 $\{a_1, a_2, \dots, a_n\}$ 中任两数的最小公倍数均大于 $2n$ 矛盾. 所以, 必有 $a_1 > \left[\frac{2n}{3}\right]$.

例 5 求所有满足下列等式的自然数 n :

$$\min_{k \in \mathbb{N}} \left(k^2 + \left[\frac{n}{k^2} \right] \right) = 2000 \quad (2.1)$$

其中, \mathbb{N} 表示全体正整数组成的集.

解 式(2.1)等价于以下两不等式: 对任意 $k \in \mathbb{N}$, 有

$$k^2 + \frac{n}{k^2} \geq 2000 \quad (2.2)$$

存在 $k_0 \in \mathbb{N}$, 使

$$k_0^2 + \frac{n}{k_0^2} < 2001 \quad (2.3)$$

由式(2.2)可推得, 对任意 $k \in \mathbb{N}$, 有

$$k^4 - 2000k^2 + n \geq 0$$

也就是

$$(k^2 - 1000)^2 + n - 1000^2 \geq 0$$

则

$$\min_{k \in \mathbb{N}} (k^2 - 1000)^2 + n - 1000^2 \geq 0$$

当 $k=32$ 时, $(k^2 - 1000)^2$ 取最小值. 所以, n 应满足 $(32^2 - 1000)^2 + n - 1000^2 \geq 0$, 即

$$n \geq 1024 \times 976 \quad (2.4)$$

另外, 由式(2.3)可推得

$$-k_0^4 + 2001k^2 - n > 0$$

也就是

$$-\left(k_0^2 - \frac{2001}{2}\right)^2 - n + \left(\frac{2001}{2}\right)^2 > 0$$

由于 $\max_{k \in \mathbb{N}} \left(- \left(k^2 - \frac{2001}{2} \right)^2 \right) = - \left(32^2 - \frac{2001}{2} \right)^2$, 所以, 式(2.3)成立的充分必要条件是

$$- \left(32^2 - \frac{2001}{2} \right)^2 - n + \left(\frac{2001}{2} \right)^2 > 0$$

即

$$n < 1024 \times 977 \tag{2.5}$$

综上所述, 满足式(2.1)的所有自然数 n 为满足条件

$$1024 \times 976 \leq n < 1024 \times 977$$

的一切自然数.

例 6 设 $f(n)$ 是数论函数, 满足 $F(n) = \sum_{d|n} f(d)$. 证明对任一正整数 m , 有

$$\sum_{n=1}^m F(n) = \sum_{k=1}^m f(k) \left[\frac{m}{k} \right]$$

证 $\sum_{n=1}^m F(n) = \sum_{d|1} f(d) + \sum_{d|2} f(d) + \sum_{d|3} f(d) + \cdots + \sum_{d|m} f(d)$
 $= (f(1)) + (f(1) + f(2)) + (f(1) + f(3)) + \cdots + (f(1)$
 $+ \cdots + f(d) + \cdots + f(m))$

根据 Gauss 函数的性质定理(9)可得: 上式中 $f(1)$ 的个数为 $\left[\frac{m}{1} \right]$, $f(2)$ 的个数为 $\left[\frac{m}{2} \right]$, \cdots , $f(m)$ 的个数为 $\left[\frac{m}{m} \right]$, 因此

$$\begin{aligned} \sum_{n=1}^m F(n) &= f(1) \left[\frac{m}{1} \right] + f(2) \left[\frac{m}{2} \right] + f(3) \left[\frac{m}{3} \right] + \cdots + f(m) \left[\frac{m}{m} \right] \\ &= \sum_{k=1}^m f(k) \left[\frac{m}{k} \right] \end{aligned}$$

例 7 设 n 是正整数, 则 n 是素数的充分必要条件是

$$S(n) + \varphi(n) = nT(n) \tag{2.6}$$

证 若 n 是素数, 则 $\varphi(n) = n-1$, $T(n) = 2$, $S(n) = n+1$, 于是, 有 $(n+1) + (n-1) = 2n$, 即式(2.6)成立. 反之, 若 n 非素数, 那么, 当 $n=1$ 时, 式(2.6)不成立. 若 n 为合数, $n = p_1^{\alpha_1} \cdots p_i^{\alpha_i}$ 是其素数分解. 下面先证两个不等式.

(1) 如 p 为任一素数, $\alpha \geq 1$, 则

$$S(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1} = \frac{p^\alpha - \frac{1}{p}}{1 - \frac{1}{p}} < \frac{p^\alpha}{1 - \frac{1}{p}} \leq \frac{p^\alpha}{1 - \frac{1}{2}} = 2p^\alpha$$

即

$$S(p^\alpha) < 2p^\alpha \tag{2.7}$$

(2) 如 p 为任一不小于 3 的素数, $\alpha \geq 1$, 则

$$S(p^\alpha) = \frac{p^\alpha - 1}{p - 1} < \frac{p^\alpha}{1 - \frac{1}{p}} \leq \frac{p^\alpha}{1 - \frac{1}{3}} = \frac{3}{2} p^\alpha$$

即

$$S(p^\alpha) < \frac{3}{2} p^\alpha \quad (2.8)$$

对于 n 的素数分解, 当 $t=1$ 时, $\alpha_1 \geq 2$. 由式(2.7)有

$$S(n) + \varphi(n) = S(p_1^{\alpha_1}) + \varphi(p_1^{\alpha_1}) < 2p_1^{\alpha_1} + p_1^{\alpha_1} = 3p_1^{\alpha_1} \leq (\alpha_1 + 1)p_1^{\alpha_1}$$

即 $S(n) + \varphi(n) < nT(n)$, 即式(2.6)不成立.

当 $t > 1$, 且设 $p_2 > p_1$ (此时 $p_2 \geq 3$), 则由式(2.7)及式(2.8)可得

$$\begin{aligned} S(n) &= S(p_1^{\alpha_1}) S(p_2^{\alpha_2}) \cdots S(p_t^{\alpha_t}) \\ &< 2p_1^{\alpha_1} \cdot \frac{3}{2} p_2^{\alpha_2} \cdots 2p_t^{\alpha_t} \\ &= 3 \cdot 2^{t-2} \cdot (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}) = 3 \cdot 2^{t-2} n \end{aligned}$$

于是

$$\begin{aligned} S(n) + \varphi(n) &< 3 \cdot 2^{t-2} \cdot n + n \\ &= (3 \cdot 2^{t-2} + 1)n \leq (3 \cdot 2^{t-2} + 2^{t-2})n \leq 2^t \cdot n \\ &\leq (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_t + 1)n = T(n) \cdot n \end{aligned}$$

即 $S(n) + \varphi(n) < nT(n)$ 不成立.

综上所述, 当式(2.6)成立时, n 必为素数.

例 8 设 n 是任一正整数, 证明

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} \quad (2.9)$$

证 $n=1$ 时, 式(2.9)显然成立, 设 $n > 1$ 且 $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ 是 n 的素因数分解. 由 Möbius 函数 $\mu(n)$ 的定义可推得

$$\mu^2(n) = \begin{cases} 0, & n \text{ 含有素数的平方因子} \\ 1, & \text{其他} \end{cases}$$

于是

$$\begin{aligned} \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} &= \sum_{d|p_1 \cdots p_t} \frac{1}{\varphi(d)} = \sum_{0 \leq \lambda_i \leq 1} \frac{1}{\varphi(p_1^{\lambda_1} \cdots p_t^{\lambda_t})} \\ &= \sum_{\lambda_1=0}^1 \cdots \sum_{\lambda_t=0}^1 \frac{1}{\varphi(p_1^{\lambda_1}) \cdots \varphi(p_t^{\lambda_t})} \\ &= \left(\sum_{\lambda_1=0}^1 \frac{1}{\varphi(p_1^{\lambda_1})} \right) \cdots \left(\sum_{\lambda_t=0}^1 \frac{1}{\varphi(p_t^{\lambda_t})} \right) \end{aligned}$$

$$\begin{aligned}
 &= \left(1 + \frac{1}{p_1 - 1}\right) \cdots \left(1 + \frac{1}{p_t - 1}\right) \\
 &= \frac{p_1 \cdots p_t}{(p_1 - 1) \cdots (p_t - 1)}
 \end{aligned}$$

另外,式(2.9)的左边为

$$\frac{n}{\varphi(n)} = \frac{n}{n \prod_{p|n} \left(1 - \frac{1}{p}\right)} = \frac{1}{\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right)} = \frac{p_1 \cdots p_t}{(p_1 - 1) \cdots (p_t - 1)}$$

所以,式(2.9)成立.

上题还可这样来证明.

因 $\mu(n)$ 与 $\varphi(n)$ 是积性函数,所以, $\frac{\mu^2(n)}{\varphi(n)}$ 是积性函数,故由定理 2.3 知

$\sum_{d|p_i^{\alpha_i}} \frac{\mu^2(d)}{\varphi(d)}$ 是积性函数,从而

$$\begin{aligned}
 \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} &= \left(\sum_{d|p_1^{\alpha_1}} \frac{\mu^2(d)}{\varphi(d)}\right) \cdots \left(\sum_{d|p_t^{\alpha_t}} \frac{\mu^2(d)}{\varphi(d)}\right) \\
 &= \left(1 + \frac{\mu^2(p_1)}{\varphi(p_1)} + \frac{\mu^2(p_1^2)}{\varphi(p_1^2)} + \cdots + \frac{\mu^2(p_1^{\alpha_1})}{\varphi(p_1^{\alpha_1})}\right) \cdots \\
 &\quad \left(1 + \frac{\mu^2(p_t)}{\varphi(p_t)} + \frac{\mu^2(p_t^2)}{\varphi(p_t^2)} + \cdots + \frac{\mu^2(p_t^{\alpha_t})}{\varphi(p_t^{\alpha_t})}\right) = \left(1 + \frac{1}{\varphi(p_1)}\right) \cdots \left(1 + \frac{1}{\varphi(p_t)}\right) \\
 &= \frac{p_1 \cdots p_t}{(p_1 - 1) \cdots (p_t - 1)}
 \end{aligned}$$

例 9 对任意大于 1 的正整数 n 求证

$$\lceil \sqrt{n} \rceil + \lceil \sqrt[3]{n} \rceil + \cdots + \lceil \sqrt[n]{n} \rceil = \lceil \log_2 n \rceil + \lceil \log_3 n \rceil + \cdots + \lceil \log_n n \rceil \quad (2.10)$$

证 由于 $n \geq 2$,故存在正整数 k_2, k_3, \cdots, k_n ,使

$$\begin{aligned}
 2^{k_2} &\leq n < 2^{k_2+1} \\
 3^{k_3} &\leq n < 3^{k_3+1} \\
 &\vdots \\
 n^{k_n} &\leq n < n^{k_n+1}
 \end{aligned}$$

于是

$$\lceil \log_2 n \rceil + \lceil \log_3 n \rceil + \cdots + \lceil \log_n n \rceil = k_2 + k_3 + \cdots + k_n \quad (2.11)$$

另外,令 $S_m = \{1, 2, \cdots, \lceil \sqrt[m]{n} \rceil\}$, $m = 2, 3, \cdots, n$,则 S_m 有 $\lceil \sqrt[m]{n} \rceil$ 个元,故 $S \triangleq S_2 \cup S_3 \cup \cdots \cup S_n$ 共有 $\lceil \sqrt{n} \rceil + \lceil \sqrt[3]{n} \rceil + \cdots + \lceil \sqrt[n]{n} \rceil$ 个元素,即有

$$|S| = |S_2 \cup S_3 \cup \cdots \cup S_n| = \lceil \sqrt{n} \rceil + \lceil \sqrt[3]{n} \rceil + \cdots + \lceil \sqrt[n]{n} \rceil \quad (2.12)$$

从另一角度看,

$1 \in S_m (m = 2, 3, \dots, n)$, 即 1 在 S 中共出现 $n-1$ 次

$2 \in S_m (m = 2, 3, \dots, k_2)$, 即 2 在 S 中共出现 k_2-1 次

$3 \in S_m (m = 2, 3, \dots, k_3)$, 即 3 在 S 中共出现 k_3-1 次

⋮

$n \in S_m (m = 2, 3, \dots, k_n)$, 即 n 在 S 中共出现 k_n-1 次

所以, S 共含有 $(n-1) + (k_2-1) + (k_3-1) + \dots + (k_n-1)$ 个元素, 亦即 $k_2 + k_3 + \dots + k_n$ 个元素, 因此, 由式(2.12)便得

$[\sqrt{n}] + [\sqrt[3]{n}] + \dots + [\sqrt[n]{n}] = k_2 + k_3 + \dots + k_n = [\log_2 n] + [\log_3 n] + \dots + [\log_n n]$
即式(2.10)成立.

思考题、研究题二

1. 设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ 是 n 的素因数分解, $N(n, m)$ 表示大于 m 而与 n 互素的正整数的个数, 则

$$N(n, m) = m - \sum_{1 \leq i \leq t} \left[\frac{m}{p_i} \right] + \sum_{1 \leq i < j \leq t} \left[\frac{m}{p_i p_j} \right] + \dots + (-1)^t \left[\frac{m}{p_1 p_2 \dots p_t} \right]$$

2. 设 r, s 及 n 都是自然数, 且 $r+s=n$. 证明集合

$$\left\{ \left[\frac{n}{r} \right], \left[\frac{2n}{r} \right], \dots, \left[\frac{(r-1)n}{r} \right] \right\}$$

和集合

$$\left\{ \left[\frac{n}{s} \right], \left[\frac{2n}{s} \right], \dots, \left[\frac{(r-1)n}{s} \right] \right\}$$

构成集合的一个划分的充分必要条件是 $(r, n)=1$ 及 $(s, n)=1$.

3. 设 $S = 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \dots + \frac{1}{\sqrt{k^2}}$, 求 $[S]$ 的值.

4. 证明下列各结论.

(1) 对任意非负实数 x, y 有

$$[5x] + [5y] \geq [3x+y] + [3y+x]$$

(2) 对任意正整数 m, n , 下面的数

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

是整数.

5. 证明下列恒等式.

$$(1) \sum_{d=1}^n \varphi(d) \left[\frac{n}{d} \right] = \frac{n(n+1)}{2}.$$

$$(2) \sum_{k=1}^m S(k) = \sum_{k=1}^m k \left[\frac{m}{k} \right].$$

6. 设 n 是不等于 4 的正整数, 证明 $\varphi(n) \cdot (T(n))^2 \leq n^2$.

7. 设 G 是所有满足 $f(1) \neq 0$ 的数论函数 f 的全体, 若定义 G 的二元运算为 Dirichlet 卷积 “ $*$ ”, 证明 $(G, *)$ 构成一个 Abel 群, 其单位元 $I(n)$ 是函数 $\left[\frac{1}{n} \right]$, 即

$$I(n) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$$

设 $\theta=0$ 表示零函数(数零), “ $+$ ”表示普通函数的加法, 令 $R = G \cup \{\theta\}$, 问 $(R, *, +)$ 是否构成一个有单位元的交换环?

8. 设 $f(n)$ 是数论函数, 如果对任何互素的正整数 m 与 n , 有

$$f(mn) = f(m) + f(n)$$

则称 f 是加性函数. 若上式对任何正整数 m 与 n 成立, 则称 f 是完全加性函数. 证明

(1) $f(n) = \log_a n$ (a 是任一大于 0 的实数) 是完全加性函数.

(2) 设 $\omega(n) = \begin{cases} n \text{ 的不同素因子的个数}, & n > 1 \\ 0, & n = 1 \end{cases}$

则 $\omega(n)$ 是加性函数, 但非完全加性函数.

(3) 讨论积性函数的有关性质.

9. 设 $f(n)$ 是数论函数, 则下列恒等式成立:

$$\sum_{d=1}^n f((d, n)) = \sum_{d|n} f(d) \varphi\left(\frac{n}{d}\right)$$

其中, (d, n) 表示 d 与 n 的最大公约数.

10. 设 $l(n)$ 表示满足: $1 \leq d \leq n, (d, n) = (d+1, n) = 1$ 的 d 的个数. 证明 $l(n)$ 是积性函数, 且

$$l(n) = n \prod_{p|n} \left(1 - \frac{2}{p}\right)$$

11. 将第 10 题中的函数 $l(n)$ 的有关结论推广并证明.

12. 设 n 是正整数, 如果 $s(n) = 2n$, 则称 n 为完全数, 请读者完成下列问题.

(1) 列举几个完全数.

(2) 证明正整数 a 是偶完全数的充分必要条件是: 存在正整数 k , 使 $a = 2^k (2^{k+1} - 1)$ 且 $2^{k+1} - 1$ 是素数.

(3) 证明如果 n 是一个奇完全数, 那么, $n = p^a m^2$, 其中, p 为奇素数且 $p \equiv a \equiv 1 \pmod{4}$.

(4) 利用(3), 如果 n 是一个奇完全数, 则 $n \equiv 1 \pmod{4}$.

(5) 证明如果 $n = p^a m^2$ 是一个奇完全数, 则 $n \equiv p \pmod{8}$.

13. 设 x 是任一实数, 记 $\{x\} = x - [x] - \frac{1}{2}$, 研究该函数的性质.

14. 设 x 是任一实数, 记 $\lceil x \rceil$ 表示不小于 x 的最小整数, 如

$$\lceil 5 \rceil = 5, \quad \lceil 5.5 \rceil = 6, \quad \lceil -5.5 \rceil = -5$$

则 $\lceil x \rceil$ 是定义域为实数域的一个数论函数, 称为最小整数函数, 问关于该函数你能得出哪些结论?

第3章 同余理论

“同余”顾名思义就是“余数相同”的意思. 设 m 是任一给定的正整数, a 是任一整数, 用 m 去除 a , 则得到的余数必为 m 个数 $0, 1, \dots, m-1$ 中的一个, 于是, 所有整数可以按余数相同来分类: 余数相同的分在同一类, 否则分在不同类. 这样得到 m 个不同的类, 如此可以根据需要将整数集划分为若干个“类”(子集), 通过各个类及它们之间的关系来研究整数.

“同余”这一概念由来已久, 在 18 世纪末、19 世纪初由 Gauss 首先提出. 同余理论的应用十分广泛, 如日历推算法、弃九法, 但更重要的应用则体现在密码学中(见本书第 7 章).

3.1 同余的定义及性质

定义 3.1 设 m 是一给定的正整数, a 与 b 是两个整数. 如果用 m 分别去除 a 与 b , 若得到的余数相同, 则称 a 与 b 关于模 m 同余, 记作 $a \equiv b \pmod{m}$, 并称为同余式; 若得到的余数不相同, 则称 a 与 b 关于模 m 不同余, 记作 $a \not\equiv b \pmod{m}$.

依定义, 任何一个偶数与 0 关于模 2 同余, 任何一个奇数与 1 关于模 2 同余, 即有

$$2n \equiv 0 \pmod{2}, \quad 2n+1 \equiv 1 \pmod{2} \quad (n \in \mathbb{Z})$$

再如 $365 \equiv 5 \pmod{12} \equiv -7 \pmod{12}$.

显然, 对任何一整数 a 与 b , 均有 $a \equiv b \pmod{1}$. 对任意两个不同的素数 p 与 q , 有 $q \not\equiv p \pmod{q}$ 及 $p \not\equiv q \pmod{p}$.

关于同余的性质有如下定理.

定理 3.1(同余性质定理) 设 m 是给定的正整数, $a, b, c, a_1, b_1, c_1, a_2, b_2, c_2$ 是整数, 则有

(1) $a \equiv b \pmod{m}$, 成立的充分必要条件是 $m \mid a-b$.

(2) 同余是一个等价关系, 即有

① $a \equiv a \pmod{m}$ (反身性).

② 若 $a \equiv b \pmod{m}$, 则 $b \equiv a \pmod{m}$ (对称性).

③ 若 $a \equiv b \pmod{m}$ 且 $a \equiv c \pmod{m}$, 则 $a \equiv c \pmod{m}$ (传递性).

(3) 若 $a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m}$, 则

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}, \quad a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

(4) 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 与 $g(x) = b_n x^n + \cdots + b_1 x + b_0$ 是两个整值多项式, 且满足 $a_i \equiv b_i \pmod{m}, i = 0, 1, \cdots, n$, 则当 $a \equiv b \pmod{m}$ 时, 有

$$f(a) \equiv f(b) \equiv g(a) \equiv g(b) \pmod{m}$$

(5) 若 $a \equiv b \pmod{m}, d$ 是 m 的任一因数, 则 $a \equiv b \pmod{d}$.

(6) 若 $a \equiv b \pmod{m}, d$ 是 a, b 及 m 的任一公因数, 则 $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

(7) 若 $ac \equiv bc \pmod{m}$, 则 $a \equiv b \pmod{\frac{m}{(c, m)}}$. 特别当 $(c, m) = 1$ 时, 有 $a \equiv b \pmod{m}$.

(8) 若 $a \equiv b \pmod{m_i}, i = 1, 2$, 则 $a \equiv b \pmod{[m_1, m_2]}$, 反之亦成立. 特别当 $(m_1, m_2) = 1$ 时, 有 $a \equiv b \pmod{m_1}$ 且 $a \equiv b \pmod{m_2}$ 的充分必要条件是 $a \equiv b \pmod{m_1 m_2}$.

(9) 若 $(a, m) = 1$, 则存在 b , 使 $ab \equiv 1 \pmod{m}$. 可称 b 为 a 关于模 m 的逆, 记为 $b = a^{-1} \pmod{m}$ 或 $a^{-1} | m$.

以上性质的证明均较易, 我们证明其中几条, 为方便证明, 用符号“ \Leftrightarrow ”表示“当且仅当”.

证 (1) $a \equiv b \pmod{m} \Leftrightarrow a$ 与 b 用 m 去除有相同的余数 $\Leftrightarrow a - b$ 与 0 用 m 去除有相同的余数 $\Leftrightarrow m | a - b$.

(2) ③由(1) $a \equiv b \pmod{m}$ 且 $b \equiv c \pmod{m} \Leftrightarrow m | a - b$ 且 $m | b - c \Rightarrow m | (a - b) + (b - c) \Leftrightarrow a \equiv c \pmod{m}$.

(3) 由(1)得 $a_1 \equiv b_1 \pmod{m}$ 及 $a_2 \equiv b_2 \pmod{m} \Leftrightarrow m | a_1 - b_1$ 及 $m | a_2 - b_2 \Rightarrow m | (a_1(a_2 - b_2) + (a_1 - b_1)b_2) \Rightarrow m | (a_1 a_2 - b_1 b_2) \Leftrightarrow a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

(4) 由(3)可推得.

(6) 由(1) $ac \equiv bc \pmod{m} \Leftrightarrow m | c(a - b) \Leftrightarrow \frac{m}{(c, m)} | \frac{c}{(c, m)}(a - b) \Rightarrow \frac{m}{(c, m)} | (a - b)$
 (因为 $(\frac{m}{(c, m)}, \frac{c}{(c, m)}) = 1$) $\Leftrightarrow a \equiv b \pmod{\frac{m}{(c, m)}}$.

(8) 由(1)知 $a \equiv b \pmod{m_1}$ 且 $a \equiv b \pmod{m_2} \Leftrightarrow m_1 | a - b$ 且 $m_2 | a - b$, 即 $a - b$ 是 m_1 与 m_2 的公倍数, 从而 $[m_1, m_2] | a - b$. 再由(1)即得 $a \equiv b \pmod{[m_1, m_2]}$. 此性质可推广至任意有限个模数 m_1, m_2, \cdots, m_l 的情形.

(9) 若 $(a, m) = 1$, 则存在整数 b 与 c , 使 $ab + mc = 1$, 则 $ab - 1 = m(-c)$, 即 $m | (ab - 1)$. 由(1)得 $ab \equiv 1 \pmod{m}$.

以上性质形式简单, 证明容易, 但同余式类似普通等式的特点使其具有广泛的应用价值. 下面是若干应用同余式性质的实例.

例 3.1 求 2008^{365} 的个位数字.

解 要求一个 $0 \sim 9$ 的数 a , 使 $2008^{365} \equiv a \pmod{10}$. 由于

$$2008^{365} = (2 \times 10^3 + 8)^{365} = 10k + 8^{365}$$

所以, $2008^{365} \equiv 8^{365} \pmod{10}$. 又 $8^2 = 64 \equiv 4 \pmod{10}$, $8^4 \equiv 4^2 \equiv 6 \pmod{10}$, 因此

$$8^{365} = 8^{4 \times 91 + 1} = (8^4)^{91} \times 8 \equiv 6^{91} \times 8 \equiv 6 \times 8 \equiv 8 \pmod{10}$$

故 $a=8$.

例 3.2 求 1997^{365} 表示成 15 进制数时的个位数.

解 要求一个 $0 \sim 14$ 的数 b , 使 $1997^{365} \equiv b \pmod{15}$. 因为 $1997 = 15 \times 133 + 2$, $2^4 \equiv 1 \pmod{15}$, 所以

$$1997^{365} = (15 \times 133 + 2)^{365} \equiv 2^{365} \equiv 2^{4 \times 91 + 1} \pmod{15} \equiv (2^4)^{91} \times 2 \equiv 2 \pmod{15}$$

因此, $b=2$.

例 3.3 求 8 除 $1^5 + 2^5 + \cdots + 99^5 + 100^5$ 所得的余数.

$$\begin{aligned} \text{解 因为 } & 1^5 + 2^5 + \cdots + 99^5 + 100^5 \\ &= (1^5 + 3^5 + \cdots + 99^5) + (2^5 + 4^5 + \cdots + 100^5) \\ &= (1^5 + 3^5 + \cdots + 99^5) + 2^5(1^5 + 2^5 + \cdots + 50^5) \\ &\equiv (1^5 + 3^5 + \cdots + 99^5) \pmod{8} \end{aligned}$$

设 $2k+1$ 是任一奇数, 则 $(2k+1)^2 = 4k(k+1) + 1 \equiv 1 \pmod{8}$, 从而

$$1^5 + 3^5 + \cdots + 99^5 \equiv 1 + 3 + \cdots + 99 \equiv 4 \pmod{8}$$

所以, 要求的余数为 4.

例 3.4 设 A 是正整数, B 是 A 的各数位上的数字之和, 证明 $A \equiv B \pmod{9}$.

证 设 $A = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$, $0 \leq a_i \leq 9$, $a_n \neq 0$, 则 $B = a_n + \cdots + a_1 + a_0$. 由于 $10 \equiv 1 \pmod{9}$, $10^i \equiv 1^i \equiv 1 \pmod{9}$, i 为正整数, 所以

$$a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0 \equiv a_n \cdot 1 + \cdots + a_1 \cdot 1 + a_0 \equiv a_n + \cdots + a_1 + a_0 \pmod{9}$$

即 $A \equiv B \pmod{9}$.

例 3.5 设正整数 a 为

$$a = a_n \cdot 1000^n + \cdots + a_1 \cdot 1000 + a_0, \quad 0 \leq a_i < 1000$$

则 7 整除 a 的充分必要条件是 $7 \mid \sum_{i=0}^n (-1)^i a_i$.

证 因为 $1000 \equiv -1 \pmod{7}$, $1000^i \equiv (-1)^i \pmod{7}$, 所以, 由性质定理(4)得

$$a \equiv a_n \cdot (-1)^n + \cdots + a_1 \cdot (-1) + a_0 \pmod{7}$$

故

$$7 \mid a \Leftrightarrow 7 \mid \sum_{i=0}^n (-1)^i a_i$$

同样, 因为 $1000 \equiv -1 \pmod{11}$ 及 $1000 \equiv -1 \pmod{13}$, 可得 $11 \mid a \Leftrightarrow$

$$11 \mid \sum_{i=0}^n (-1)^i a_i \text{ 及 } 13 \mid a \Leftrightarrow 13 \mid \sum_{i=0}^n (-1)^i a_i.$$

例 3.6 证明不定方程 $x^2 - y^2 + 8az^2 = 6$ 对任何给定的整数 a 无整数解.

证 设 x_0, y_0 及 z_0 是该不定方程的一组整数解, 即有

$$x_0^2 - y_0^2 + 8az_0^2 = 6 \quad (3.1.1)$$

将上式关于 2 取模得 $x_0^2 - y_0^2 \equiv 0 \pmod{2}$. 因此, x_0 与 y_0 有相同的奇偶性. 再将式(3.1.1)关于 4 取模得 $x_0^2 - y_0^2 \equiv 2 \pmod{4}$. 因此, x_0 与 y_0 同为奇数. 于是, $x_0^2 \equiv y_0^2 \equiv 1 \pmod{8}$. 将式(3.1.1)关于 8 取模便得 $0 \equiv 6 \pmod{8}$ 矛盾, 故原不定方程无整数解.

例 3.7 诸如 88, 686, 4554, 12321 之类的正整数, 即一个正整数, 若从左往右看与从右往左看均同一数, 则称此数为回文数. 证明

(1) 偶位数的回文数是 11 的倍数.

(2) 奇位数的回文数关于模 3 同余于该数的中位数字与其左侧(或右侧)的各数字之差.

证 (1) 设 $A = a_1 a_2 \cdots a_n a_n \cdots a_2 a_1$ 是偶位数的回文数, 则

$$A = a_1 \cdot 10^{2n-1} + a_2 \cdot 10^{2n-2} + \cdots + a_n \cdot 10^n + a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1$$

即

$$A = a_1 \cdot (10^{2n-1} + 1) + a_2 \cdot 10(10^{2n-3} + 1) + \cdots + a_n \cdot 10^{n-1}(10 + 1) \quad (3.1.2)$$

显然, 当 k 为奇数时, 有 $10^k + 1 \equiv 0 \pmod{11}$. 从而由式(3.1.2)知, $A \equiv 0 \pmod{11}$, 即 A 是 11 的倍数.

(2) 设 $B = b_1 b_2 \cdots b_n b_n \cdots b_2 b_1$ 是奇位数的回文数, 则

$$\begin{aligned} B &= b_1 \cdot 10^{2n} + b_2 \cdot 10^{2n-1} + \cdots + b_n \cdot 10^{n+1} + b_n \cdot 10^n + b_n \cdot 10^{n-1} + \cdots + b_2 \cdot 10 + b_1 \\ &= b_1(10^{2n} + 1) + b_2 \cdot 10(10^{2n-2} + 1) + \cdots + b_n \cdot 10^{n-1}(10^2 + 1) + b_n \cdot 10^n \end{aligned} \quad (3.1.3)$$

显然, 当 l 为偶数时, 有 $10^l + 1 \equiv -1 \pmod{3}$. 又对任何正整数 m , 有 $10^m \equiv 1 \pmod{3}$, 所以, 由式(3.1.3) 即得

$$B \equiv -b_1 - b_2 - \cdots - b_n + b_n \equiv b - b_1 - b_2 - \cdots - b_n \pmod{3}$$

例 3.8 证明从任意 n 个自然数中总可以找到 k ($k \leq n$) 个数, 使它们的和能被 n 整除.

证 设 a_1, a_2, \cdots, a_n 是任意给定的 n 个自然数, 记 $S_m = \sum_{k=1}^m a_k, m = 1, 2, \cdots, n$. 由于任何一个正整数关于模 n 同余于 $0, 1, 2, \cdots, (n-1)$, 所以, 如果 $S_m \not\equiv 0 \pmod{n}, m = 1, 2, \cdots, n$, 则 S_1, S_2, \cdots, S_n 中必有两个关于模 n 同余, 不妨设 $S_i \equiv S_j \pmod{n}, 1 \leq i < j \leq n$, 即 $S_i - S_j \equiv 0 \pmod{n}$, 亦即 $a_{j+1} + \cdots + a_i \equiv 0 \pmod{n}$.

例 3.9 证明对任何整数 $n, f(n) = \frac{7}{15}n + \frac{1}{3}n^3 + \frac{1}{5}n^5$ 均是一个整数.

证 只要证明对任意正整数 n 有

$$7n + 5n^3 + 3n^5 \equiv 0 \pmod{15} \quad (3.1.4)$$

即可.

由于

$$7n + 5n^3 + 3n^5 \equiv n + 2n^3 \equiv n^3 - n \pmod{3}$$

而

$$n^3 - n = n(n-1)(n+1) = (n-1)n(n+1)$$

是 3 的倍数,故

$$7n + 5n^3 + 3n^5 \equiv 0 \pmod{3} \quad (3.1.5)$$

又 $7n + 5n^3 + 3n^5 \equiv 2n - 2n^5 \equiv 2(n - n^5) \pmod{5}$, 而 $n^5 - n = (n-1)n(n+1) \times (n^2 + 1)$ 及 $n \equiv 0$ 或 ± 1 或 $\pm 2 \pmod{5}$. 当 $n \equiv 0$ 或 $\pm 1 \pmod{5}$ 时, $(n-1)n(n+1) \equiv 0 \pmod{5}$. 当 $n \equiv \pm 2 \pmod{5}$ 时, $n^2 + 1 \equiv 0 \pmod{5}$, 因此, 不论 n 为何整数, 均有 $n^5 - n \equiv 0 \pmod{5}$, 故

$$7n + 5n^3 + 3n^5 \equiv 0 \pmod{5} \quad (3.1.6)$$

因为 $(3, 5) = 1$, 所以, 由性质定理(8)及式(3.1.5)与式(3.1.6)即可推得式(3.1.4)成立.

例 3.10 设 $S = \{1, 2, \dots, 400\}$, $T = \{a_1, a_2, \dots, a_{200}\}$ 是 S 的一个子集, 且满足

(1) T 中任两个数之和不等于 401.

(2) $\sum_{i=1}^{200} a_i = 38452$.

证明 T 中的奇数的个数是 4 的倍数, 且 T 中所有数字的平方和为一定数.

证 由 $a_i \neq 401 - a_j$ 对任何 $1 \leq i, j \leq 200$ 成立知

$$S = \{a_1, a_2, \dots, a_{200}\} \cup \{401 - a_1, 401 - a_2, \dots, 401 - a_{200}\}$$

所以

$$\sum_{n=1}^{400} n^2 = \sum_{i=1}^{200} a_i^2 + \sum_{i=1}^{200} (401 - a_i)^2 = 2 \sum_{i=1}^{200} a_i^2 - 802 \sum_{i=1}^{200} a_i + 401^2 \times 200$$

即

$$200 \times 401 \times 267 = 2 \sum_{i=1}^{200} a_i^2 - 802 \times 38452 + 401^2 \times 200 \quad (3.1.7)$$

若记 T 中奇数的个数为 x , 则将式(3.1.7)关于 8 取模得

$$0 \equiv 2x - 0 + 0 \pmod{8}$$

亦即

$$x \equiv 0 \pmod{4}$$

因此, T 中奇数的个数是 4 的倍数. 再由式(3.1.7)可求得 $\sum_{i=1}^{200} a_i^2 = 10045852$.

练习 3.1

- (1) 求 1999^{365} 的最后两位数字.
- (2) 求 1999^{2000} 表示成 17 进制数时的个位数及最后两位数.
2. 证明 $3^{2000} + 4^{1999} \equiv 0 \pmod{5}$.
3. 证明若一个三位数的数字(0~9 的数)是相邻的三个数字,且百位上的数字大于个位上的数字,则该位数与它的数字次序相反的三位数的差等于 198.
4. 设十进制自然数 $21a39b8$ ($0 \leq a, b \leq 9$) 为 99 的倍数,求 a 与 b .
5. 试证不定方程 $x^2 + y^2 + z^2 = 15$ 没有整数解.
6. 设 n 为正整数,证明 $330 \mid 6^{2n} - 5^{2n} - 11$.
7. 假设 $131 \mid \underbrace{11 \cdots 1}_n$, 求 $n = ?$
8. 试证 $7 \mid 2222^{5555} + 5555^{2222}$, 并问 7 能否整除 $3333^{4444} + 4444^{3333}$?
9. 设 n 是任一给定的正整数,证明一定存在一个能被 n 整除的正整数 m , m 由数字 0 和 1 组成,且位数不大于 n .
10. 试证在任给 100 个整数中,一定存在两整数,使得它们的和或差能被 196 整除.

3.2 同余类与剩余类

定义 3.2 设 m 是一给定的正整数,则任意整数 a 关于模 m 同余 0 或 1, 或 $2, \dots$, 或 $m-1$. 于是,可将整数集划分成 m 个类:所有与 r ($0 \leq r \leq m-1$) 同余的整数归为一类. 显然,在同一类中的任两个整数关于模 m 一定同余,而不在同一类中的任两个整数关于模 m 一定不同余. 每一个这样的类称为模 m 的同余类或模 m 的剩余类. 从每个类中任取出一数,则得到的这 m 个数就称为模 m 的完全剩余系,简称为 m 的完系.

若记 $\bar{r}[m]$ 为 r 所在的模 m 的同余类(或在明确模 m 的情况下简记为 \bar{r}), 则有下列性质定理.

定理 3.2 设 m 是一给定的正整数,则有

- (1) $\bar{r}[m] = \{r + km \mid k \in \mathbb{N}\}$.
- (2) $\bar{r}[m] = \bar{s}[m] \Leftrightarrow m \mid r - s$.
- (3) 对任意两个整数 r, s , 或者 $\bar{r}[m] = \bar{s}[m]$, 或者 $\bar{r}[m] \cap \bar{s}[m] = \emptyset$.
- (4) k 个数 a_1, a_2, \dots, a_k 构成的完系的充分必要条件是 $k = m$, 且当 $i \neq j$ 时, 有 $a_i \not\equiv a_j \pmod{m}$.

以上性质由定义可直接得知.

根据完系的定义,对于给定的正整数 m ,模 m 的完系有无限个,下面给出几个常用的完系.

(1) 模 m 的最小非负完全剩余系.

$$0, 1, \dots, m-1$$

(2) 模 m 的最小正完全剩余系.

$$1, 2, \dots, m$$

(3) 模 m 的最大非正完全剩余系.

$$-(m-1), -(m-2), \dots, -1, 0$$

(4) 模 m 的绝对值最小完全剩余系.

m 为偶数时,

$$-\frac{m}{2}, \dots, -1, 0, 1, \dots, \frac{m}{2}-1 \quad \text{或} \quad -\frac{m}{2}+1, \dots, -1, 0, 1, \dots, \frac{m}{2}$$

m 为奇数时,

$$-\frac{m-1}{2}, \dots, -1, 0, 1, \dots, \frac{m-1}{2}$$

定理 3.3 若 a_1, a_2, \dots, a_m 是 m 的一个完系, a 与 b 是任意两整数且 $(a, m) = 1$, 则

$$aa_1 + b, aa_2 + b, \dots, aa_m + b$$

亦是 m 的完系.

证 由定理 3.2 中(4)得,只要证明对任何 $i \neq j$, 有 $aa_i + b \not\equiv aa_j + b \pmod{m}$ 即可.

如果 $aa_i + b \equiv aa_j + b \pmod{m}$, 则有 $aa_i \equiv aa_j \pmod{m}$. 因 $(a, m) = 1$, 由定理 3.1 中(7)即得 $a_i \equiv a_j \pmod{m}$, 这与 a_1, a_2, \dots, a_m 为 m 的完系矛盾, 所以, $aa_i + b \not\equiv aa_j + b \pmod{m}$.

例 3.11 若 a_1, a_2, \dots, a_m 是 m 的完系, $a, b \in \mathbb{Z}$ 且 $(a, m) = 1$, 则 $aa_i + b$ 除以 m 的最小非负余数之和为 $\frac{1}{2}m(m-1)$.

证 由定理 3.3 知, $aa_1 + b, aa_2 + b, \dots, aa_m + b$ 是 m 的一个完系. 因此, $aa_i + b (i=1, 2, \dots, m)$ 除以 m 而得的 m 个最小非负余数构成 m 的一个完系, 即它们构成 m 的最小非负完全剩余系, 所以, 它们的和为 $0+1+2+\dots+(m-1) = \frac{1}{2}m(m-1)$.

定理 3.4 若 m 是偶数, $\{x_1, x_2, \dots, x_m\}$ 及 $\{y_1, y_2, \dots, y_m\}$ 均是 m 的完系. $a, b \in \mathbb{Z}$ 且 $a+b \equiv 0 \pmod{2}$, 证明 $\{ax_1 + by_1, ax_2 + by_2, \dots, ax_m + by_m\}$ 不是 m 的完系.

证 由 $\{x_1, x_2, \dots, x_m\}$ 及 $\{y_1, y_2, \dots, y_m\}$ 是 m 的完系知

$$\{x_1, x_2, \dots, x_m\} \equiv \{1, 2, \dots, m\} \pmod{m}$$

$$\{y_1, y_2, \dots, y_m\} \equiv \{1, 2, \dots, m\} \pmod{m}$$

从而由 $m \equiv 0 \pmod{m}$ 得

$$\sum_{i=1}^m x_i \equiv \sum_{i=1}^m i \equiv \frac{m(m+1)}{2} \equiv \frac{m}{2} \pmod{m}$$

同理可得 $\sum_{i=1}^m y_i \equiv \frac{m}{2} \pmod{m}$.

若 $\{ax_1 + by_1, ax_2 + by_2, \dots, ax_m + by_m\}$ 是 m 的完系, 则应有

$$\sum_{i=1}^m (ax_i + by_i) \equiv \frac{m}{2} \pmod{m}$$

但是

$$\begin{aligned} \sum_{i=1}^m (ax_i + by_i) &\equiv a \sum_{i=1}^m x_i + b \sum_{i=1}^m y_i \equiv a \cdot \frac{m}{2} + b \cdot \frac{m}{2} \\ &\equiv (a+b) \cdot \frac{m}{2} \equiv ((a+b)/2)m \equiv 0 \pmod{m} \end{aligned}$$

矛盾. 所以, $\{ax_1 + by_1, ax_2 + by_2, \dots, ax_m + by_m\}$ 不是 m 的完系.

例 3.12 设 a 与 m 是给定的两整数, $m > 1$ 且 $(a, m) = 1$, 证明

$$\sum_{k=1}^{m-1} \left[\frac{ak}{m} \right] = \frac{1}{2}(a-1)(m-1)$$

证 因 $0, 1, \dots, m-1$ 是 m 的完系且 $(a, m) = 1$, 故 $0, 1a, 2a, \dots, (m-1)a$ 也是 m 的完系, 所以, $0, 1a, 2a, \dots, (m-1)a$ 分别除 m 而得的(最小非负的)余数集是 $\{0, 1, 2, \dots, m-1\}$, 于是

$$\begin{aligned} \sum_{k=1}^{m-1} \left[\frac{ak}{m} \right] &= \sum_{k=0}^{m-1} \left[\frac{ak}{m} \right] = \sum_{k=0}^{m-1} \frac{ak}{m} - \sum_{k=0}^{m-1} \left\{ \frac{ak}{m} \right\} \\ &= \frac{a}{m} \sum_{k=0}^{m-1} k - \sum_{i=0}^{m-1} \frac{i}{m} = \frac{a}{m} \cdot \frac{m(m-1)}{2} - \frac{1}{m} \cdot \frac{m(m-1)}{2} \\ &= \frac{1}{2}(a-1)(m-1) \end{aligned}$$

在模 m 的同余类中, 有些类中的每个数均与 m 互素, 如 1 所在的同余类中每个数均与 m 互素. 若 $m=8$, 则同余类 $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ 中的每个数均与 8 互素, 这样的同余类我们将给它们一个特定的名称.

定义 3.3 设 m 是一个大于 1 的正整数, 定义

- (1) 模 m 的同余类 \bar{r} 称为模 m 的一个简化同余类, 如果 $(r, m) = 1$.
- (2) 在模 m 的所有简化同余类中各取一数, 称这组数为模 m 的一个简化剩余系, 又称简系.

如果 \bar{r} 是模 m 的一个简化同余类, a 是 \bar{r} 中任一整数, 则 $a - r \equiv 0 \pmod{m}$, 即存在整数 k 使 $a = r + km$, 从而由 $(r, m) = 1$ 得 $(a, m) = 1$. 因此, 模 m 的同余类是

模 m 的一个简化同余类的充分必要条件, 该余类中的每个数均与 m 互素, 且由此可知, m 的简系中的每个数皆与 m 互素, 于是有下列定理.

定理 3.5 k 个整数 a_1, a_2, \dots, a_k 构成 m 的简系的充分必要条件如下.

- (1) $k = \varphi(m)$.
- (2) $(a_i, m) = 1$.
- (3) $a_i \not\equiv a_j \pmod{m}, i \neq j$.

证 必要性 由简系的定义知 a_1, a_2, \dots, a_k 是从模 m 的所有简化剩余类中各取一数而构成的. $\bar{1}, \bar{2}, \dots, \bar{m}$ 是模 m 的一个完全剩余类, 则模 m 的所有简化剩余类组成的集合是

$$\{\bar{r} \mid (r, m) = 1, 1 \leq r \leq m\}$$

由 Euler 函数的定义可知: 满足上面集合中条件的 r 共有 $\varphi(m)$ 个, 因此, 模 m 的简化剩余类共有 $\varphi(m)$ 个, 故 $k = \varphi(m)$, 即条件(1)成立, 而条件(2)及条件(3)由简系的定义即知成立.

充分性 由必要性证明知, 模 m 的简化剩余类共有 $\varphi(m)$ 个, 条件(1)及(2)说明 a_1, a_2, \dots, a_k 是模 m 的简化剩余类中选取的 $\varphi(m)$ 个整数, 再由条件(3)即知: a_1, a_2, \dots, a_k 是从模 m 的全部 $\varphi(m)$ 个简化剩余类中各选取的一数而成, 所以, 依定义知 a_1, a_2, \dots, a_k 是 m 的一个简系.

利用定理 3.5 有下列结论.

定理 3.6 设 a 与 b 是满足 $(a, m) = 1$ 及 $m \mid b$ 的两个整数, 若 $a_1, a_2, \dots, a_{\varphi(m)}$ 是 m 的简系, 则

$$a a_1 + b, a a_2 + b, \dots, a a_{\varphi(m)} + b$$

亦是 m 的一个简系.

证 利用定理 3.4, 由 $(a, m) = 1$ 及 $m \mid b$ 便得, $(a a_i + b, m) = (a a_i, m) = (a_i, m) = 1$. 且当 $i \neq j$ 时, 有 $a a_i + b \equiv a a_j + b \pmod{m}$, 则 $a a_i \equiv a a_j \pmod{m}$, 于是, 由 $(a, m) = 1$ 得 $a_i \equiv a_j \pmod{m}$, 这与 $a_1, a_2, \dots, a_{\varphi(m)}$ 为 m 的简系矛盾. 故 $a a_i + b \not\equiv a a_j + b \pmod{m}$, 所以

$$a a_1 + b, a a_2 + b, \dots, a a_{\varphi(m)} + b$$

构成 m 的简系.

定义 3.4 设 m 是一正整数, 则所有不超过 m 且与 m 互素的 $\varphi(m)$ 个数构成 m 的一个简系, 称该系为 m 的最小正简化剩余系(可简称最小正简系或缩系).

例如, 8 的最小正简系为 1, 3, 5, 7. 15 的最小正简系为 1, 2, 4, 7, 8, 11, 13, 14.

例 3.13 设 m 是大于 1 的整数, a 与 b 分别是满足 $(a, m) = 1$ 及 $m \mid b$ 的任意两个整数, 则有

$$\sum_x \left\{ \frac{ax + b}{m} \right\} = \frac{\varphi(m)}{2}$$

其中,求和表示对 x 取遍 m 的简系.

证 由定理 3.6 知,当 x 取遍 m 的简系时, $ax+b$ 也取遍 m 的简系,因此,用 m 除 $ax+b$ 所得的余数 $r(x)$ 取遍 m 的最小正简系.

设 $r_1, r_2, \dots, r_{\varphi(m)}$ 是 m 的最小正简系,则 $\{r_1, r_2, \dots, r_{\varphi(m)}\} = \{m-r_1, m-r_2, \dots, m-r_{\varphi(m)}\}$, 所以

$$\begin{aligned} \sum_x \left\{ \frac{ax+b}{m} \right\} &= \sum_x \frac{r(x)}{m} = \frac{r_1}{m} + \frac{r_2}{m} + \dots + \frac{r_{\varphi(m)}}{m} \\ &= \frac{m-r_1}{m} + \frac{m-r_2}{m} + \dots + \frac{m-r_{\varphi(m)}}{m} \end{aligned}$$

因此

$$2 \left(\frac{r_1}{m} + \frac{r_2}{m} + \dots + \frac{r_{\varphi(m)}}{m} \right) = \varphi(m) \cdot 1$$

即

$$\frac{r_1}{m} + \frac{r_2}{m} + \dots + \frac{r_{\varphi(m)}}{m} = \frac{1}{2} \varphi(m)$$

故

$$\sum_x \left\{ \frac{ax+b}{m} \right\} = \frac{\varphi(m)}{2}$$

例 3.14 若 p 为奇素数, m 是任一正整数且满足 $2^m \not\equiv 1 \pmod{p}$, 证明

$$1^m + 2^m + \dots + (p-1)^m \equiv 0 \pmod{p}$$

证 因 p 为素数, 故 $1, 2, \dots, p-1$ 是 p 的简系, 又 $(2, p) = 1$, 从而由定理 3.6 知

$$2 \times 1, 2 \times 2, \dots, 2 \times (p-1)$$

也是 p 的简系, 因此得

$$1^m + 2^m + \dots + (p-1)^m \equiv (2 \times 1)^m + (2 \times 2)^m + \dots + (2 \times (p-1))^m \pmod{p}$$

即有

$$(2^m - 1)(1^m + 2^m + \dots + (p-1)^m) \equiv 0 \pmod{p}$$

亦即

$$p \mid (2^m - 1)(1^m + 2^m + \dots + (p-1)^m)$$

但 $p \nmid (2^m - 1)$, 所以必有

$$p \mid 1^m + 2^m + \dots + (p-1)^m$$

于是

$$1^m + 2^m + \dots + (p-1)^m \equiv 0 \pmod{p}$$

例 3.15 设 $m = m_1 m_2$, $(m_1, m_2) = 1$, a 与 b 是满足条件 $(a, b) = 1$, $m_1 \mid b$ 及 $m_2 \mid a$ 的任意两个整数, 则

(1) 当 x 取遍 m_1 的完系, y 取遍 m_2 的完系时, $ax+by$ 取遍 m 的完系.

(2) 当 x 取遍 m_1 的简系, y 取遍 m_2 的简系时, $ax+by$ 取遍 m 的简系.

我们只证明(2).

证 首先, 设 $x_1, x_2, \dots, x_{\varphi(m_1)}$ 是 m_1 的简系, $x_1, x_2, \dots, x_{\varphi(m_2)}$ 是 m_2 的简系, 则

$$\{ax+by \mid x \in \{x_1, \dots, x_{\varphi(m_1)}\}, y \in \{y_1, \dots, y_{\varphi(m_2)}\}\}$$

共有 $\varphi(m_1)\varphi(m_2)$ 个数, 即 $\varphi(m_1m_2)$ ($=\varphi(m)$) 个数, 定理 3.4 的第(1)条成立.

其次, 如果 $ax_i + by_j \equiv ax_l + by_k \pmod{m_1m_2}$, 那么, $ax_i + by_j \equiv ax_l + by_k \pmod{m_1}$, 由 $m_1 \mid b$ 得 $ax_i \equiv ax_l \pmod{m_1}$. 再由 $(a, b) = 1$ 知 $(a, m_1) = 1$, 从而有 $x_i \equiv x_l \pmod{m_1}$, 即有 $i = l$. 同理可证 $j = k$. 因此, 定理 3.5 的第(3)条成立.

最后证 $(ax_i + by_j, m_1m_2) = 1$ 成立.

因为 $(x_i, m_1) = 1$, 又由 $(a, b) = 1$ 及 $m_1 \mid b$ 知, $(a, m_1) = 1$, 故 $(ax_i, m_1) = 1$. 再由 $m_1 \mid b$ 可得

$$(ax_i + by_j, m_1) = 1$$

同理可证

$$(ax_i + by_j, m_2) = 1$$

因此, 由 $(m_1, m_2) = 1$, 即得

$$(ax_i + by_j, m_1m_2) = 1$$

从而根据定理 3.5 便知

$$\{ax_i + by_j \mid i = 1, \dots, \varphi(m_1), j = 1, \dots, \varphi(m_2)\}$$

是 $m = m_1m_2$ 的简系.

特殊情形, 可取 $a = m_2, b = m_1$.

练 习 3.2

1. 分别针对下列三种情况求模 15 的一个完系, 使以下成立.

(1) 该完系的每个数是偶数.

(2) 该完系的每个数是奇数.

(3) 该完系的每个数是绝对值最小的.

2. 将题 1 中的“完系”换成“简系”后解此题.

3. 将题 1 的“模 15”换成“模 12”后能否完成此题?

4. 设 a_1, a_2, \dots, a_k 是模 $m (> 2)$ 的一个简系, 证明 $\sum_{i=1}^k a_i \equiv 0 \pmod{m}$.

5. 证明从任意 m 个整数中一定可选出若干个数, 使其和是 m 的倍数.

6. 设 p 是一个素数, 证明

$$\{x + p^{s-t}y \mid x \text{ 取值 } 0, 1, \dots, p^{s-t} - 1; y \text{ 取值 } 0, 1, \dots, p^t - 1; t \leq s\}$$

构成模 p^s 的一个完系.

7. 求模 3 的一个完系 $\{a_1, a_2, a_3\}$ 及模 5 的一个完系 $\{b_1, b_2, b_3, b_4, b_5\}$, 使得以下成立.

(1) $\{a_i b_j \mid i=1, 2, 3; j=1, 2, 3, 4, 5\}$ 构成模 15 的一个完系.

(2) $\{a_i + b_j \mid i=1, 2, 3; j=1, 2, 3, 4, 5\}$ 及 $\{a_i b_j \mid i=1, 2, 3; j=1, 2, 3, 4, 5\}$ 同时是模 15 的完系.

8. 将题 7 的“完系”换成“简系”后结论仍成立吗?

9. 设 m_1, m_2 是正整数, 证明: 当 x 取遍 m_1 的完系及 y 取遍 m_2 的完系时, $x + m_1 y$ 取遍 $m_1 m_2$ 的完系.

10. 将题 9 中的“完系”换成“简系”后, 结论是否仍成立? 若不成立, 那么在什么情况下成立?

3.3 同余理论中的几个著名定理

本节将介绍简化剩余系的重要应用.

定理 3.7 (Euler 定理) 设 m 是任一给定的正整数, a 是任一整数且 $(a, m) = 1$, 则有

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad (3.3.1)$$

证 设 $x_1, x_2, \dots, x_{\varphi(m)}$ 是 m 的一个简系, 则由 $(a, m) = 1$ 及定理 3.6 知, $ax_1, ax_2, \dots, ax_{\varphi(m)}$ 亦是 m 的一个简系, 因此有

$$x_1 x_2 \cdots x_{\varphi(m)} \equiv ax_1 ax_2 \cdots ax_{\varphi(m)} \pmod{m}$$

即

$$a^{\varphi(m)} x_1 x_2 \cdots x_{\varphi(m)} \equiv 1 \cdot (x_1 x_2 \cdots x_{\varphi(m)}) \pmod{m} \quad (3.3.2)$$

而由于 $(x_i, m) = 1, i=1, 2, \dots, \varphi(m)$, 故 $(x_1 x_2 \cdots x_{\varphi(m)}, m) = 1$, 由定理 3.1 中 (7) 及式 (3.3.2) 便得

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

定理 3.8 (Fermat 定理) 若 p 是一素数, a 是任一整数, 则有

$$a^p \equiv a \pmod{p} \quad (3.3.3)$$

证 若 $(p, a) = 1$, 则由 Euler 定理及 $\varphi(p) = p - 1$ 得 $a^{p-1} \equiv 1 \pmod{p}$, 再由 $a \equiv a \pmod{p}$ 便有 $a^p \equiv a \pmod{p}$.

若 $(p, a) \neq 1$, 即 $p \mid a$, 则 $a^p \equiv 0 \equiv a \pmod{p}$, 即有 $a^p \equiv a \pmod{p}$, 所以, 式 (3.3.3) 成立.

例 3.16 求 1999^{2001} 除 70 的余数是多少?

解 因 $(1999, 70) = 1$, $\varphi(70) = \varphi(2) \cdot \varphi(5) \cdot \varphi(7) = 24$, 所以, 由 Euler 定理得

$$1999^{24} \equiv 1 \pmod{70}$$

而 $2001 = 83 \times 24 + 9$ 及 $1999 = 28 \times 70 + 39$, 故

$$1999^{2001} = (1999^{24})^{83} \times 1999^9 \equiv 1^{83} \times 1999^9 \equiv 1999^9 \equiv 39^9 \equiv 29 \pmod{70}$$

所以, 1999^{2001} 除 70 的余数是 29.

例 3.17 求证 $1^{2010} + 2^{2010} + \dots + 2012^{2010}$ 是 2011 的倍数.

证 因 2011 是素数, 故 $\varphi(2011) = 2010$. 于是, 由 Euler 定理得

$$k^{2010} \equiv 1 \pmod{2011}, \quad k = 1, 2, \dots, 2010, 2012$$

从而

$$\begin{aligned} & 1^{2010} + 2^{2010} + \dots + 2010^{2010} + 2011^{2010} + 2012^{2010} \\ & \equiv 1 + 1 + \dots + 1 + 0 + 1 \equiv 2011 \equiv 0 \pmod{2011} \end{aligned}$$

这说明 $1^{2010} + 2^{2010} + \dots + 2012^{2010}$ 是 2011 的倍数.

例 3.18 证明对于任意整数 n , 有 $n^7 \equiv n \pmod{42}$.

证 由 Fermat 定理, $n^7 \equiv n \pmod{7}$. 此外

$$\begin{aligned} n^7 - n &= n(n^6 - 1) = n(n^2 - 1)(n^4 - n^2 + 1) \\ &= (n-1)n(n+1)(n^4 - n^2 + 1) \equiv 0 \pmod{6} \end{aligned}$$

从而有

$$n^7 - n \equiv 0 \pmod{42}$$

例 3.19 若 $(a, 10) = 1$, 则 $a^{100n+1} \equiv a \pmod{1000}$, 其中, n 为非负整数.

证 因 $1000 = 8 \times 125$ 及 $(a, 10) = 1$ 知, $(a, 8) = 1$ 及 $(a, 125) = 1$, 由 Euler 定理有

$$a^{\varphi(8)} \equiv 1 \pmod{8} \quad \text{及} \quad a^{\varphi(125)} \equiv 1 \pmod{125}$$

由于 $\varphi(8) = 4$ 及 $\varphi(125) = 100$, 故有

$$\begin{aligned} a^{100n+1} &\equiv (a^4)^{25n} \cdot a \equiv 1^{25n} \cdot a \equiv a \pmod{8} \\ a^{100n+1} &\equiv a^{100n} \cdot a \equiv (a^{100})^n \cdot a \equiv 1^n \cdot a \equiv a \pmod{125} \end{aligned}$$

所以, 由 $(8, 125) = 1$ 即得 $a^{100n+1} \equiv a \pmod{1000}$.

例 3.20 设 a 是大于 1 的整数, 证明 $a^{2^n} + 1$ 的奇素因数是 $2^{n+1}k + 1$ 的形状. 其中, n 是非负整数.

证 当 $n = 0$ 时结论显然成立.

归纳假设结论对 $n-1$ 成立, 即 $a^{2^{n-1}} + 1$ 的素因数是 $2^n k + 1$ 的形状.

设 p 是 $a^{2^n} + 1$ 的任一素因数, 则由 $a^{2^n} + 1 = (a^2)^{2^{n-1}} + 1$ 及归纳假设知 p 具有 $2^n k + 1$ 的形状. 设 $p = 2^n t + 1$, 因 p 是 $a^{2^n} + 1$ 的素因数, 故 $a^{2^n} + 1 \equiv 0 \pmod{p}$, 即 $a^{2^n} \equiv -1 \pmod{p}$. 于是

$$(a^{2^n})^t \equiv (-1)^t \pmod{p}$$

即有 $a^{p-1} \equiv (-1)^t \pmod{p}$. 而由 Euler 定理有 $a^{p-1} \equiv 1 \pmod{p}$, 从而 $(-1)^t \equiv$

$1 \pmod{p}$, 即 t 为偶数. 设 $t = 2l$, 则 $p = 2^n t + 1 = 2^{n+1} l + 1$, 结论对 n 成立. 由归纳法原理, 本题结论成立.

例 3.21 设 m 是正整数, 如果 $a^{m-1} \equiv 1 \pmod{m}$, 且对于 $m-1$ 的任一真约数 n 都有 $a^n \not\equiv 1 \pmod{m}$, 则 m 是素数.

证 设 d 是满足 $a^x \equiv 1 \pmod{m}$ 的最小正整数, 由带余除法可令

$$m-1 = dq + r, \quad 0 \leq r \leq d$$

于是

$$a^r = a^{(m-1)-dq} = (a^{m-1}) \cdot (a^d)^{-q} \equiv 1 \cdot 1^{-q} \equiv 1 \pmod{m}$$

从而由 d 的最小性知 $r=0$. 这样, d 是 $m-1$ 的约数, 由题设知 $d=m-1$. 另外, 因 $(a^{m-1}, m)=1$, 所以, $(a, m)=1$, 由 Euler 定理, $a^{\varphi(m)} \equiv 1 \pmod{m}$, 于是, 由上述说明可得 $\varphi(m) \geq m-1$. 但当 $m > 1$ 时, 恒有 $\varphi(m) \leq m-1$, 故必有 $\varphi(m) = m-1$. 所以, m 必为素数.

注 (1) 该结论的逆命题不成立, 即当 m 是素数时, 可能有 $d|m-1$ 使 $a^d \equiv 1 \pmod{m}$. 如取 $m=5, a=4$, 则有 $d=2$ 使 $d|5-1$ 且 $4^2 \equiv 1 \pmod{5}$.

(2) 若将条件改为“存在正整数 $a (> 1)$ 使 $a^{m-1} \equiv 1 \pmod{m}$, 且对于 $m-1$ 的任一真约数 n 有 $a^n \not\equiv 1 \pmod{m}$ ”, 则 m 是素数. 反之, m 为素数时上条件是否成立? 该问题作为一道思考题供读者研究.

定理 3.9 (Wilson 定理) 证明正整数 p 为素数的充分必要条件是

$$(p-1)! \equiv -1 \pmod{p} \quad (3.3.4)$$

证 必要性 当 $p=2$ 及 3 时, 式(3.3.4)显然成立. 下设 $p > 3$.

证明的思路是使 $p-3$ 个整数 $2, 3, \dots, p-2$ 分成 $\frac{p-3}{2}$ 个整数对, 每一对的乘积关于模 p 与 1 同余, 这样, 就得 $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$.

任取 $a \in \{2, 3, \dots, p-2\}$, 由 $(a, p)=1$ 及 $1, 2, \dots, p-1$ 为 p 的简系知, $a, 2a, \dots, (p-1)a$ 亦是 p 的简系. 于是, 存在唯一的 $r \in \{1, 2, \dots, p-1\}$ 使

$$r \cdot a \equiv 1 \pmod{p} \quad (3.3.5)$$

由 $2 \leq a \leq p-2$ 可得 $a \neq r$ 及 $r \neq 1, p-1$. 因此, 当 $a \in \{2, 3, \dots, (p-1)/2\}$ 时, 必有 $r \in \{(p-1)/2+1, \dots, p-2\}$, 使得 $r \cdot a \equiv 1 \pmod{p}$, 即有 $S = (p-3)/2$ 对 (a_i, r_i) , 使

$$r_i \cdot a_i \equiv 1 \pmod{p} \quad (3.3.6)$$

其中, $a_i \in \{2, 3, \dots, (p-1)/2\}$, $r_i \in \{(p-1)/2+1, \dots, p-2\}$. 所以, 由式(3.3.6)有

$$2 \cdot 3 \cdot \dots \cdot (p-2) = \prod_{i=1}^S a_i \cdot \prod_{i=1}^S r_i = \prod_{i=1}^S (a_i r_i) \equiv 1 \pmod{p}$$

因此, $(p-1)! \equiv -1 \pmod{p}$.

充分性 若 p 非素数, 那么, p 有真约数 $q (> 1)$, 于是, 一方面由题设

$(p-1)! \equiv -1 \pmod{p}$ 推得 $(p-1)! \equiv -1 \pmod{q}$. 另一方面, 由 $q \mid (p-1)!$ 推得 $(p-1)! \equiv 0 \pmod{q}$, 矛盾, 因此 p 必为素数.

Wilson 定理在同余理论中有许多应用, 下面是两个例子.

例 3.22 设 p 是大于 2 的素数, 证明二次同余方程 $x^2 + 1 \equiv 0 \pmod{p}$ 有解的充分必要条件是 p 具有 $4k+1$ 的形状.

证 必要性 设 a 是 $x^2 + 1 \equiv 0 \pmod{p}$ 的一解, 即 $a^2 \equiv -1 \pmod{p}$, 于是, $(a, p) = 1$. 由 Euler 定理得

$$(a^2)^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \pmod{p}$$

从而

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

所以, $\frac{p-1}{2}$ 是偶数, 即 p 是 $4k+1$ 的形状.

充分性 若 p 是 $4k+1$ 的形状, 则 $\frac{p-1}{2}$ 是偶数, 那么

$$\begin{aligned} (p-1)! &= \left(1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right) \left(\left(\frac{p-1}{2}+1\right)\left(\frac{p-1}{2}+2\right)\cdots(p-2)(p-1)\right) \\ &= \left(1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right) \cdot \left(\left(p-\frac{p-1}{2}\right)\left(p-\frac{p-3}{2}\right)\cdots(p-2)(p-1)\right) \\ &= \left(1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right) \cdot \left((p-1)(p-2)\cdots\left(p-\frac{p-1}{2}\right)\right) \\ &\equiv \left(1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}\right) \cdot \left((-1)(-2)\cdots\left(-\frac{p-1}{2}\right)\right) \\ &\equiv (-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 2^2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right)^2 \\ &\equiv 1^2 \cdot 2^2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right)^2 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p} \end{aligned}$$

而由 Wilson 定理 $(p-1)! \equiv -1 \pmod{p}$, 所以有 $\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1 \equiv 0 \pmod{p}$, 即

$\left(\frac{p-1}{2}\right)!$ 是二次同余方程 $x^2 + 1 \equiv 0 \pmod{p}$ 的解.

例 3.23 设 p 为奇素数, 证明 $2^2 \cdot 4^2 \cdot \cdots \cdot (p-1)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.

证 由于 $(p-1)! = (1 \cdot 3 \cdot \cdots \cdot (p-2)) \cdot (2 \cdot 4 \cdot \cdots \cdot (p-1))$

$$\begin{aligned} &= ((p-2)(p-4)\cdots(p-(p-1))) \cdot (2 \cdot 4 \cdot \cdots \cdot (p-1)) \\ &\equiv ((-2)(-4)\cdots(-(p-1))) \cdot (2 \cdot 4 \cdot \cdots \cdot (p-1)) \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{2}} (2 \cdot 4 \cdot \cdots \cdot (p-1)) \cdot (2 \cdot 4 \cdot \cdots \cdot (p-1)) \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{2}} \cdot (2^2 \cdot 4^2 \cdot \cdots \cdot (p-1)^2) \pmod{p} \end{aligned}$$

另外,由 Wilson 定理 $(p-1)! \equiv -1 \pmod{p}$, 故有

$$-1 \equiv (-1)^{\frac{p-1}{2}} (2^2 \cdot 4^2 \cdot \cdots \cdot (p-1)^2) \pmod{p}$$

亦即

$$2^2 \cdot 4^2 \cdot \cdots \cdot (p-1)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

作为本节的结束,我们来介绍 Euler 定理及 Fermat 定理在研究分数与小数的互化时的应用.

由于任何一个分数(小数)均可表示成一个整数与一个 $(0,1)$ 上的分数(小数)的和,所以下面考虑的分数、小数均在 $(0,1)$ 上.

定义 3.5 (1) 设 $a = 0 \cdot a_1 a_2 \cdots a_n \cdots$ ($0 \leq a_n \leq 9$ 且无限个 a_n 不为零) 是一个无限小数. 如果存在两个整数 $u (\geq 0)$ 与 $v (> 0)$, 使得 $a_{u+i} = a_{u+jv+i}$, $i = 1, 2, \cdots, v, j = 0, 1, 2, \cdots$, 则称 a 是一个(无限)循环小数, 此时可记 $a = 0 \cdot a_1 a_2 \cdots a_u \dot{a}_{u+1} \cdots \dot{a}_{u+v}$.

(2) 若 a 是一无限循环小数, 由于上述存在的 u 及 v 不一定唯一, 如下:

$$a = 0.231231231\cdots = 0.\dot{2}\dot{3}\dot{1} = 0.2\dot{3}\dot{1}\dot{2} = 0.23\dot{1}\dot{2}\dot{3} = 0.\dot{2}\dot{3}\dot{1}\dot{2}\dot{3}\dot{1}$$

如果找到的 u 及 v 是最小的, 则称 $a_{u+1}, a_{u+2}, \cdots, a_{u+v}$ 为循环节. v 称为循环节的长度; 如果 $u=0$, 则称 a 为纯循环小数, 否则称为混循环小数.

定理 3.10 既约真分数 $\frac{a}{b}$ 可化为纯循环小数的充分必要条件是 $(b, 10) = 1$.

证 充分性 因 $(b, 10) = 1$, 由 Euler 定理得 $10^{\phi(b)} \equiv 1 \pmod{b}$. 设 v 是使 $10^v \equiv 1 \pmod{b}$ 成立的最小正整数, 则存在满足条件 $0 < q < 10^v - 1$ 的正整数 q , 使

$$10^v \frac{a}{b} = q + \frac{a}{b} \quad (3.3.7)$$

设有 Euclid 算式

$$\left. \begin{aligned} q &= 10q_1 + a_v \\ q_1 &= 10q_2 + a_{v-1} \\ &\cdots \\ q_{v-1} &= 10q_v + a_1 \end{aligned} \right\} \quad (3.3.8)$$

其中, $0 \leq a_i < 10$ 及 $q_i \geq 0, i = 1, 2, \cdots, v$.

由式(3.3.8)得 $q = 10^v q_v + 10^{v-1} a_1 + \cdots + 10 a_{v-1} + a_v$. 因为 $0 < q < 10^v - 1$, 故 $q_v = 0$ 且 a_1, a_2, \cdots, a_v 不能全为 0 或全为 9. 由式(3.3.7)得

$$\frac{a}{b} = \frac{q}{10^v} + \frac{1}{10^v} \cdot \frac{a}{b}$$

即

$$\frac{a}{b} = 0 \cdot a_1 a_2 \cdots a_v + \frac{1}{10^v} \cdot \frac{a}{b} \quad (3.3.9)$$

重复应用式(3.3.9)即推得

$$\frac{a}{b} = 0. \dot{a}_1 \dot{a}_2 \cdots \dot{a}_v$$

充分性得证.

必要性 若 $\frac{a}{b}$ 是既约真分数, 且 $\frac{a}{b} = 0. \dot{a}_1 \dot{a}_2 \cdots \dot{a}_v$, 则

$$\begin{aligned} \frac{a}{b} &= 0. a_1 a_2 \cdots a_v \cdot a_1 a_2 \cdots a_v \cdots \\ &= 10^{-v} (a_1 \cdot 10^{v-1} + a_2 \cdot 10^{v-2} + \cdots + a_v \cdot 10^{v-v}) + 10^{-v} \cdot 0. \dot{a}_1 \dot{a}_2 \cdots \dot{a}_v \\ &= 10^{-v} \left(q + \frac{a}{b} \right) \end{aligned}$$

其中, $q = a_1 \cdot 10^{v-1} + a_2 \cdot 10^{v-2} + \cdots + a_v \cdot 10^{v-v}$, 即有 $a(10^v - 1) = bq$, 由 $\frac{a}{b}$ 是既约分数知 $b | (10^v - 1)$, 亦即 $10^v \equiv 1 \pmod{b}$. 显然有 $(b, 10) = 1$.

定理 3.11 既约真分数 $\frac{a}{b}$ 可化为混循环小数, 且其不循环部分的位数是 $s (\geq 1)$ 的充分必要条件是 $b = 2^\alpha \cdot 5^\beta \cdot b_1$, 且 $(b_1, 10) = 1$, 及 $\max\{\alpha, \beta\} = s$.

证 充分性 不妨设 $\alpha \geq \beta$, 则 $s = \alpha$, $10^s \cdot \frac{a}{b} = 10^\alpha \cdot \frac{a}{b} = \frac{5^{\alpha-\beta} \cdot a}{b_1}$.

令 $\frac{5^{\alpha-\beta} \cdot a}{b_1} = q + \frac{a_1}{b_1}$, 其中, $0 < a_1 < b_1$, $0 \leq q < 10^\alpha$. 由 $(a, b) = 1$ 及 $(b_1, 10) = 1$ 可得 $(a_1, b_1) = 1$.

据定理 3.10, 可把 $\frac{a_1}{b_1}$ 表示成纯循环小数

$$\frac{a_1}{b_1} = 0. \dot{c}_1 \cdots \dot{c}_t \tag{3.3.10}$$

可设 $q = q_1 \cdot 10^{\alpha-1} + q_2 \cdot 10^{\alpha-2} + \cdots + q_\alpha$, $0 \leq q_i < 10$, 则

$$\frac{a}{b} = 0. q_1 \cdots q_\alpha \dot{c}_1 \cdots \dot{c}_t$$

再若

$$\frac{a}{b} = 0. m_1 \cdots m_u \dot{d}_1 \cdots \dot{d}_t \quad (u < \alpha)$$

那么

$$10^u \frac{a}{b} - \left[10^u \frac{a}{b} \right] = 0. \dot{d}_1 \cdots \dot{d}_t$$

由定理 3.10, 可设该纯循环小数为 $\frac{a_2}{b_2}$, 其中, $(b_2, 10) = 1$, 于是可得

$$10^u \frac{a}{b} = \frac{a'}{b_2} \left(a' = \left[10^u \frac{a}{b} \right] b_2 + a_2 \right)$$

即有

$$10^u b_2 a = a' b \quad (3.3.11)$$

因为 $(a, b) = 1$, 及 $(b_2, 10) = 1$, 知 $(ab_2, 2^s) = 1$. 由式(3.3.11)及 $2^s | b$ 便推得 $2^s | 10^u$, 即有 $2^s | 2^u$, 这与 $u < s$ 矛盾. 因此, $\frac{a}{b}$ 化为小数后不循环的位数是 s .

必要性 设 $\frac{a}{b} = 0. q_1 \cdots q_s \dot{c}_1 \cdots \dot{c}_t$ 则

$$10^s \frac{a}{b} = q_1 \cdot 10^{s-1} + \cdots + q_s + 0. \dot{c}_1 \cdots \dot{c}_t$$

记 $q = q_1 \cdot 10^{s-1} + \cdots + q_s$, 那么

$$\frac{10^s a - qb}{b} = 0. \dot{c}_1 \cdots \dot{c}_t$$

设 $\frac{10^s a - qb}{b} = \frac{a_1}{b_1}$ 是既约真分数, 则由定理 3.10 知, $(b_1, 10) = 1$ 且

$$b = \frac{10^s a b_1}{q b_1 + a_1} \quad (3.3.12)$$

由 $(a, b) = 1$ 可得 $a | q b_1 + a_1$. 令 $q b_1 + a_1 = a q'$, 则式(3.3.12)变为 $b = \frac{10^s}{q'} \cdot b_1$. 由 $(q b_1 + a_1, b_1) = (a_1, b_1) = 1$ 及 $b_1 | b(q b_1 + a_1)$ 得 $b_1 | b$, 故 $\frac{10^s}{q'}$ 是整数. 可设 $q' = 2^u 5^v$, 那么有

$$b = 2^{s-u} 5^{s-v} b_1 \quad (3.3.13)$$

其中, $(b_1, 10) = 1$ 且 $0 \leq u, v \leq s$.

如果 $u = v = s$, 由定理 3.10 知 $\frac{a}{b}$ 化为小数时是纯循环小数, 与题设矛盾.

设 u 与 v 不全为 s , 且全不为 0, 则 $s > \max\{s-u, s-v\} > 0$. 那么, 由充分性的证明知 $\frac{a}{b}$ 化为小数时是混循环小数, 其不循环部分的位数是 $\max\{s-u, s-v\}$. 但 $\max\{s-u, s-v\} < s$, 与题设矛盾. 因此, u 与 v 中必有一为零. 令 $s-u = \alpha, s-v = \beta$, 则式(3.3.13)化为 $b = 2^\alpha 5^\beta \cdot b_1$, 其中, $(b_1, 10) = 1$, 且 $\max\{\alpha, \beta\} = s$.

例 3.24 将 $\frac{7}{13}$ 及 $\frac{37}{440}$ 表示成循环小数的形式, 并求其非循环部分的位数及循环环节长度.

解 $\frac{7}{13} = 0. \dot{5} \dot{3} \dot{8} \dot{4} \dot{6} \dot{1}$, 该小数是纯循环小数, 其循环环节长度是 6. 易证 $t=6$ 是

使 $10^t \equiv 1 \pmod{13}$ 成立的最小正整数.

$\frac{37}{440} = 0.084\dot{0}\dot{9}$, 该数是混循环小数, 不循环部分的位数是 3, 循环节长度是 2,

且显然不循环部分的位数 3 是 $440 = 2^3 \times 5 \times 11$ 的因子 2 与 5 的幂中最大者, 而循环长度 2 是使 $10^t \equiv 1 \pmod{11}$ 成立的最小正整数.

练习 3.3

1. 证明 $1777^{1885} \equiv 27 \pmod{41}$ 及 $63! \equiv 61! \pmod{71}$.

2. 求 243^{402} 的最后三位数字.

3. 若某个一位数的 17 次幂的个位数是 7, 求该数.

4. 设 p 为素数, a_1, a_2, \dots, a_n 是整数, 证明

$$(1) (a_1 + a_2 + \dots + a_n)^p \equiv a_1^p + a_2^p + \dots + a_n^p \pmod{p}.$$

(2) 利用上式(1)证明 Fermat 定理.

5. 设 p 是一个大于 3 且不等于 11 的素数, 则 $p^{10} \equiv 1 \pmod{264}$.

6. 设 p, q 是任意两个互异素数, 证明

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

7. 利用 Wilson 定理证明下列结论:

(1) 若 p 是大于 5 的素数, 则 $(p-1)! + 2 \equiv 1 \pmod{p}$.

(2) 若 p 是任意素数, 则 $\sum_{k=1}^{p-1} k | ((p-1)! - p + 1)$.

8. 设 p 为奇素数, r_1, r_2, \dots, r_{p-1} 是 $1, 2, \dots, p-1$ 的一个排列, 证明 $r_1, 2r_2, \dots, (p-1)r_{p-1}$ 不是模 p 的简系.

9. 求一个既约分数的分母, 使它化成混循环小数后满足

(1) 循环节左边有一个数码, 循环节也只有一个数码.

(2) 循环节左边有两个数码, 循环节也只有两个数码.

10. 设 p 为奇素数, 证明

$$1^2 \cdot 3^2 \cdot (p-2)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

11. 证明如果 a 与 m 是两个互素的正整数, 则有 $1 + a + a^2 + \dots + a^{\varphi(m)} \equiv 0 \pmod{m}$.

12. 假定 $a^{\frac{m-1}{2}} \equiv -1 \pmod{m}$, 并且对于 $m-1$ 的任意真约数 $n, a^n \not\equiv 1 \pmod{m}$, 那么 m 是素数.

13. 设 $\frac{a}{b}$ 是一个既约分数, p 是 b 的最大素因子. 证明将 $\frac{a}{b}$ 表示成循环小数后, 其循环节长度是方程 $10^t \equiv 1 \pmod{p}$ 的最小正整数解.

3.4 一次同余方程

同余方程可以说是同余理论的核心,如著名的中国剩余定理(孙子定理)及在公钥密码学很有应用价值的 Legendre 符号均源自于同余方程.

定义 3.6 设 m 是一个大于 1 的正整数, $f(x)$ 是变量 x 的整系数多项式,称同余式

$$f(x) \equiv 0 \pmod{m} \quad (3.4.1)$$

为 x 的模 m 的一元同余方程,简称模 m 的同余方程. 如果 $f(x)$ 是一个 n 次多项式,且 $f(x)$ 的首项系数不能被 m 整除,则称方程(3.4.1)是模 m 的 n 次同余方程.

例如, $5x^3 - 25x^2 + 7x + 1 \equiv 0 \pmod{12}$ 是一个 3 次同余方程.

定义 3.7 如果整数 x_0 满足 $f(x_0) \equiv 0 \pmod{m}$,那么,所有关于模 m 同余于 x_0 的整数均满足方程(3.4.1). 由此,称 $x \equiv x_0 \pmod{m}$ 是方程(3.4.1)的一个解.

若 $x \equiv x_1 \pmod{m}$ 及 $x \equiv x_2 \pmod{m}$ 均为方程(3.4.1)的解,但 $x_1 \not\equiv x_2 \pmod{m}$,则称它们是方程(3.4.1)的不同的解. 显然,同余方程(3.4.1)至多有 m 个不同的解(两两不同余的解),方程(3.4.1)的不同解的个数称为解数.

如同余方程 $5x^3 - 25x^2 + 7x + 1 \equiv 0 \pmod{12}$ 有解 $x \equiv \pm 1, \pm 5, \pm 7, \pm 11 \pmod{12}$,但是, $1 \equiv -11 \pmod{12}$, $-1 \equiv 11 \pmod{12}$, $5 \equiv -7 \pmod{12}$, $-5 \equiv 7 \pmod{12}$,故该同余方程只有 4 个不同的解, $x \equiv \pm 1, \pm 5 \pmod{12}$,其解数为 4.

如果方程(3.4.1)的次数较高,则一般不易求解. 本节先讨论一次同余方程

$$ax + b \equiv 0 \pmod{m}, \text{ 其中, } m \nmid a \quad (3.4.2)$$

设 $(a, m) = d$, 如果方程(3.4.2)有解 $x \equiv x_0 \pmod{m}$, 则 $a \cdot x_0 + b \equiv 0 \pmod{m}$, 则由 $d \mid m$ 及 $d \mid ax_0$ 知 $d \mid b$, 这说明 $d \mid b$ 是方程(3.4.2)有解的必要条件.

下面将证明该条件也是方程(3.4.2)有解的充分条件.

定理 3.12 同余方程(3.4.2)有解的充分必要条件是 $d \mid b$. 当方程(3.4.2)有解时,其解数为 d , 若 $x \equiv x_0 \pmod{m}$ 为方程(3.4.2)的一个, 则其 d 个解为

$$x \equiv x_0 + \frac{m}{d}k \pmod{m}, \quad k = 0, 1, \dots, d-1 \quad (3.4.3)$$

证 必要性已经证明. 现证其充分性. 设 $d \mid b$, 由方程(3.4.2)得

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \pmod{\frac{m}{d}} \quad (3.4.2)'$$

因 $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, 故由 Euler 定理知 $\left(\frac{a}{d}\right)^{\varphi\left(\frac{m}{d}\right)} \equiv 1 \pmod{\frac{m}{d}}$. 将方程(3.4.2)' 两

端乘 $\left(\frac{a}{d}\right)^{\varphi\left(\frac{m}{d}\right)-1}$ 便得

$$\left(\frac{a}{d}\right)^{\varphi\left(\frac{m}{d}\right)} x + \frac{b}{d} \cdot \left(\frac{a}{d}\right)^{\varphi\left(\frac{m}{d}\right)-1} \equiv 0 \pmod{\frac{m}{d}}$$

即

$$x \equiv -\frac{b}{d} \left(\frac{a}{d}\right)^{\varphi\left(\frac{m}{d}\right)-1} \pmod{\frac{m}{d}} \quad (3.4.4)$$

这说明方程(3.4.4)是方程(3.4.2)'的一个解. 进而可以验证 $x \equiv -\frac{b}{d} \left(\frac{a}{d}\right)^{\varphi\left(\frac{m}{d}\right)-1} \pmod{\frac{m}{d}}$ 是方程(3.4.2)的一个解, 充分性得证.

若 $x \equiv x_0 \pmod{m}$ 是方程(3.4.2)的一个解, 则易证

$$x \equiv x_0 + \frac{m}{d}k \pmod{m} \quad (k = 0, 1, \dots, d-1)$$

是方程(3.4.2)的 d 个不同的解.

如果 $x \equiv x_1 \pmod{m}$ 是方程(3.4.2)的任一解, 即 $ax_1 + b \equiv 0 \pmod{m}$, 则由 $x \equiv x_0 \pmod{m}$ 得

$$a(x_1 - x_0) \equiv 0 \pmod{m}$$

于是, $m | a(x_1 - x_0)$, 从而 $\frac{m}{d} \mid \frac{a}{d}(x_1 - x_0)$. 因为 $\left(\frac{m}{d}, \frac{a}{d}\right) = 1$, 故有 $\frac{m}{d} \mid (x_1 - x_0)$, 亦

即存在整数 t , 使得 $x_1 = x_0 + \frac{m}{d}t$. 设 $t = ld + k$, $0 \leq k \leq d-1$, 则

$$x_1 = x_0 + \frac{m}{d}(ld + k) = x_0 + \frac{m}{d}k + ml \equiv x_0 + \frac{m}{d}k \pmod{m}$$

即

$$x_1 = x_0 + \frac{m}{d}k \pmod{m}, \quad 0 \leq k \leq d-1$$

所以, 方程(3.4.2)的任一解均是方程(3.4.3)的形式.

由定理 3.12 的证明中的式(3.4.4), 有下列结论.

推论 3.1 当 $(a, m) = 1$ 时, 同余方程(3.4.2)有唯一解

$$x \equiv -b \cdot a^{\varphi(m)-1} \pmod{m} \quad (3.4.5)$$

直观上看, 当模 m 较大时, 由于计算 $a^{\varphi(m)-1}$ 不易, 所以, 利用方程(3.4.5)来求得同余方程的解一般不太实际.

例 3.25 求下列同余方程的解:

$$(1) 3x + 5 \equiv 0 \pmod{4}. \quad (2) 58x - 87 \equiv 0 \pmod{47}.$$

$$(3) 1103x \equiv 531 \pmod{2132}. \quad (4) 129x \equiv 831 \pmod{1101}.$$

解 (1) 因 $(3, 4) = 1$, 该方程有唯一解. 由方程(3.4.5)可得, $x \equiv 1 \pmod{4}$ 是所求方程的解.

(2) 因 $(58, 47) = 1$, 该方程有唯一解. 由于 $58^{\varphi(47)-1}$ 不易计算, 因此, 不可利用方程(3.4.5)来求其解. 因 $58 \equiv 11(\pmod{47}), 87 \equiv -7(\pmod{47})$, 故原方程等价于

$$11x \equiv -7(\pmod{47})$$

由于 $(4, 47) = 1$, 将方程两端乘 4 后得

$$44x \equiv -28(\pmod{47})$$

即

$$3x \equiv 28(\pmod{47})$$

再由 $(16, 47) = 1$, 方程两端乘 16 后得

$$48x \equiv 448(\pmod{47})$$

即

$$x \equiv 25(\pmod{47})$$

(3) 因 $(1103, 2132) = 1$ (其实 1103 是素数), 所以该方程有唯一解. 由原方程得

$$2132y \equiv -531(\pmod{1103})$$

即

$$1029y \equiv -531(\pmod{1103})$$

因 $(1103, 3) = 1$. 两端除 3 得

$$343y \equiv -177(\pmod{1103}) \quad (3.4.6)$$

由方程(3.4.6)得

$$1103z \equiv 177(\pmod{343})$$

即

$$74z \equiv 177(\pmod{343}) \quad (3.4.7)$$

则

$$343u \equiv -177(\pmod{74})$$

即

$$47u \equiv -29(\pmod{74}) \quad (3.4.8)$$

或

$$-27u \equiv 45(\pmod{74})$$

因 $(74, 9) = 1$ 两端除 9 得

$$-3u \equiv 5(\pmod{74})$$

又有

$$74v \equiv 5(\pmod{3})$$

亦即

$$2v \equiv 2(\pmod{3}) \quad (3.4.9)$$

显然, $v_0 = 1$ 是方程 (3.4.9) 的一个解. 于是, $u_0 = \frac{5+74 \times (-1)}{-3} = 23$ 是方程 (3.4.8) 的一个整数解, 从而 $z_0 = \frac{177+343 \times 23}{74} = 109$ 是方程 (3.4.7) 的一个整数解, 因此, $y_0 = \frac{-177+1103 \times 109}{343} = 350$ 是方程 (3.4.6) 的一个整数解, $x_0 = \frac{531+2132 \times 350}{1103} = 677$ 是原方程的一个整数解, 故原方程的解为 $x \equiv 677 \pmod{2132}$.

(4) 因 $(129, 1101) = 3 \mid 831$, 故原方程有三个解. 化简原方程得

$$43x \equiv 277 \pmod{367} \quad (3.4.10)$$

因 $(43, 367) = 1$, 故方程 (3.4.10) 有唯一解, 将其解形式地表示为

$$x \equiv \frac{277}{43} \pmod{367}$$

将分子、分母同加模数 367 得 $x \equiv \frac{277+367}{43+367} \equiv \frac{644}{410} \pmod{367}$, 再分子、分母约去 2 得 $x \equiv \frac{322}{205} \pmod{367}$, 将分子加上 -367 , 得 $x \equiv \frac{-45}{205} \pmod{367}$, 约去 5 得 $x \equiv \frac{-9}{41} \pmod{367}$, 分子、分母同乘 9 得 $x \equiv \frac{-81}{369} \pmod{367}$, 将分子加 367, 分母加 -367 后得 $x \equiv \frac{286}{2} \pmod{367}$, 约去 2 得 $x \equiv \frac{143}{1} \pmod{367}$, 即 $x \equiv 143 \pmod{367}$ 是同余方程 (3.4.10) 的解, 从而 $x \equiv 143 \pmod{1101}$ 是原方程的一个解. 依据定理 3.12, 原方程的三个解为

$$x \equiv 143, 143 + 367, 143 + 367 \times 2 \pmod{1101}$$

即 $x \equiv 143, 510, 877 \pmod{1101}$.

在例 3.25 的求解过程中, 求解(1)用的是公式法方程 (3.4.5), 或称定理求解法. 求解(2)是用与模互素的数乘或除同余方程的两端, 使 x 的系数逐渐减小, 以达到求解的目的, 此法可称为数乘法. 求解(3)的方法是不断交换同余方程的模, 使模逐步减小, 求出解, 再将该解倒推, 最后得出原方程的解. 这是因为: 从同余方程 (3.4.2) 交换模得同余方程 $my \equiv b \pmod{a}$. 假如 y_0 是该方程的一个整数解, 那么, $x_0 = \frac{my_0 - b}{a}$ 是方程 (3.4.2) 的一个整数解, 因此, $x \equiv x_0 \pmod{m}$ 是方程 (3.4.2) 的一个解. 此解法可称为交换模法. 求解(4)的方法其原理同求解(1)的方法, 只不过这里是采用一种简便的形式表达法, 均是利用同余式的性质求解, 其步骤是: 先将同余方程 (3.4.2) 两边约去因数得同余方程

$$a_1 x_1 + b_1 \equiv 0 \pmod{m_1}, (a_1, m_1) = 1 \quad (3.4.2)''$$

然后将方程(3.4.2)''的解形式地表示为 $x \equiv -\frac{b_1}{a_1} \pmod{m_1}$, $-\frac{b_1}{a_1}$ 仅是一个分数形式的符号,再将分子或分母减去或加上模的倍数及分子、分母乘以不为0的整数或约去一个与模数互素的数等若干次(这相当于对同余式的两边使用同余的性质),使分母的绝对值变小,直至最后将“分数”变成整数,即得方程(3.4.2)''的解,由此便可求得方程(3.4.2)的解,此法可称为分式法. 又有如下例子.

例 3.26 求解同余方程 $1593x \equiv 1125 \pmod{1926}$.

解 因 $(1593, 1926) = 9 \mid 1125$, 所以, 同余方程有 9 个解, 将其简化得

$$177x \equiv 125 \pmod{214}$$

因此

$$\begin{aligned} x &\equiv \frac{125}{177} \equiv \frac{125 + 214}{177} \equiv \frac{339}{177} \equiv \frac{113}{59} \equiv \frac{113 \times 5}{59 \times 5} \equiv \frac{565}{295} \\ &\equiv \frac{137}{81} \equiv \frac{137 + 214}{81} \equiv \frac{351}{81} \equiv \frac{13}{3} \equiv \frac{13 \times 71}{3 \times 71} \equiv \frac{923}{213} \equiv \frac{67}{-1} \\ &\equiv -67 \equiv 147 \pmod{214} \end{aligned}$$

所以原方程的 9 个解为

$$x \equiv 147, 361, 575, 789, 1003, 1217, 1431, 1645, 1859 \pmod{1926}$$

对于给定的一个同余方程,用何种方法求解简单方便? 若模 m 较小,则用公式法直接求简单. 若模 m 较大,则用数乘法、交换模法和分式法求解简捷,应视具体情况而定.

练习 3.4

1. 下列同余方程有无解? 有解时有几个解?

(1) $1998x \equiv 1999 \pmod{2000}$. (2) $111x \equiv 1110 \pmod{1011}$.

(3) $891x + 918 \equiv 0 \pmod{198}$. (4) $ax + 54 \equiv 0 \pmod{45}$.

2. b 取何值时, 方程 $14x \equiv b \pmod{114}$ 满足以下条件.

(1) 在 $0 \leq x < 114$ 中有多于一个的解? (2) 无解.

3. 利用 3.4 节提到的几种方法, 求解下列同余方程.

(1) $3x + 12 \equiv 0 \pmod{15}$. (2) $49x - 84 \equiv 0 \pmod{104}$.

(3) $5x \equiv 2 \pmod{7}$. (4) $71x \equiv 1997 \pmod{1999}$.

(5) $999x \equiv 909 \pmod{9999}$. (6) $2001x \equiv 2010 \pmod{2100}$.

4. 已知某一正整数的 99 次方除以 97 后得余数 7, 而该正整数的 100 次方除以 97 后得余数 79, 问该正整数除以 97 后得到的余数是多少?

3.5 一次同余方程组与孙子定理

定义 3.8 有多个同余方程构成的组合称为同余方程组. 称式(3.5.1)为一次同余方程组.

$$\begin{cases} a_1x + b_1 \equiv 0 \pmod{m_1} \\ a_2x + b_2 \equiv 0 \pmod{m_2} \\ \vdots \\ a_nx + b_n \equiv 0 \pmod{m_n} \end{cases} \quad (3.5.1)$$

其中, m_1, m_2, \dots, m_n 是正整数.

如果存在整数 x_0 , 使 $a_ix_0 + b_i \equiv 0 \pmod{m_i}, i=1, 2, \dots, n$, 则称 $x \equiv x_0 \pmod{m}$ 是方程(3.5.1)的一个解, 这里, $m = [m_1, m_2, \dots, m_n]$.

本节的目的就是讨论方程(3.5.1)的解的问题.

若方程(3.5.1)有解, 则方程(3.5.1)中每个同余方程有解; 反之, 若方程(3.5.1)中某个同余方程无解, 则方程(3.5.1)无解. 所以, 要研究方程(3.5.1)的解, 可转化为研究下列同余方程的解:

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \vdots \\ x \equiv c_n \pmod{m_n} \end{cases} \quad (3.5.2)$$

定理 3.13 若 m_1, m_2, \dots, m_n 是 n 个两两互素的正整数, 则方程(3.5.2)关于模 $m = m_1m_2 \cdots m_n$ 有唯一解.

$$x \equiv \frac{m}{m_1}x_1c_1 + \frac{m}{m_2}x_2c_2 + \cdots + \frac{m}{m_n}x_nc_n \pmod{m} \quad (3.5.3)$$

其中, x_i 是 $\frac{m}{m_i}x \equiv 1 \pmod{m_i}$ 的一个整数解 ($i=1, 2, \dots, n$).

证 存在性 由 m_1, m_2, \dots, m_n 两两互素知 $\left(\frac{m}{m_i}, m_i\right) = 1$, 则由定理 3.12 知, 同余方程

$$\frac{m}{m_i}x \equiv 1 \pmod{m_i} \quad (i=1, 2, \dots, n) \quad (3.5.4)$$

有唯一解, 设为 $x \equiv x_i \pmod{m_i}$, 即有 $\frac{m}{m_i}x_i \equiv 1 \pmod{m_i}$, 从而由 $m_i \mid \frac{m}{m_j} (i \neq j)$ 得

$$\frac{m}{m_1}x_1c_1 + \frac{m}{m_2}x_2c_2 + \cdots + \frac{m}{m_n}x_nc_n \equiv \frac{m}{m_i}x_ic_i \equiv 1 \cdot c_i \equiv c_i \pmod{m_i}$$

这说明

$$x \equiv \frac{m}{m_1} x_1 c_1 + \frac{m}{m_2} x_2 c_2 + \cdots + \frac{m}{m_n} x_n c_n \pmod{m}$$

是方程(3.5.2)的一个解.

唯一性 若 $x \equiv x_1 \pmod{m}$ 及 $x \equiv x_2 \pmod{m}$ 是方程(3.5.2)的两个解, 则有 $x_1 \equiv c_i \pmod{m_i}$ 及 $x_2 \equiv c_i \pmod{m_i}$, $i=1, 2, \dots, n$. 于是, $x_1 \equiv x_2 \pmod{m_i}$, 从而由 m_i ($i=1, 2, \dots, n$) 两两互素得 $x_1 \equiv x_2 \pmod{m_1 \cdots m_n}$, 亦即 $x_1 \equiv x_2 \pmod{m}$. 这说明 $x_1 \pmod{m}$ 与 $x_2 \pmod{m}$ 是方程(3.5.2)的同一个解, 所以, 方程(3.5.2)只有一个解.

定理 3.13 的存在性的证明过程具体给出了在 m_i 两两互素的情况下同余方程组(3.5.2)的解法: 首先分别求出每个方程

$$\frac{m}{m_i} x \equiv 1 \pmod{m_i} \quad (i=1, 2, \dots, n)$$

的一个整数解 x_i , 然后代入式(3.5.3)计算化简即得方程组(3.5.2)的解.

定理 3.13 其实就是著名的孙子剩余定理, 国际上一般称之为中国剩余定理 (Chinese remainder theorem, CTR 定理).

公元 5 世纪前后, 我国出现了一部著作《孙子兵法》, 书中提出了这样一个问题: “今有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何?” 该问题简称“物不知数”问题.

如设所要求的物数为 x , 则 x 就是下列同余方程组(3.5.5)的一个正整数解:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \quad (3.5.5)$$

对于“物不知数”问题的解法, 《孙子算经》中记述: “凡三三数之剩一, 置七十; 五五数之剩一, 置二十一; 七七数之剩一, 则置十五; 一百零六以上, 以一百零五减知即得.”

明朝程大位在 1593 年出的一部著作《算经统宗》中关于“物不知数”问题有一首解法歌诀: “三人同行七十稀, 五树梅花二十一支, 七子团圆整半月, 除百零五便得知.” 也就是说, 该问题的解答是 $x \equiv 70 \times 2 + 21 \times 3 + 15 \times 2 \equiv 233 \equiv 23 \pmod{105}$.

我国古代数学家杨辉 1275 年在他的著作《续古摘奇算法》中给出了若干类似的求物数的问题, 如: ① “二数余一, 五数余二, 七数余三, 九数余四, 问本数?” ② “十一数余三, 十二数余二, 十三数余一, 问本数?”

这类问题利用孙子定理很容易求解, 如要解问题②, 设该数为 x , 则得同余方程组为

$$\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 2 \pmod{12} \\ x \equiv 1 \pmod{13} \end{cases}$$

这里, $m_1=11, m_2=12, m_3=13, m=11 \times 12 \times 13=1716=1716$. 显然, m_1, m_2, m_3 两两互素. 分别解同余方程 $\frac{m}{m_i}x \equiv 1 \pmod{m_i}, i=1, 2, 3$, 即分别解 $156x \equiv 1 \pmod{11}, 143x \equiv 1 \pmod{12}$ 及 $132x \equiv 1 \pmod{13}$, 各得其整数解为 $x_1=6, x_2=-1$, 及 $x_3=7$. 于是, 由孙子定理得

$$x \equiv 156 \times 6 \times 3 + 143 \times (-1) \times 2 + 132 \times 7 \times 1 \equiv 3446 \equiv 14 \pmod{1716}$$

所以, 适合该问题的最小数是 14.

例 3.27 解同余方程组

$$\begin{cases} x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 5x \equiv 7 \pmod{9} \end{cases}$$

解 该方程组形同方程(3.5.1), 先化为方程(3.5.2)的形式, 即

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{9} \end{cases}$$

再利用孙子定理, 解形如方程(3.5.4)的三个方程: $63x \equiv 1 \pmod{5}, 45x \equiv 3 \pmod{7}$ 及 $35x \equiv 5 \pmod{9}$. 解得 $x_1=2, x_2=-2$ 及 $x_3=-1$ 分别是上述同余方程的一个整数解, 则由方程(3.5.3)得原同余方程组的唯一解为

$$x \equiv 63 \times 2 \times 1 + 45 \times (-2) \times 3 + 35 \times (-1) \times 5 \equiv -319 \equiv 311 \pmod{315}$$

例 3.28 解同余方程组

$$\begin{cases} 3x \equiv 11 \pmod{28} \\ 5x \equiv 17 \pmod{44} \end{cases}$$

解 分别解同余方程

$$3x \equiv 11 \pmod{28} \quad \text{及} \quad 5x \equiv 17 \pmod{44}$$

得

$$x \equiv 13 \pmod{28} \quad \text{及} \quad x \equiv 21 \pmod{44}$$

于是, 原同余方程组等价于

$$\begin{cases} x \equiv 13 \pmod{28} \\ x \equiv 21 \pmod{44} \end{cases} \quad (3.5.6)$$

由于 $(28, 44)=4 \neq 1$, 所以, 不能直接利用孙子定理来求解.

因 $x \equiv 13 \pmod{28}$ 等价于方程组

$$\begin{cases} x \equiv 13 \pmod{4} \\ x \equiv 13 \pmod{7} \end{cases}$$

而 $x \equiv 21 \pmod{44}$ 等价于方程组

$$\begin{cases} x \equiv 21 \pmod{4} \\ x \equiv 21 \pmod{11} \end{cases}$$

所以,原方程组等价于

$$\begin{cases} x \equiv 13 \pmod{4} \\ x \equiv 13 \pmod{7} \\ x \equiv 21 \pmod{4} \\ x \equiv 21 \pmod{11} \end{cases}$$

亦即等价于

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 6 \pmod{7} \\ x \equiv 10 \pmod{11} \end{cases} \quad (3.5.7)$$

最后利用孙子定理,解同余方程组(3.5.7)得 $x \equiv 153 \pmod{308}$,即原方程组的解为 $x \equiv 153 \pmod{308}$.

此题也可以这样来解.

因 $3x \equiv 11 \pmod{28}$ 及 $5x \equiv 17 \pmod{28}$ 分别等价于

$$\begin{cases} 3x \equiv 11 \pmod{4} \\ 3x \equiv 11 \pmod{7} \end{cases} \quad \text{及} \quad \begin{cases} 5x \equiv 17 \pmod{4} \\ 5x \equiv 17 \pmod{11} \end{cases}$$

从而原方程等价于

$$\begin{cases} 3x \equiv -1 \pmod{4} \\ 3x \equiv 4 \pmod{7} \\ 5x \equiv 1 \pmod{4} \\ 5x \equiv 6 \pmod{11} \end{cases}$$

亦即

$$\begin{cases} x \equiv 1 \pmod{4} \\ 3x \equiv 4 \pmod{7} \\ 5x \equiv 6 \pmod{11} \end{cases}$$

然后,如例 3.27 那样解最后这个方程组即可.

例 3.29 解同余方程组

$$\begin{cases} 2x \equiv 4 \pmod{8} \\ 15x \equiv 18 \pmod{33} \end{cases}$$

解 因方程 $2x \equiv 4 \pmod{8}$ 有两个解 $x \equiv 2, 6 \pmod{8}$, 方程 $15x \equiv 18 \pmod{33}$ 有三个解 $x \equiv -1, 10, 21 \pmod{33}$. 于是,原同余方程组的解为下列 6 个同余方程组

的全部解:

$$\begin{cases} x \equiv 2 \pmod{8} \\ x \equiv -1 \pmod{33} \end{cases}, \quad \begin{cases} x \equiv 2 \pmod{8} \\ x \equiv 10 \pmod{33} \end{cases}, \quad \begin{cases} x \equiv 2 \pmod{8} \\ x \equiv 10 \pmod{33} \end{cases}$$

$$\begin{cases} x \equiv 6 \pmod{8} \\ x \equiv -1 \pmod{33} \end{cases}, \quad \begin{cases} x \equiv 6 \pmod{8} \\ x \equiv 10 \pmod{33} \end{cases}, \quad \begin{cases} x \equiv 6 \pmod{8} \\ x \equiv 21 \pmod{33} \end{cases}$$

分别利用孙子定理解之使得原同余方程组的 6 个解.

$$x = 98, 10, 186, 230, 142, 54 \pmod{264}$$

例 3.30 解下列三元一次同余方程组:

$$\begin{cases} x - 2y + 3z \equiv 4 \pmod{19} & (3.5.8) \\ 3x + 4y - 5z \equiv 6 \pmod{19} & (3.5.9) \\ 5x - 6y + 7z \equiv 8 \pmod{19} & (3.5.10) \end{cases}$$

解 由式(3.5.9) - 3 × 式(3.5.8) 及式(3.5.10) - 5 × 式(3.5.8) 得

$$5y - 7z \equiv -3 \pmod{19} \quad (3.5.11)$$

$$y - 2z \equiv -3 \pmod{19} \quad (3.5.12)$$

再由式(3.5.11) - 5 × 式(3.5.12) 得 $3z \equiv 12 \pmod{19}$, 即 $z \equiv 4 \pmod{19}$. 将之代入式(3.5.12) 便得 $y \equiv 5 \pmod{19}$, 将 $y \equiv 5 \pmod{19}$ 及 $z \equiv 4 \pmod{19}$ 代入式(3.5.8) 得 $x \equiv 2 \pmod{19}$. 所以, 原方程组的解为

$$\begin{cases} x \equiv 2 \pmod{19} \\ y \equiv 5 \pmod{19} \\ z \equiv 4 \pmod{19} \end{cases}$$

例 3.30 的解法类似于普通三元一次方程组的解法, 即消元法. 这里, 关键是要注意一个同余方程的模是否相同: 在消元过程中, 乘或除以的每个因子是否与模互素.

最后, 应该注意到, 只有当同除方程组(3.5.2) 的 n 个模两两互素时, 才可运用孙子定理, 而对于较一般的情况, 则有下面的结论.

定理 3.14 同余方程组(3.5.2) 有解的充分必要条件是对任何 $i, j: 1 \leq i < j \leq k$, 有

$$c_i \equiv c_j \pmod{(m_i, m_j)}$$

若方程组(3.5.2) 有解, 则对模 $[m_1, \dots, m_n]$ 有唯一解.

证 证 $n=2$ 的情形.

必要性 若 $x=c$ 满足方程组(3.5.2), 则有

$$\begin{cases} c \equiv c_1 \pmod{m_1} \\ c \equiv c_2 \pmod{m_2} \end{cases}$$

从而有 $(m_1, m_2) \mid c - c_1$ 及 $(m_1, m_2) \mid c - c_2$, 于是, $(m_1, m_2) \mid c_1 - c_2$, 即有 $c_1 \equiv c_2 \pmod{(m_1, m_2)}$. 必要性成立.

充分性 如 $c_1 \equiv c_2 \pmod{(m_1, m_2)}$, 即 $(m_1, m_2) \mid c_1 - c_2$, 则由定理 3.12 知同余方程 $m_1 y \equiv c_2 - c_1 \pmod{m_2}$ 有解, 设为 $y = y_0 \pmod{m_2}$, 因此有

$$\begin{cases} c_1 + m_1 y_0 \equiv c_1 \pmod{m_1} \\ c_1 + m_1 y_0 \equiv c_2 \pmod{m_2} \end{cases}$$

这说明 $x = c_1 + m_1 y_0$ 是方程 (3.5.2) 的一个整数解. 充分性成立.

唯一性 设 x_1, x_2 均是方程 (3.5.2) 的解, 则有

$$\begin{cases} x_1 \equiv c_1 \pmod{m_1} \\ x_1 \equiv c_2 \pmod{m_2} \end{cases} \quad \text{及} \quad \begin{cases} x_2 \equiv c_1 \pmod{m_1} \\ x_2 \equiv c_2 \pmod{m_2} \end{cases}$$

由此可得

$$\begin{cases} x_1 \equiv x_2 \pmod{m_1} \\ x_1 \equiv x_2 \pmod{m_2} \end{cases}$$

即

$$\begin{cases} m_1 \mid x_1 - x_2 \\ m_2 \mid x_1 - x_2 \end{cases}$$

则 $x_1 - x_2$ 是 m_1 与 m_2 的公倍数, 从而 $x_1 - x_2$ 是 $[m_1, m_2]$ 的倍数. 于是, 有

$$x_1 - x_2 \equiv 0 \pmod{[m_1, m_2]} \quad \text{或} \quad x_1 \equiv x_2 \pmod{[m_1, m_2]}$$

所以, 方程 (3.5.2) 有解时, 关于模 $[m_1, m_2]$ 只有唯一解.

练习 3.5

1. 解下列同余方程组.

$$(1) \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 2 \pmod{8} \\ x \equiv 3 \pmod{9} \end{cases}$$

$$(2) \begin{cases} 11x \equiv 7 \pmod{10} \\ 3x + 10 \equiv 0 \pmod{11} \\ 5x - 3 \equiv 0 \pmod{13} \end{cases}$$

$$(3) \begin{cases} 8x \equiv 6 \pmod{12} \\ 3x \equiv 6 \pmod{15} \end{cases}$$

$$(4) \begin{cases} x - 6 \equiv 0 \pmod{35} \\ 3x - 11 \equiv 0 \pmod{55} \\ 5x - 2 \equiv 0 \pmod{33} \end{cases}$$

2. 解答下列各题.

(1) 有物不知其数. 三数余一, 五数余二, 七数余三, 十一数余四, 问该物数.

(2) 今有数不知总数. 以五累减之无剩, 以七百十五累减之剩十, 以二百四十七累减之剩一百四十, 以三百九十一累减之剩二百四十五, 以一百八十七累减之剩一百零九, 问总数若干?

3. 有一计算机病毒每隔十三天连续发作两天, 有一次该病毒刚好在星期六、星期日发作, 问该病毒至少要几星期后又在星期六发作?

4. 解下列多元一次同余方程组.

$$(1) \begin{cases} 3x+4y \equiv 5 \pmod{11} \\ 5x+7y \equiv 2 \pmod{11} \end{cases} \quad (2) \begin{cases} x-2y \equiv 3 \pmod{7} \\ 3x+y \equiv 4 \pmod{7} \end{cases}$$

$$(3) \begin{cases} x-5y+3z \equiv 8 \pmod{29} \\ 7x+y+4z \equiv 3 \pmod{29} \\ -3x-4y+z \equiv -1 \pmod{29} \end{cases}$$

5. 求既能被 7 除余 3, 又能被 11 除余 4 的所有三位自然数之和.

6. 试求一个满足下列条件的最大的负整数, 该负整数用 15 除余 8, 用 10 除余 3, 用 8 除余 1.

7. 设 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 是 m 的标准素因数分解, 则同余方程

$$ax + b \equiv 0 \pmod{m}$$

与同余方程组

$$\begin{cases} ax + b \equiv 0 \pmod{p_1^{\alpha_1}} \\ \vdots \\ ax + b \equiv 0 \pmod{p_k^{\alpha_k}} \end{cases}$$

同解.

3.6 素数模的高次同余方程

设 $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$, $a_0 \not\equiv 0 \pmod{m}$ 是一个次数 $n \geq 1$ 的整系数多项式, 若 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 是 m 的素因数分解, 则容易证明下面的定理 3.15.

定理 3.15 同余方程

$$f(x) \equiv 0 \pmod{m} \quad (3.6.1)$$

与同余方程组

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ \vdots \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}} \end{cases} \quad (3.6.2)$$

同解.

因此, 要解同余方程 (3.6.1), 需先解每个同余方程

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}}, \quad i = 1, 2, \cdots, k \quad (3.6.3)$$

根据潘承洞、潘承彪著的《简明数论》中 § 26 的定理 1 及推论 2, 可以由同余方程 $f(x) \equiv 0 \pmod{p_i}$ 的解来求得式 (3.6.3) 的解, 所以, 本节着重讨论素数模的同余方程 (3.6.4) 的解的问题.

$$f(x) \equiv 0 \pmod{p} \quad (3.6.4)$$

其中, p 为素数, $p \nmid a_0$ (a_0 为 $f(x)$ 的首项系数). 此时, 若 $\partial(f(x)) = n$ (即 $f(x)$ 的次

数为 n), 则称式(3.6.4)是一个 n 次同余方程.

当 p 及 $f(x)$ 的次数均较小时, 只要将 p 的完全剩余系中的数代入式(3.6.4)就可求得它的全部解. 但当 p 及 $f(x)$ 的次数只要有一个较大时, 这种验证式的求解方法则不实际, 需另寻其他途径.

设 $\partial(f(x))=n$, 若 $n \geq p$, 则由带余除法, 存在 $q(x)$ 与 $r(x)$ 使

$$f(x) = (x^p - x)q(x) + r(x)$$

其中, $r(x) = 0$ 或 $\partial(r(x)) < p$.

由 Fermat 定理知 $x^p - x \equiv 0 \pmod{p}$, 从而有 $f(x) \equiv r(x) \pmod{p}$. 于是, $f(x) \equiv 0 \pmod{p}$ 与 $r(x) \equiv 0 \pmod{p}$ 同解, 因此, 只须解一个次数不大于模数的同余方程即可.

例 3.31 解同余方程

$$x^8 - 2x^7 + x^6 - 7x^5 + 6x - 7 \equiv 0 \pmod{5}$$

解 显然, 原同余方程与下列同余方程同解:

$$x^8 - 2x^7 + x^6 - 2x^5 + x - 2 \equiv 0 \pmod{5} \quad (3.6.5)$$

用 $x^5 - x$ 除 $x^8 - 2x^7 + x^6 - 2x^5 + x - 2 \equiv 0 \pmod{5}$ 可得与方程(3.6.5)同解的同余方程

$$x^4 - 2x^3 + x^2 - x - 2 \equiv 0 \pmod{5} \quad (3.6.6)$$

将 5 的完全剩余系 $\pm 2, \pm 1, 0$ 代入验算即知, $x \equiv 2 \pmod{5}$ 是同余方程(3.6.6)的解, 即 $x \equiv 2 \pmod{5}$ 是原同余方程的唯一解.

例 3.32 利用 Fermat 定理化简如下同余方程:

$$\begin{aligned} &9x^{26} - 5x^{24} + 25x^{18} - 11x^{16} + 3x^{13} - 6x^{10} + 4x^8 + 15x^6 \\ &- 4x^5 + 5x^3 + 8x - 66^6 \equiv 0 \pmod{7} \end{aligned}$$

解 首先将左边每项系数的绝对值化为比 7 小的数. 因 $(66, 7) = 1$, 由 Fermat 定理可得 $66^6 \equiv 1 \pmod{7}$. 又 $9 \equiv 2, -5 \equiv 2, 25 \equiv -3, -11 \equiv 3, -6 \equiv 1, 15 \equiv 1 \pmod{7}$, 所以, 原同余方程化简为

$$\begin{aligned} &2x^{26} + 2x^{24} - 3x^{18} + 3x^{16} + 3x^{13} + x^{10} + 4x^8 + x^6 \\ &- 4x^5 - 2x^3 + x - 1 \equiv 0 \pmod{7} \end{aligned} \quad (3.6.7)$$

再将同余方程(3.6.7)左边的多项式除以 $x^7 - x$ 得余式

$$-4x^5 + 4x^4 - 2x^3 - x^2 + 4x - 1$$

从而原方程化简成下列同余方程:

$$3x^5 + 4x^4 - 2x^3 - x^2 + 4x - 1 \equiv 0 \pmod{7} \quad (3.6.8)$$

本题也可以这样来化简同余方程: 由 $x^7 \equiv x \pmod{7}$ 可得

$$x^{26} \equiv x^2, x^{24} \equiv x^6, x^{18} \equiv x^6, x^{16} \equiv x^4, x^{13} \equiv x, x^{10} \equiv x^4, x^8 \equiv x^2$$

从而式(3.6.7)化简成

$$2x^2 + 2x^6 - 3x^6 + 3x^4 + 3x + x^4 + 4x^2 + x^6 - 4x^5 - 2x^3 + x - 1 \equiv 0 \pmod{7}$$

即 $3x^5 + 4x^4 - 2x^3 - x^2 + 4x - 1 \equiv 0 \pmod{7}$, 亦即式(3.6.8).

若要求本题同余方程的解, 则只需将模 7 的完全剩余系 $\pm 3, \pm 2, \pm 1$ 及 0 代入式(3.6.8)中验算即可求得其解.

定理 3.16 设 n 次同余方程(3.6.4)有 k 个不同解 $x \equiv \alpha_i \pmod{p}, i=1, 2, \dots, k$, 且 $k \leq n$, 则存在 $(n-k)$ 次多项式 $g(x)$ 使

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)g(x) \pmod{p}$$

证 用 $x - \alpha_1$ 除 $f(x)$, 由带余除法, 存在 $q_1(x)$ 及 r_1 使

$$f(x) = (x - \alpha_1)q_1(x) + r_1 \quad (r_1 \text{ 为常数}, q_1(x) \text{ 的首项系数为 } a_0)$$

因 $f(\alpha_1) \equiv 0 \pmod{p}$, 故有 $r_1 \equiv 0 \pmod{p}$, 从而

$$f(x) \equiv (x - \alpha_1)q_1(x) \pmod{p} \quad (3.6.9)$$

其中, $q_1(x)$ 是 $n-1$ 次多项式.

$x \equiv \alpha_i \pmod{p} (i=2, \dots, k)$ 是 $f(x) \equiv 0 \pmod{p}$ 的 $k-1$ 个不同的解. 由式(3.6.9)得

$$(\alpha_i - \alpha_1)q_1(\alpha_i) \equiv 0 \pmod{p}$$

于是, 由 $\alpha_i \not\equiv \alpha_1 \pmod{p}$ 得 $q_1(\alpha_i) \equiv 0 \pmod{p}$. 这说明 $x \equiv \alpha_i \pmod{p} (i=2, \dots, k)$ 是 $q_1(x) \equiv 0 \pmod{p}$ 的 $k-1$ 个不同的解, 利用归纳可知, 存在 $(n-1) - (k-1) = n-k$ 次且首项系数为 a_0 的多项式 $g(x)$, 使

$$q_1(x) \equiv (x - \alpha_2) \cdots (x - \alpha_k)g(x) \pmod{p}$$

则

$$f(x) \equiv (x - \alpha_1)q_1(x) \equiv (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)g(x) \pmod{p}$$

即

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)g(x) \pmod{p}$$

定理 3.17 (Lagrange 定理) 同余方程(3.6.4)的不同解的个数不大于其次数.

证 对 $f(x)$ 的次数用数学归纳法. 当 $\partial(f(x))=1$ 时, 定理显然成立.

假设 $\partial(f(x))=n-1$ 时定理成立, 则 $\partial(f(x))=n$ 时, $f(x) \equiv 0 \pmod{p}$ 或者无解(结论成立), 或者至少有一个解, 设为 $x \equiv a \pmod{p}$. 由定理 3.16, 设 $f(x) \equiv (x-a)g(x) \pmod{p}$, 其中, $g(x)$ 是 $n-1$ 次多项式, 首项系数是 a_0 . 由归纳假设, $g(x) \equiv 0 \pmod{p}$ 的不同余解的个数不大于 $n-1$.

若 $x \equiv b \pmod{p}$ 是式(3.6.4)的任一解, 则有 $0 \equiv f(b) \equiv (b-a)g(b) \pmod{p}$. 因此, 有 $(b-a) \equiv 0 \pmod{p}$, 或 $g(b) \equiv 0 \pmod{p}$, 即式(3.6.4)的任一解, 或者是 $x \equiv a \pmod{p}$ 的解, 或者是 $g(x) \equiv 0 \pmod{p}$ 的解. 从而由假设知式(3.6.4)的不同解的个数不大于 $1+(n-1)$, 即不大于 n .

推论 3.2 设 p 是素数, 且 $d|(p-1)$, 那么同余式

$$x^d - 1 \equiv 0 \pmod{p}$$

恰有 d 个解.

证 由于 $d|(p-1)$, 则存在整数 k 使得 $p-1=dk$, 因此

$$x^{p-1} - 1 = (x^d - 1)f(x)$$

其中, $f(x) = x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1$ 是一个次数为 $d(k-1) = p-1-d$ 的整系数多项式. 由定理 3.17 可得同余式 $f(x) \equiv 0 \pmod{p}$ 至多有 $p-1-d$ 个解.

由 Fermat 定理知, $x^{p-1} - 1 \equiv 0 \pmod{p}$ 恰有 $p-1$ 个不同余的解, 也就是 $1, 2, \cdots, p-1$. 由于 $x^{p-1} - 1 \equiv 0 \pmod{p}$ 的任意一个解 $x=a$, 若不是同余式 $f(x) \equiv 0 \pmod{p}$ 的解, 则一定是同余式 $x^d - 1 \equiv 0 \pmod{p}$ 的解. 这是因为由 $0 \equiv a^{p-1} - 1 \equiv (a^d - 1)f(a) \pmod{p}$ 及 $p \nmid f(a)$ 可得 $p|a^d - 1$. 因此, $x^d - 1 \equiv 0 \pmod{p}$ 至少有 $p-1 - (p-1-d) = d$ 个解. 另外, 由定理 3.17 可知 $x^d - 1 \equiv 0 \pmod{p}$ 至多有 d 个解, 因此, $x^d - 1 \equiv 0 \pmod{p}$ 恰有 d 个解.

定理 3.18 若 $n \leq p, a_0 = 1$, 同余方程 (3.6.4) 有 n 个不同余解的充分必要条件是存在 $p-n$ 次整系数多项式 $g(x)$ 使得

$$x^p - x \equiv f(x)g(x) \pmod{p}$$

证 必要性 设同余方程 (3.6.4) 有 n 个不同余的解, 则由带余除法可得

$$x^p - x \equiv f(x)g(x) + r(x)$$

其中, $g(x), r(x)$ 为整系数多项式, 并且 $\partial(g(x)) = p-n$ 及 $\partial(r(x)) < n$.

由 Fermat 定理知, 同余方程 (3.6.4) 的 n 个解都是 $x^p - x \equiv 0 \pmod{p}$ 的解, 从而也是 $r(x) \equiv 0 \pmod{p}$ 的解. 但由定理 3.17 得, $r(x) \equiv 0 \pmod{p}$ 的解不超过 $n-1$ 个, 因此, $r(x)$ 的系数只能是 p 的倍数, 即, $r(x) \equiv 0 \pmod{p}$. 因此, $x^p - x \equiv f(x) \times g(x) \pmod{p}$.

充分性 由已知, 可设存在 $p-n$ 次整系数多项式 $g(x)$ 使

$$x^p - x \equiv f(x)g(x) \pmod{p}$$

则由 Fermat 定理得知, $f(x)g(x) \equiv 0 \pmod{p}$ 有 p 个解.

设 $f(x) \equiv 0 \pmod{p}$ 与 $g(x) \equiv 0 \pmod{p}$ 的解数分别为 k 与 h , 则有 $p \leq k+h$. 另外, 由定理 3.17 知, $k \leq n$ 且 $h \leq p-n$, 则 $k+h \leq p$, 从而 $p = k+h$, 即 $k=n$.

练习 3.6

1. 化简下列同余式.

$$(1) 2x^{18} + 5x^{16} - 20x^{13} - 3x^{11} + 25x^{10} + 4x^8 + 16x^6 - x^3 + 5x + 8 \equiv 0 \pmod{7}.$$

$$(2) 25x^{25} + 20x^{23} - 3x^{15} - 30x^{12} + 6x^{11} + 15x^7 + 3x^5 + 16x^3 - 7x \equiv 0 \pmod{11}.$$

$$(3) 3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 \pmod{5}.$$

$$(4) 2x^{17} + 6x^{16} + x^{14} + 5x^{12} + 3x^{11} + 2x^{10} + x^9 + 5x^8 + 2x^7 + 3x^5 + 4x^4 + 6x^3 + 4x^2 + x + 4 \equiv 0 \pmod{7}.$$

2. 将下列同余方程化简成首项系数为 1 的等价同余方程.

(1) $49x^5 + 25x^3 - 6x^2 + 3x - 10 \equiv 0 \pmod{23}$.

(2) $3x^{11} + 3x^8 + 5 \equiv 0 \pmod{7}$.

(3) $4x^{20} + 3x^{13} + 2x^7 + 3x - 2 \equiv 0 \pmod{5}$.

(4) $2x^{15} - 3x^{10} + 8x^6 + 7x^5 + 6x^3 + 2x - 8 \equiv 0 \pmod{7}$.

3. 把下列同余方程化成与它等价的同式连乘积, 并求它们的解.

(1) $14x^5 - 6x^4 + 8x^3 + 6x^2 - 13x + 5 \equiv 0 \pmod{7}$.

(2) $8x^4 + 3x^3 + x + 9 \equiv 0 \pmod{7}$.

(3) $x^7 + 10x^6 + x^5 + 20x^4 + 8x^3 - 18x^2 + 3x + 1 \equiv 0 \pmod{13}$.

(4) $x^4 + x + 4 \equiv 0 \pmod{11}$.

4. 利用定理 3.18 证明下列结论.

(1) $x^6 \equiv 1 \pmod{19}$ 的解数为 6.

(2) 方程 $x^6 - 4x^5 + 6x^4 + 6x^3 + 3x^2 - 2x + 3 \equiv 0 \pmod{13}$ 解的个数为 6.

5. 求下列同余方程的解.

(1) $x^7 - 2x^6 - 7x^5 + x + 2 \equiv 0 \pmod{5}$.

(2) $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod{5}$.

6. 设 $n|p-1, n>1, (a, p)=1$. 证明同余式

$$x^n \equiv a \pmod{p}$$

有解的充分必要条件是 $a^{\frac{p-1}{n}} \equiv 1 \pmod{p}$. 并且在有解的情况下就有 n 个解.

7. 设 n 是正整数, $(n, p-1)=k$, 证明 $x^n \equiv 1 \pmod{p}$ 有 k 个解.

3.7 利用 Maple 计算同余式与求解同余方程

在 Maple 中, 求某表达式 e 关于某正整数 m 的同余值有 3 个 Maple 函数: $e \bmod m$, $\text{modp}(e, m)$ 及 $\text{mods}(e, m)$. 其中, $\text{modp}(e, m)$ 与 $\text{mods}(e, m)$ 分别表示关于模 m 对表达式 e 的系数取非负的余数与绝对值最小的余数, 而 $e \bmod m$ 可表示为 $\text{modp}(e, m)$ 或 $\text{mods}(e, m)$, 它通过定义 $'\text{mod}': = \text{modp}$ 或 $'\text{mod}': = \text{mods}$ 来实现. 如下所示:

```
>modp(9 * x^3 + 15 * x^2 + 4 * x - 3, 11);
          9x^3 + 4x^2 + 4x + 8
```

```
>mods(9 * x^3 + 15 * x^2 + 4 * x - 3, 11);
          - 2x^3 + 4x^2 + 4x - 3
```

本章例 3.1 的计算如利用 modp 函数来计算则非常快.

```
>modp(2008^(365), 10);
```

例 3.3 的计算用 Maple 编程来计算很方便.

```
> modp(sum(i^5, i = 1..100), 8);
4
```

对于练习 3.3 第 7 题第(1)小题, 可用 Maple 程序验证如下:

```
> with(numtheory):
F: = proc(p)
if isprime(p) = true and mods((p-1)! + 2, p) - 1 = 0 then print(true) else print
(false)
end if:
end:
```

例如

```
> F(1000), F(7919);
false
true
```

这里, 7919 是第 1000 个素数.

对于练习 3.3 第 10 题, 则可用 Maple 程序验证.

```
> with(numtheory):
V: = proc(p)
local re, le;
re: = mods(mul((2 * k - 1)^2, k = 1..(p-1)/2), p);
le: = (-1)^((p+1)/2);
if isprime(p) = true and re = le then print(true) else print(false) end if:
end:
> V(10000), V(104729);
false, true
```

这里, 104729 是第 1000 个素数.

关于同余方程的求解, Maple 中有其相应的函数 `msolve()`, 如下所示:

```
> msolve(5 * x^3 - 25 * x^2 + 7 * x + 1, 12)
{x = 1}, {x = 5}, {x = 7}, {x = 11}
```

即同余方程 $5x^3 - 25x^2 + 7x + 1 \equiv 0 \pmod{12}$ 有 4 个解: 1, 5, 7, 11.

相应于中国剩余定理的求解, 同余方程组 (3.5.2) 的 Maple 函数是 `chrem()`. 如方程组 (3.5.5) 的求解.

```
> chrem([2, 3, 2], [3, 5, 7]);
23
```

但是, 对于方程组 (3.5.1), 则用 `chrem()`, 一般不能直接给出该方程组的解, 它给出的只是 x 的一个线性函数, 它取各模后分别等于该模所对应的方程的右端. 具体地说, 给定方程组

$$\begin{cases} f_1 \equiv 0 \pmod{m_1} \\ f_2 \equiv 0 \pmod{m_2} \\ \vdots \\ f_n \equiv 0 \pmod{m_n} \end{cases}$$

其中, m_1, m_2, \dots, m_n 两两互素, 每个 f_k 是多项式, 则 $\text{chrem}([f_1, f_2, \dots, f_n], [m_1, m_2, \dots, m_n])$ 给出的解 f 是一个满足 $f \equiv f_k \pmod{m_k}$ 的多项式. 要求同余方程组 (3.5.1) 的解, 则需要先求出每个方程的解, 然后再利用 $\text{chrem}()$ 进行求解. 可编程如下:

```
>chrem_new := proc(L::list, m::list)
  local i, s, x, u;
  s := nops(L);
  for i from 1 to s do
    x[i] := RootOf(L[i]) mod m[i];
  end do;
  u := [seq(x[i], i = 1..s)];
  chrem(u, M);
end;
```

用得到的新 Maple 函数 chrem_new , 可对例 3.27 求解.

```
>chrem_new([x-1, 3*x-2, 5*x-7], [5, 7, 9]);
```

311

对于模数 m_1, m_2, \dots, m_n 非两两互素的情况, 则不能用 chrem_new 对同余方程组 (3.5.1) 求解, 但可以利用 Maple 中函数 $\text{msolve}()$ 来得到一个求解同余方程组 (3.5.1) 解的新 Maple 函数 $\text{chrem_Ext}()$.

```
>chrem_Ext := proc(L::list, m::list)
  local s, M, A, i;
  s := nops(L);
  M := ilcm(op(m));
  for i from 1 to s do
    A[i] := (M/m[i]) * L[i]
  od;
  msolve({seq(A[i] = 0, i = 1..s)}, M);
end;
```

如解例 3.28 的同余方程组.

```
>chrem_Ext([3*x-11, 5*x-17], [28, 44]);
```

{x = 153}

解例 3.29 得其解为

```
>chrem_Ext([2 * x - 4, 15 * x - 18], [8, 33]);
{x = 88_Z4 + 44_Z5~ + 10}
```

这里, $_Z4\sim$ 与 $_Z5\sim$ 分别表示两个取整数的变量. 即对 $_Z4\sim$ 与 $_Z5\sim$ 取任意整数时 $x=88_Z4+44_Z5\sim+10$ 都是该方程的解. 但关于模 264 不同的解只有 6 个, 即 $(_Z4\sim, _Z5\sim)$ 分别等于 $(0, 0), (0, 1), (1, 0), (1, 1), (1, 2), (1, 3)$ 时对应的 6 个解: 10, 54, 98, 142, 186, 230.

因同余方程组

$$\begin{cases} x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{6} \\ 5x \equiv 7 \pmod{9} \end{cases}$$

中的第二个方程无解, 故该方程组无解, 所以, 当用 `chrem_Ext()` 解此方程组时, 没有结果输出.

```
>chrem_Ext([1 * x - 1, 3 * x - 2, 5 * x - 7], [5, 6, 9]);
```

对于如例 3.30 所表示的线性同余方程组的求解, 或更一般的形如同余矩阵方程

$$\mathbf{AX} = \mathbf{b} \pmod{m} \quad (\mathbf{A}, \mathbf{b} \text{ 及 } \mathbf{X} \text{ 分别表示矩阵、常向量及未知向量})$$

的求解, 可用 Maple 中的函数 `Linsolve(A, b) mod m`. 例 3.30 可求解如下:

```
>A := matrix([[1, -2, 3], [3, 4, -5], [5, -6, 7]]);
b := vector([4, 6, 8]);
Linsolve(A, b) mod 19;
[2, 5, 4]
```

第3章综合例题

例 1 设 α 是一个正整数, 若存在 $a > 1$ 及 $n > 1$, 使 $\alpha = a^n$, 则称 α 是一个完全方幂.

(1) $504 \mid n^9 - n^3$.

(2) 证明当 p 为素数时, $2^p + 3^p$ 不是完全方幂.

证 (1) 因为 $504 = 7 \times 8 \times 9$, 且 7, 8, 9 两两互质, 故只需证 7, 8, 9 分别整除 $n^9 - n^3$ 即可. 事实上, 由 $n^7 \equiv n \pmod{7}$ 可知 $n^9 \equiv n^3 \pmod{7}$. 当 $(n, 8) \neq 1$ 时, 显然有 $n^9 \equiv n^3 \equiv 0 \pmod{8}$. 当 $(n, 8) = 1$ 时, 有 $n^2 \equiv 1 \pmod{8}$, 则 $(n^2)^3 \equiv 1^3 \pmod{8}$, 即 $n^6 \equiv 1 \pmod{8}$, 从而有 $n^9 \equiv n^3 \pmod{8}$. 当 $(n, 9) \neq 1$ 时, 显然有 $n^9 \equiv n^3 \equiv 0 \pmod{9}$. 当 $(n, 9) = 1$ 时, 由 Euler 定理有 $n^6 \equiv 1 \pmod{9}$, 有 $n^9 \equiv n^3 \pmod{9}$. 综上便得 $n^9 \equiv n^3 \pmod{7 \times 8 \times 9}$, 即 $n^9 \equiv n^3 \pmod{504}$ 或 $504 \mid n^9 - n^3$.

(2) 当 $p=2, 5$ 时, 可验证命题成立. 现设素数 $p=2k+1 \neq 5$ (k 为某些自然

数), 因为

$$2^p + 3^p = (2+3)(2^{2k} - 2^{2k-1} \times 3 + 2^{2k-2} \times 3^2 - \cdots + 3^{2k})$$

所以, $2^p + 3^p$ 含有因数 5, 而若 $2^p + 3^p$ 是完全方幂, 则至少还有一个因数 5.

设 $M = 2^{2k} - 2^{2k-1} \times 3 + 2^{2k-2} \times 3^2 - \cdots + 3^{2k}$, 则

$$\begin{aligned} M &\equiv 2^{2k} - 2^{2k-1} \times (-2) + 2^{2k-2} \times (-2)^2 - \cdots + (-2)^{2k} \\ &\equiv 2^{2k} + 2^{2k} + 2^{2k} + \cdots + 2^{2k} = (2k+1)2^{2k} \equiv p \cdot 2^{p-1} \pmod{5} \end{aligned}$$

又 $p \not\equiv 0 \pmod{5}$, $2^{p-1} \not\equiv 0 \pmod{5}$, 则 M 不含因数 5, 因而 $2^p + 3^p$ 不是完全方幂.

例 2 此例介绍一种利用同余式检验整数四则运算(包括乘方)的计算结果是否正确的快速方法.

假设要检验 n 个整数 a_1, \cdots, a_n 的和 $\sum_{i=1}^n a_i$ 或乘积 $\prod_{i=1}^n a_i$ 的计算是否正确. 记 a_i 的各位数字之和为 r_i , 和 $\sum_{i=1}^n a_i = S$ 与积 $\prod_{i=1}^n a_i = T$ 的各位数字之和分别为 s 与 t , 则由 $10^k \equiv 1 \pmod{9}$ 对任何正整数成立可得 $a_i \equiv r_i \pmod{9}$, $S \equiv s \pmod{9}$, $T \equiv t \pmod{9}$, 于是有 $\sum_{i=1}^n r_i \equiv s \pmod{9}$ 及 $\prod_{i=1}^n r_i \equiv t \pmod{9}$. 这就是说, 如果和 $\sum_{i=1}^n a_i$ (或乘积 $\prod_{i=1}^n a_i$) 的计算结果正确, 那么, a_1, \cdots, a_n 的各位数字之和的和(或各位数字之和的积)关于模 9 同余于和 $\sum_{i=1}^n a_i$ 的各位数字之和(或同余于乘积 $\prod_{i=1}^n a_i$ 的各位数字之和).

例 3 检验下面运算结果是否有错.

$$(1) 7964 + 2359 = 10223. \quad (2) 3748 \times 6236 = 23372528.$$

$$(3) 3718 \times 62336 \times 527564 = 122271001205872.$$

解 (1) 由于 $7964 \equiv 7+9+6+4 \equiv 8 \pmod{9}$, $2359 \equiv 2+3+5+9 \equiv 1 \pmod{9}$, $10223 \equiv 1+0+2+2+3 \equiv 8 \pmod{9}$. 由于 $8+1 \not\equiv 8 \pmod{9}$, 所以上述加法运算结果是不正确的.

(2) $3748 \equiv 4 \pmod{9}$, $6236 \equiv 8 \pmod{9}$, $23372528 \equiv 5 \pmod{9}$. 因为 $4 \times 8 \equiv 32 \equiv 5 \pmod{9}$, 所以, 上述乘法式子有可能是正确的, 实际上它是正确的.

(3) $3718 \equiv 1 \pmod{9}$, $62336 \equiv 2 \pmod{9}$, $527564 \equiv 2 \pmod{9}$, $122271001205872 \equiv 4 \pmod{9}$. 因为 $1 \times 2 \times 2 \equiv 4 \pmod{9}$, 所以, 该乘积的计算结果可能正确, 但实际上经检验该计算结果不正确(左边的计算结果为 122271001295872).

注 ① 由于验算中只会涉及求整数的各位数字关于模 9 的求和, 所以, 这时如果整数中出现有数字 9, 或者有几个数字之和等于 9, 那么, 可将是 9 的数字以及和为 9 的那几个数直接去掉, 从而把这种验算的方法叫弃九法; ② 弃九法只是一

个判别整数四则运算结果成立与否的必要条件,而非充分条件.

例 4 若 2 月 9 日是星期二,试问再过 $1949^{1979^{2000}}$ 天是星期几?

解 因为 $1949=7\times 278+3$, $1949^k=3^k(\text{mod}7)$. 又 $(3,7)=1$, 由 Euler 定理得 $3^{\varphi(7)}=3^6\equiv 1(\text{mod}7)$. 又 $\varphi(6)=2$, $(5,6)=1$, $5^2\equiv 1(\text{mod}6)$, 所以有

$$1979^{2000}=(6\times 329+5)^{2000}\equiv 5^{2000}\equiv 5^{2\times 1000}\equiv 1(\text{mod}6)$$

从而有

$$1949^{1979^{2000}}\equiv 3^{1979^{2000}}\equiv 3^{1(\text{mod}6)}\equiv 3(\text{mod}7)$$

因此,再过 $1949^{1979^{2000}}$ 天是星期五.

例 5 求出最小的正整数 n ,使得 $\frac{n}{2}$ 是一个整数的平方, $\frac{n}{3}$ 是一个整数的三次方, $\frac{n}{5}$ 是一个整数的五次方.

解 由于所要求的正整数 n 应具有“最小性”,设满足条件的正整数为 $n=2^\alpha\cdot 3^\beta\cdot 5^\gamma$, 则应有

$$\alpha\equiv 1(\text{mod}2), \quad \beta\equiv 0(\text{mod}2), \quad \gamma\equiv 0(\text{mod}2)$$

$$\alpha\equiv 0(\text{mod}3), \quad \beta\equiv 1(\text{mod}3), \quad \gamma\equiv 0(\text{mod}3)$$

$$\alpha\equiv 0(\text{mod}5), \quad \beta\equiv 0(\text{mod}5), \quad \gamma\equiv 1(\text{mod}5)$$

由孙子定理分别求解关于 α , β , γ 的同余方程组,可求得

$$\alpha\equiv 15(\text{mod}30), \quad \beta\equiv 10(\text{mod}30), \quad \gamma\equiv 6(\text{mod}30)$$

故满足条件的正整数为 $n=2^{15}\times 3^{10}\times 5^6$.

例 6 设 $f(n)\in\mathbb{N}$ 是使和式 $\sum_{k=1}^{f(n)} k$ 能被 n 整除的最小数. 证明当且仅当 $n=2^m$ 时, $f(n)=2n-1$, 其中, $m\in\mathbb{Z}$, $m\geq 0$.

证 (1) 首先证明若 $n=2^m$, $m\in\mathbb{Z}$, $m\geq 0$, 则 $f(n)=2n-1$ 是使和式 $\sum_{k=1}^{f(n)} k$ 能被 n 整除的最小数.

一方面, 因为 $\sum_{k=1}^{2n-1} k=(2n-1)n$, 所以, $\sum_{k=1}^{2n-1} k$ 能被 n 整除. 另一方面, $2n-1$ 是满足条件的最小数. 这是因为若 $l\leq 2n-2$, 则 $\sum_{k=1}^l k=\frac{1}{2}l(l+1)$. 由于 $l, l+1$ 中有一个是奇数, 且 $l+1\leq 2n-1=2^{m+1}-1$, 于是, $2^{m+1}\nmid l(l+1)$, 从而 $2^m\nmid \frac{1}{2}l(l+1)$.

(2) 再证若 $f(n)=2n-1\in\mathbb{N}$ 是使 $n\mid \sum_{k=1}^{f(n)} k$ 成立的最小数, 则必有 $n=2^m$, $m\in\mathbb{Z}$, $m\geq 0$. 否则, 当 n 不是 2 的方幂时, 设 $n=2^m p$, $m\in\mathbb{Z}$, $m\geq 0$, $p>1$, p 是奇数.

由于 $(2^{m+1}, p) = 1$, 故由孙子定理可知同余方程组

$$\begin{cases} x \equiv 0 \pmod{2^{m+1}} \\ x \equiv p-1 \pmod{p} \end{cases}$$

有解, 即存在正整数 $l (0 < l < 2^{m+1} \cdot p = 2n)$ 满足上述同余方程组, 且 $2n-1$ 与 $2n$ 都不是上述同余方程组的解, 这是因为 $2n-1 \not\equiv 0 \pmod{2^{m+1}}, 2n \not\equiv p-1 \pmod{p}$. 因而 $l < 2n-1$, 且满足 $2^{m+1} | l$ 及 $p | l+1$, 于是有 $2^m p \left| \frac{l(l+1)}{2} \right.$, 从而 $f(n) \leq l < 2n-$

1, 这说明 $2n-1$ 不是使 $n \left| \sum_{k=1}^{f(n)} k \right.$ 成立的最小的 $f(n)$, 所以命题成立.

例 7 设 p 是大于 3 的素数, 且 $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2} = \frac{a}{b}, a, b \in \mathbb{N}, (a, b) = 1$. 证明 $p | a$.

证 对于不超过 $p-1$ 的自然数 k , 由于 $(k, p) = 1$, 所以存在唯一的不超过 $p-1$ 的自然数 x , 满足 $kx \equiv 1 \pmod{p}$. 而且当 $k=1$ 或 $p-1$ 有 $x=k=1$ 或 $p-1$. 当 $2 \leq k \leq p-2$ 时, 有 $2 \leq x \leq p-2$ 且 $x \neq k$, 故当 k 取遍 $1, 2, \dots, p-1$ 时, x 也取遍 $1, 2, \dots, p-1$.

因 $(p, (p-1)!) = 1$, 故由 $kx \equiv 1 \pmod{p}$ 可得

$$(p-1)! kx \equiv (p-1)! \pmod{p} \quad \text{或} \quad (p-1)! x \equiv \frac{(p-1)!}{k} \pmod{p}$$

所以

$$\begin{aligned} \frac{((p-1)!)^2 a}{b} &= \sum_{k=1}^{p-1} \frac{((p-1)!)^2}{k^2} \equiv \sum_{x=1}^{p-1} ((p-1)!)^2 x^2 \\ &\equiv ((p-1)!)^2 \frac{p(p-1)(2p-1)}{6} \pmod{p} \end{aligned}$$

因为 p 是大于 3 的素数, 所以 $p-1 \geq 4$, 故 $(p-1)!$ 含有因数 6, 从而

$$((p-1)!)^2 \frac{p(p-1)(2p-1)}{6} \pmod{p}$$

是 p 的倍数, 即 $\frac{((p-1)!)^2 a}{b} \equiv 0 \pmod{p}$. 因为 $((p-1)!, p) = 1$, 所以 $((p-1)!)^2,$

$p) = 1$, 从而 $\frac{a}{b} \equiv 0 \pmod{p}$, 因此, $a \equiv 0 \pmod{p}$.

例 8 设 $k \geq 2, n_1, n_2, \dots, n_k$ 为自然数, 且满足

$$n_2 | (2^{n_1} - 1), n_3 | (2^{n_2} - 1), \dots, n_k | (2^{n_{k-1}} - 1), n_1 | (2^{n_k} - 1)$$

证明 $n_1 = n_2 = \dots = n_k = 1$.

证 设 n_1, n_2, \dots, n_k 中有一数大于 1, 不妨设 $n_1 > 1$. 由 $n_1 | (2^{n_k} - 1)$ 得 $2^{n_k} - 1 > 1$, 即 $2^{n_k} > 2$, 所以 $n_k > 1$. 由此可证 $n_{k-1} > 1$, 同理可证 $n_{k-2} > 1, \dots, n_2 > 1$.

设 n_i 的最小素因子是 p_i , 则有 $p_i | (2^{n_i} - 1)$, 即 $2^{n_i} \equiv 1 \pmod{p_i}$. 另由 Fermat 定理知 $2^{p_i-1} \equiv 1 \pmod{p_i}$. 设 $d = (n_i, p_i - 1)$, 则存在整数 x, y 使 $d = xn_i + y(p_i - 1)$, 于是, $2^d = (2^{n_i})^x \cdot (2^{p_i-1})^y \equiv 1 \pmod{p_i}$, 从而 $d > 1$, 故 $p_i \leq d \leq p_i - 1 < p_i$ ($d \geq p_i$ 是因为 p_i 是 n_i 的最小素因子).

同理可证 $p_2 < p_3, \dots, p_{k-1} < p_k, p_k < p_1$, 从而 $p_1 < p_1$ 矛盾.

综上所述, 即有 $n_1 = n_2 = \dots = n_k = 1$.

例 9 在一个圆周上排列着 9192 个数码, 已知从其中某个位置的数码开始, 沿着顺时针方向, 用这些数码顺次组成的 9192 位数是 37 的倍数. 证明从其他任意一个数码开始, 沿顺时针方向用这些数码组成的 9192 位数也是 37 的倍数.

证 不妨设这 9192 个数码从某个位置开始按顺时针方向记为 $a_1, a_2, \dots, a_{9192}$. 由已知, $\overline{a_1 a_2 \dots a_{9192}} \equiv 0 \pmod{37}$. 下面只需证 $\overline{a_2 a_3 \dots a_{9192} a_1} \equiv 0 \pmod{37}$, 便可知命题成立.

$$\begin{aligned} \text{因为 } \overline{a_2 a_3 \dots a_{9192} a_1} &= 10 \overline{a_2 a_3 \dots a_{9192}} + a_1, \text{ 所以} \\ &= 10 \overline{a_1 a_2 \dots a_{9192}} - \overline{a_2 a_3 \dots a_{9192} a_1} \\ &= 10 \times (a_1 \times 10^{9191} + \overline{a_2 a_3 \dots a_{9192}}) - 10 \overline{a_2 a_3 \dots a_{9192}} - a_1 \\ &= a_1 \times (10^{9192} - 1) \end{aligned}$$

由于 $9192 \equiv 0 \pmod{3}$. 令 $9192 = 3n$, 则

$$10^{9192} = 10^{3n} = (10^3)^n = (37 \times 27 + 1)^n \equiv 1 \pmod{37}, \text{ 即 } 10^{9192} - 1 \equiv 0 \pmod{37}$$

另由已知有 $10 \overline{a_1 a_2 \dots a_{9192}} \equiv 0 \pmod{37}$, 从而 $\overline{a_2 a_3 \dots a_{9192} a_1} \equiv 0 \pmod{37}$. 命题得证.

例 10 (1) 形如 $F_n = 2^{2^n} + 1$ 的数 ($n \geq 0$) 叫 Fermat 定数. 求证 F_0, F_1, F_2, F_3, F_4 为素数, 但 F_5 是合数.

(2) 证明存在 $k \in \mathbb{N}$, 使得对于任意 $n \in \mathbb{N}$, $k \cdot 2^n + 1$ 都是合数.

证 (1) $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ 都是素数. 下面证明 F_5 是合数.

令 $a = 2^7, b = 5$, 则 $a - b^3 = 3, 1 + ab - b^4 = 1 + (a - b^3)b = 1 + 3b = 2^4$, 于是

$$\begin{aligned} F_5 &= (2a)^4 + 1 = 2^4 a^4 + 1 = (1 + ab - b^4) a^4 + 1 \\ &= (1 + ab) a^4 + (1 - a^4 b^4) = (1 + ab)(a^4 + (1 - ab)(1 + a^2 b^2)) \end{aligned}$$

而 $1 + ab = 641$ (素数), 即 $641 | F_5$.

(2) 证明分两步.

① 设 $a_i = F_i, i = 0, 1, 2, 3, 4, a_5 = 641, a_6 = \frac{F_5}{a_5} = \frac{2^{32} + 1}{641}$. 则有

$$\begin{aligned} 2^{32} + 1 &= (2^{32} - 1) + 2 = (2^{16} + 1)(2^8 + 1)(2^4 + 1)(2^2 + 1)(2 + 1)(2 - 1) + 2 \\ &= a_0 a_1 a_2 a_3 a_4 + 2 \equiv 2 \pmod{a_m}, m = 0, 1, 2, 3, 4 \end{aligned}$$

这说明素数 $a_m \nmid 2^{32} + 1$, 即有 $(2^{32} + 1, a_m) = 1, m = 0, 1, 2, 3, 4$. 由此可知 $a_0, a_1, a_2, a_3, a_4, a_5, a_6$ 两两互质.

② 由孙子定理, 同余方程组 $x \equiv -1 \pmod{a_6}, x \equiv 1 \pmod{a_m}, m = 0, 1, 2, \dots, 5$ 有解, 设为 k , 且满足 $k > \max\{a_0, a_1, a_2, a_3, a_4, a_5, a_6\}$.

下面证明对任意 $n \in \mathbb{N}$ 及上述 $k, k \cdot 2^n + 1$ 是合数.

记 $n = 2^m p, m \in \mathbb{Z}, m \geq 0, p$ 为奇数, 则当 $m \in \{0, 1, 2, 3, 4\}$ 时, 有

$$k \cdot 2^n + 1 \equiv 2^n + 1 \equiv (2^{2^m})^p + 1 \equiv (a_m - 1)^p + 1 \equiv (-1)^p + 1 \equiv 0 \pmod{a_m}$$

当 $m = 5$ 时, 有

$$k \cdot 2^n + 1 \equiv 2^n + 1 \equiv (2^{32})^p + 1 \equiv [(2^{32} + 1) - 1]^p + 1 \equiv (-1)^p + 1 \equiv 0 \pmod{a_5}$$

当 $m \geq 6$ 时, 有

$$k \cdot 2^n + 1 \equiv -2^n + 1 \equiv -(2^{32})^{2^{m-5} \cdot p} + 1 \equiv -(-1)^{2^{m-5} \cdot p} + 1 \equiv -1 + 1 \equiv 0 \pmod{a_6}$$

此外, 由于对任意 $n \in \mathbb{N}, k \cdot 2^n + 1 (> k)$ 大于 $a_0, a_1, a_2, a_3, a_4, a_5, a_6$ 中的任一数, 且至少被其中之一整除, 从而它是合数.

例 11 设 6666^{6666} 的各位数字之和为 a, a 的各位数字之和为 b, b 的各位数字之和为 c , 则 $c = ?$

解 因为 $6666^{6666} < (10^4)^{6666} = 10^{26664}$, 所以 6666^{6666} 最多是一个 26665 位数的数. 因此 $a \leq 26665 \times 9 = 239985$, 即 a 最多是一个 6 位数的数, 且首位不超过 2. 所以 $b \leq 2 + 5 \times 9 = 47$, 即 b 最多是一个两位数的数, 且首位不超过 4, 从而有 $c \leq 4 + 9 = 13$.

另外, $6666^{6666} = (3 \times 2222)^{6666} = (3^2)^{3333} \times (2222)^{6666} \equiv 0 \pmod{9}$, 所以由本章综合例题中的例 2 得 $c \equiv b \equiv a \equiv 6666^{6666} \equiv 0 \pmod{9}$. 显然满足条件 $1 \leq c \leq 13$ 及 $c \equiv 0 \pmod{9}$ 的 c 只能为 9, 即 $c = 9$.

思考题、研究题三

1. 把从 1 开始的自然数依次写下来, 直写到第 201 位为止, 就是

$$\overbrace{12345678910111213 \dots}^{201}$$

试问这个数除以 3 的余数等于几?

2. 已知任意一个整数, 将其各位数字相加, 其和可为一位或多位数, 如不是一位数, 又将各位数字相加, 如此下去, 直到得到一位数为止. 若所得一位数为 2, 3, 5, 6 之一, 试证原数不可能是正整数的平方或立方.

3. 假设整数 2008^n 与 2008^m 的最末三位数相等, 求正整数 n 和 m , 使 $n > m \geq 1$ 且 $m + n$ 取最小值.

4. 设 $n \in \mathbb{N}$, 整数 k 与 n 互质, 且 $0 < k < n$. 令 $M = \{1, 2, \dots, n-1\}$, 给 M 中每

个数染上黑白两种颜色中的一种,染法如下:

- (1) 对 M 中每个 i, i 与 $n-i$ 同色.
- (2) 对 M 中每个 $i, i \neq k, i$ 与 $|k-i|$ 同色.

证明 M 中所有的数必被染上同一种颜色.

5. 求具有下述性质的 $n \in \mathbb{N}$: 存在 $0, 1, \dots, n-1$ 的一个排列 a_1, a_2, \dots, a_n , 使得

$$a_1, a_1 a_2, a_1 a_2 a_3, \dots, a_1 a_2 \cdots a_n$$

恰好构成模 n 的完系.

6. 设 p 是奇素数, $1 \leq k < p, n = kp^2 + 1$, 且 $2^k \not\equiv 1 \pmod{n}, 2^{n-1} \equiv 1 \pmod{n}$, 证明 n 是素数.

7. 设 $n > 1$ 为奇数, k, l 分别是最小的使 $kn+1$ 及 ln 为平方数的正整数, 证明 n 为素数的充要条件是 k 与 l 均大于 $n/4$.

8. 证明对任意正整数 n , 均存在连续 n 个正整数, 使其中任一个都不能表示成两个整数的平方和.

9. 点坐标 (a, b) 中元素 a 与 b 均为整数时称为整点; 若 a 与 b 又互素, 则称点 (a, b) 为既约整点. 证明, 对给定正整数 n , 存在一个整点, 它与每个既约整点的距离都大于 n .

10. 证明下面两个结论.

(1) 存在 n 个连续的整数, 使得其中每一个数都有一个因子不能整除这个数列中的其他整数.

(2) 设 k 是给定的正整数. 证明, 存在 n 个连续的整数, 使得其中每一个数都可以被 k 个不同的素因子整除, 并且这 k 个素因子都不整除数列中其他数.

第 4 章 整数的阶与原根

本章依据 Euler 定理,介绍关于整数模的阶、原根、指数、 k 次剩余的定义及其相关性质,并对原根的存在条件做了详细的证明.此外,还介绍了如何利用 Maple 数学软件来求关于整数模的阶、原根、指数及 k 次剩余等问题.

4.1 整数的阶及其性质

由 Euler 定理知,若 $(a, m) = 1, m > 1$, 则 $a^{\varphi(m)} \equiv 1 \pmod{m}$, 那么, 是否存在比 $\varphi(m)$ 更小的正整数 d , 使得 $a^d \equiv 1 \pmod{m}$ 成立呢? 答案是肯定的.

定义 4.1 设 $(a, m) = 1, m > 1$, d 是使 $a^d \equiv 1 \pmod{m}$ 成立的最小正整数, 则称 d 为 a 关于模 m 的阶^①, 记作 $\text{ord}_m(a)$.

例如, 若 $m = 7, a = 2$, 则 $2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1 \pmod{7}$, 因此, $\text{ord}_7(2) = 3$.

需要强调的是: 在定义 4.1 中要求 $(a, m) = 1, m > 1$. 事实上, 如果 $(a, m) > 1$, 由定理 3.12 可知同余式 $ax \equiv 1 \pmod{m}$ 无解, 因此, 当 $d \geq 1$ 时, 同余式 $a^d \equiv 1 \pmod{m}$ 不成立.

关于阶有以下结论.

定理 4.1 设 $(a, m) = 1, m > 1$. 如果 $\text{ord}_m(a) = d$, 则 $a^k \equiv a^l \pmod{m}$, 当且仅当 $k \equiv l \pmod{d}$.

证 由 $\text{ord}_m(a) = d$ 得 $a^d \equiv 1 \pmod{m}$. 如果 $k \equiv l \pmod{d}$, 则 $k = l + dt$, 因此

$$a^k = a^{l+dt} = a^l \cdot (a^d)^t \equiv a^l \pmod{m}$$

另外, 假设 $a^k \equiv a^l \pmod{m}$, 则由带余除法定理知, 存在整数 q 和 r , 使得 $k - l = dq + r$, 其中, $0 \leq r < d$. 那么

$$a^k = a^{l+dq+r} = a^l \cdot (a^d)^q a^r \equiv a^l a^r \equiv a^k a^r \pmod{m}$$

因为 $(a^k, m) = 1$, 所以 $a^r \equiv 1 \pmod{m}$. 而 $0 \leq r < d$, 故 $r = 0$, 即 $k \equiv l \pmod{d}$.

推论 4.1 设 $(a, m) = 1, m > 1$, 并且 $\text{ord}_m(a) = d$, 则 $a^n \equiv 1 \pmod{m}$ 当且仅当 $d \mid n$.

证 若 $d \mid n$, 则存在整数 t 使得 $n = dt, a^n = a^{dt} = (a^d)^t \equiv 1 \pmod{m}$. 反之, 设正

^① 在不同的教科书中对这一概念一般有这三种不同的称呼. 如在熊全淹的《初等整数论》中称为“阶数”, 在潘承洞、潘承彪的《初等数论》中称为“指数”, 在柯召、孙琦的《数论讲义》中则称“次数”, 这里我们使用“阶”这一名称.

整数 n 满足 $a^n \equiv 1 \pmod{m}$. 由带余除法定理可知, 存在整数 q 和 r , 使得 $n = dq + r$, 其中, $0 \leq r < d$. 于是, $a^n = a^{dq+r} = (a^d)^q a^r \equiv a^r \pmod{m}$, 从而得 $a^r \equiv 1 \pmod{m}$, 而 $0 \leq r < d$, 所以 $r = 0$, 即 $d \mid n$.

推论 4.2 设 $(a, m) = 1, m > 1$, 并且 $\text{ord}_m(a) = d$, 则 $d \mid \varphi(m)$.

证 由 Euler 定理可知, $a^{\varphi(m)} \equiv 1 \pmod{m}$, 再由推论 4.1 直接可得 $d \mid \varphi(m)$.

例 4.1 设 $(a, m) = 1, m > 1$. 如果 $\text{ord}_m(a) = d$, 则 $1, a, a^2, \dots, a^{d-1}$ 关于模数 m 两两不同余.

证 假设结论不成立, 则至少存在一对数 $i, j: 0 \leq i < j \leq d-1$, 使 $a^j \equiv a^i \pmod{m}$, 于是有 $a^{j-i} \equiv 1 \pmod{m}$, 而 $0 < j-i \leq d-1$, 与 $\text{ord}_m(a) = d$ 矛盾.

例 4.2 若 $(a, m) = 1, (b, m) = 1, m > 1$. $\text{ord}_m(a) = d_1, \text{ord}_m(b) = d_2$, 且 $(d_1, d_2) = 1$, 则 $\text{ord}_m(ab) = d_1 d_2$.

证 因为 $(a, m) = 1, (b, m) = 1$, 所以 $(ab, m) = 1$, 因此 $\text{ord}_m(ab)$ 存在.

设 $\text{ord}_m(ab) = d$, 则 $(ab)^d \equiv 1 \pmod{m}$, 因此

$$a^{d_2 d} \equiv a^{d_2 d} b^{d_2 d} \equiv ((ab)^d)^{d_2} \equiv 1 \pmod{m}$$

由推论 4.1 得 $d_1 \mid d_2 d$. 由于 $(d_1, d_2) = 1$, 所以 $d_1 \mid d$. 同理可得 $d_2 \mid d$. 再由 $(d_1, d_2) = 1$ 可得

$$d_1 d_2 \mid d \quad (4.1.1)$$

另外, $(ab)^{d_1 d_2} \equiv (a^{d_1})^{d_2} (b^{d_2})^{d_1} \equiv 1 \pmod{m}$. 由推论 4.1 得

$$d \mid d_1 d_2 \quad (4.1.2)$$

由式(4.1.1)及式(4.1.2)便得 $d = d_1 d_2$.

定理 4.2 设 $(a, m) = 1, m > 1$, 并且 $\text{ord}_m(a) = d$, 则 $\text{ord}_m(a^\lambda) = \frac{d}{(\lambda, d)}$.

证 设 $\text{ord}_m(a^\lambda) = d_1$, 则 $(a^\lambda)^{d_1} = a^{\lambda d_1} \equiv 1 \pmod{m}$. 由推论 4.1 可得 $d \mid \lambda d_1$, 于是

$$\frac{d}{(\lambda, d)} \mid \frac{\lambda}{(\lambda, d)} \cdot d_1$$

因 $\left(\frac{d}{(\lambda, d)}, \frac{\lambda}{(\lambda, d)}\right) = 1$, 故

$$\frac{d}{(\lambda, d)} \mid d_1 \quad (4.1.3)$$

另外, 由 $(a^\lambda)^{\frac{d}{(\lambda, d)}} \equiv (a^d)^{\frac{\lambda}{(\lambda, d)}} \equiv 1 \pmod{m}$ 得

$$d_1 \mid \frac{d}{(\lambda, d)} \quad (4.1.4)$$

由式(4.1.3)及式(4.1.4)得 $d_1 = \frac{d}{(\lambda, d)}$.

例 4.3 设 p 是素数, a 是大于 1 的正整数, 并且 $\text{ord}_p(a) = d$, 则 a 的方幂中恰有 $\varphi(d)$ 个关于模 p 两两不同余的整数, 它们关于模 p 的阶都是 d .

证 由 $\text{ord}_p(a) = d$ 可得 $1, a, a^2, \dots, a^{d-1}$ 关于模 p 两两不同余, 因此它们是同余式

$$x^d \equiv 1 \pmod{m}$$

的全部解.

对于任意的一个数 $a^\lambda, 0 \leq \lambda \leq d-1$, 由定理 4.2 可得 a^λ 关于模数 p 的阶为 d 的充要条件是 $(d, \lambda) = 1$. 因此, 恰有 $\varphi(d)$ 个数关于模 p 两两不同余.

定理 4.3 设 p 是素数, $d | p-1$, 则阶是 d , 且关于模 p 互不同余的整数的个数是 $\varphi(d)$.

证 设 $1 \leq d \leq p-1$, $\psi(d)$ 表示 $1, 2, \dots, p-1$ 中关于模 p 的阶为 d 的个数. 因 $1, 2, \dots, p-1$ 中任意的一个数的阶都等于且只等于 $p-1$ 的某个因数, 故 $\psi(d) \geq 0$, 且

$$\sum_{d|p-1} \psi(d) = p-1 \quad (4.1.5)$$

另外, 由第 2 章 Euler 函数基本性质定理知

$$\sum_{d|p-1} \varphi(d) = p-1 \quad (4.1.6)$$

下面证明对于 $p-1$ 的每一个因子 d , 都有 $\varphi(d) \geq \psi(d)$.

对于 $p-1$ 的每一个因子 d , $\psi(d) = 0$, 或 $\psi(d) > 0$. 若 $\psi(d) = 0$, 则 $\varphi(d) \geq \psi(d)$ 已经成立. 若 $\psi(d) > 0$, 则存在阶为 d 的整数 a , 那么, d 个整数 a, a^2, \dots, a^d 关于模 p 两两不同余, 且都满足同余方程

$$x^d - 1 \equiv 0 \pmod{p} \quad (4.1.7)$$

由定理 3.17 的推论知式(4.1.7)没有其他解. 也就是说, 任意阶为 d 的整数必与 a, a^2, \dots, a^d 中的某个数关于模 p 同余. 由例 4.3 知 a 的方幂中恰有 $\varphi(d)$ 个整数的阶为 d , 也就是只有满足 $(k, d) = 1$ 的 a^k , 其阶为 d . 因此, $\psi(d) \leq \varphi(d)$. 从而由式(4.1.5)与式(4.1.6)得

$$\sum_{d|p-1} (\varphi(d) - \psi(d)) = 0$$

因而对任何满足 $d | p-1$ 的 d , 有 $\psi(d) = \varphi(d)$.

在定理 4.3 中, 特别地有: 当 $d = p-1$ 时, 有 $\varphi(p-1)$ 个互异的不大于 $p-1$ 的数, 它们的阶都是 $p-1 = \varphi(p)$, 这样的数称为 p 的原根, 将在下节讨论.

练 习 4.1

1. 求解下列各题.

(1) 求出 3 和 11 关于模 50 的阶.

- (2) 对 12 的每个因子 d , 求出所有满足 $\text{ord}_{13}(a)=d$ 及 $1 \leq a \leq 12$ 的整数 a .
2. 设 $(a, m)=1, m > 1$, 并且 $\text{ord}_m(a)=d$, 则有 $\varphi(d)$ 个数 a^λ (λ 满足 $(\lambda, d)=1, 0 < \lambda \leq d$) 关于模 m 的阶都是 d .
3. 证明 m 是一个素数的充分必要条件是存在某个整数 a , 其对模 m 的阶是 $m-1$.
4. 设 p 是奇素数, $a > 1$, 证明下列结论.
- (1) $a^p - 1$ 的奇素数因子是 $a - 1$ 的因子或是形如 $2pk + 1$ 的整数, 其中, k 是整数.
- (2) $a^p + 1$ 的奇素数因子是 $a + 1$ 的因子或是形如 $2pk + 1$ 的整数, 其中, k 是整数.
5. 设 $(a, m)=1$ 且 $\text{ord}_m(a)=st$ (s, t 是两个正整数), 则 $\text{ord}_m(a^t)=s$.
6. 设 p 是奇素数, 证明同余式 $x^{p-2} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p}$ 恰有 $p-2$ 个互不同余的解, 它们是 $2, 3, \dots, p-1$.

4.2 原根的存在条件

设 $(a, m)=1, m > 1, \text{ord}_m(a)=d$. 由推论 4.2 可知 $d | \varphi(m)$, 那么, a 满足什么条件时它的阶为 $\varphi(m)$ 呢?

定义 4.2 设 $(a, m)=1, m > 1$, 若 $\text{ord}_m(a)=\varphi(m)$, 则称 a 为模数 m 的一个原根, 或者简称为 m 的一个原根.

换言之, 如果对于所有的正整数 $k < \varphi(m)$, 都有 $a^k \not\equiv 1 \pmod{m}$, 则称 a 为模数 m 的一个原根.

例如, 3 是模数 7 的原根, 也是模数 10 的原根. 但是, 并非所有的模数 m 都有原根, 如模数 8 就没有原根, 因为 $\varphi(8)=4$, 而 $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$.

例 4.4 设 $(a, m)=1, m > 1, a_1, a_2, \dots, a_{\varphi(m)}$ 是小于 m 且与 m 互素的不同的正整数. 如果 a 是模数 m 的一个原根, 那么

$$a, a^2, \dots, a^{\varphi(m)}$$

与 $a_1, a_2, \dots, a_{\varphi(m)}$ 按一定的顺序对应关于模 m 同余.

证 因为 $(a, m)=1$, 所以对任何 $k: 1 \leq k \leq \varphi(m)$, 有 $(a^k, m)=1$, 于是 a^k 与某个 a_i 关于模 m 同余. 由定理 4.1 可知集合 $\{a, a^2, \dots, a^{\varphi(m)}\}$ 中的 $\varphi(m)$ 个数关于模 m 两两不同余, 因此, 集合 $\{a, a^2, \dots, a^{\varphi(m)}\}$ 中的每个数“与且仅与”集合 $\{a_1, a_2, \dots, a_{\varphi(m)}\}$ 中的某个数关于模 m 同余.

定理 4.4 设 $m > 1$. 若模数 m 有原根, 则 m 必为 $2, 4, p^l$ 或 $2p^l$, 其中, $l \geq 1, p$ 为奇素数.

证 (1) 设 $l \geq 3$ 且 $(a, 2^l)=1$. 证 $a^{2^{l-2}} \equiv 1 \pmod{2^l}$ 恒成立.

由 $(a, 2^l) = 1$ 可设 $a = 2\lambda + 1$, 于是

$$a^2 = (2\lambda + 1)^2 = 4\lambda^2 + 4\lambda + 1 = 4\lambda(\lambda + 1) + 1 \equiv 1 \pmod{8}$$

因此, 当 $l=3$ 时结论成立.

假设 $l=k-1$ 时结论成立, 即 $a^{2^{k-3}} \equiv 1 \pmod{2^{k-1}}$, 亦即存在某个整数 λ 使得

$$a^{2^{k-3}} = 1 + \lambda 2^{k-1}$$

则 $l=k$ 时, $a^{2^{k-2}} = (1 + \lambda 2^{k-1})^2 \equiv 1 \pmod{2^k}$, 结论也成立. 由数学归纳法可知同余式 $a^{2^{l-2}} \equiv 1 \pmod{2^l}$ 成立. 换言之, 当 $l \geq 3$ 时, 整数 2^l 没有原根.

(2) 设 $m = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}$ ($p_1 < p_2 < \cdots < p_s, s \geq 2$) 为模数 m 的标准分解式.

由 Euler 定理可知, 任意与 p_i 互素的整数 a , 必有 $a^{\varphi(p_i^{l_i})} \equiv 1 \pmod{p_i^{l_i}}$.

设 $l = [\varphi(p_1^{l_1}), \varphi(p_2^{l_2}), \dots, \varphi(p_s^{l_s})]$, 则 $a^l \equiv 1 \pmod{m}$, 故当 $l < \varphi(m)$ 时, m 无原根.

当 $p > 2$ 时, $\varphi(p^l)$ 为偶数. 若 m 有两个不同的奇素因子, 不妨设为 p_i, p_j , 则 $\varphi(p_i^{l_i} \cdot p_j^{l_j}) = \varphi(p_i^{l_i})\varphi(p_j^{l_j})$ 且 $\varphi(p_i^{l_i})$ 与 $\varphi(p_j^{l_j})$ 都为偶数. 令

$$n = \frac{\varphi(p_i^{l_i} \cdot p_j^{l_j})}{2} = \frac{\varphi(p_i^{l_i})\varphi(p_j^{l_j})}{2}$$

由 Euler 定理可知 $a^{\varphi(p_i^{l_i})} \equiv 1 \pmod{p_i^{l_i}}$, 因此

$$a^n = (a^{\varphi(p_i^{l_i})})^{\frac{\varphi(p_j^{l_j})}{2}} \equiv 1 \pmod{p_i^{l_i}}$$

同理可得

$$a^n = (a^{\varphi(p_j^{l_j})})^{\frac{\varphi(p_i^{l_i})}{2}} \equiv 1 \pmod{p_j^{l_j}}$$

由 $(p_i, p_j) = 1$ 得 $a^n \equiv 1 \pmod{(p_i^{l_i} \cdot p_j^{l_j})}$, 而 $n = \frac{\varphi(p_i^{l_i} \cdot p_j^{l_j})}{2} < \varphi(p_i^{l_i} \cdot p_j^{l_j})$,

所以 m 无原根. 若 m 有原根, 则 m 必为 $2^{l_1}, p^l, 2^c p^l$ ($l_1 > 0, l > 0, c > 0$) 三种情况之一.

再根据上面的讨论知, 当 $c \geq 2$ 时, $m = 2^c p^l$ 无原根. 由 (1) 的证明可知 $l_1 > 2$ 时, m 亦无原根. 因此, 若模数 m 有原根, 则 m 必为 $2, 4, p^l$ 或 $2p^l$.

由定理 4.4 的证明可知, 当 $k \geq 3$ 时, 模数 2^k 没有原根, 也就是说, 不存在奇数, 其关于模 2^k 的阶是 2^{k-1} , 然而存在奇数, 其对于模数 2^k 的阶是 2^{k-2} .

为了证明定理 4.4 的逆命题也成立, 利用下面的定理.

定理 4.5 设 $(a, p) = 1$, p 是奇素数并且 $\text{ord}_p(a) = d$. 设 k_0 是使 $a^d \equiv 1 \pmod{p^{k_0}}$ 成立的最大正整数, 那么, 当 $k = 1, 2, \dots, k_0$ 时, a 关于模 p^k 的阶是 d ; 当 $k \geq k_0$ 时, a 关于模 p^k 的阶是 dp^{k-k_0} .

证 分三步来证明该定理.

(1) 由 $a^d \equiv 1 \pmod{p^{k_0}}$ 知存在一个整数 u_0 , $(u_0, p) = 1$ 使 $a^d = 1 + u_0 p^{k_0}$. 设 e 是 a 关于模 p^k 的阶, 则 $a^e \equiv 1 \pmod{p^k}$, $a^e \equiv 1 \pmod{p}$, 因此 $d | e$. 而当 $1 \leq k \leq k_0$

时,由 $a^d = 1 + u_0 p^{k_0}$ 可知 $a^d = 1 + v_0 p^k$, 其中, $v_0 = u_0 \cdot p^{k_0 - k}$, 故 $e | d$, 所以 $e = d$.

(2) 设 $j \geq 0$, 下面用数学归纳法证明存在一个整数 u_j , 使得

$$a^{dp^j} = 1 + p^{j+k_0} u_j, \text{ 且 } (u_j, p) = 1 \quad (4.2.1)$$

由(1)知当 $j=0$ 时命题成立.

假设对于某个整数 $j \geq 0$ 命题成立, 则

$$\begin{aligned} a^{dp^{j+1}} &= (1 + p^{j+k_0} u_j)^p = 1 + p^{1+j+k_0} u_j + \sum_{i=2}^p \binom{p}{i} p^{i(j+k_0)} u_j^i \\ &= 1 + p^{1+j+k_0} u_j + p^{2+(j+k_0)} v_j = 1 + p^{1+j+k_0} (u_j + p v_j) \\ &= 1 + p^{1+j+k_0} u_{j+1} \end{aligned}$$

其中, $u_{j+1} = u_j + p v_j$. 由于 $(u_j, p) = 1$, 所以 $(u_{j+1}, p) = 1$. 因此, 对于一切 $j \geq 0$, 式(4.2.1)成立.

(3) 当 $k \geq k_0 + 1$ 时, 则 $j = k - k_0 \geq 1$. 归纳假设 a 关于模 p^{k-1} 的阶是 dp^{j-1} , a 关于模 p^k 的阶是 e_k . 那么, 由 $a^{e_k} \equiv 1 \pmod{p^k}$ 可得 $a^{e_k} \equiv 1 \pmod{p^{k-1}}$, 因此 $dp^{j-1} | e_k$. 再由(2)证得的结论式(4.2.1), 可得

$$a^{dp^{j-1}} = 1 + p^{k-1} u_{j-1} \not\equiv 1 \pmod{p^k}$$

所以, dp^{j-1} 是 e_k 的真因子.

另外, 由

$$a^{dp^j} = 1 + p^{j+k_0} u_j \equiv 1 \pmod{p^k}$$

可得 $e_k | dp^j$. 因此, a 关于模 p^k 的阶是 $e_k = dp^j = dp^{k-k_0}$.

说明 在证明定理 4.5 时, 在(2)中用数学归纳法证明了结论式(4.2.1); 在(3)中用数学归纳法证明了当 $k > k_0$ 时, a 关于模 p^k 的阶是 dp^j .

定理 4.6 设 p 是奇素数, 如果 g 是 p 的一个原根, 那么, 对于所有的 $k \geq 2$, p^k 的原根是 g 或 $g + p$; 如果 g 是 p^k 的一个原根且 $g_1 \in \{g, g + p^k\}$ 是奇数, 则 g_1 是 $2p^k$ 的一个原根.

证 (1) 设 g 是 p 的一个原根, 则 $\text{ord}_p(g) = p-1$. 设 k_0 是使 $p^{k_0} | (g^{p-1} - 1)$ 成立的最大正整数. 由定理 4.5 可得, 如果 $k_0 = 1$, 则 g 关于模 p^k 的阶就是 $(p-1)p^{k-1} = \varphi(p^k)$. 因此, 对于一切 $k \geq 1$, g 是 p^k 的一个原根.

如果 $k_0 \geq 2$, 则存在整数 v 使得 $g^{p-1} = 1 + p^2 v$. 由二项式定理可得

$$\begin{aligned} (g+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} g^{p-1-i} p^i \equiv g^{p-1} + (p-1)g^{p-2} p \pmod{p^2} \\ &\equiv 1 + p^2 v + g^{p-2} p^2 - g^{p-2} p \pmod{p^2} \equiv 1 - g^{p-2} p \pmod{p^2} \\ &\not\equiv 1 \pmod{p^2} \end{aligned}$$

于是, $g+p$ 是 p 的一个满足条件

$$(g+p)^{p-1} = 1 + pu_0, \quad (u_0, p) = 1 \quad (4.2.2)$$

的原根.

设 $k \geq 2$, $\text{ord}_p^k(g+p) = l$, 则有

$$(g+p)^l \equiv 1 \pmod{p^k} \text{ 且 } (p-1) \mid l$$

另外, 由式(4.2.2) 有

$$(g+p)^{(p-1)^i} = (1+pu_0)^{p^i} = 1 + p^{i+1}u_i, \quad i = 1, 2, 3, \dots$$

其中, $u_i \equiv u_0 \pmod{p}$, 即有 $u_i \not\equiv 0 \pmod{p}$, 从而得 $(g+p)^{(p-1)^{k-1}} \equiv 1 \pmod{p^k}$. 但当 $1 \leq i < k-1$ 时, 有 $(g+p)^{(p-1)^i} \not\equiv 1 \pmod{p^k}$, 可得 $l = (p-1)p^{k-1} = \varphi(p^k)$. 因此, 对于一切 $k \geq 1$, $g+p$ 是 p^k 的一个原根.

(2) 如果 g 是 p^k 的一个原根, 那么, $g+p^k$ 也是 p^k 的一个原根. 显然, p^k 是奇数, 所以, g 和 $g+p^k$ 中一个奇数一个偶数. 设 $g_1 \in \{g, g+p^k\}$ 是奇数. 因为 $(g, p^k) = (g+p^k, p^k) = 1$, 所以 $(g_1, p^k) = 1$. 因为 $\varphi(p^k) \leq \text{ord}_{2p^k}(g_1) \leq \varphi(2p^k)$, 而 $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$, 从而得 $\text{ord}_{2p^k}(g_1) = \varphi(2p^k)$, 即 g_1 是 $2p^k$ 的一个原根.

由定理 4.3~定理 4.6 可知: 设 $m > 1$, 则整数 m 有一个原根的充分必要条件是 m 为 $2, 4, p^l$ 或 $2p^l$, 其中, $l \geq 1, p$ 为奇素数.

例 4.5 如果 $m > 2, n > 2$, 且 $(m, n) = 1$, 那么, mn 没有原根.

证 设有整数 a 满足 $(a, nm) = 1$, 则 $(a, m) = 1, (a, n) = 1$. 记 $h = [\varphi(m), \varphi(n)], d = (\varphi(m), \varphi(n))$. 由于 $\varphi(m), \varphi(n)$ 都是偶数, 故有 $d \geq 2$ 且

$$h = \frac{\varphi(m)\varphi(n)}{d} = \frac{\varphi(mn)}{d} \leq \frac{\varphi(mn)}{2}$$

由 Euler 定理可知 $a^{\varphi(m)} \equiv 1 \pmod{m}$. 因此, 有 $a^h = (a^{\varphi(m)})^{\frac{\varphi(n)}{d}} \equiv 1^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{m}$. 同理, $a^h \equiv 1 \pmod{n}$. 再由 $(m, n) = 1$ 可知 $a^h \equiv 1 \pmod{mn}$. 这就说明, 任意与 mn 互素的整数 a , 对模 mn 的阶均不超过 $\varphi(mn)/2$, 故 mn 没有原根.

通过例 4.5 也可以得到, 如果 n 能被两个奇素数整除, 或者 n 是形如 $n = 2^m p^k$ (p 是奇素数, 且 $m \geq 2$) 的整数 n , 那么, 整数 n 没有原根(证明留给读者).

练 习 4.2

1. 设 p 是奇素数, 则模数 p 的 $\varphi(p-1)$ 个原根的乘积关于模 p 同余于 1.
2. 设 p 是奇素数, $a \neq \pm 1, (a, p) = 1, \text{ord}_p(a) = d$, 且 k_0 是使 $a^d \equiv 1 \pmod{p^{k_0}}$ 成立的最大正整数. 如果 $k \geq k_0$ 是同余式 $a^k \equiv 1 \pmod{p^k}$ 的一个解, 那么 $\frac{p^k}{k} < \frac{a^d}{d}$.
3. 证明同余式 $9^k \equiv 1 \pmod{7^k}$ 无解.
4. 如果 g 是模数 p^2 的一个原根, 那么对一切 $k \geq 2, g$ 是模数 p^k 的一个原根.

5. 已知结论:任意的素数 p 都有原根. 利用这个结论证明 Wilson 定理(提示:如果素数 p 的一个原根是 r , 则 $(p-1)! \equiv r^{1+2+\dots+(p-1)} \pmod{p}$).

4.3 原根的个数及求法

已经知道设 $m > 1$, 则模数 m 有原根的充分与必要条件是 m 为 $2, 4, p^l$ 或 $2p^l$, 其中, $l \geq 1, p$ 为奇素数. 下面的定理告诉我们对于这样的 m 有多少个原根.

定理 4.7 设 $m > 1$, 模数 m 有原根 g , 则 m 恰有 $\varphi(\varphi(m))$ 个关于模 m 不同余的原根, 它们是由集合

$$S = \{g^t \mid 1 \leq t \leq \varphi(m), (t, \varphi(m)) = 1\}$$

中的数给出.

证 设 g 是 m 的一个原根, 则 $\text{ord}_m(g) = \varphi(m)$. 由于 $\varphi(m)$ 个整数

$$1, g, \dots, g^{\varphi(m)-1}$$

关于模 m 两两不同余, 因此, 它们构成 m 的一组简化剩余系. 设 a 是 m 的任一原根, 则存在某个整数 $k: 1 \leq k \leq \varphi(m)$, 使 $g^k \equiv a \pmod{m}$. 由定理 4.2 可知, a 关于模的阶为

$$\frac{\varphi(m)}{(\varphi(m), k)} = \varphi(m)$$

故 $(\varphi(m), k) = 1$, 即 a 与 S 中的一个数关于模 m 同余.

另外, S 中的任意一个数关于模 m 的阶均为 $\varphi(m)$, 因而均是原根. 而 S 中的数关于模 m 两两不同余, 因此, S 给出了关于模 m 全部两两不同余的原根, 共 $\varphi(\varphi(m))$ 个.

例 4.6 已知 2 是模数 11 的一个原根, 求出模数 11 的所有原根.

解 因为 $\varphi(11) = 10$ 且 2 是模数 11 的一个原根, 所以, $\{1, 2, \dots, 2^9\}$ 是模数 11 的一组简化剩余系. 由于 $1, 2, \dots, 9$ 中与 10 互素的整数有 $\varphi(10) = 4$ 个, 它们是 1, 3, 7, 9. 所以, 由定理 4.7 及 $2^1 \equiv 2 \pmod{11}, 2^3 \equiv 8 \pmod{11}, 2^7 \equiv 7 \pmod{11}, 2^9 \equiv 6 \pmod{11}$ 可得, 模数 11 的所有原根是 2, 6, 7, 8.

由定理 4.6 可知, 对于奇素数 p 及 $l \geq 1$, 如果已知模数 p 的一个原根, 可以直接求出模数 p^l 或 $2p^l$ 的一个原根. 因此, 求出模数 m 的所有原根的关键是求出奇素数 p 的一个原根. 下面的两个定理对解决这个问题有一定的帮助.

定理 4.8 设 $m > 2$, $\varphi(m)$ 的所有不同的素因子是 q_1, q_2, \dots, q_s , 且 $(g, m) = 1$, 则 g 是 m 的一个原根的充分必要条件是

$$g^{\varphi(m)/q_i} \not\equiv 1 \pmod{m}, \quad i = 1, 2, \dots, s \quad (4.3.1)$$

证 若 g 是 m 的一个原根, 则 $\text{ord}_m(g) = \varphi(m)$, 但 $0 < \frac{\varphi(m)}{q_i} < \varphi(m), i = 1, 2,$

..., s , 所以, 式(4.3.1)成立.

反之, 若式(4.3.1)成立. 设 $\text{ord}_m(g) = d$ 且不妨设 $d < \varphi(m)$. 由推论 4.2 可知 $d \mid \varphi(m)$. 所以, $\frac{\varphi(m)}{d}$ 是大于 1 的整数, 故存在 $\varphi(m)$ 的某个素因子 q_i 整除 $\frac{\varphi(m)}{d}$, 即 $\frac{\varphi(m)}{d} = q_i u$, 亦即 $\frac{\varphi(m)}{q_i} = du$, 故 $g^{\varphi(m)/q_i} = g^{du} \equiv 1 \pmod{m}$, 这与式(4.3.1)矛盾, 则必有 $d = \varphi(m)$, 即 g 是 m 的一个原根.

定理 4.9 设 p 为奇素数, $\text{ord}_p(a) = d, d < p - 1$, 则 $a^\lambda, \lambda = 1, 2, \dots, d$ 都不是 p 的原根.

证 因为 $a^\lambda (\lambda = 1, 2, \dots, d)$ 关于模 p 的阶是 $\frac{d}{(d, \lambda)}$ 而 $\frac{d}{(d, \lambda)} \leq d < p - 1$, 所以, a^λ 都不是 p 的原根.

例 4.7 求出 41 的所有原根.

解 由于 $\varphi(41) = 40 = 2^3 \times 5$, 故从 $2^{40/2} \equiv 3^{40/5} \equiv 4^{40/2} \equiv 5^{40/2} \equiv 1 \pmod{41}$ 及定理 4.8, 可知, 1, 2, 3, 4, 5 都不是 41 的原根. 因 $6^{40/2} \equiv 40 \not\equiv 1 \pmod{41}$ 且 $6^{40/5} \equiv 10 \not\equiv 1 \pmod{41}$, 所以, 6 是 41 的一个原根. 类似于例 4.6 可以求出 41 的所有原根为 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35, 共 $\varphi(\varphi(41)) = 16$ 个.

练 习 4.3

1. 求 41^2 的一个原根.
2. 证明如果素数 $p = 2^\lambda + 1, \left(\frac{a}{p}\right) = -1$, 则 a 是 p 的一个原根.
3. 设 p 是奇素数, 求同余式 $x^{p-1} \equiv 1 \pmod{p^s}, s \geq 1$ 的全部解.
4. 素数 71 有一个原根 7, 求出 71 的所有原根, 并求 71^2 和 2×71^2 的一个原根.
5. 设 p 是奇素数. 证明
 - (1) p^n 与 $2p^n$ 的原根个数相同.
 - (2) p^n 的任意原根 r 也是 p 的原根 (提示: 设 $\text{ord}_p(r) = k$, 证明: $r^{pk} \equiv 1 \pmod{p^2}, \dots, r^{p^{n-1}k} \equiv 1 \pmod{p^n}$, 因此, $\varphi(p^n) \mid p^{n-1}k$).
6. 设 p 是奇素数, r 是 p^n 的一个原根, 则 r 是 $2p^n$ 的原根的充分必要条件是 r 为奇数.

4.4 指数及 k 次剩余

如果 m 有一个原根 g , 则 $g, g^2, \dots, g^{\varphi(m)}$ 组成模数 m 的一组缩系. 因此, 对任意与 m 互素的整数 n , 存在整数 $a (1 \leq a \leq \varphi(m))$ 使得 $n \equiv g^a \pmod{m}$. 由于原根有上述重要性质, 可以给出下面的定义.

定义 4.3 设 g 是 m 的一个原根, n 是任意一个与 m 互素的正整数, 则必存在一正整数 a 使得

$$n \equiv g^a \pmod{m}, \quad 0 \leq a \leq \varphi(m)$$

我们称 a 为 n 关于模 m 的指数, 记作 $a = \text{ind}_g n$ (在不引起混淆情况下可简记为 $a = \text{ind } n$). 若 b 为任意整数使得 $n \equiv g^b \pmod{m}$ 成立, 则 $b \equiv \text{ind } n \pmod{\varphi(m)}$.

说明 由于模数 m 的原根存在的充分必要条件是 m 必为 $2, 4, p^l$ 或 $2p^l$, 其中, $l \geq 1, p$ 为奇素数. 所以讨论指数时, m 必为 $2, 4, p^l$ 或 $2p^l$, 其中, $l \geq 1, p$ 为奇素数.

关于指数, 具有类似对数的性质.

定理 4.10 设 g 是模数 m 的一个原根, $(ab, m) = 1$. 则

$$(1) \text{ind}_g ab \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}.$$

$$(2) \text{ind}_g a^l \equiv l \text{ind}_g a \pmod{\varphi(m)} (l \geq 0).$$

$$(3) \text{ind}_g 1 = 0, \text{ind}_g g = 1, \text{ind}_g (-1) = \frac{\varphi(m)}{2} (m > 2).$$

$$(4) \text{ 设 } g_1 \text{ 也是 } m \text{ 的一个原根, 则有 } \text{ind}_g a \equiv \text{ind}_{g_1} a \cdot \text{ind}_{g_1} g_1 \pmod{\varphi(m)}.$$

证 (1) 设 $\lambda_1 = \text{ind}_g a, \lambda_2 = \text{ind}_g b$, 则 $a \equiv g^{\lambda_1} \pmod{m}, b \equiv g^{\lambda_2} \pmod{m}$, 因此

$$ab \equiv g^{\lambda_1 + \lambda_2} \pmod{m}$$

即 $\text{ind}_g ab \equiv \lambda_1 + \lambda_2 \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}$.

(2) 设 $\lambda_1 = \text{ind}_g a$, 则 $a \equiv g^{\lambda_1} \pmod{m}$, 因此 $a^l \equiv g^{l\lambda_1} \pmod{m}$, 即

$$\text{ind}_g a^l \equiv l\lambda_1 \equiv l \text{ind}_g a \pmod{\varphi(m)}$$

(3) 设 $m > 2$, 则有 $\varphi(m) \equiv 0 \pmod{2}$. 显然, $m = 4$ 时结论成立. 故只需证明 $m = p^l$ 或 $2p^l$, 其中, $l \geq 1, p$ 为奇素数时结论成立.

由 $g^{\varphi(m)} \equiv 1 \pmod{p^l}$ 得

$$(g^{\varphi(m)/2} - 1)(g^{\varphi(m)/2} + 1) \equiv 0 \pmod{p^l}$$

于是, $p^l \mid g^{\varphi(m)/2} - 1$ 或 $p^l \mid g^{\varphi(m)/2} + 1$ (如果有 $p \mid g^{\varphi(m)/2} - 1$ 且 $p \mid g^{\varphi(m)/2} + 1$, 则 $p \mid (g^{\varphi(m)/2} + 1) - (g^{\varphi(m)/2} - 1)$, 即有 $p \mid 2$, 矛盾). 但由于 g 是 m 的一个原根, 因此

$$g^{\varphi(m)/2} \equiv -1 \pmod{p^l}$$

同理, 当 $m = 2p^l$ 时, 亦有 $g^{\varphi(m)/2} \equiv -1 \pmod{p^l}$. 因 $(2, g) = 1$, 所以, 亦有 $g^{\varphi(m)/2} \equiv -1 \pmod{2}$, 故得

$$g^{\varphi(m)/2} \equiv -1 \pmod{2p^t}$$

因此, $\text{ind}_g(-1) = \varphi(m)/2$.

(4) 由定理 4.7 可知存在 $t: 1 \leq t \leq \varphi(m), (t, \varphi(m)) = 1$ 使得 $g_1 \equiv g^t \pmod{m}$.

设 $\lambda_1 = \text{ind}_{g_1} a$, 则 $a \equiv g_1^{\lambda_1} \equiv g^{t\lambda_1} \pmod{m}$, 即有

$$\text{ind}_g a \equiv t\lambda_1 = t \text{ind}_{g_1} a = \text{ind}_g g_1 \cdot \text{ind}_{g_1} a \pmod{\varphi(m)}$$

定义 4.4 设 m, k, a 是整数, 且 $m \geq 2, k \geq 2, (a, m) = 1$. 如果存在整数 x 使得

$$x^k \equiv a \pmod{m} \tag{4.4.1}$$

成立, 则称 a 是模 m 的 k 次剩余; 否则, 称 a 是模 m 的 k 次非剩余.

定理 4.11 设 p 是素数, $k \geq 2, d = (k, p-1), (a, p) = 1$, 且 g 是 p 的一个原根, 那么, a 是模 p 的 k 次剩余的充分必要条件是

$$\text{ind}_g(a) \equiv 0 \pmod{d}$$

当且仅当

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$$

如果 a 是模数 p 的 k 次剩余, 那么, 同余式 $x^k \equiv a \pmod{p}$ 恰有 d 个解关于模 p 两两不同余.

证 设 $l = \text{ind}_g(a)$, 其中, g 是 p 的一个原根. 同余式 $x^k \equiv a \pmod{p}$ 有解当且仅当存在一个整数 y 使得

$$g^y \equiv x \pmod{p}$$

且

$$g^{ky} \equiv g^l \pmod{p} \tag{4.4.2}$$

由定理 4.1 得式(4.4.2)关于 y 有解当且仅当

$$ky \equiv l \pmod{p-1} \tag{4.4.3}$$

关于 y 有解. 由定理 2.1 得同余式(4.4.3)关于 y 有解的充分必要条件是 $(k, p-1) | l$, 即 $l = \text{ind}_g(a) \equiv 0 \pmod{d}$, 其中, $d = (k, p-1)$. 因此, 模 p 的 k 次剩余恰好在 $(p-1)/d$ 个剩余类 $g^{id} + p\mathbb{Z} (i=0, 1, \dots, (p-1)/d-1)$ 中, 而且

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$$

当且仅当

$$(p-1)l/d \equiv 0 \pmod{p-1}$$

当且仅当

$$\text{ind}_g(a) \equiv 0 \pmod{d}$$

如果同余式(4.4.3)有解, 那么, 由定理 3.12 可知恰有 d 个关于模 $p-1$ 两两不同余的解. 因此, $x^k \equiv a \pmod{p}$ 恰有 d 个解 $x = g^y$ 关于模 p 两两不同余.

推论 4.3 设 p 是素数, $k \geq 2, (k, p-1) = 1$. 如果 $(a, p) = 1$ 且 a 是模 p 的 k 次剩余, 则 $x^k \equiv a \pmod{p}$ 有唯一的解.

利用指数理论可以求某些特殊类型同余方程的解. 例如, 对于二项式同余方程

$$x^k \equiv a \pmod{m} \quad (4.4.4)$$

其中, $(a, m) = 1, k \geq 2, m$ 是正整数且有一个原根. 由定理 4.10 可知, 同余方程 (4.4.4) 等价于线性同余方程

$$k \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\varphi(m)} \quad (4.4.5)$$

其中, $\operatorname{ind} x$ 未知. 如果 $d = (k, \varphi(m))$ 且 $d \nmid \operatorname{ind} a$, 那么, 式 (4.4.5) 无解; 如果 $d \mid \operatorname{ind} a$, 那么, 恰有 d 个 $\operatorname{ind} x$ 满足式 (4.4.5). 因此, 式 (4.4.4) 有 d 个互不同余的解. 下面举例说明.

例 4.8 已知 2 是 13 的一个原根, 求同余式 $4x^9 \equiv 7 \pmod{13}$ 的所有解.

解 首先计算 $2^1, 2^2, \dots, 2^{12} \pmod{13}$.

$$\begin{aligned} 2^1 &\equiv 2, & 2^5 &\equiv 6, & 2^9 &\equiv 5 \\ 2^2 &\equiv 4, & 2^6 &\equiv 12, & 2^{10} &\equiv 10 \\ 2^3 &\equiv 8, & 2^7 &\equiv 11, & 2^{11} &\equiv 7 \\ 2^4 &\equiv 3, & 2^8 &\equiv 9, & 2^{12} &\equiv 1 \end{aligned}$$

因此, 可以构造的指数表如表 4.1 所示.

表 4.1

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6

由于同余式 $4x^9 \equiv 7 \pmod{13}$ 有解当且仅当

$$\operatorname{ind}_2 4 + 9 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 7 \pmod{12}$$

有解. 由上面的指数表可知, $\operatorname{ind}_2 4 = 2, \operatorname{ind}_2 7 = 11$, 因此, $9 \operatorname{ind}_2 x \equiv 11 - 2 \equiv 9 \pmod{12}$, 这等价于同余方程 $\operatorname{ind}_2 x \equiv 1 \pmod{4}$, 解之得 $\operatorname{ind}_2 x \equiv 1, 5, 9$. 再利用上面的指数表可得 $x \equiv 2, 6, 5 \pmod{13}$.

对于一般的正整数 m , 有类似于定理 4.11 的结论.

定理 4.12 设 m 是正整数且有原根. 若 $(a, m) = 1$, 则同余式 $x^k \equiv a \pmod{m}$ 有解的充分必要条件是

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m} \quad (4.4.6)$$

其中, $d = (k, \varphi(m))$. 若有解, 则恰有 d 个解.

请读者自证该结论.

练习 4.4

1. 利用指数理论解同余方程 $x^3 \equiv 8 \pmod{19}$.
2. 分别求模 11 所有的五次剩余与六次剩余.

3. 如果 $p \equiv 2 \pmod{3}$, 任意整数 a , 若 $p \nmid a$, 那么, a 是模 p 的三次剩余.
4. 证明 $x^3 \equiv 3 \pmod{19}$ 无解, 但 $x^3 \equiv 11 \pmod{19}$ 有三个不同余的解.
5. 给定同余式 $x^3 \equiv a \pmod{p}$, 其中, $p \geq 5$ 是奇素数且 $(a, p) = 1$. 证明
 - (1) 如果 $p \equiv 1 \pmod{6}$, 那么, $x^3 \equiv a \pmod{p}$ 或者无解, 或者有三个解.
 - (2) 如果 $p \equiv 5 \pmod{6}$, 那么, $x^3 \equiv a \pmod{p}$ 有唯一解.
6. 设 x_a 是使得 $x^3 \equiv a \pmod{11}$ 成立的最小非负整数, 计算当 $a = 1, 2, \dots, 10$ 时 x_a 的值.
7. 设 $\alpha \geq 3$. 证明当 $2 \nmid k$ 时, 2^α 的 k 次剩余的个数是 $2^{\alpha-1}$. 而当 $2 \mid k$ 时, 2^α 的 k 次剩余的个数是 $\frac{2^{\alpha-2}}{(k, 2^{\alpha-2})}$.
8. 设 p 是奇素数, 且 $(k, p-1) = 1$. 则 $1^k, 2^k, 3^k, \dots, (p-1)^k$ 组成模 p 的一个缩系.
9. 利用原根性质证明 Wilson 定理.

4.5 利用 Maple 计算关于整数模的阶与原根

在 Maple 中, 用于求某整数 a 关于模 m 的阶的函数是 $\text{order}(a, m)$, 但必须先调用数论软件包“numtheory”. 如下所示:

```
>with(numtheory):
order(2, 7); order(13, 100); order(8, 12);
3
20
FAIL
```

这说明 $\text{ord}_7(2) = 3$, $\text{ord}_{100}(13) = 20$, 但 $\text{ord}_{12}(8) = \text{FAIL}$, 即 8 关于模 12 的阶不存在(因为 8 与 12 不互素).

利用 Maple 编程, 可对定理 4.3 进行验证.

```
>with(numtheory):
Th4_3: = proc(p::posint, d::posint)
local l, i, s;
l := 0;
for i from 1 to p-1
do s[i] := order(i, p);
if s[i] = d then l := l + 1 else l := l end if;
end do;
if l = phi(d) then print('Theory 4.3 is true for the pair'(p, d)):
else
```

```
print('Theory 4.3 is false for the pair'(p,d):
```

```
end if;
```

```
end;
```

如

```
>Th4_3(17,8);Th4_3(17,9);
```

```
Theory 4.3 is true for the pair (17,8)
```

```
Theory 4.3 is false for the pair (17,9)
```

对于练习 4.1 中第 1 题,如不采用编程计算则比较麻烦,利用 Maple 编程则很容易给出解答.请读者自己尝试.

在 Maple 中,函数 $\text{primroot}(m)$ 与 $\text{primroot}(g,m)$ 分别表示求模 m 的第一个原根与模 m 的比 g 大的下一个原根.如下所示:

```
>primroot(41); primroot(6,41);
```

```
6
```

```
7
```

```
>primroot(27), primroot(20,27), primroot(23,27);
```

```
2, 23, FAIL
```

这表示 27 的第一个原根是 2,比 20 大的原根是 23,比 23 大的原根不存在.

如果要求出模 m 的全部原根,可编程如下:

```
>with(numtheory):
```

```
allprimroot:=proc(m::posint)
```

```
local g,d,l,t;
```

```
l:=0;
```

```
for g from 1 to m-1
```

```
do d:=order(g,m):
```

```
if d=phi(m) then l:=l+1: t[l]:=g end if;
```

```
end do;
```

```
print(seq(t[i],i=1..l));
```

```
end;
```

如求 41 的全部原根.

```
>allprimroot(41);
```

```
6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35
```

又如求 58 的全部原根.

```
>allprimroot(58);
```

```
3, 11, 15, 19, 21, 27, 31, 37, 39, 43, 47, 55
```

在 Maple 中,函数 $\text{index}(x,a,m)$ 与 $\text{index}(x,a,m,'c')$ (或 $\text{mlog}(x,a,m)$ 与 $\text{mlog}(x,a,m,'c')$,其功能与前面两个函数分别一样)用于求模 m 的以 a 为底的 x 的离散对数,但有参数 c 时,则表示所有关于模 c 与 $\text{index}(x,a,m)$ 同余的整数均

是模 m 的以 a 为底的 x 的离散对数. 如下所示:

```
> index(9, 4, 11), index(9, 4, 11, 'c'), c;
3, 3, 5
```

上面的运算结果表示模 11 的以 4 为底的 9 的离散对数是 3, 同时, 对任意整数 $k, 3+5k$ 均是模 11 的以 4 为底的 9 的离散对数.

当 a 是模 m 的一个原根时, 则该离散对数即是 x 关于模 m 的指数. 如果要直接求在不需知道原根的情况下 x 关于模 m 的指数, 则可使用函数 $\text{index}(x, \text{primroot}(m), m)$. 如下所示:

```
> index(36, primroot(97), 97);
```

16

第 4 章综合例题

例 1 设 p 是奇素数, a 是大于 1 的正整数. 如果 q 是 $a^p - 1$ 的适合 $q \nmid a - 1$ 的素因子, 则必有 $q = 2pk + 1$, 其中, k 是正整数.

证 设 q 是 $a^p - 1$ 的素因子, 则 $(a, q) = 1$, 并且 $a^p \equiv 1 \pmod{q}$. 设 $\text{ord}_q(a) = d$, 则 $d \mid p$. 而 p 是奇素数, 因此, d 仅为 1 或 p . 当 $d = 1$ 时, 可得 $q \mid a - 1$, 与题设矛盾, 因此 $d = p$. 由 Euler 定理得 $p \mid \varphi(q)$. 因 q 是 $a^p - 1$ 的素因子, 所以, $\varphi(q) = q - 1$, 故 $p \mid q - 1$. 由 $q > p > 2$ 知 q 是奇素数, 因此, $2p \mid q - 1$, 即 $q = 2pk + 1$.

例 2 设 k 是正整数, 则有

$$5^{2^k} \equiv 1 + 3 \times 2^{k+2} \pmod{2^{k+4}}$$

证 对 k 用归纳法证明该同余等式.

当 $k = 1$ 时,

$$5^{2^1} = 25 \equiv 1 + 3 \times 2^3 \pmod{2^5}$$

当 $k = 2$ 时,

$$5^{2^2} = 625 = 1 + 48 + 576 \equiv 1 + 3 \times 2^4 \pmod{2^6}$$

即 $k = 1, 2$ 时, 命题成立.

假设对于 $k \geq 3$ 命题成立, 则存在整数 t 使得

$$5^{2^k} = 1 + 3 \times 2^{k+2} + 2^{k+4} \cdot t = 1 + 2^{k+2}(3 + 4t)$$

由于 $k \geq 3$, 所以, $2k + 4 > k + 5$. 因此

$$\begin{aligned} 5^{2^{k+1}} &= (5^{2^k})^2 = (1 + 2^{k+2}(3 + 4t))^2 \\ &\equiv 1 + 2^{k+3}(3 + 4t) \pmod{2^{2k+4}} \\ &\equiv 1 + 3 \times 2^{k+3} \pmod{2^{k+5}} \end{aligned}$$

例 3 设 k 是正整数. 如果 $k \geq 3$, 那么, 5 关于模 2^k 的阶为 2^{k-2} ; 如果 $a \equiv 1 \pmod{4}$, 那么, 存在唯一的整数 $i \in \{0, 1, \dots, 2^{k-2} - 1\}$ 使得 $a \equiv 5^i \pmod{2^k}$ 成立; 如果

$a \equiv 3 \pmod{4}$, 那么, 存在唯一的整数 $i \in \{0, 1, \dots, 2^{k-2} - 1\}$ 使得 $a \equiv -5^i \pmod{2^k}$ 成立.

证 当 $k=3$ 时, $\text{ord}_8(5)=2$, 且

$$1 \equiv 5^0 \pmod{8}, 3 \equiv -5^1 \pmod{8}, 5 \equiv 5^1 \pmod{8}, 7 \equiv -5^0 \pmod{8}$$

当 $k \geq 4$ 时, 由例 2 有

$$5^{2^{k-2}} \equiv 1 + 3 \times 2^k \pmod{2^{k+2}} \equiv 1 \pmod{2^k}$$

且

$$5^{2^{k-3}} \equiv 1 + 3 \times 2^{k-1} \pmod{2^{k+1}} \equiv 1 + 3 \times 2^{k-1} \pmod{2^k} \not\equiv 1 \pmod{2^k}$$

因此, 5 对模 2^k 的阶为 2^{k-2} , 且当 $i \in \{0, 1, \dots, 2^{k-2} - 1\}$ 时, 5^i 关于模 2^k 两两不同余.

由于对一切 i 都有 $5^i \equiv 1 \pmod{4}$, 并且在 0 到 2^k 之间的 2^{k-1} 个奇数中, 恰有一半即 2^{k-2} 个数关于模 4 同余于 1. 因此, 如果 $a \equiv 1 \pmod{4}$, 那么, 同余式

$$5^i \equiv a \pmod{2^k}$$

有唯一解.

如果 $a \equiv 3 \pmod{4}$, 则有 $-a \equiv 1 \pmod{4}$, 那么, 同余式

$$-a \equiv 5^i \pmod{2^k} \text{ 或 } a \equiv -5^i \pmod{2^k}$$

有唯一解.

例 4 利用阶的定义及性质证明 $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

证 设 $(a^m - 1, a^n - 1) = d$, 则

$$a^m \equiv 1 \pmod{d}$$

$$a^n \equiv 1 \pmod{d}$$

设 $\text{ord}_d(a) = t$, 则 $t | m, t | n$, 于是 $t | (m, n)$. 因此

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

故

$$d | (a^{(m,n)} - 1) \quad (4.1)$$

另外, 因为 $(m, n) | m, (m, n) | n$, 所以, $(a^{(m,n)} - 1) | (a^m - 1)$, 且 $(a^{(m,n)} - 1) | (a^n - 1)$. 因此

$$(a^{(m,n)} - 1) | d \quad (4.2)$$

由式(4.1)和式(4.2)可得 $(a^m - 1, a^n - 1) = k = a^{(m,n)} - 1$.

例 5 (1) 设 p 是素数, 那么, 存在 p 的原根 r 使得 $r^{p-1} \not\equiv 1 \pmod{p^2}$.

(2) 设 p 是素数, 那么, 存在 p 的原根 r 使对一切整数 $k \geq 2$, 都有

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

证 (1) 由定理 4.4 可知, p 有原根, 设为 r . 如果 $r^{p-1} \equiv 1 \pmod{p^2}$, 那么, 结论成立. 否则, 即 $r^{p-1} \not\equiv 1 \pmod{p^2}$. 用 $r' = r + p$ 替换 r , 那么, r' 也是 p 的一个原根, 由二项式定理可得

$$(r')^{p-1} \equiv (r+p)^{p-1} \equiv (r)^{p-1} + (p-1) \cdot p \cdot r^{p-2} \pmod{p^2}$$

由于 $r^{p-1} \equiv 1 \pmod{p^2}$, 因此

$$(r')^{p-1} \equiv 1 - p \cdot r^{p-2} \pmod{p^2}$$

由 r 是模 p 的一个原根知 $(r, p) = 1$, 于是 $p \nmid r^{p-2}$. 故

$$(r')^{p-1} \not\equiv 1 \pmod{p^2}$$

综上所述, 存在 p 的原根 r 使得 $r^{p-1} \not\equiv 1 \pmod{p^2}$.

(2) 对 k 用数学归纳法进行证明.

当 $k=2$ 时, 由(1)知结论成立.

假设对于某个整数 $k > 2$ 时命题成立, 即存在 p 的原根 r 使对一切整数 $k \geq 2$, 都有

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \quad (4.3)$$

那么, 对于 $k+1$, 因为 $(r, p^{k-1}) = (r, p^k) = 1$, 所以由 Euler 定理可得

$$r^{p^{k-2}(p-1)} = r^{\varphi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$$

因此, 再由式(4.3)知, 存在整数 $a (p \nmid a)$ 使得

$$r^{p^{k-2}(p-1)} = 1 + ap^{k-1} \quad (4.4)$$

将方程(4.4)两端都取 p 次幂得

$$r^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p \equiv 1 + ap^k \pmod{p^{k+1}}$$

由 $p \nmid a$ 可得

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$$

即结论对 $k+1$ 也成立.

由归纳法得知, 对于一切整数 $k \geq 2$ 时, 结论成立.

例 6 设 a 是一个正整数. 如果 n 是一个正合数且满足 $a^n \equiv a \pmod{n}$, 则称 n 是以 a 为底的伪素数. 证明下列结论.

(1) 设 $m = a^n - 1$, 这里, a 与 n 是两个正整数, 则有 $\text{ord}_m a = n$.

(2) 如果 p 与 q 是互异的奇素数, 则 pq 是以 2 为底的伪素数当且仅当 $\text{ord}_q 2 \mid p-1$ 及 $\text{ord}_p 2 \mid q-1$ 成立.

(3) 如果 p 与 q 是互异的奇素数, 则 pq 是以 2 为底的伪素数当且仅当 $M_p M_q = (2^p - 1)(2^q - 1)$ 是以 2 为底的伪素数.

证 (1) 显然有 $a^n \equiv 1 \pmod{m}$. 且对任何小于 n 的正整数 k , 有 $(a^n - 1) \nmid (a^k - 1)$, 即 $m \nmid (a^k - 1)$, 亦即有 $a^k \not\equiv 1 \pmod{m}$, 因而 $\text{ord}_m a = n$.

(2) 设 pq 是以 2 为底的伪素数, 即有 $2^{pq} \equiv 2 \pmod{pq}$. 则有

$$2^{(p-1)(q-1) + (p-1) + (q-1)} \equiv 1 \pmod{pq}$$

由 Euler 定理有

$$2^{\varphi(pq)} \equiv 1 \pmod{pq}$$

亦即 $2^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

因此

$$2^{(p-1)+(q-1)} \equiv 1 \pmod{pq}$$

从而得

$$\begin{cases} 2^{(p-1)+(q-1)} \equiv 1 \pmod{p} \\ 2^{(p-1)+(q-1)} \equiv 1 \pmod{q} \end{cases}$$

再利用 Euler 定理即得

$$\begin{cases} 2^{q-1} \equiv 1 \pmod{p} \\ 2^{p-1} \equiv 1 \pmod{q} \end{cases}$$

所以

$$\begin{cases} \text{ord}_p 2 \mid q-1 \\ \text{ord}_q 2 \mid p-1 \end{cases}$$

反之,将上述证明过程倒推即可.

(3) 如果 pq 是以 2 为底的伪素数, 即有 $2^{pq} \equiv 2 \pmod{pq}$, 则有 $\text{ord}_p 2 \mid q-1$, 即有 $2^{q-1} \equiv 1 \pmod{p}$, 因而 $2^q - 1 \equiv 1 \pmod{p}$. 另由 Fermat 定理可得 $2^p - 1 \equiv 1 \pmod{p}$, 从而存在 $k, l \in \mathbb{Z}$, 使得

$$2^{(2^p-1)(2^q-1)} = 2^{(1+kp)(1+lp)} = 2 \cdot 2^{(kl+l+k)p}$$

另外, 由(1)知 $\text{ord}_{2^p-1} 2 = p$, 于是, $2^{(kl+l+k)p} \equiv 1 \pmod{(2^p-1)}$. 因而得

$$2^{(2^p-1)(2^q-1)} = 2 \cdot 2^{(kl+l+k)p} \equiv 2 \pmod{(2^p-1)}$$

由 p 与 q 的对称性可得

$$2^{(2^p-1)(2^q-1)} \equiv 2 \pmod{(2^q-1)}$$

再由例 4 知 $(2^p-1)(2^q-1) = 2^{(p,q)} - 1 = 2 - 1 = 1$, 故得

$$2^{(2^p-1)(2^q-1)} \equiv 2 \pmod{(2^p-1)(2^q-1)}$$

即 $M_p M_q = (2^p-1)(2^q-1)$ 是以 2 为底的伪素数.

反之, 若 $(2^p-1)(2^q-1)$ 是以 2 为底的伪素数, 则有

$$2^{(2^p-1)(2^q-1)} \equiv 2 \pmod{(2^p-1)(2^q-1)}$$

于是, $2^{(2^p-1)(2^q-1)} \equiv 2 \pmod{(2^p-1)}$, 即有 $2^{(2^p-1)(2^q-1)-1} \equiv 1 \pmod{(2^p-1)}$. 从而由(1)得 $(2^p-1)(2^q-1) - 1 \equiv 0 \pmod{p}$. 由 Euler 定理有 $2^p - 1 \equiv 1 \pmod{p}$, 因而有 $(2^q-1) - 1 \equiv 0 \pmod{p}$, 即 $2^q \equiv 2 \pmod{p}$. 亦即得到

$$2^q \equiv 2 \pmod{p} \quad (4.5)$$

由 Euler 定理有

$$2^p \equiv 2 \pmod{p} \quad (4.6)$$

将式(4.6)两边取 q 次方幂得 $2^{pq} \equiv 2^q \pmod{p}$, 然后利用式(4.5)得

$$2^{pq} \equiv 2 \pmod{p} \quad (4.7)$$

同理可得

$$2^{pq} \equiv 2 \pmod{q} \quad (4.8)$$

从而由式(4.7)与式(4.8)得

$$2^{pq} \equiv 2 \pmod{pq}$$

即 pq 是以 2 为底的伪素数.

思考题、研究题四

1. 证明 $2^{13}-1$ 与 $2^{2^4}+1$ 是素数, 但 $2^{11}-1$ 与 $2^{2^5}+1$ 不是素数(不使用任何程序语言编程证明).

2. 设 n 是大于 1 的正整数. 证明下列结论.

(1) 如果 $F_n=2^{2^n}+1$ 是素数, 则 3 是 F_n 的一个原根.

(2) 设 $m=2^n+1$. 如果 m 是素数, 则 3 是 m 的一个原根, 且模 m 的任意一个二次非剩余均是模 m 的原根.

(3) $m=2^n+1$ 是素数的充要条件是 $3^{(m-1)/2} \equiv -1 \pmod{m}$.

3. 设 r 是奇素数 p 的一个原根. 证明 p 的二次剩余的乘积与 $r^{(p^2-1)/4}$ 关于模数 p 同余; p 的二次非剩余的乘积与 $r^{(p-1)^2/4}$ 关于模数 p 同余.

4. 设 $n>1$, p 是奇素数且 $p>3^{2^{n-1}}/2^n$, 则 3 是形如 $2^n p+1$ 的素数的一个原根.

5. 设 p 是奇素数, 则如果 p^n 和 $2p^n$ 的原根个数相同, 那么, p^2 的原根一定是 p^n ($n \geq 2$) 的原根.

6. 设 p 是奇素数, r 是 p^2 的一个原根. 证明同余方程 $x^{p-1} \equiv 1 \pmod{p^2}$ 的解恰好是 $r^p, r^{2p}, \dots, r^{(p-1)p}$.

7. 若 p 为奇素数, 则 p 的 $\varphi(p-1)$ 个原根的乘积与 $(-1)^{\varphi(p-1)}$ 关于模 p 同余.

8. 设 n 是一个正整数, d 是一个选定的与 $\varphi(n)$ 互素的大于 1 的正整数, e 是同余方程 $dx \equiv 1 \pmod{\varphi(n)}$ 的满足 $1 < e \leq \varphi(n)$ 的解, 则 (d, n) 称为 RSA 公钥密码体制的私钥, (e, n) 称为 RSA 公钥密码体制的公钥. 设 P 是要加密的明文, C 是用公钥加密后得到的密文, 即 $C \equiv P^d \pmod{n}$. 令

$$C_1 \equiv C^e \pmod{n}, C_2 \equiv C_1^e \pmod{n}, \dots, C_i \equiv C_{i-1}^e \pmod{n}, \dots$$

(1) 证明对任意正整数 j , 有 $C_j \equiv C^{e^j} \pmod{n}$.

(2) 证明存在正整数 k , 使 $C_k \equiv C \pmod{n}$, $C_{k-1} = P$, 并且 $k \mid \text{ord}_{\varphi(n)} e$.

(3) 取 $n=2773$, $e=17$, 密文 $C=1504$, 找出明文 $P=?$

注 该题所叙述的找明文的循环方法称为 RSA 循环攻击法.

9. 设 $n=p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ 是正整数 n 的素因数分解. 证明使 n 成为伪素数的, 且关于模 n 不同余的底个数是

$$\prod_{i=1}^t (n-1, p_i-1)$$

10. 设 $f(x)$ 是次数为 $n-1$ 的整系数多项式, p 是一个素数, x_1, x_2, \dots, x_n 是 n 个关于模 p 不同余的整数.

(1) 证明对任何整数 x , 有

$$f(x) \equiv \sum_{j=1}^n f(x_j) \prod_{\substack{i=1 \\ i \neq j}}^n (x - x_i)(x_j - x_i)^{-1} \pmod{p}$$

其中, $(x_j - x_i)^{-1}$ 是 $x_j - x_i$ 的关于模 p 的逆. 上同余式称为 $f(x)$ 关于模 p 的拉格朗日插值(Lagrange interpolation)多项式.

(2) 如果 $f(x)$ 是一个次数为 3 的整系数多项式, 且关于模 11, $f(1), f(2), f(3)$ 分别同余于 8, 2, 4, 求 $f(5)$ 关于模 11 的最小正余数. 并由此求 $f(x) \pmod{11}$.

第 5 章 平方剩余

本章将介绍产生于二次同余方程的几个重要的概念及其相关性质与定理,包括二次剩余、Legendre 符号、Jacobi 符号及 Gauss 二次互反律.

5.1 二次剩余

定义 5.1 设 m 是正整数, a 是整数且满足 $(a, m) = 1$, 如果同余方程

$$x^2 \equiv a \pmod{m} \quad (5.1.1)$$

有整数解, 则称 a 是模 m 的二次剩余或平方剩余, 记作 $a \in \mathbb{Q}_m$. 否则, 称 a 是模 m 的二次非剩余或平方非剩余, 记作 $a \in \overline{\mathbb{Q}}_m$.

例如, 1, 3, 4, 5, 9 模 11 的二次剩余; 2, 6, 7, 8, 10 是模 7 的二次非剩余; 1, 9, 11 是模 14 的二次剩余; 3, 5, 13 是模 14 的二次非剩余.

显然, 如果 $a \equiv b \pmod{m}$, 那么, a 是模 m 的二次剩余当且仅当 b 是模 m 的二次剩余. 因此, 一个给定的整数是否为模 m 的二次剩余? 只需要考虑模 m 的简系中的对应元素是否为模 m 的二次剩余.

由于一般正整数模的二次剩余问题可转化成其不同素因子的二次剩余问题, 所以, 下面只涉及素数模的二次剩余的情形.

例 5.1 对于模 $p=13$, 判断 $1, 2, \dots, 12$ 中哪些数是模 13 的二次剩余? 那些数是模 13 的二次非剩余?

解 为了确定 $1, 2, \dots, 12$ 中哪些是模 13 的二次剩余, 需要知道, 当 a 取遍集合 $\{1, 2, \dots, 12\}$ 时, 哪些同余方程

$$x^2 \equiv a \pmod{13}$$

有解.

已知整数 $1, 2, \dots, 12$ 的平方是 $1^2 \equiv 12^2 \equiv 1 \pmod{13}$, $2^2 \equiv 11^2 \equiv 4 \pmod{13}$, $3^2 \equiv 10^2 \equiv 9 \pmod{13}$, $4^2 \equiv 9^2 \equiv 3 \pmod{13}$, $5^2 \equiv 8^2 \equiv 12 \pmod{13}$, $6^2 \equiv 7^2 \equiv 10 \pmod{13}$.

由上面的计算结果可知, 模 13 的二次剩余是 1, 3, 4, 9, 10, 12. 二次非剩余是 2, 5, 6, 7, 8, 11.

对于给定的奇素数 p , Euler 给出了判断一个整数 a 是否为模 p 的二次剩余的判别方法.

定理 5.1 (Euler 准则) 设 p 是奇素数且 $(a, p) = 1$, 那么, 整数 a 是模 p 的二次剩余的充分且必要条件是

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

证法一 设 a 是模 p 的二次剩余, 则 $x^2 \equiv a \pmod{p}$ 有一个整数解, 设为 x_1 . 由 Fermat 小定理可得

$$a^{\frac{p-1}{2}} \equiv (x_1^2)^{\frac{p-1}{2}} \equiv (x_1)^{p-1} \equiv 1 \pmod{p}$$

反之, 设 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, r 是模 p 的一个原根, 那么, 存在整数 k ($1 \leq k \leq p-1$) 使得 $a \equiv r^k \pmod{p}$. 因此

$$r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$$

由 r 是模 p 的一个原根可得 $(p-1) \mid k(p-1)/2$, 于是 k 是偶数. 设 $k = 2j$, 则有

$$(r^j)^2 \equiv r^{2j} \equiv r^k \equiv a \pmod{p}$$

这说明 r^j 是同余方程 $x^2 \equiv a \pmod{p}$ 的一个解, 即 a 是模 p 的二次剩余.

证法二 充分性与证法一相同, 下面证必要性.

设 a 是模 p 的二次剩余, 则 $x^2 \equiv a \pmod{p}$ 有两个解 $x = x_1$ 和 $x = p - x_1$, 其中, x_1 满足 $1 \leq x_1 \leq p-1$. 如果把 x_1 和 $p - x_1$ 从集合 $\{1, 2, \dots, p-1\}$ 中去掉, 那么, 剩余的 $p-3$ 个整数可以分成 $(p-3)/2$ 个整数对 c, c' , 使得 $c \cdot c' \equiv a \pmod{p}$. 这样, 就可得 $(p-3)/2$ 个同余式

$$\begin{aligned} c_1 \cdot c'_1 &\equiv a \pmod{p} \\ c_2 \cdot c'_2 &\equiv a \pmod{p} \\ &\vdots \\ c_{(p-3)/2} \cdot c'_{(p-3)/2} &\equiv a \pmod{p} \end{aligned}$$

另外, 还有同余式

$$x_1(p - x_1) \equiv -x_1^2 \equiv -a \pmod{p}$$

将以上 $(p-1)/2$ 个同余式对应两边相乘可得

$$c_1 \cdot c'_1 \cdot c_2 \cdot c'_2 \cdot \dots \cdot c_{p-1/2} \cdot c'_{p-1/2} \cdot x_1 \cdot (p - x_1) \equiv -a^{(p-1)/2} \pmod{p}$$

由上面的讨论可得 $c_1, c'_1, c_2, c'_2, \dots, c_{p-1/2}, c'_{p-1/2}, x_1, (p - x_1)$ 是 $1, 2, \dots, p-1$ 的重新排列, 于是有

$$c_1 \cdot c'_1 \cdot c_2 \cdot c'_2 \cdot \dots \cdot c_{p-1/2} \cdot c'_{p-1/2} \cdot x_1 \cdot (p - x_1) = (p-1)!$$

由 Wilson 定理可得 $(p-1)! \equiv -1 \pmod{p}$, 因此得

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

例 5.2 (定理 5.1 的推论) 设 p 是奇素数且 $(a, p) = 1$, 那么, 整数 a 是模 p 的二次非剩余的充分且必要条件是

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

证法一 如果 p 是奇素数且 $(a, p) = 1$, 由 Fermat 小定理可得 $a^{p-1} - 1 \equiv 0 \pmod{p}$. 于是

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv a^{p-1} - 1 \equiv 0 \pmod{p}$$

因此

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ 或 } a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

成立, 且不能同时成立. 假若同时成立, 则有 $1 \equiv -1 \pmod{p}$ 或 $p \mid 2$, 这与 p 是奇素数矛盾.

既然模 p 的二次非剩余不满足 $a^{(p-1)/2} \equiv 1 \pmod{p}$, 那么, 必满足 $a^{(p-1)/2} \equiv -1 \pmod{p}$. 反之, 若 $a^{(p-1)/2} \equiv -1 \pmod{p}$, 则由定理 5.1 可知 a 是模 p 的二次非剩余.

证法二 由定理 5.1, 充分性显然, 下面只证必要性.

设 a 是模 p 的二次非剩余, c 是 $1, 2, \dots, p-1$ 中的任意一个整数, 则存在唯一的一个整数 $c' \in \{1, 2, \dots, p-1\}$ 使得 $cx = a \pmod{p}$, 且 $c \neq c'$, 否则有 $c^2 \equiv a \pmod{p}$, 这与 a 是模 p 的二次非剩余矛盾. 于是, 从 1 到 $p-1$ 的整数可分成 $(p-1)/2$ 个整数对 c, c' , 满足 $c \cdot c' \equiv a \pmod{p}$. 这样就可得 $(p-1)/2$ 个同余式

$$\begin{aligned} c_1 \cdot c'_1 &\equiv a \pmod{p} \\ c_2 \cdot c'_2 &\equiv a \pmod{p} \\ &\vdots \\ c_{(p-1)/2} \cdot c'_{(p-1)/2} &\equiv a \pmod{p} \end{aligned}$$

将以上 $(p-1)/2$ 个同余式两端对应相乘可得

$$c_1 \cdot c'_1 \cdot c_2 \cdot c'_2 \cdot \dots \cdot c_{(p-1)/2} \cdot c'_{(p-1)/2} \equiv a^{(p-1)/2} \pmod{p}$$

由上面的讨论可得 $c_1, c'_1, c_2, c'_2, \dots, c_{(p-1)/2}, c'_{(p-1)/2}$ 是 $1, 2, \dots, p-1$ 的重新排列, 于是 $c_1 \cdot c'_1 \cdot c_2 \cdot c'_2 \cdot \dots \cdot c_{(p-1)/2} \cdot c'_{(p-1)/2} = (p-1)!$. 再由 Wilson 定理可得 $(p-1)! \equiv -1 \pmod{p}$, 因此

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

练习 5.1

1. 分别找出素数 11, 13, 17 的所有二次剩余.
2. 分别找出整数 8, 11, 12, 19 的所有二次非剩余.
3. 证明对于奇素数 p , 模 p 的二次剩余与整数 $1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$ 关于模 p 同余.
4. 证明若 a 是奇素数模 p 的二次剩余, 那么, a 不是模 p 的原根.
5. 证明若 p 是奇素数, 则

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{(\rho+5)(p-1)}{8}}$$

6. 对于奇素数 p , 如果 $ab \equiv r \pmod{p}$, 且 r 是模 p 的二次剩余, 那么, a, b 同为模 p 的二次剩余, 或者同为模 p 的二次非剩余.

7. 设 p 是奇素数. 如果 a, b 同为模 p 的二次剩余, 或者同为模 p 的二次非剩余, 那么, 同余式 $a \cdot x^2 \equiv b \pmod{p}$ 有解.

8. 设 $n > 2, (a, n) = 1$. 证明若 a 是模 n 的二次剩余, 那么, $a^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}$.

5.2 Legendre 符号

由 Euler 准则可以判定一个整数是否为模 p 的二次剩余. 但是, 当 p 很大的时候, 这种判断方法计算起来有一定困难, 不实用. 利用下面我们介绍的 Legendre 符号, 则可得到一个计算上相对简便的判别方法.

定义 5.2 设 p 是奇素数, 模 p 的 Legendre 符号定义为

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & (a, p) = 1 \text{ 且 } a \text{ 是模数 } p \text{ 的二次剩余} \\ -1, & (a, p) = 1 \text{ 且 } a \text{ 是模数 } p \text{ 的二次非剩余} \\ 0, & p \mid a \end{cases}$$

注意: 如果 p 是奇素数, 那么, 同余式 $x^2 \equiv 1 \pmod{p}$ 只有解 $x \equiv \pm 1 \pmod{p}$, 而且如果 $\epsilon, \epsilon' \in \{-1, 0, 1\}$ 且 $\epsilon \equiv \epsilon' \pmod{p}$, 那么, $p \mid (\epsilon - \epsilon')$, 因此 $\epsilon = \epsilon'$. 特别地, 如果 $\left(\frac{a}{p}\right) \equiv \epsilon \pmod{p}$, 则 $\left(\frac{a}{p}\right) = \epsilon$.

定理 5.2 (Legendre 符号性质定理) 设 p 是奇素数, $(a, p) = 1, (b, p) = 1$, 则

$$(1) \text{ 如果 } a \equiv b \pmod{p}, \text{ 那么, } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

$$(2) \left(\frac{a^2}{p}\right) = 1.$$

$$(3) \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \text{ (该性质也称为 Euler 准则)}.$$

(4) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, 一般地, 如果整数 a 的素因子分解式为 $a = \pm 2^{r_0} q_1^{r_1} q_2^{r_2} \cdots q_k^{r_k}$, 那么

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2}{p}\right)^{r_0} \left(\frac{q_1}{p}\right)^{r_1} \left(\frac{q_2}{p}\right)^{r_2} \cdots \left(\frac{q_k}{p}\right)^{r_k}$$

$$(5) \left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

证 (1) 显然.

(2) 对于同余式 $x^2 \equiv a^2 \pmod{p}$, a 就是它的解, 因此 $\left(\frac{a^2}{p}\right) = 1$.

(3) 由定理 5.1 直接可得 $\left(\frac{a}{b}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(4) 由(3)可得

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} \pmod{p} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod{p} \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}$$

由于 Legendre 符号为 1 或 -1 , 假若 $\left(\frac{ab}{p}\right) \neq \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$, 那么 $1 \equiv -1 \pmod{p}$, 矛盾. 因此, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

(5) 由(3)直接可得.

例 5.3 判断同余式 $x^2 \equiv -38 \pmod{13}$ 是否有解?

解 Legendre 符号 $\left(\frac{-38}{13}\right) = \left(\frac{-1}{13}\right) \left(\frac{38}{13}\right) = \left(\frac{38}{13}\right)$, 又因为 $38 \equiv 12 \pmod{13}$, 且 $12 = 3 \times 2^2$, 于是

$$\left(\frac{38}{13}\right) = \left(\frac{12}{13}\right) = \left(\frac{3 \times 2^2}{13}\right) = \left(\frac{3}{13}\right)$$

再由

$$\left(\frac{3}{13}\right) \equiv 3^{\frac{13-1}{2}} \equiv 3^6 \equiv 27^2 \equiv 1 \pmod{13}$$

故同余式 $x^2 \equiv -38 \pmod{13}$ 有解.

本题也可这样来求 Legendre 符号 $\left(\frac{-38}{13}\right)$.

$$\left(\frac{-38}{13}\right) = \left(\frac{-1}{13}\right) \left(\frac{38}{13}\right) = \left(\frac{-1}{13}\right) \left(\frac{39-1}{13}\right) = \left(\frac{-1}{13}\right) \left(\frac{-1}{13}\right) = 1$$

定义 5.3 设 p 是奇素数, S 是含有 $(p-1)/2$ 个整数的集合, 如果 $S \cup (-S) = S \cup \{-s \mid s \in S\}$ 是模 p 的简系(简化剩余系)的集合, 那么, 称 S 为模 p 的一个 Gauss 集合.

例如, $\left\{1, 2, \dots, \frac{p-1}{2}\right\}$ 和 $\{2, 4, \dots, p-1\}$ 都是模 p 的一个 Gauss 集合.

由定义 5.3 可知: 如果 S 是模 p 的一个 Gauss 集合, 那么, 对于任意的整数 a , $(a, p) = 1$, 一定存在 $s \in S$ 和 $\epsilon \in \{1, -1\}$ 使得 $a \equiv \epsilon s \pmod{p}$ 成立. 并且进一步可得: s, ϵ 是由 a 唯一确定的. 即如果 S 是模 p 的一个 Gauss 集合, 且 $s \equiv s' \pmod{p}$, 那么 $s = s'$.

定理 5.3(Gauss 引理) 设 p 是奇素数, a 是任意与 p 互素的整数, 且 S 是模 p 的一个 Gauss 集合, 那么, 对于任意的 $s \in S$, 存在唯一的整数 $u_a(s) \in S$, $\epsilon_a(s) \in \{1, -1\}$, 使得

$$as \equiv \epsilon_a(s)u_a(s) \pmod{p}$$

并且

$$\left(\frac{a}{p}\right) = \prod_{s \in S} \epsilon_a(s) = (-1)^m$$

其中, m 是 S 中满足 $\epsilon_a(s) = -1$ 的 s 的个数.

证 存在性显然成立, 下面证唯一性.

由于 S 是模 p 的一个 Gauss 集合, 设 $s, s' \in S$, 如果 $u_a(s) = u_a(s')$, 则有

$$\begin{aligned} as' &\equiv \epsilon_a(s')u_a(s') \pmod{p} \equiv \epsilon_a(s')u_a(s) \pmod{p} \\ &\equiv \epsilon_a(s')\epsilon_a(s)\epsilon_a(s)u_a(s) \pmod{p} \equiv \pm as \pmod{p} \end{aligned}$$

则由 $(a, p) = 1$ 知, 可将 a 从同余式两边消去得 $s \equiv \pm s' \pmod{p}$. 但由于 $s, s' \in S$, 而若 $s' \equiv -s \pmod{p}$, 则 $s' \in -S$, 矛盾(因 $S \cap (-S) = \emptyset$). 因此, 必有 $s \equiv s' \pmod{p}$, 即 $s = s'$. 这说明对任意的 $s \in S$, 存在唯一的整数 $u_a(s) \in S, \epsilon_a(s) \in \{1, -1\}$ 使得

$$as \equiv u_a(s)\epsilon_a(s) \pmod{p}$$

对任意的与 p 互素的整数 a , 显然映射 $u_a: s \rightarrow u_a(s)$ (对任何 $s \in S$) 是 S 的一个置换, 因此有

$$\prod_{s \in S} s = \prod_{s \in S} u_a(s)$$

从而有

$$\begin{aligned} a^{\frac{p-1}{2}} \prod_{s \in S} s &= \prod_{s \in S} as \equiv \prod_{s \in S} \epsilon_a(s)u_a(s) \pmod{p} \\ &\equiv \prod_{s \in S} \epsilon_a(s) \prod_{s \in S} u_a(s) \pmod{p} \equiv \prod_{s \in S} \epsilon_a(s) \prod_{s \in S} s \pmod{p} \end{aligned}$$

因 $(\prod_{s \in S} s, p) = 1$, 故可两边同除以 $\prod_{s \in S} s$ 得

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv \prod_{s \in S} \epsilon_a(s) \pmod{p}$$

由于同余式两端都是 ± 1 , 所以有

$$\left(\frac{a}{p}\right) = \prod_{s \in S} \epsilon_a(s) = (-1)^m$$

例 5.4 利用 Gauss 引理计算 Legendre 符号 $\left(\frac{3}{11}\right)$.

解 取模 11 的一个 Gauss 集合为 $S = \{2, 4, 6, 8, 10\}$, 则有

$$\begin{aligned} 3 \times 2 &\equiv 6 \pmod{11} \\ 3 \times 4 &\equiv (-1) \times 10 \pmod{11} \\ 3 \times 6 &\equiv (-1) \times 4 \pmod{11} \\ 3 \times 10 &\equiv 8 \pmod{11} \end{aligned}$$

因此, 有 $m = 2$ 个 $s \in S$ 使得 $\epsilon_a(s) = -1$, 所以, $\left(\frac{3}{11}\right) = (-1)^2 = 1$. 也就是说, 3 是模

11 的二次剩余. 事实上, $5^2 \equiv 6^2 \equiv 3 \pmod{11}$, 即 5, 6 是 3 模 11 的两个平方根.

例 5.5 设 p 是奇素数, 则有

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

证 取模 p 的 Gauss 集合为 $S = \{1, 2, 3, \dots, (p-1)/2\}$, 那么

$$\{2s \mid s \in S\} = \{2, 4, \dots, p-1\}$$

由 Gauss 引理得

$$\left(\frac{2}{p}\right) = (-1)^m$$

其中, m 是 S 中使得 $\epsilon_2(s) = -1$ 的 s 的个数.

如果 $1 \leq 2s \leq (p-1)/2$, 那么 $2s \in S$, 因此有 $u_2(s) = 2s$ 且 $\epsilon_2(s) = 1$. 如果 $(p-1)/2 \leq 2s \leq p-1$, 那么, $1 \leq p-2s \leq (p-1)/2$, 因此 $p-2s \in S$. 由于 $2s \equiv -(p-2s) \pmod{p}$, 因此有 $u_2(s) = p-2s$ 且 $\epsilon_2(s) = -1$. 所以, m 是 S 中使得 $(p+1)/2 \leq 2s \leq p-1$ 的 s 的个数, 即满足不等式关系

$$(p+1)/4 \leq s \leq (p-1)/2 \tag{5.2.1}$$

的正整数 s 的个数.

由于 p 是奇素数, 那么, p 关于模 8 同余于 1, 3, 5, 7 之一. 因此, 只需讨论下列 4 种情况.

(1) 如果 $p \equiv 1 \pmod{8}$, 可设 $p = 8k + 1$, 则 $(-1)^{(p^2-1)/8} = (-1)^{2k(4k+1)} = 1$. 另外, $s \in S$ 满足式(5.2.1)当且仅当

$$2k + \frac{1}{2} \leq s \leq 4k$$

于是得 $m = 2k$, $\left(\frac{2}{p}\right) = (-1)^{2k} = 1 = (-1)^{2k(4k+1)} = (-1)^{(p^2-1)/8}$.

(2) 如果 $p \equiv 3 \pmod{8}$, 设 $p = 8k + 3$, 即有 $(-1)^{(p^2-1)/2} = (-1)^{(2k+1)(4k+1)} = -1$. 另外, $s \in S$ 满足式(5.2.1)当且仅当

$$2k + 1 \leq s \leq 4k + 1$$

即 $m = 2k + 1$, 于是 $\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1 = (-1)^{(p^2-1)/8}$.

(3) 如果 $p \equiv 5 \pmod{8}$, 可设 $p = 8k + 5$, 则 $(-1)^{(p^2-1)/2} = (-1)^{(2k+1)(4k+3)} = -1$. 另外, $s \in S$ 满足式(5.2.1)当且仅当

$$2k + 1 + \frac{1}{2} \leq s \leq 4k + 2$$

即 $m = 2k + 1$, $\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1$.

(4) 如果 $p \equiv 7 \pmod{8}$, 可设 $p = 8k + 7$, 则 $(-1)^{(p^2-1)/2} = (-1)^{2(2k+3)(2k+1)} = 1$. 另外, $s \in S$ 满足式(5.2.1)当且仅当

$$2k+2 \leq s \leq 4k+3$$

即 $m=2k+2, \left(\frac{2}{p}\right) = (-1)^{2k+2} = 1 = (-1)^{(p^2-1)/2}$.

为更方便快捷地计算 Legendre, 下面介绍 Gauss 二次互反律.

定理 5.4 (Gauss 二次互反律) 设 p, q 是两个互异的奇素数, 则有

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

或

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)$$

证 设 $S = \{1, 2, \dots, (p-1)/2\}, T = \{1, 2, \dots, (q-1)/2\}$, 那么, S, T 分别是模 p, q 的 Gauss 集合. 令

$$S \times T = \{(s, t) \mid s \in S, t \in T\}$$

则 $S \times T$ 表示 \mathbb{R}^2 上的格点 (即坐标都是整数的点) 矩形, 且所含元素的个数为

$$|S \times T| = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

下面求出在矩形内满足不等式

$$1 \leq pt - qs \leq \frac{p-1}{2} \quad (5.2.2)$$

的格点 (s, t) 的个数 m .

如果 $s \in S, t_1, t_2 \in T$, 且格点 $(s, t_1), (s, t_2)$ 都满足式 (5.2.2), 则有

$$p|t_1 - t_2| = |(pt_1 - qs) - (pt_2 - qs)| < \frac{p-1}{2} + \frac{p-1}{2} < p$$

因此, $t_1 = t_2$. 因而断定: 对任意的 $s \in S$, 存在至多一个 $t \in T$ 满足式 (5.2.2). 如果某格点 $(s, t) \in S \times T$ 满足不等式式 (5.2.2), 那么

$$pt - qs = s' \in S \text{ 且 } qs \equiv -s' \pmod{p}$$

由 Gauss 引理可得 $u_q(s) = s'$ 且 $\varepsilon_q(s) = -1$.

反之, 如果 $s \in S$ 且 $\varepsilon_q(s) = -1$, 那么, $qs \equiv -u_q(s) \pmod{p}$, 即存在一个整数 t 使得

$$qs = -u_q(s) + pt$$

由于

$$0 < pt = qs + u_q(s) \leq \frac{q(p-1)}{2} + \frac{p-1}{2} = \frac{(q+1)(p-1)}{2}$$

因此

$$1 \leq t \leq \frac{(q+1)(p-1)}{2p} < \frac{q+1}{2}$$

由 q 是奇素数知

$$1 \leq t \leq \frac{q-1}{2}$$

因此, $t \in T$ 且格点 $(s, t) \in S \times T$ 满足式(5.2.2).

依据上面的讨论可知, 格点 $(s, t) \in S \times T$ 满足式(5.2.2)的个数 m 等于 S 中满足 $\varepsilon_q(s) = -1$ 的 s 的个数. 由 Gauss 引理可得

$$\left(\frac{q}{p}\right) = (-1)^m$$

同理可得

$$\left(\frac{p}{q}\right) = (-1)^n$$

其中, n 等于 $S \times T$ 中满足 $1 \leq qs - pt \leq \frac{q-1}{2}$ 的格点个数, 亦即满足

$$-\frac{q-1}{2} \leq pt - qs \leq -1$$

的格点个数.

由于对任意的 $s \in S, t \in T$ 都有 $pt - qs \neq 0$, 因此

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{m+n}$$

其中, $m+n$ 等于 $S \times T$ 中满足 $-\frac{q-1}{2} \leq pt - qs \leq \frac{p-1}{2}$ 的格点个数.

设 M 表示 $S \times T$ 中满足 $pt - qs > \frac{p-1}{2}$ 的格点个数, N 表示 $S \times T$ 中满足

$pt - qs < -\frac{q-1}{2}$ 的格点个数, 则有

$$m + n + M + N = |S \times T| = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

定义 $S \times T$ 到 $S \times T$ 的一个映射:

$$\varphi: (s, t) \mapsto (s', t')$$

其中, $s' = \frac{p+1}{2} - s, t' = \frac{q+1}{2} - t$.

易证 φ 是一个双射.

且如果 $(s, t) \in S \times T$ 且 $pt - qs > \frac{p-1}{2}$, 则

$$\begin{aligned} pt' - qs' &= p\left(\frac{q+1}{2} - t\right) - q\left(\frac{p+1}{2} - s\right) = \frac{p}{2} - pt - \frac{q}{2} + qs \\ &= -(pt - qs) + \frac{p-1}{2} - \frac{q-1}{2} \end{aligned}$$

$$< -\frac{q-1}{2}$$

这说明 M 中的任一格点 (s, t) , 均存在 N 中的格点 (s', t') 与其对应, 因此, $M \leq N$.

同理, 如果 $(s, t) \in S \times T$ 且 $pt - qs < -\frac{q-1}{2}$, 那么

$$\begin{aligned} pt' - qs' &= p\left(\frac{q+1}{2} - t\right) - q\left(\frac{p+1}{2} - s\right) \\ &= \frac{p}{2} - pt - \frac{q}{2} + qs \\ &= -(pt - qs) + \frac{p-1}{2} - \frac{q-1}{2} \\ &> \frac{p-1}{2} \end{aligned}$$

这说明 $M \geq N$. 故 $M = N$, 从而有

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{m+n} = (-1)^{m+n+2M} = (-1)^{m+n+M+N} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

上述证明比较繁琐, 我们将在后面的综合例题中介绍一个比较简洁的证法. 利用二次互反律计算 Legendre 符号有时非常有效.

例 5.6 计算 $\left(\frac{1185}{1583}\right)$.

解 因为 1583 是素数, 而 $1185 = 3 \times 5 \times 79$. 所以, 由 Legendre 符号性质定理可得

$$\left(\frac{1185}{1583}\right) = \left(\frac{3}{1583}\right) \times \left(\frac{5}{1583}\right) \times \left(\frac{79}{1583}\right)$$

再由二次互反律可得

$$\begin{aligned} \left(\frac{1185}{1583}\right) &= \left(\frac{1583}{3}\right) (-1)^{\frac{1582}{2} \cdot \frac{2}{2}} \times \left(\frac{1583}{5}\right) (-1)^{\frac{1582}{2} \cdot \frac{4}{2}} \times \left(\frac{1583}{79}\right) (-1)^{\frac{1582}{2} \cdot \frac{78}{2}} \\ &= \left(\frac{1583}{3}\right) \times \left(\frac{1583}{5}\right) \times \left(\frac{1583}{79}\right) \\ &= \left(\frac{2}{3}\right) \times \left(\frac{3}{5}\right) \times \left(\frac{3}{79}\right) \\ &= -\left(\frac{5}{3}\right) (-1)^{\frac{1}{2} \cdot \frac{2}{2}} \times \left(\frac{79}{3}\right) (-1)^{\frac{78}{2} \cdot \frac{2}{2}} \\ &= \left(\frac{2}{3}\right) \times \left(\frac{1}{3}\right) \\ &= -1 \end{aligned}$$

练习 5.2

1. 计算下列 Legendre 符号.

$$(1) \left(\frac{8}{5}\right), \quad (2) \left(\frac{15}{17}\right), \quad (3) \left(\frac{2008}{73}\right), \quad (4) \left(\frac{2009}{1583}\right).$$

2. 判断下列方程是否有解. 如有解则求出其全部不同余的解.

$$(1) x^2 \equiv 58 \pmod{77}, \quad (2) x^2 \equiv 429 \pmod{523},$$

$$(3) x^2 - 4x - 7 \equiv 0 \pmod{11}, \quad (4) x^2 - 3x + 5 \equiv 0 \pmod{79}.$$

3. 如果正整数 a 与素数 p 互素, 则

$$\sum_{k=1}^{p-1} \left(\frac{ka}{p}\right) = 0$$

4. 证明当且仅当 p 是形如 $6n-1$ 的素数时, -3 是模 p 的二次非剩余.

5. 设 p, q 都是形如 $4n+3$ 的奇素数, 利用二次互反律证明如果 $x^2 \equiv p \pmod{q}$ 无解, 则 $x^2 \equiv q \pmod{p}$ 有两个解.

6. 设奇素数 $p \equiv -1 \pmod{4}$, 证明

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0 \quad (\text{提示: 利用 } \left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right) \left(\frac{-1}{p}\right))$$

7. 设素数 $p \nmid a$, 证明二次同余方程 $ax^2 + bx + c \equiv 0 \pmod{p}$ 的解的个数为 $1 + \left(\frac{b^2 - 4ac}{p}\right)$.

5.3 Jacobi 符号

在计算 Legendre 符号 $\left(\frac{a}{p}\right)$ 时, 往往需要将 a 分解成标准形式. 当 a 较大时, 这种分解不仅很麻烦, 而且耗时很大. 本节介绍的 Jacobi 符号可有助于解决此问题.

定义 5.4 设 m 是一个正奇数, a 是与 m 互素的正整数, 且 $m = p_1 p_2 \cdots p_n$ (其中 p_1, p_2, \dots, p_n 是可以相同的素数), 定义

$$\prod_{i=1}^n \left(\frac{a}{p_i}\right)$$

为 a 对模 m 的 Jacobi 符号, 记作 $\left(\frac{a}{m}\right)$.

例 5.7 计算 $\left(\frac{2008}{1001}\right)$.

解 $\left(\frac{2008}{1001}\right) = \left(\frac{2008}{7 \times 11 \times 13}\right)$

$$\begin{aligned}
 &= \left(\frac{2008}{7}\right) \left(\frac{2008}{11}\right) \left(\frac{2008}{13}\right) \\
 &= \left(\frac{6}{7}\right) \left(\frac{6}{11}\right) \left(\frac{6}{13}\right) \\
 &= \left(\frac{2}{7}\right) \left(\frac{3}{7}\right) \left(\frac{2}{11}\right) \left(\frac{3}{11}\right) \left(\frac{2}{13}\right) \left(\frac{3}{13}\right) \\
 &= -1
 \end{aligned}$$

定理 5.5 (Jacobi 符号性质定理) 设 m, m' 都是正奇数, $(a, m) = 1, (a, m') = 1, (b, m) = 1, (b, m') = 1$, 那么

$$(1) \text{ 如果 } a \equiv b \pmod{m}, \text{ 则 } \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$

一般地, 设 m 的标准分解式为

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

则

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_t}\right)^{\alpha_t}$$

$$(2) \left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{m'}\right).$$

$$(3) \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right).$$

$$(4) \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = \begin{cases} 1 & m \equiv 1 \pmod{4} \\ -1 & m \equiv 3 \pmod{4} \end{cases}.$$

$$(5) \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} 1 & m \equiv 1, 7 \pmod{8} \\ -1 & m \equiv 3, 5 \pmod{8} \end{cases}.$$

(6) 当 $(m, m') = 1$ 时, 有

$$\left(\frac{m'}{m}\right) \left(\frac{m}{m'}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{m'-1}{2}}$$

或

$$\left(\frac{m'}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{m'-1}{2}} \left(\frac{m}{m'}\right)$$

该性质亦称为二次互反律.

证 (1)、(2)、(3)的证明显然, 下面只证(4)、(5)及(6).

(4) 当 m 为奇素数时显然成立. 现设 m 非素数且 $m = p_1 p_2 \cdots p_n$ 是其素数分解, 其中的 p_i 可能有相同的. 由于

$$m = \prod_{i=1}^n p_i = \prod_{i=1}^n (1 + (p_i - 1)) = 1 + \sum_{i=1}^n (p_i - 1) + R_n$$

其中, R_n 是 $2^n - n - 1$ 个项的和, 且每个和项至少是两个 $p_i - 1$ 的积. 由于每个 p_i

都是奇素数,因此, R_n 的每个和项是 4 的倍数,所以

$$(-1)^{\frac{m-1}{2}} = (-1)^{\frac{\sum_{i=1}^n (p_i-1)}{2}} = (-1)^{\sum_{i=1}^n \frac{p_i-1}{2}} = \prod_{i=1}^n (-1)^{\frac{p_i-1}{2}}$$

从而由 Jacobi 符号的定义得

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^n \left(\frac{-1}{p_i}\right) = \prod_{i=1}^n (-1)^{\frac{p_i-1}{2}} = (-1)^{\frac{m-1}{2}}$$

(5) 证明类似于(4)的证明,请读者自证(注意:此时将 m^2 表示成 $= 1 +$

$\sum_{i=1}^n (p_i^2 - 1) + S_n$,其中, S_n 中每个和项是 64 的倍数).

(6) 设 $m = \prod_{i=1}^n p_i, m' = \prod_{j=1}^{n'} q_j$,其中, $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_{n'}$ 都是素数,则

$$\begin{aligned} \left(\frac{m'}{m}\right) \left(\frac{m}{m'}\right) &= \left(\prod_{i=1}^n \prod_{j=1}^{n'} \left(\frac{q_j}{p_i}\right)\right) \cdot \left(\prod_{i=1}^n \prod_{j=1}^{n'} \left(\frac{p_i}{q_j}\right)\right) \\ &= \prod_{i=1}^n \prod_{j=1}^{n'} \left(\frac{q_j}{p_i}\right) \left(\frac{p_i}{q_j}\right) = \prod_{i=1}^n \prod_{j=1}^{n'} (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} \\ &= (-1)^{\sum_{i=1}^n \sum_{j=1}^{n'} \frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} = (-1)^{\sum_{i=1}^n \frac{p_i-1}{2} \cdot \sum_{j=1}^{n'} \frac{q_j-1}{2}} \end{aligned}$$

在(4)中已证明 $\frac{m-1}{2} \equiv \sum_{i=1}^n \frac{(p_i-1)}{2} \pmod{2}, \frac{m'-1}{2} \equiv \sum_{j=1}^{n'} \frac{(q_j-1)}{2} \pmod{2}$,

因此得

$$\left(\frac{m'}{m}\right) \left(\frac{m}{m'}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{m'-1}{2}}$$

由于任何 Jacobi 符号的值为 ± 1 ,故将上式两边分别乘 $\left(\frac{m}{m'}\right)$,即得

$$\left(\frac{m'}{m}\right) \left(\frac{m}{m'}\right)^2 = (-1)^{\frac{m-1}{2} \cdot \frac{m'-1}{2}} \left(\frac{m}{m'}\right)$$

亦即

$$\left(\frac{m'}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{m'-1}{2}} \left(\frac{m}{m'}\right)$$

例 5.8 计算 $\left(\frac{111}{1001}\right)$ 的值.

解 由 Jacobi 符号的性质定理(3)可得

$$\left(\frac{111}{1001}\right) = \left(\frac{3 \times 37}{1001}\right) = \left(\frac{3}{1001}\right) \left(\frac{37}{1001}\right)$$

利用 Jacobi 符号性质定理(6)分别计算 $\left(\frac{3}{1001}\right)$ 与 $\left(\frac{37}{1001}\right)$ 如下:

$$\left(\frac{3}{1001}\right) = (-1)^{\frac{1}{2} \cdot \frac{1000}{2}} \left(\frac{1001}{3}\right) = \left(\frac{1001}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{37}{1001}\right) = (-1)^{\frac{36}{2} \cdot \frac{1000}{2}} \left(\frac{1001}{37}\right) = \left(\frac{1001}{37}\right) = \left(\frac{2}{37}\right) = (-1)^{\frac{37^2-1}{8}} = (-1)^{171} = -1$$

于是得

$$\left(\frac{111}{1001}\right) = \left(\frac{3}{1001}\right) \left(\frac{37}{1001}\right) = 1$$

例 5.9 若 m 是正奇数, 且 $(a, m) = 1$, 如果 Jacobi 符号 $\left(\frac{a}{m}\right) = -1$, 则 a 是模 m 的二次非剩余; 反之, 若 a 是模 m 的二次非剩余, 则 $\left(\frac{a}{m}\right) = -1$ 不一定成立.

证 若 a 是模 m 的二次剩余, 那么, 同余方程 $x^2 \equiv a \pmod{m}$ 有解, 因而对 m 的任何素数因子 p , 同余方程 $x^2 \equiv a \pmod{p}$ 均有解.

设 m 的标准分解式为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$. 如果 $\left(\frac{a}{m}\right) = -1$, 则

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_t}\right)^{\alpha_t} = -1$$

由于对每个 $i=1, 2, \dots, t$, 有 $\left(\frac{a}{p_i}\right) = \pm 1$, 因此, 必有某 $j \in \{1, 2, \dots, t\}$, 使得 $\left(\frac{a}{p_j}\right)^{\alpha_j} = -1$, 即 $\left(\frac{a}{p_j}\right) = -1$, 这说明 a 为模 p_j 的二次非剩余, 即同余方程 $x^2 \equiv a \pmod{p_j}$ 无解. 因此, 当 $\left(\frac{a}{m}\right) = -1$ 时, a 必是模 m 的二次非剩余. 但是, 当 a 是模 m 的二次非剩余, 则 $\left(\frac{a}{m}\right) = -1$ 不一定成立. 如取满足 $p \equiv -1 \pmod{4}$ 的素数 p , $m = p^2$, 则方程 $x^2 \equiv -1 \pmod{m}$ 无解, 但 $\left(\frac{-1}{m}\right) = \left(\frac{-1}{p^2}\right) = \left(\frac{-1}{p}\right)^2 = (-1)^2 = 1$. 又如 Jacobi 符号 $\left(\frac{11}{391}\right) = 1$, 但 $x^2 \equiv 11 \pmod{391}$ 无解.

练习 5.3

1. 计算下列 Jacobi 符号.

$$(1) \left(\frac{11}{21}\right). \quad (2) \left(\frac{127}{110}\right). \quad (3) \left(\frac{1231}{1230}\right). \quad (4) \left(\frac{2008}{2009}\right).$$

2. 利用计算 Jacobi 符号的方法求下列 Legendre 符号的值.

$$(1) \left(\frac{853}{1409}\right). \quad (2) \left(\frac{777}{2777}\right). \quad (3) \left(\frac{2114}{6269}\right).$$

3. 利用 Jacobi 符号说明下列同余方程哪些无解, 哪些有解?

$$(1) x^2 \equiv 78 \pmod{787}. \quad (2) x^2 \equiv 100 \pmod{1333}.$$

$$(3) x^2 \equiv -1305 \pmod{1459}, \quad (4) x^2 \equiv 108 \pmod{19291}.$$

4. 求与 15 互素的正整数 m , 使得 Jacobi 符号 $\left(\frac{15}{m}\right) = 1$.

5. 设 a 是正整数, b 是正奇数. 证明

$$\left(\frac{a}{2a+b}\right) = (-1)^{\frac{a(a-1)}{2}} \left(\frac{a}{b}\right)$$

6. 设 m 是非平方正奇数. 证明存在整数 a 使得

$$(a, m) = 1 \text{ 且 } \left(\frac{a}{m}\right) = -1$$

7. 利用上题证明下列结论.

(1) $\sum_k \left(\frac{k}{n}\right) = 0$, 其中, 求和表示对 k 取遍 n 的简系.

(2) 证明在模 n 的简系中, 使 $\left(\frac{k}{n}\right) = 1$ 的 k 的个数等于使 $\left(\frac{k}{n}\right) = -1$ 的 k 的个数.

5.4 利用 Maple 计算 Legendre 符号与 Jacobi 符号

在 Maple 中, 计算 Legendre 符号与 Jacobi 符号的函数分别是 $\text{legendre}(a, p)$ 与 $\text{jacobi}(a, b)$, 因这两个函数都是数论, 所以, 在使用这两个函数前必须先调用数论软件包“numtheory”. 如下所示:

```
>with(numtheory):
legendre(74, 101);
jacobi(2008, 1001);
-1
-1
```

即 $\left(\frac{74}{101}\right) = -1, \left(\frac{2008}{1001}\right) = -1$.

又如

```
>jacobi(-286, 4272943);
legendre(120, 110);
1
```

Error, invalid input: numtheory: - legendre expects its 2nd argument, p, to be of type Or(prime, Not(constant)), but received 110.

上面计算说明 $\left(\frac{-286}{4272943}\right) = 1$, 但在计算 $\text{legendre}(120, 110)$ 时, 由于输入的第一个整数 110 非素数, 所以提示输入出错.

在求一些涉及较大参数的 Legendre 符号与 Jacobi 符号时,手算往往是很不实际的,如计算 $\left(\frac{2000008}{373587989}\right)$ 与 $\left(\frac{3200001}{111111111111111}\right)$, 而利用 Maple 函数则可较快地计算出它们的值分别为 1 和 -1.

当函数 $\text{legendre}(a, p)$ 或 $\text{Jacobi}(a, b)$ 中的两个参数不互素时,则输出的计算为 0. 如下所示:

```
>legendre (14, 7);
Jacobi (21, 69);
0
0
```

也可以通过编一个简单的 Maple 程序来计算 Legendre 符号与 Jacobi 符号.

```
>Legendre: = proc(n, p)
  local L;
  if irem(n, p) = 0 then
    L: = 0;
  elif r((p-1)/2) mod p = 1 then
  >   L: = 1;
    else L: = -1;
  fi;
  L;
end;
```

例如,分别求 $\left(\frac{195}{1901}\right)$, $\left(\frac{74}{101}\right)$ 及 $\left(\frac{365}{1847}\right)$ 的值.

```
>Legendre(74, 101), Legendre(195, 1901), Legendre(365, 1847);
-1, -1, 1
```

利用 Pepin 检测定理(本章综合例 3),可判定一个 Fermat 数 $F_m = 2^{2^m} + 1$ 是否为素数. 但当 m 很大时,不利用编程来判断 $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$ 是否成立一般较困难. 但利用 $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$ 编写的判断 F_m 是否为素数的 Maple 程序在 m 较大时也不是很有效,如下所示:

```
>with(numtheory):
isFmPrime: = proc(m::posint)
local r, s, t;
r: = 2^(2^m) + 1;
s: = (r-1)/2;
t: = mods(3^s, r);
if t = -1 printf("F[ %d] is prime!", m);
else
```

```

printf("F[ %d] is not prime!", m):
end if;
end;

```

上面的程序函数 isFmPrime() 的功用是当输入 m 的值后, 判断 Fermat 数 $F[m]=2^{2^m}+1$ 是否为素数. 如下所示:

```

> isFmPrime(4);
F[4] is prime!

```

这表示当 $m=4$ 时, $F[m]$ 是素数. 但当 $m=5$ 时, 函数 isFmPrime() 则不能判断 $F[m]$ 是否为素数, 这是因为程序运行中数据 3^{2^5-1} 太大, 造成数据溢出, 不能继续运行. 感兴趣的读者可考虑对该程序函数进行优化.

下面介绍一个新的计算 Jacobi 符号的算法.

设 a 是正整数, b 是与 a 互素的奇正整数, 且 $a > b$. 对 a 与 b 作带余除法, 并将余数分解成 2 的非负整数幂与奇正整数之积, 可得

$$r_0 = r_1 q_1 + 2^{t_1} r_2, \quad r_0 = a, \quad r_1 = b$$

再对 r_1 与 r_2 作带余除法, 并将余数分解成 2 的非负整数幂与奇正整数之积. 如此继续, 直至作某第 n 次带余除法后得到的余数是 2 的非负整数幂, 即可得

$$\begin{aligned}
 r_1 &= r_2 q_2 + 2^{t_2} r_3 \\
 r_2 &= r_3 q_3 + 2^{t_3} r_4 \\
 &\vdots \\
 r_{n-2} &= r_{n-1} q_{n-1} + 2^{t_{n-1}} r_n \\
 r_{n-1} &= r_n q_n + 2^{t_n} r_{n+1}
 \end{aligned}$$

那么, 利用 Jacobi 符号性质定理可证得

$$\left(\frac{a}{b}\right) = (-1)^{\sum_{i=1}^n \frac{t_i(r_i^2-1)}{8} + \sum_{j=1}^{n-1} \frac{(r_j-1)(r_{j+1}-1)}{4}}$$

下面是用 Maple 编程实现该算法的程序函数 Jacobi().

```

> with(numtheory):
Jacobi := proc(a::posint, b::posint)
local i, q, r, s, t, n, u, v;
if igcd(2 * a, b) <> 1 then printf("The input is error, please input again!")
else
n := 1:
r[0] := a: r[1] := b: q[2] := iquo(r[0], r[1]):
r[2] := irem(r[0], r[1]):
t[1] := 0:
while igcd(r[2], 2) <> 1 do
t[1] := t[1] + 1:

```

```

r[2]: = r[2]/2:
      end do:
for i from 0 while r[i+2]<>1
do
  n: = n+1:
  q[i+2]: = iquo(r[i+1],r[i+2]):
  r[i+3]: = irem(r[i+1],r[i+2]):
  t[i+2]: = 0:
  while igcd(r[i+3],2)<>1 do
    t[i+2]: = t[i+2]+1:
    r[i+3]: = r[i+3]/2:
  end do:
  end do:
u: = add(t[k] * (r[k]^2 - 1)/8, k=1..n):
v: = add((r[k] - 1) * (r[k+1] - 1)/4, k=1..n-1):
print((-1)^(u+v));
end if:
end;

```

例如,可分别求得 Jacobi 符号 $\left(\frac{44401}{11119}\right)$ 与 $\left(\frac{20000008}{11111119}\right)$ 的值分别为 1 和 -1.

```

>Jacobi(44401,11119);
Jacobi(20000008,11111119);

```

1

-1

第5章综合例题

例1 如果 p 和 $2p+1$ 都是奇素数,那么,整数 $(-1)^{(p-1)/2} \cdot 2$ 是 $2p+1$ 的一个原根.

证 分 $p \equiv 1 \pmod{4}$ 与 $p \equiv 3 \pmod{4}$ 两种情况来讨论.

(1) 当 $p \equiv 1 \pmod{4}$ 时,有 $(-1)^{(p-1)/2} \cdot 2 = 2$. 由于 $\varphi(2p+1) = 2p$, 所以, 2 对模 $2p+1$ 的阶只能是 $1, 2, p, 2p$ 中之一. 由例 5.6 可得

$$\left(\frac{2}{2p+1}\right) \equiv (-1)^{((2p+1)^2-1)/8} \equiv (-1)^{p(p+1)/2} \equiv -1 \pmod{2p+1}$$

另外,由 Legendre 符号性质定理(3)可得 $\left(\frac{2}{2p+1}\right) \equiv 2^{(2p+1-1)/2} \equiv 2^p \pmod{2p+1}$, 因而 $2^p \equiv -1 \pmod{2p+1}$, 即 2 对模 $2p+1$ 的阶不可能为 p . 此外, 2 对模 $2p+1$ 的阶也不能为 $1, 2$. 因此, 2 对模 $2p+1$ 的阶只能是 $2p$, 故 2 是

模 $2p+1$ 的一个原根.

(2) 当 $p \equiv 3 \pmod{4}$ 时, 有 $(-1)^{(p-1)/2} \cdot 2 = -2$. 且由例 5.6 及 Legendre 符号性质定理(3) 可得

$$\begin{aligned} \left(\frac{-2}{2p+1}\right) &= \left(\frac{-1}{2p+1}\right) \left(\frac{2}{2p+1}\right) \equiv (-1)^p (-1)^{\frac{(2p+1)^2-1}{8}} \\ &= (-1)(-1)^{p(p+1)/2} = -1 \pmod{2p+1} \end{aligned}$$

及 $\left(\frac{-2}{2p+1}\right) \equiv (-2)^p \pmod{2p+1}$, 则有 $(-2)^p \equiv -1 \pmod{2p+1}$, 从而知 -2 对模 $2p+1$ 的阶不可能是 p , 所以, -2 是模 $2p+1$ 的一个原根.

例 2 证明形如 $8n+3$ 的素数有无穷多个.

证 设形如 $8n+3$ 的素数只有有限个 p_1, p_2, \dots, p_t . 令 $m = (p_1 p_2 \cdots p_t)^2 + 2$, 则 $m \equiv 3 \pmod{8}$. 设 p 是 m 的任一素因子, 则 $p \neq p_i$ 且 $(p_1 p_2 \cdots p_t)^2 + 2 \equiv 0 \pmod{p}$, 即 $(p_1 p_2 \cdots p_t)^2 \equiv -2 \pmod{p}$, 亦即 -2 是模 p 的二次剩余, 因此 $\left(\frac{-2}{p}\right) = 1$. 但另外 $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = (-1)^{(p-1)/2} (-1)^{(p^2-1)/8} = (-1)^{(p+5)(p-1)/8}$, 故 $(p+5)(p-1)/8$ 应为偶数, 于是 $p = 8n+1$ 或 $p = 8n+3$. 但由 $m \equiv 3 \pmod{8}$ 知 m 的素因数不能全为 $8n+1$ 的形式, 故 m 的素因数必有形如 $8n+3$ 的. 这说明除 p_1, p_2, \dots, p_t 外还有形如 $8n+3$ 的素数, 矛盾.

例 3 Fermat 数 $F_m = 2^{2^m} + 1$ 是素数当且仅当 $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$. 且当 F_m 是素数时, 3 是 F_m 的一个原根.

证 充分性 设 $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$, 两边平方得

$$3^{F_m-1} \equiv 1 \pmod{F_m}$$

若 p 是 F_m 的任一素因子, 则 $3^{(F_m-1)/2} \equiv -1 \pmod{p}$ 且 $3^{F_m-1} \equiv 1 \pmod{p}$, 于是 $\text{ord}_p 3 \uparrow \frac{F_m-1}{2}$ 但 $\text{ord}_p 3 \mid (F_m-1)$, 即 $\text{ord}_p 3 \uparrow 2^{2^m-1}$ 但 $\text{ord}_p 3 \mid 2^{2^m}$, 因而有 $\text{ord}_p 3 = 2^{2^m} = F_m - 1$. 另一方面, 由 Fermat 小定理知 $3^{p-1} \equiv 1 \pmod{p}$, 于是 $\text{ord}_p 3 \leq p-1$, 即得 $F_m - 1 \leq p-1$, 亦即 $F_m \leq p$, 从而由 p 是 F_m 的素因子得 $F_m = p$ 是素数.

必要性 设 $F_m = 2^{2^m} + 1$ 是素数, 则由 Legendre 符号性质定理(3) 得

$$\left(\frac{3}{F_m}\right) \equiv 3^{\frac{F_m-1}{2}} \pmod{F_m}$$

另外, 由二次互反律得

$$\left(\frac{3}{F_m}\right) = (-1)^{\frac{F_m-1}{2}} \left(\frac{F_m}{3}\right) = \left(\frac{F_m}{3}\right)$$

由于 $F_m \equiv -1 \pmod{3}$, 所以 $\left(\frac{F_m}{3}\right) = \left(\frac{-1}{3}\right) = -1$, 因此得 $3^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}$.

当 F_m 是素数时, 有 $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$, 即有 $3^{(F_m-1)} \equiv 1 \pmod{F_m}$ 或 $3^{\varphi(F_m)} \equiv 1 \pmod{F_m}$, 且 $3^{\varphi(F_m)/2} \equiv -1 \pmod{F_m}$. 从而推得对任何正整数 k , $3^k \not\equiv 1 \pmod{F_m}$, 因而 3 是 F_m 的一个原根.

注 在一些文献中, 例 3 被称为 Pepin 检测定理.

例 4 证明二次互反律.

证 这里用另一方法重新证明二次互反律, 整个证明过程分三个步骤.

(1) 先证 Gauss 引理. 这里 Gauss 引理的描述与定理 5.3 的叙述不同: 设 p 是奇素数, n 是任一正整数, 且 $p \nmid n$. 如 m 是下列 $(p-1)/2$ 个数:

$$n, 2n, \dots, (p-1)n/2$$

中取模 p 后其最小正余数大于 $p/2$ 的个数, 则 $\left(\frac{n}{p}\right) = (-1)^m$. 下面证明此结论.

记 a_1, a_2, \dots, a_m 及 b_1, b_2, \dots, b_l ($l = (p-1)/2 - m$) 分别表示所有 $n, 2n, \dots, ((p-1)/2)n$ 取模 p 后得到的最小正余数大于 $p/2$ 者与小于 $p/2$ 者, 则对任意 i ($1 \leq i \leq m$) 与 k ($1 \leq k \leq (p-1)/2 - m$), 有 $p - a_i \neq b_k$. 否则, 若有 $b_i = p - a_s$, 则 $p = a_s + b_i$. 由 a_s 及 b_i 的定义知, 存在正整数 c 与 d 满足 $cn + dn \equiv 0 \pmod{p}$ 及 $1 \leq c, d \leq (p-1)/2$. 于是, $p \mid (c+d)n$, 亦即 $p \mid (c+d)$ 或 $p \mid n$, 这不可能成立. 因此有

$$\{p - a_1, p - a_2, \dots, p - a_m, b_1, b_2, \dots, b_k\} = \{1, 2, \dots, (p-1)/2\}$$

从而

$$\prod_{i=1}^m (p - a_i) \prod_{j=1}^l b_j = \prod_{k=1}^{(p-1)/2} k$$

由于上等式左端等于

$$\begin{aligned} \prod_{i=1}^m (p - a_i) \prod_{j=1}^l b_j &\equiv (-1)^m \prod_{i=1}^m a_i \prod_{j=1}^l b_j \equiv (-1)^m \prod_{k=1}^{(p-1)/2} kn \\ &\equiv (-1)^m n^{(p-1)/2} \prod_{k=1}^{(p-1)/2} k \pmod{p} \end{aligned}$$

于是有

$$n^{(p-1)/2} \equiv (-1)^m \pmod{p}$$

故由 Legendre 符号性质定理(3)得

$$\left(\frac{n}{p}\right) = (-1)^m$$

(2) 设 p 为奇素数, q 是与 $2p$ 互素的正整数, 则有

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p}\right]}$$

对任意满足 $1 \leq s \leq (p-1)/2$ 的正整数 s , 由带余除法定理可设

$$sq = p \left[\frac{sq}{p} \right] + r_s, \quad 0 \leq r_s < p$$

将上式两边对 s 求和,得

$$\prod_{s=1}^{(p-1)/2} sq = p \sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right] + \sum_{s=1}^{(p-1)/2} r_s$$

即有

$$q \cdot \frac{p^2-1}{8} = p \sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right] + \sum_{s=1}^{(p-1)/2} r_s \quad (5.1)$$

不妨设 r_1, r_2, \dots, r_m 为 $r_1, r_2, \dots, r_{(p-1)/2}$ 中所有大于 $p/2$ 的余数,则

$$\{p-r_1, p-r_2, \dots, p-r_m, r_{m+1}, r_{m+2}, \dots, r_{(p-1)/2}\} = \{1, 2, \dots, (p-1)/2\}$$

于是

$$\sum_{i=1}^m (p-r_i) + \sum_{j=m+1}^{(p-1)/2} r_j = \sum_{k=1}^{(p-1)/2} k$$

即有

$$mp - \sum_{i=1}^m r_i + \sum_{j=m+1}^{(p-1)/2} r_j = \frac{p^2-1}{8} \quad (5.2)$$

由式(5.1)与式(5.2)推得

$$mp = (1-q) \frac{p^2-1}{8} + p \sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right] + 2 \sum_{s=m+1}^{(p-1)/2} r_s$$

从而由 p 是奇数得

$$\begin{aligned} (-1)^m &= (-1)^{mp} = (-1)^{(1-q)\frac{p^2-1}{8} + p \sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right] + 2 \sum_{s=m+1}^{(p-1)/2} r_s} \\ &= (-1)^{(1-q)\frac{p^2-1}{8}} \cdot (-1)^{p \sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right]} \cdot (-1)^{2 \sum_{s=m+1}^{(p-1)/2} r_s} \\ &= (-1)^{p \sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right]} \\ &= (-1)^{\sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right]} \end{aligned}$$

所以得

$$\left(\frac{q}{p} \right) = (-1)^m = (-1)^{\sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right]}$$

(3) 证明结论: 设 p 与 q 是互异的奇素数, 则有

$$\sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right] + \sum_{t=1}^{(q-1)/2} \left[\frac{tp}{q} \right] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

如图 5.1 所示, 整个矩形中所含格点的个数等于直线 $y = \frac{q}{p}x$ 所分成的两个三角形内所含格点的个数之和. 由于上、下三角形内以及矩形内所含格点的个数分别为

$$\sum_{t=1}^{(q-1)/2} \left[\frac{tp}{q} \right], \sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right] \quad \text{及} \quad \frac{p-1}{2} \cdot \frac{q-1}{2}$$

因此即有

$$\sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right] + \sum_{t=1}^{(q-1)/2} \left[\frac{tp}{q} \right] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

依据(2)与(3)所证即得

$$\begin{aligned} \left(\frac{q}{p} \right) \cdot \left(\frac{p}{q} \right) &= (-1)^{\sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right]} \cdot (-1)^{\sum_{t=1}^{(q-1)/2} \left[\frac{tp}{q} \right]} \\ &= (-1)^{\sum_{s=1}^{(p-1)/2} \left[\frac{sq}{p} \right] + \sum_{t=1}^{(q-1)/2} \left[\frac{tp}{q} \right]} \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \end{aligned}$$

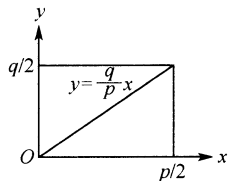


图 5.1

例 5 本例介绍二次互反律的一个新证明方法,它是 2004 年 Kim 发表在美国数学月刊第 111 卷第 1 期的一篇文章中的一个比较简单的新证明。

证 证明分为 6 步. 设 p 与 q 是互异的奇素数,且令

$$R = \{a \mid 1 \leq a \leq (pq-1)/2, (a, pq) = 1\}, S = \{a \mid 1 \leq a \leq (pq-1)/2, (a, p) = 1\},$$

$$T = \{q \cdot 1, q \cdot 2, \dots, q \cdot (p-1)/2\}, A = \prod_{a \in R} a, \text{ 则}$$

(1) T 是 S 的真子集,且 $R = S - T$.

$$(2) A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p} \right) \pmod{p}.$$

这是因为由(1)得

$$\begin{aligned} A &= \prod_{a \in R} a = \prod_{a \in S-T} a = \frac{\prod_{a \in S} a}{\prod_{a \in T} a} \\ &= \frac{\prod_{i=1}^{(p-1)/2} \left(\frac{(q-1)p}{2} + i \right) \cdot \prod_{k=0}^{(q-3)/2} \prod_{l=1}^{p-1} (kp+l)}{\left(\frac{p-1}{2} \right)! \cdot q^{\frac{p-1}{2}}} \\ &\equiv \frac{\prod_{i=1}^{(p-1)/2} i \cdot \prod_{k=0}^{(q-3)/2} \prod_{l=1}^{p-1} l}{\left(\frac{p-1}{2} \right)! \cdot q^{\frac{p-1}{2}}} \pmod{p} \\ &\equiv \frac{((p-1)!)^{(q-1)/2}}{q^{\frac{p-1}{2}}} \pmod{p} \end{aligned}$$

再由 Wilson 定理及 Legendre 符号性质定理(3)有 $(p-1)! \equiv -1 \pmod{p}$,

$\left(\frac{q}{p} \right) \equiv q^{(p-1)/2} \pmod{p}$, 从而得

$$\left(\frac{q}{p}\right)A \equiv (-1)^{\frac{q-1}{2}} \pmod{p}$$

即

$$A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$$

(3) 由 $A = \prod_{a \in R} a$ 中 p 与 q 的对称性即得

$$A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}$$

(4) 如果 $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$, 则由(2)与(3)即得

$$A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{pq}, \quad \text{或 } A \equiv \pm 1 \pmod{pq}$$

反之,若 $A \equiv 1 \pmod{pq}$, 则 $A \equiv 1 \pmod{p}$ 且 $A \equiv 1 \pmod{q}$. 因此,由(2)与(3)即得

$$(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \equiv 1 \pmod{p} \quad \text{与} \quad (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \equiv 1 \pmod{q}$$

由于 $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right)$ 与 $(-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$ 等于 1 或 -1, 故必得 $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = 1$.

若 $A \equiv -1 \pmod{pq}$, 则同理可证 $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = -1$.

所以,当且仅当 $A \equiv \pm 1 \pmod{pq}$ 时,有 $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$.

(5) 现证明 $A \equiv 1$ 或 $-1 \pmod{pq}$ 当且仅当 $p \equiv q \equiv 1 \pmod{4}$.

令

$$U = \{a \in R \mid a^2 \equiv \pm 1 \pmod{pq}\}$$

对任 $a \in R$, 方程 $ax \equiv 1 \pmod{pq}$ 在 pq 的最小正缩系中存在唯一解 a' , 即 $a' \in R$ 或 $a' \in R' = \{z \mid (pq-1)/2 < z \leq pq-1, (z, pq) = 1\}$. 当 $a' \in R'$ 时, 令 $a'' = pq - a'$, 则 $a'' \in R$ 且 $aa'' \equiv -1 \pmod{pq}$. 因此, 对应关系 $a \mapsto a'$ 或 $a \mapsto a''$ 是 R 上的一个一一对应. 在积 $A = \prod_{a \in R} a$ 将整数 a 与 $a' (\neq a)$ 或 $a'' (\neq a)$ 配对相乘, 则得到

$$A = \prod_{a \in R} a \equiv \pm \prod_{a \in U} a \pmod{pq}$$

另外, 由中国剩余定理知同余方程 $x^2 \equiv 1 \pmod{pq}$ 在 R 中恰有 2 个不同的解 1 与 $c (\in R)$, 而同余方程 $x^2 \equiv -1 \pmod{pq}$ 当且仅当 $p \equiv q \equiv 1 \pmod{4}$ 时在 R 中恰有

2个不同的解 ι 与 $\iota \cdot c$, 则当且仅当 $p \equiv q \equiv 1 \pmod{4}$ 时, 有

$$\begin{aligned} A &\equiv \pm \prod_{a \in U} a \equiv \pm (1 \cdot c \cdot \iota \cdot (\iota \cdot c)) \equiv \pm (\iota^2 \cdot c^2) \\ &\equiv \pm (-1 \cdot 1) \equiv \mp 1 \pmod{pq} \end{aligned}$$

否则,

$$A \equiv \pm \prod_{a \in U} a \equiv \pm (1 \cdot c) \equiv \pm c \not\equiv \pm 1 \pmod{pq}$$

(6) 由(4)与(5)的证明得知

$$\text{当且仅当 } p \equiv q \equiv 1 \pmod{4} \text{ 时, } (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

即

$$\text{当且仅当 } p \equiv q \equiv 1 \pmod{4} \text{ 时, } \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{q-1}{2}}$$

(7) 由于

$$\frac{p+1}{2} \cdot \frac{q+1}{2} \equiv \begin{cases} 1 \pmod{2}, & \text{当且仅当 } p \equiv q \equiv 1 \pmod{4} \\ 0 \pmod{2}, & \text{否则} \end{cases}$$

因而

$$\begin{aligned} \frac{p-1}{2} \cdot \frac{q-1}{2} &= \frac{pq - p - q + 1}{4} = \frac{pq + p + q + 1}{4} - \frac{(p-1) + (q-1)}{2} - 1 \\ &\equiv \frac{p+1}{2} \cdot \frac{q+1}{2} + \frac{p-1}{2} + \frac{q-1}{2} + 1 \pmod{2} \\ &\equiv \begin{cases} \frac{p-1}{2} + \frac{q-1}{2} \pmod{2}, & \text{当且仅当 } p \equiv q \equiv 1 \pmod{4} \\ \frac{p-1}{2} + \frac{q-1}{2} + 1 \pmod{2}, & \text{否则} \end{cases} \end{aligned}$$

所以, 当且仅当 $p \equiv q \equiv 1 \pmod{4}$ 成立时, 有

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

而当且仅当 $p \equiv q \equiv 1 \pmod{4}$ 不成立时, 有

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = -(-1)^{\frac{p-1}{2} + \frac{q-1}{2}} = (-1)^{\frac{p-1}{2} + \frac{q-1}{2} + 1} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

总之, 对任何互异的素数 p 与 q , 有

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

思考题、研究题五

1. 利用二次互反律证明对任意奇素数 p , 有

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{12} \\ -1, & p \equiv -1 \pmod{12} \end{cases}$$

2. 如果 p 为奇素数, 那么, $\sum_{a=1}^{p-2} \left(\frac{a(a+1)}{p}\right) = -1$.

3. 若 $p=2^k+1$ 是一个素数, 那么, 模 p 的二次非剩余一定是模 p 的原根.

4. 证明如果 p 和 $q=2p+1$ 都是素数, 那么, -4 是 q 的一个原根; 如果 p 和 $q=4p+1$ 都是素数, 那么, 2 是 q 的一个原根.

5. 设 p, q 是互异的两个奇素数. 证明

$$\sum_{\substack{x_1+\dots+x_q \equiv q \pmod{p} \\ 1 \leq x_i \leq p-1}} \left(\frac{x_1 \cdots x_q}{p}\right) \equiv 1 \pmod{q}$$

这里求和是对所有满足条件 $x_1 + \dots + x_q \equiv q \pmod{p}$ 及 $1 \leq x_i \leq p-1 (i=1, \dots, q)$ 的有序 q -元整数组 (x_1, \dots, x_q) 进行.

6. 设 p 为奇素数, a, b, c 是整数, 证明下列结论.

(1) 同余方程

$$x^2 - y^2 \equiv a \pmod{p}$$

解的个数为

$$\begin{cases} p-1, & p \nmid a \\ 2p-1, & p \mid a \end{cases}$$

(2) 证明求和等式

$$\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right) = \begin{cases} -1, & p \nmid a \\ p-1, & p \mid a \end{cases}$$

(3) 设 $p \nmid a, \Delta = b^2 - 4ac$, 则

$$\sum_{x=0}^{p-1} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right), & p \nmid \Delta \\ (p-1)\left(\frac{a}{p}\right), & p \mid \Delta \end{cases}$$

(4) 设 $p \nmid ab$, 则同余方程

$$ax^2 + by^2 \equiv c \pmod{p}$$

解的个数为

$$N = \begin{cases} p - \left(\frac{-ab}{p}\right), & p \nmid c \\ p + (p-1)\left(\frac{-ab}{p}\right), & p \mid c \end{cases}$$

7. 设 a 与 $b=r_0$ 是两个互异的奇素数,且有

$$\begin{aligned} a &= r_0 q_1 + \varepsilon_1 r_1 \\ r_0 &= r_1 q_2 + \varepsilon_2 r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + \varepsilon_n r_n \end{aligned}$$

对所有 $i=1, 2, \dots, n$, q_i 是非负偶整数, r_i 是满足条件 $r_i < r_{i-1}$ 及 $r_n=1$ 的正整数, $\varepsilon_i = \pm 1$.

(1) 证明

$$\left(\frac{a}{b}\right) = (-1)^{\sum_{i=1}^n \frac{r_{i-1}-1}{2} \cdot \frac{\varepsilon_i r_i - 1}{2}}$$

(2) 设 N 是满足条件 $1 \leq i \leq n$ 及 $r_{i-1} \equiv \varepsilon_i r_i \equiv 3 \pmod{4}$ 的所有正整数 i 的个数, 则

$$\left(\frac{a}{b}\right) = (-1)^N$$

8. 设 p 与 q 是互异的奇素数, $i = \sqrt{-1}$. 证明下列结论.

(1) 设 n 是正整数, e 是自然对数的底. 证明对任意满足 $0 \leq k \leq n-1$ 的整数 k , $e^{(2\pi i/n)k}$ 是 n 次单位根, 且是 n 次本原单位根的充要条件是 $(k, n) = 1$.

(2) 设 ζ 是 n 次单位根, $k \equiv l \pmod{n}$, 则 $\zeta^k = \zeta^l$. 且如果 ζ 是 n 次本原单位根, 则 $k \equiv l \pmod{n}$ 当且仅当 $\zeta^k = \zeta^l$.

(3) 令 $f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i \sin(2\pi z)$. 则有 $f(z+1) = f(z)$, $f(-z) = -f(z)$, 且 $n/2$ 是 $f(z)$ 的唯一实零点.

(4) 令 $\zeta = e^{2\pi i/n}$, 则 $x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y)$.

(5) 若 n 是奇正整数, 则

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right)$$

(6) 若 a 是与 p 互素的整数, 则

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right)$$

(7) 利用以上结论证明二次互反律.

第 6 章 不定方程理论

系数为整数、未知数个数少于方程个数的方程或方程组称为不定方程. 不定方程是初等数论中的一个重要内容. 最基本的方程是二元一次不定方程. 本章在 6.1 节介绍了二元一次不定方程的有解的判别条件及解法. 多元一次不定方程可转化成若干个二元一次方程来进行求解. 在其后的三节中简单讲述了整数的平方和表示及勾股不定方程的求解问题, 它们其实都是二次(伪)齐次不定方程的求解问题^①. 不定方程中最著名的方程是 6.5 节介绍的 Fermat 方程(亦即 Fermat 最后定理所涉及的 n 次齐次不定方程), 其次是二次伪齐次的 Pell 方程 $x^2 - dy^2 = n$. Pell 方程的求解问题是多年来初等数论研究的一个热点课题, 取得的有关研究成果也非常丰富. 对求解 Pell 方程感兴趣的读者可参考华罗庚的经典著作《数论导引》第十二章 § 13 及 Rosen 所著《初等数论及其应用》13.4 节, 本书不讨论 Pell 方程的求解问题. 6.6 节介绍了利用 Maple 数学软件求解一些不定方程问题.

6.1 一次不定方程

定义 6.1 二元一次不定方程是

$$a_1x + a_2y = b \quad (6.1.1)$$

其中, b, a_1, a_2 是给定的整数且 $a_1a_2 \neq 0$.

定理 6.1 方程(6.1.1)有整数解的充分与必要条件是

$$(a_1, a_2) \mid b$$

证 如果方程(6.1.1)有解, 那么, 由 $(a_1, a_2) \mid a_1$ 及 $(a_1, a_2) \mid a_2$ 得 $(a_1, a_2) \mid b$. 反之, 设 $(a_1, a_2) = d \mid b, b = dd_1$. 由 Bezout 恒等式可知, 存在整数 u, v 使得 $a_1u + a_2v = d$, 于是, 两边乘 d_1 得 $a_1ud_1 + a_2vd_1 = dd_1$. 取 $x = ud_1, y = vd_1$, 则得到方程(6.1.1)的一组解.

例 6.1 求方程

$$3x + 15y = 17$$

^① 这里称一个不定方程是伪齐次的, 如果该不定方程中每个非常数项的未知数的次数和是相同的; 不含常数项的伪齐次不定方程称为齐次不定方程.

的整数解.

解 由于 $(3, 15)=3$, 而 $3 \nmid 17$, 由定理 6.1 可知方程 $3x+15y=17$ 无整数解. 当方程(6.1.1)有解时, 可以用下面的定理求出其所有解.

定理 6.2 设 $(a_1, a_2)=1$, 且方程(6.1.1)有一组整数解 $x=x_0, y=y_0$, 则方程(6.1.1)的一切解可表示成

$$x = x_0 + a_2 t, \quad y = y_0 - a_1 t \quad (6.1.2)$$

其中, $t=0, \pm 1, \pm 2, \dots$.

证 由 $x=x_0, y=y_0$ 是方程(6.1.1)一组整数解, 得 $a_1 x_0 + a_2 y_0 = b$, 因此

$$a_1(x_0 + a_2 t) + a_2(y_0 - a_1 t) = a_1 x_0 + a_2 y_0 = b$$

即对任意的整数 t , 方程(6.1.2)是方程(6.1.1)的解.

反之, 设 x_1, y_1 是为方程(6.1.1)的任意一组解, 则

$$a_1 x_1 + a_2 y_1 = b$$

与

$$a_1 x_0 + a_2 y_0 = b$$

同时成立, 因此

$$a_1(x_0 - x_1) + a_2(y_0 - y_1) = 0$$

而 $(a_1, a_2)=1$, 因此, $a_2 \mid (x_1 - x_0), a_1 \mid (y_1 - y_0)$. 若设 $x_1 - x_0 = a_2 t$, 即 $x_1 = x_0 + a_2 t$, 代入方程(6.1.1)可得 $y = y_0 - a_1 t$.

当 $(a_1, a_2)=1, a_1 > 0, a_2 > 0$ 时, 利用辗转相除法可以求出方程(6.1.1)的一组特解(见 1.3 节), 即

$$x = (-1)^{n-1} Q_n, \quad y = (-1)^n P_n$$

其中, $P_0=1, P_1=q_1, P_k=q_k P_{k-1} + P_{k-2}, Q_0=0, Q_1=1, Q_k=q_k Q_{k-1} + Q_{k-2}, k=2, 3, \dots, n$.

推论 6.1 设 $(a_1, a_2)=d$, 方程(6.1.1)有一组整数解 $x=x_0, y=y_0$, 则方程(6.1.1)的一切解(即通解)可表示成

$$x = x_0 + \frac{a_2}{d} t, \quad y = y_0 - \frac{a_1}{d} t \quad (6.1.3)$$

其中, $t=0, \pm 1, \pm 2, \dots$.

例 6.2 求方程

$$7x + 4y = 100$$

的整数解.

解 先解 $7x+4y=1$. 由于 $(7, 4)=1$, 因此, 方程 $7x+4y=1$ 有一组整数解 $x=(-1)^{2-1}=-1, y=(-1)^2 \times 2=2$, 故得原方程 $7x+4y=100$ 的一组特解, 如下:

$$x = -100, \quad y = 200$$

由定理 6.2 可得其一切解可表示成

$$x = -100 - 4t, \quad y = 200 + 7t, \quad t = 0, \pm 1, \pm 2, \dots$$

例 6.3 求方程

$$111x - 321y = 75$$

的一切整数解.

解 由于 $(111, -321) = 3 \mid 75$, 故方程有解, 且原方程和 $37x + 107y = 25$ 是同解方程. 首先, 方程 $37x + 107y = 1$ 有特解 $x = (-1)^2 \times 9 = 9, y = (-1)^3 \times 26 = -26$. 因此, 方程 $37x + 107y = 25$, 也即方程 $111x - 321y = 75$ 的一切解可表示成

$$x = -26 \times 25 - 107t, \quad y = -9 \times 25 + 37t, \quad t = 0, \pm 1, \pm 2, \dots$$

定义 6.2 所谓多元一次方程就是可以表示成下列形式的方程:

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c \quad (6.1.4)$$

其中, a_1, a_2, \dots, a_n, c 都是整数, 且 $n \geq 2, a_1a_2 \dots a_n \neq 0$.

类似于定理 6.1 可给出方程(6.1.4)是否有解的判别方法.

定理 6.3 方程(6.1.4)有整数解的充分必要条件是

$$(a_1, a_2, \dots, a_n) \mid c$$

证 设 $d = (a_1, a_2, \dots, a_n)$. 如果方程(6.1.4)有解, 即存在 n 个整数 x'_1, x'_2, \dots, x'_n 使得

$$a_1x'_1 + a_2x'_2 + \dots + a_nx'_n = c$$

则由 $d \mid a_i (i=1, 2, \dots, n)$ 得 $d \mid c$. 反之, 若 $d \mid c$, 则存在整数 q 使得 $c = dq$. 由于 $d = (a_1, a_2, \dots, a_n)$, 由裴蜀恒等式可知, 存在整数 y_1, y_2, \dots, y_n 使得

$$a_1y_1 + a_2y_2 + \dots + a_ny_n = d$$

于是, $x_i = qy_i (i=1, 2, \dots, n)$ 就是方程(6.1.4)的一组解.

下面给出求方程(6.1.4)一切解的一种方法.

设方程(6.1.4)有整数解. 令 $d_i = (a_1, a_2, \dots, a_i), i=2, 3, \dots, n$, 构造如下系列方程:

$$\begin{aligned} a_1x_1 + a_2x_2 &= d_2y_2 \\ d_2y_2 + a_3x_3 &= d_3y_3 \\ &\vdots \\ d_{n-2}y_{n-2} + a_{n-1}x_{n-1} &= d_{n-1}y_{n-1} \\ d_{n-1}y_{n-1} + a_nx_n &= c \end{aligned}$$

首先求出最后一个方程的一切解, 即通解, 然后将关于 y_{n-1} 的通解形式代入倒数第二个方程求出其通解形式, 依此类推可以得到方程(6.1.4)的通解.

例 6.4 求方程

$$9x_1 + 24x_2 - 5x_3 = 1000$$

的一切整数解.

解 由于 $(9, 24) = 3$, $(3, -5) = 1$, 即有 $(9, 24, -5) = 1$, 故方程有整数解. 考虑方程

$$9x_1 + 24x_2 = 3y_2 \quad (6.1.5)$$

与

$$3y_2 - 5x_3 = 1000 \quad (6.1.6)$$

由定理 6.2 可得方程(6.1.6)的通解为

$$\begin{cases} y_2 = 2000 + 5t_1 \\ x_3 = 1000 + 3t_1 \end{cases}$$

其中, $t_1 = 0, \pm 1, \pm 2, \dots$.

将 $y_2 = 2000 + 5t_1$ 代入方程(6.1.5)中, 再利用定理 6.2 求得其通解为

$$\begin{cases} x_1 = 6000 + 15t_1 - 8t_2 \\ x_2 = -2000 - 5t_1 + 3t_2 \end{cases}$$

其中, $t_2 = 0, \pm 1, \pm 2, \dots$. 从而得原方程的通解为

$$\begin{cases} x_1 = 6000 + 15t_1 - 8t_2 \\ x_2 = -2000 - 5t_1 + 3t_2 \\ x_3 = 1000 + 3t_1 \end{cases}$$

其中, $t_1, t_2 = 0, \pm 1, \pm 2, \dots$.

练习 6.1

1. 解下列不定方程.

(1) $15x + 25y = 100$. (2) $306x - 360y = 630$.

2. 解下列三元一次不定方程.

(1) $39x - 24y + 9z = 78$. (2) $50x - 45y + 36z = 10$.

3. 设 $(a, b) = 1, a > 0, b > 0$, 则凡大于 $ab - a - b$ 的数都可以表示成

$$ax + by, \quad x \geq 0, y \geq 0$$

但 $ab - a - b$ 不能表示成上述形式.

4. 把 100 分成 4 份, 第一份可被 2 整除, 第二份可被 3 整除, 第三份可被 7 整除, 则最后一份可被 11 整除.

5. 设西瓜 5 元一个, 菠萝 1 元一个, 西红柿 10 个 1 元, 用 50 元买西瓜、菠萝、西红柿共 100 个, 问每样水果各买了多少个?

6.2 整数的平方和表示

1770 年, Lagrange 证明了一个非常著名的定理, 即每一个正整数都能表示成 4 个整数平方和, 其中, 允许有 $0 = 0^2$ 存在.

首先来探讨满足什么条件的素数可以表示成两个整数的平方和形式? 先给出一个引理如下.

引理 6.1 如果 m, n 都可以表示成两个整数的平方和, 那么, mn 也可以表示成两个整数的平方和.

证 设 $m = a^2 + b^2, n = c^2 + d^2$, 其中, a, b, c, d 为整数. 那么

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

并非所有的素数都可以表示成两个整数的平方和, 如 $3 = a^2 + b^2$ 就没有整数解, 即 3 不能表示成两个整数的平方和. 进一步有下面的定理.

定理 6.4 形如 $4k+3$ 的素数 p 都不可以表示成两个整数的平方和.

证 对于任意的整数 a , 则有 $a \equiv 0, 1, 2$ 或 $3 \pmod{4}$. 因此, $a^2 \equiv 0$ 或 $1 \pmod{4}$, 对任意的整数 a, b , 有

$$a^2 + b^2 \equiv 0, 1 \text{ 或 } 2 \pmod{4}$$

而 $p = 4k + 3 \equiv 3 \pmod{4}$, 因此, $p = a^2 + b^2$ 无整数解.

由上面的定理 6.4 得知, 形如 $4k+3$ 的素数都不可以表示成两个整数的平方和. 但是, 关于模 4 同余 1 的所有素数都可以表示成两个整数的平方和. 为了证明这个结论, 我们借助著名的“抽屉原理”.

引理 6.2(抽屉原理) 如果把 n 个物品放到 m 个盒子中, 且 $n > m$, 那么, 一定有某个盒子中至少有两个物品.

用数学语言表达“抽屉原理”就是: 集合 S 含有 n 个元素, 如果集合 S 的 m 个子集的并集正好是 S , 且 $n > m$, 那么, 一定存在 S 的某个子集含有至少两个元素.

定理 6.5 设 p 是奇素数, $(a, p) = 1$, 那么, 同余方程

$$ax \equiv y \pmod{p}$$

存在一组解 (x_0, y_0) , 满足 $0 < |x_0| < \sqrt{p}$ 且 $0 < |y_0| < \sqrt{p}$.

证 设 $k = [\sqrt{p}] + 1$. 考虑整数集合

$$S = \{ax - y \mid 0 \leq x \leq k - 1, 0 \leq y \leq k - 1\}$$

由于 S 含有 $k^2 (> p)$ 个元素, 因此, 根据抽屉原理可得知 S 中至少有两个元素, 不妨设为 $ax_1 - y_1$ 和 $ax_2 - y_2$, 它们对模数 p 同余, 且 $x_1 \neq x_2, y_1 \neq y_2$. 于是, $a(x_1 - x_2) = y_1 - y_2 \pmod{p}$. 令 $x_0 = x_1 - x_2, y_0 = y_1 - y_2$, 则 (x_0, y_0) 是同余式 $ax \equiv y \pmod{p}$ 的一个解.

如果 x_0 或 y_0 等于零, 那么, 由 $(a, p) = 1$ 可得 x_0 和 y_0 都等于零, 这与 $x_1 \neq x_2, y_1 \neq y_2$ 矛盾, 因此, $0 < |x_0| \leq k - 1 < \sqrt{p}, 0 < |y_0| \leq k - 1 < \sqrt{p}$.

定理 6.6 奇素数 p 可以表示成两个整数平方和的充分必要条件是

$$p \equiv 1 \pmod{4}$$

证 由定理 6.4 即知,若奇素数能表示成两个整数的平方和,则必有 $p \equiv 1 \pmod{4}$. 反之,如果 $p \equiv 1 \pmod{4}$,那么, -1 是模数 p 的二次剩余,即存在一个整数 a ,使得 $a^2 \equiv -1 \pmod{p}$. 事实上,取 $a = ((p-1)/2)!$ 即可. 又由于 $(a, p) = 1$,则由定理 6.5 可知同余式

$$ax \equiv y \pmod{p}$$

有一组解 x_0, y_0 , 满足 $0 < |x_0| < \sqrt{p}$ 及 $0 < |y_0| < \sqrt{p}$. 因此,有

$$-x_0^2 \equiv a^2 x_0^2 \equiv (ax_0)^2 \equiv y_0^2 \pmod{p}$$

则 $x_0^2 + y_0^2 \equiv 0 \pmod{p}$, 亦即存在某正整数 $k \geq 1$, 使得

$$x_0^2 + y_0^2 = kp$$

但由于 $0 < |x_0| < \sqrt{p}$, $0 < |y_0| < \sqrt{p}$, 故有 $0 < x_0^2 + y_0^2 < 2p$, 因此, $k=1$, 即 $p = x_0^2 + y_0^2$.

推论 6.2 形如 $4k+1$ 的奇素数 p 可唯一地(不考虑被加数的次序)表示成两个正整数的平方和.

证 假设奇素数 p 可以表示成

$$p = a^2 + b^2 = c^2 + d^2$$

其中, a, b, c, d 都是正整数, 那么

$$a^2 d^2 - b^2 c^2 = p(d^2 - b^2) \equiv 0 \pmod{p}$$

于是, $ad - bc \equiv 0 \pmod{p}$ 或 $ad + bc \equiv 0 \pmod{p}$. 由于 a, b, c, d 都小于 \sqrt{p} , 于是

$$ad - bc = 0 \text{ 或 } ad + bc = p$$

如果 $ad + bc = p$, 那么

$$p^2 = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2$$

于是 $ac = bd$, 由此可得出 $ad = bc$ 或 $ac = bd$.

假设 $ad = bc$, 那么, $a | bc$, 由于 $(a, b) = 1$, 于是, $a | c$. 设 $c = ka$, 那么, $ad = bc = b(ka)$, 即有 $d = bk$. 但

$$p = c^2 + d^2 = k^2(a^2 + b^2)$$

于是, $k=1$, 因此, $a=c, b=d$. 同理可证, 当 $ac = bd$ 时, 可得 $a=d$, 且 $b=c$. 由此证得奇素数 p 可唯一地表示成两个整数平方和.

例 6.5 把素数 $p=13$ 表示成两个整数的平方和.

解 取 $a = ((13-1)/2)! = 6! \equiv 5 \pmod{13}$. 为了求同余式 $5x \equiv y \pmod{13}$ 的一个解, 考虑集合 $S = \{5x - y | 0 \leq x, y < 4\}$. 对应 x, y 的取值得到集合 S 中的元素表为

$y \backslash x$	0	1	2	3
0	0	5	10	15
1	-1	4	9	14
2	-2	3	8	13
3	-3	2	7	12

对表中 S 的元素取模 13 得

$y \backslash x$	0	1	2	3
0	0	5	10	2
1	12	4	9	1
2	11	3	8	0
3	10	2	7	12

利用此表找得满足方程 $5x \equiv y \pmod{13}$ 及 $0 < |x_0| < \sqrt{13}$ 与 $0 < |y_0| < \sqrt{13}$ 的一组解为 $x_0 = 3, y_0 = 2$. 于是, $13 = 3^2 + 2^2$.

已经证明了形如 $4k+1$ 的奇素数 p 可以唯一地(不考虑被加数的次序)表示成两个整数平方和, 而其他的整数也有可能表示成两个整数的平方和, 例如, $10 = 1^2 + 3^2$.

下面来看看具有什么形式的正整数可以表示成两个整数的平方和.

定理 6.7 设正整数 $n = q^2 m$, 其中, m 无平方因子. 那么, n 能表示成两个整数的平方和当且仅当 m 没有形如 $4k+3$ 的素因子.

证 假设 m 没有形如 $4k+3$ 的素因子. 如果 $m=1$, 那么, $n = q^2 + 0^2$. 如果 $m > 1$, 设 $m = p_1 p_2 \cdots p_r$ 是 m 的不同素因子分解式. 每一个 $p_i (i=1, 2, \dots, r)$ 等于 2 或形如 $4k+1$, 而 2 或形如 $4k+1$ 的奇素数都可以表示成两个整数的平方和. 再由恒等式

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

可知, 能表示成两个整数平方和的任意有限多个整数的乘积也能表示成两个整数的平方和. 于是, 存在整数 s, t , 使得 $m = s^2 + t^2$, 因此有

$$n = q^2 m = q^2 (s^2 + t^2) = (qs)^2 + (qt)^2$$

反之, 设 n 能表示成两个整数的平方和, 即

$$n = q^2 m = a^2 + b^2$$

设 p 是 $m (> 1)$ 的任意一个素因子. 如果 $d = (a, b)$, 那么, 存在整数 r, s , 使 $a = rd$ 与 $b = sd$ 且 $(r, s) = 1$, 于是有

$$d^2 (r^2 + s^2) = q^2 m$$

已知 m 无平方因子, 得 $d^2 \mid q^2$. 因此, 存在某个整数 k 使得

$$r^2 + s^2 = \left(\frac{q}{d}\right)^2 \cdot m = kp$$

于是得

$$r^2 + s^2 \equiv 0 \pmod{p}$$

由于 $(r, s) = 1$, 因此, $(r, p) = 1$ 或 $(s, p) = 1$. 不妨设 $(r, p) = 1$, 则存在整数 r' 使 $r \cdot r' \equiv 1 \pmod{p}$. 把同余式 $r^2 + s^2 \equiv 0 \pmod{p}$ 两端同乘 $(r')^2$ 可得

$$(sr')^2 + 1 \equiv 0 \pmod{p} \text{ 或 } (sr')^2 \equiv -1 \pmod{p}$$

即 -1 是模数 p 的二次剩余, 因此有 $p \equiv 1 \pmod{4}$, 故 m 没有形如 $4k+3$ 的素因子.

推论 6.3 正整数 n 能表示成两个整数的平方和当且仅当形如 $4k+3$ 的素因子是偶数次方幂.

例 6.6 分别把 459, 153, 54145 表示成两个整数的平方和.

解 由于 $459 = 3^3 \times 17$, 而素数 3 的方幂是 3, 为奇数, 因此, 由推论可知 459 不能表示成两个整数的平方和.

由于 $153 = 3^2 \times 17$, 而素数 3 的方幂是 2 为偶数且 $17 \equiv 1 \pmod{4}$, 因此, 153 可以表示成两个整数的平方和. 事实上, $153 = 3^2 \times (4^2 + 1^2) = 12^2 + 3^2$.

$54145 = 5 \times 7^2 \times 13 \times 17 = 7^2(2^2 + 1^2)(3^2 + 2^2)(4^2 + 1^2)$, 两次利用引理 6.1 的证明可得 $54145 = 231^2 + 28^2$.

练 习 6.2

1. 分别把 113, 229, 373 表示成两个整数的平方和.
2. 证明下列结论.
 - (1) 形如 $2^n (n=1, 2, \dots)$ 的整数可表示成两个整数的平方和.
 - (2) 如果 $n \equiv 3$ 或 $6 \pmod{9}$, 那么, n 不能表示成两个整数的平方和.
 - (3) 每一个 Fermat 数 $F_n = 2^{2^n} + 1 (n \geq 1)$ 可表示成两个整数的平方和.
 - (4) 如果 n 是一个奇完全数(如果存在^①), 则它可表示成两个整数的平方和.
3. 证明素数 p 可表示成两个整数的平方和当且仅当同余式 $x^2 + 1 \equiv 0 \pmod{p}$ 有解.
4. 证明正整数 n 可表示成两个整数的平方和当且仅当 $n = 2^m a^2 b$, 其中, $m \geq 0$, a 是奇数, b 的每一个素因子都形如 $4k+1$.

^① 由于至今还没有发现奇完全数的例子, 所以人们提出猜想“不存在奇完全数”. 为证明此猜想, 目前已证了两个重要结论: a. 不能被 3 整除的奇完全数至少含有 11 个不同的素因子; b. 如果奇完全数存在, 则它必大于 10^{200} .

6.3 整数表示为多个整数的平方和

我们已经知道,并非所有的正整数都能表示成两个整数的平方和.如 14, 33, 67 不能表示成两个整数的平方和,但它们却可以表示成三个整数的平方和.

$$14 = 3^2 + 2^2 + 1^2, \quad 33 = 5^2 + 2^2 + 2^2, \quad 67 = 7^2 + 3^2 + 3^2$$

那么,哪些整数可以表示成三个整数的平方和(允许出现平方项 0^2)? 首先有下面的结论.

定理 6.8 形如 $4^n(8m+7)$ ($n \geq 1, m \in \mathbb{Z}$) 的正整数不能表示成三个整数的平方和.

证 (1) 先证明形如 $8m+7$ 的正整数不能表示成三个整数的平方和.

对任意的整数 a , 有 $a^2 \equiv 0, 1$ 或 $4 \pmod{8}$, 于是, 对任意的整数 a, b, c ,

$$a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5 \text{ 或 } 6 \pmod{8}$$

而 $8m+7 \equiv 7 \pmod{8}$, 因此, $8m+7 = a^2 + b^2 + c^2$ 无整数解.

(2) 假设存在整数 a, b, c 使得

$$4^n(8m+7) = a^2 + b^2 + c^2$$

那么, a, b, c 必全为偶数, 设 $a = 2a_1, b = 2b_1, c = 2c_1$, 则有

$$4^{n-1}(8m+7) = a_1^2 + b_1^2 + c_1^2$$

如果 $n-1 \geq 1$, 重复上面的步骤, 最终可以得到 $8m+7$ 可以表示成三个整数的平方和, 这与(1)的证明矛盾.

依据前面的结果, 存在一些整数既不能表示成两个整数的平方和, 也不能表示成三个整数的平方和(如 15 和 23. 更一般地, 如既可表示成形如 $8m+7$ 又可表示成 $4k+3$ 的素数). 但是, 任意正整数都可以表示成 4 个整数的平方和! 这是一个非常有意思的结论.

定理 6.9 如果整数 m, n 都可以表示成 4 个整数的平方和, 那么, mn 也可以表示成 4 个整数的平方和.

证 设 $m = a_1^2 + a_2^2 + a_3^2 + a_4^2, n = b_1^2 + b_2^2 + b_3^2 + b_4^2$, 其中, a_i, b_i ($i=1, 2, 3, 4$) 是整数, 那么

$$\begin{aligned} mn &= (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\ &= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 \\ &\quad + (a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4)^2 + (a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2)^2 \end{aligned}$$

定理 6.10 如果 p 是奇素数, 那么, 同余方程

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

存在一个解 x_0, y_0 , 满足 $0 \leq x_0 \leq (p-1)/2$ 及 $0 \leq y_0 \leq (p-1)/2$.

证 首先构造两个集合

$$S_1 = \left\{ 1+0^2, 1+1^2, 1+2^2, \dots, 1+\left(\frac{p-1}{2}\right)^2 \right\}$$

$$S_2 = \left\{ -0^2, -1^2, -2^2, \dots, -\left(\frac{p-1}{2}\right)^2 \right\}$$

显然, S_1 中的任意两个元素对模 p 不同余. 否则, 如果 $1+x_1^2 \equiv 1+x_2^2 \pmod{p}$, 那么, 有 $x_1 \equiv x_2 \pmod{p}$ 或者 $x_1 \equiv -x_2 \pmod{p}$. 由于 $0 \leq x_1 \leq \frac{(p-1)}{2}$, $0 \leq x_2 \leq \frac{(p-1)}{2}$, 于是, $0 < x_1 + x_2 < p$ 或 $x_1 = x_2 = 0$, 因此, 必有 $x_1 \equiv x_2 \pmod{p}$ 成立, 从而 $x_1 = x_2$.

同理可证, S_2 中的任意两个元素对模 p 也不同余. 由于 S_1 和 S_2 共包含 $2(1+(p-1)/2) = p+1$ 个整数, 由抽屉原理可知, S_1 中某个元素一定与 S_2 中的某个元素关于模 p 同余, 也就是说, 存在 x_0, y_0 使得

$$1+x_0^2 \equiv -y_0^2 \pmod{p}, \quad \text{即 } x_0^2 + y_0^2 + 1 \equiv 0 \pmod{p}$$

其中, $0 \leq x_0 \leq \frac{(p-1)}{2}$, $0 \leq y_0 \leq \frac{(p-1)}{2}$.

推论 6.4 如果 p 是奇素数, 那么, 存在整数 $k < p$ 使得 kp 可以表示成 4 个整数的平方和.

证 根据定理 6.10 可知, 对于一个适当的整数 k , 存在整数 x_0, y_0 使得

$$x_0^2 + y_0^2 + 1^2 + 0^2 = kp$$

其中, $0 \leq x_0 \leq (p-1)/2$, $0 \leq y_0 \leq (p-1)/2$. 于是可得

$$kp = x_0^2 + y_0^2 + 1^2 < p^2/4 + p^2/4 + 1 < p^2$$

因此, $k < p$.

例 6.7 把 51 表示成 4 个整数的平方和.

解 $51 = 3 \times 17$. 对于 $p = 17$ 利用定理 6.10. 首先

$$S_1 = \{1, 2, 5, 10, 17, 26, 37, 50, 65\}$$

$$S_2 = \{0, -1, -4, -9, -16, -25, -36, -49, -64\}$$

对 S_1 的元素取模 17 得到 $S'_1 = \{1, 2, 5, 10, 0, 9, 3, 16, 14\}$, 对 S_2 的元素取模 17 得 $S'_2 = \{0, 16, 13, 8, 1, 9, 15, 2, 4\}$. 显然, S'_1 中的元素 2 与 S'_2 中的元素 2 对模 17 同余, 即有 $1+1^2 \equiv 2 \equiv -7^2 \pmod{17}$, 亦即 $1^2 + 7^2 + 1 \equiv 0 \pmod{17}$. 因此, 由推论 6.4 得到 $3 \cdot 17 = 1^2 + 1^2 + 7^2 + 0^2$.

定理 6.11 任意素数 p 都可以表示成 4 个整数的平方和.

证 当 $p=2$ 时命题显然成立, 因为 $2=1^2+1^2+0^2+0^2$.

设 p 为奇素数. 由推论 6.4 知, 存在小于 p 的且使 kp 能表示成 4 个整数平方和的最小正整数 k , 即存在正整数 x, y, z, w , 使

$$kp = x^2 + y^2 + z^2 + w^2$$

证明 k 是奇数. 若 k 是偶数, 那么, x, y, z, w 都是偶数, 或都是奇数, 或两个奇数两个偶数, 于是可不妨假定

$$x \equiv y \pmod{2}, \quad z \equiv w \pmod{2}$$

从而

$$\frac{x-y}{2}, \quad \frac{x+y}{2}, \quad \frac{z-w}{2}, \quad \frac{z+w}{2}$$

都是整数, 且有

$$\frac{kp}{2} = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2$$

因此, $(k/2)p$ 能表示成 4 个整数的平方和, 这与 k 的最小性矛盾.

现在证明 $k=1$. 否则, 由于 k 是奇数, 且最小的奇数是 3, 因此, 可取到 a, b, c, d 使得

$$a \equiv x \pmod{k}, \quad b \equiv y \pmod{k}, \quad c \equiv z \pmod{k}, \quad d \equiv w \pmod{k}$$

且

$$|a| < \frac{k}{2}, \quad |b| < \frac{k}{2}, \quad |c| < \frac{k}{2}, \quad |d| < \frac{k}{2}$$

(如为了得到整数 a , 取 x 被 k 整除所得的余数 r . 当 $r < \frac{k}{2}$ 时, 令 $a=r$; 当 $r > \frac{k}{2}$ 时, 令 $a=r-k$) 于是有

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k}$$

从而存在某个非负整数 t , 使得

$$a^2 + b^2 + c^2 + d^2 = tk$$

又由于 $|a| < \frac{k}{2}, |b| < \frac{k}{2}, |c| < \frac{k}{2}, |d| < \frac{k}{2}$, 于是得

$$0 \leq tk = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{k}{2}\right)^2 = k^2$$

若 $t=0$, 则有 $a=b=c=d=0$, 于是, k 整除 x, y, z, w 中每一个数, 进而可得 $k^2 | kp$ 或 $k | p$, 这与 $1 < k < p$ 矛盾, 因此, $t \neq 0$. 再由 $tk < k^2$, 可得 $t < k$.

令 $r = xa + yb + zc + wd, s = xb - ya + zd - wc, t = xc - za + wb - yd, u = xd - wa + yc - zb$, 则可得

$$k^2 tp = (kp)(tk) = (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = r^2 + s^2 + t^2 + u^2$$

此外, 由 $r = xa + yb + zc + wd \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{k}$ 可得 $k | r$, 由 $s = xb - ya + zd - wc \equiv ab - ba + cd - dc \equiv 0 \pmod{k}$ 可得 $k | s$. 同理, 可得 $k | t, k | u$. 因此有

$$tp = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2$$

其中, $\frac{r}{k}, \frac{s}{k}, \frac{t}{k}, \frac{u}{k}$ 都是整数, 且有 $0 < t < k$, 这与 k 的最小性矛盾, 故 $k=1$.

利用定理 6.11 可得下面的 Lagrange 四平方定理^①.

定理 6.12 任意正整数 n 都可以表示成 4 个整数的平方和.

证 当 $n=1$ 时, 由 $1=1^2+0^2+0^2+0^2$ 可知命题成立. 当 $n>1$ 时, 设 n 的标准分解式为 $n=p_1 p_2 \cdots p_r$, 其中, p_1, p_2, \cdots, p_r 是素数, 则由定理 6.9 和定理 6.11 可知命题成立.

例 6.8 把 555 表示成四个整数的平方和.

解 由于 $555=3 \times 5 \times 37$, 因此

$$\begin{aligned} 555 &= 3 \times 5 \times 37 = (1^2 + 1^2 + 1^2 + 0^2) \cdot (1^2 + 2^2 + 0^2 + 0^2) \cdot (1^2 + 6^2 + 0^2 + 0^2) \\ &= ((1^2 + 1^2 + 1^2 + 0^2) \cdot (1^2 + 2^2 + 0^2 + 0^2)) \cdot (1^2 + 6^2 + 0^2 + 0^2) \\ &= (3^2 + 1^2 + 1^2 + 2^2) \cdot (1^2 + 6^2 + 0^2 + 0^2) \\ &= 9^2 + 17^2 + 11^2 + 8^2 \end{aligned}$$

练 习 6.3

1. 证明对于任意给定的整数 n , n 或 $3n$ 可以表示成三个整数的平方和.
2. 证明 $n=459$ 不能表示成两个整数的平方和, 但能表示成三个整数的平方和.
3. 证明下列结论.
 - (1) 任意正奇数都可以表示成 $a^2 + b^2 + 2c^2$ (a, b, c 是整数) 的形式.
 - (2) 任意的正整数 n 或者可以表示成 $a^2 + b^2 + c^2$ 的形式, 或者可以表示成 $a^2 + b^2 + 2c^2$ 的形式 (a, b, c 是整数).
4. 已知 $15=3^2+2^2+1^2+1^2$, $34=4^2+4^2+1^2+1^2$, 分别将 $105, 945=3^2 \times 7 \times 15$ 以及 $3570=7 \times 15 \times 34$ 表示成 4 个整数的平方和.
5. 证明任意奇数都可以表示成 4 个整数的平方和, 且其中两个数是连续的 (提示: 先证对于 $n>0$, $4n+1$ 可以表示成三个整数的平方和, 且只有一个数是奇数).
6. 任意正整数 $n(\geq 170)$ 都可表示成 5 个正整数的平方和 (提示: 存在整数 a, b, c, d 使 $n-169=a^2+b^2+c^2+d^2$, 且 $169=13^2=12^2+5^2=12^2+4^2+3^2=10^2+8^2+2^2+1^2$).

6.4 勾股不定方程 $x^2 + y^2 = z^2$

在我国古代经典数学著述《周髀算经》中(“算经十书”中最早的一种), 载有“勾

^① Lagrange (1736—1813) 出生于意大利, 数学家. 因四平方定理最初由 Lagrange 于 1770 年给出证明, 所以该定理又称 Lagrange 四平方定理.

广三,股修四,径隅五”(即勾三股四弦五),意即直角三角形的两条直角边是 3 及 4,则斜边是 5.若分别用 a, b, c 记勾,股,弦之长,则有 $a^2 + b^2 = c^2$.也就是说,直角三角形的三条边长满足方程

$$x^2 + y^2 = z^2 \quad (6.4.1)$$

此方程又称商高不定方程.本节讨论该不定方程的整数解.3,4,5 是该不定方程的一组正整数解.同样,可以验证 5,12,13;8,15,17;7,24,25;20,21,29 也是该不定方程正整数解.

定义 6.3 设 x, y, z 是不定方程(6.4.1)的一组正整数解,则称 x, y, z 为一组勾股数.西方称勾股数为毕达哥拉斯三元数组.若 $(x, y, z) = 1$,则称 x, y, z 是本原勾股数或本原毕达哥拉斯三元数组.例如,3,4,5;5,12,13;12,35,37 都是本原勾股数.

由于不定方程(6.4.1)的解称为勾股数,所以又称该不定方程为勾股不定方程.

显然, $x=y=z=0, x=0, y=\pm z$ 或 $y=0, x=\pm z$ 都是方程(6.4.1)的一组解.除此外,方程(6.4.1)的每组解都不包含零.要求方程的一切整数解,只要求出一切正整数解就可,因此假定 $x>0, y>0, z>0$.

设 $d=(a, b, c)>0$,若 a, b, c 是方程(6.4.1)的一组解,则 $\frac{a}{d}, \frac{b}{d}, \frac{c}{d}$ 也是方程(6.4.1)的一组解.又因为 $(a, b, c)=1$ 当且仅当 $(b, c)=1$,因此只需讨论 $x^2 + y^2 = z^2$ 且 $x>0, y>0, z>0, (y, z)=1$ 的情况就可以了.

引理 6.3 如果 x, y, z 是一组本原勾股数,那么, x, y 一奇一偶.

证 若 x, y 都是偶数,则 $2 | (x^2 + y^2)$,那么, $2 | z$,因此, $(x, y, z) \geq 2$,这与 x, y, z 是一组本原勾股数矛盾.

同样,若 x, y 都是奇数,则 $x^2 \equiv 1 \pmod{4}, y^2 \equiv 1 \pmod{4}$,那么

$$z^2 = x^2 + y^2 \equiv 2 \pmod{4}$$

但对任意正整数 $n, n^2 \equiv 0, 1 \pmod{4}$,故上同余式不可能成立.因此, x, y 必为一奇一偶.

引理 6.4 如果 $ab=c^n$,且 $(a, b)=1$,那么, a, b 都是 n 次方幂,即存在整数 a_1, b_1 ,使得 $a = a_1^n, b = b_1^n$.

证 不失一般性,设 $a>1, b>1$,且 a, b 的素因子标准分解式分别为

$$a = p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r}, \quad b = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

由 $(a, b)=1$ 可知 $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ 全不相同.因此, ab 的素因子标准分解式为

$$ab = p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

设 c 的素因子标准分解式为

$$c = u_1^{l_1} u_2^{l_2} \cdots u_t^{l_t}$$

那么,由 $ab=c^n$ 可得

$$p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s} = u_1^{n l_1} u_2^{n l_2} \cdots u_t^{n l_t} \quad (6.4.2)$$

于是, $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ 是 u_1, u_2, \dots, u_t 的某个排列,且 $n l_1, n l_2, \dots, n l_t$ 是相应的 $i_1, i_2, \dots, i_r, j_1, j_2, \dots, j_s$ 的一个排列. 因此, $i_1, i_2, \dots, i_r, j_1, j_2, \dots, j_s$ 都是 n 的倍数. 如果记

$$a_1 = p_1^{i_1/n} p_2^{i_2/n} \cdots p_r^{i_r/n}, \quad b_1 = q_1^{j_1/n} q_2^{j_2/n} \cdots q_s^{j_s/n}$$

那么, $a = a_1^n, b = b_1^n$.

由上面两个引理可得到一个重要的结论,即下面的定理 6.13.

定理 6.13 x, y, z 是不定方程(6.4.1)的满足条件

$$2 \mid x, x > 0, y > 0, z > 0, (y, z) = 1 \quad (6.4.3)$$

的一组正整数解,当且仅当 x, y, z 可分别表示成

$$x = 2st, \quad y = s^2 - t^2, \quad z = s^2 + t^2 \quad (6.4.4)$$

其中, s, t 满足 $s > t > 0, (t, s) = 1$, 且 $s \not\equiv t \pmod{2}$.

证 必要性 假设 x, y, z 是不定方程(6.4.1)的一组满足条件(6.4.3)的解,则 y, z 都是奇数,因此, $z - y, z + y$ 都是偶数.

设 $z - y = 2u, z + y = 2v$, 则 $(u, v) = 1$. 否则,若 $(u, v) = d > 1$, 那么, $d \mid (u - v), d \mid (u + v)$, 于是,有 $d \mid y, d \mid z$, 即有 $d \mid (y, z)$, 因而 $d \mid 1$, 矛盾.

由不定方程(6.4.1)可得

$$x^2 = z^2 - y^2 = (z - y)(z + y)$$

因此

$$(x/2)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right) = uv$$

从而由引理 6.4 知, u, v 都是完全平方数, 设 $u = s^2, v = t^2$, 其中, s, t 都是正整数. 于是得

$$z = u + v = s^2 + t^2$$

$$y = u - v = s^2 - t^2$$

$$x = 2st$$

由于 s, t 的公因子既整除 y 又整除 z , 而 $(y, z) = 1$, 因此, $(s, t) = 1$. 另外, 若 s, t 都是奇数, 或都为偶数, 则 y, z 都是偶数, 这与 $(y, z) = 1$ 矛盾. 因此, $s \not\equiv t \pmod{2}$.

充分性 设 s, t 满足 $s > t > 0, (t, s) = 1$, 且 $s \not\equiv t \pmod{2}$. 将方程(6.4.4)代入不定方程(6.4.1)检验可知, x, y, z 是不定方程(6.4.1)的一组解. 下面证明 $(y, z) = 1$.

假设 $(y, z) = d > 1$, 且 p 是 d 的素因子, 则由 s, t 是一奇一偶知 y, z 均是奇数, 因而 $p \neq 2$, 进而由 $p \mid z, p \mid y$ 可得 $p \mid (z + y), p \mid (z - y)$, 即 $p \mid 2s^2, p \mid 2t^2$. 因此, $p \mid s, p \mid t$, 这与 $(t, s) = 1$, 矛盾.

说明 在定理 6.13 中假定 x 为偶数的情形. 类似地, 若考虑 x, y, z 是不定方程(6.4.1)的一组满足条件 $2|y, x>0, y>0, z>0, (x, z)=1$ 的任意一组解, 那么, x, y, z 可以表示成

$$x = s^2 - t^2, \quad y = 2st, \quad z = s^2 + t^2$$

其中, s, t 满足 $s>t>0, (t, s)=1$, 且 $s \not\equiv t \pmod{2}$.

例 6.9 在一组勾股数中, 如果弦与股的差是 1, 那么, 不定方程(6.4.1)的解之形式为

$$2a+1, \quad 2a^2+2a, \quad 2a^2+2a+1$$

其中, a 为任意整数.

证法一 设 x, y, z 是一组勾股数, 且弦与股的差是 1, 则 y 必为偶数, 而 x, z 为奇数. 令 $x=2a+1$, 其中, a 为任意整数. 则

$$x^2 = z^2 - y^2 = (z+y)(z-y) = (2a+1)^2$$

另外, 由 $z-y=1$ 得方程组

$$\begin{cases} z-y=1 \\ z+y=(2a+1)^2 \end{cases}$$

解之得 $y=2a^2+2a, z=2a^2+2a+1$.

证法二 设 x, y, z 是一组勾股数. 因弦与股的差是 1, 所以, y 为偶数, x, z 为奇数, 且 $(y, z)=1$. 由定理 6.13 得

$$x = s^2 - t^2, \quad y = 2st, \quad z = s^2 + t^2$$

其中, s, t 满足 $s>t>0, (t, s)=1$, 且 $s \not\equiv t \pmod{2}$.

由 $z-y=1$ 得 $s^2+t^2-2st=1$, 亦即 $(s-t)^2=1$. 因 $s>t>0$, 所以, $s=t+1$. 因此

$$x = s^2 - t^2 = 2t+1, \quad y = 2st = 2t^2 + 2t, \quad z = s^2 + t^2 = 2t^2 + 2t + 1$$

练习 6.4

1. 求下列方程的正整数解.

(1) $x^2 + y^2 = (y+1)^2$. (2) $x^2 + 2y^2 = z^2$.

2. 证明如果 $n \not\equiv 2 \pmod{4}$, 那么, 存在一组本原勾股数 x, y, z , 使得 x 或 y 等于 n .

3. 证明 3, 4, 5 是唯一的一组连续的本原勾股数.

4. 找出所有的面积等于周长的直角三角形.

5. 如果 x, y, z 是一组本原勾股数, 证明 $x+y, x-y \equiv 1$ 或 $7 \pmod{8}$.

6. 如果 x, y, z 是一组本原勾股数, 证明 $12|xy, 60|xyz$.

7. 证明如果 x, y, z 是一组本原勾股数, 且 $z-y=2$, 那么, 存在一个整数 $t (>1)$ 使得

$$x = 2t, \quad y = t^2 - 1, \quad z = t^2 + 1$$

6.5 Fermat 最后定理简介

法国数学家 Fermat 大约在 1630 年研究丢番图《算术》一书中有关毕达哥拉斯方程时,用法文在该书的页边上写下了一个结论.

当 n 大于 2 时,方程

$$x^n + y^n = z^n \quad (6.5.1)$$

无正整数解. 这就是数学史上著名的 Fermat 最后定理或称 Fermat 大定理.

Fermat 在记下这个结论的同时,又写下一个附注:“我已发现一个确实美妙的证明,这里页边空白太小,写不下.”后来,人们找遍 Fermat 的手迹也没有找到这一“美妙的证明”,只发现 Fermat 给出了 $n=4$ 的证明.

引理 6.5 方程 $x^4 + y^4 = z^2$ 无正整数解.

证 假设方程 $x^4 + y^4 = z^2$ 有正整数解,不妨设 x_0, y_0, z_0 是该方程的所有正整数解中使 $z = z_0$ 是最小的一组正整数解,则 $(x_0, y_0) = 1$. 否则,如果 $(x_0, y_0) = d > 1$,那么,令 $x_0 = dx_1, y_0 = dy_1, z_0 = d^2 z_1$,则有 $x_1^4 + y_1^4 = z_1^2$ 且 $0 < z_1 < z_0$,这与 z_0 的最小性矛盾.

由 $x_0^4 + y_0^4 = z_0^2$, 即 $(x_0^2)^2 + (y_0^2)^2 = z_0^2$ 且 x_0^2, y_0^2 为一奇一偶,不妨设 x_0^2 为偶数. 依据定理 6.13 可知,存在正整数 s, t 使得

$$x_0^2 = 2st, \quad y_0^2 = s^2 - t^2, \quad z_0 = s^2 + t^2$$

其中, $(s, t) = 1, s > t > 0$, 且 s, t 为一奇一偶.

若 s 为偶数,则 $1 \equiv y_0^2 = s^2 - t^2 \equiv 0 - 1 \equiv 3 \pmod{4}$, 矛盾. 因此, t 为偶数, s 为奇数. 记 $t = 2r$, 那么, $x_0^2 = 2st = 4sr$, 即 $(x_0/2)^2 = sr$. 由引理 6.4, s 与 r 都是完全平方数,即存在正整数 z_1, w_1 使得 $s = z_1^2, r = w_1^2$.

对于方程 $y_0^2 = s^2 - t^2$, 即 $t^2 + y_0^2 = s^2$. 由 $(s, t) = 1$ 得 $(t, y_0, s) = 1$. 于是,依据定理 6.13, 存在互素的正整数 $u > v > 0$, 使得

$$t = 2uw, \quad y_0 = u^2 - v^2, \quad s = u^2 + v^2$$

因 $uv = t/2 = r = w_1^2$. 再次利用引理 6.4, 可知 u, v 都是完全平方数, 因而存在正整 x_1, y_1 , 使得 $u = x_1^2, v = y_1^2$. 于是, 得 $z_1^2 = s = u^2 + v^2 = x_1^4 + y_1^4$, 亦即

$$x_1^4 + y_1^4 = z_1^2, \quad \text{且 } 0 < z_1 \leq z_1^2 = s \leq s^2 < s^2 + t^2 = z_0$$

这说明由假设方程 $x^4 + y^4 = z^2$ 的一组整数解 x_0, y_0, z_0 得到了另一组解 x_1, y_1, z_1 , 且满足 $0 < z_1 < z_0$, 这与 z_0 的最小性矛盾. 因此, 方程 $x^4 + y^4 = z^2$ 没有正整数解.

定理 6.14 方程 $x^4 + y^4 = z^4$ 无正整数解.

证 假设方程 $x^4 + y^4 = z^4$ 有一组正整数解 x_0, y_0, z_0 , 那么, x_0, y_0, z_0^2 就是不

定方程 $x^4 + y^4 = z^2$ 的一组正整数解. 但由引理 6.5 知 $x^4 + y^4 = z^2$ 没有正整数解, 矛盾. 因此, 假设不成立, 即方程 $x^4 + y^4 = z^4$ 无正整数解.

现在再来简单地讨论一下一般情形的 Fermat 最后定理.

当 $n > 2$ 时, n 或者是 2 的方幂或者能被某个奇素数 p 整除. 若 n 是 2 的方幂, 则存在某个整数 $k \geq 1$ 使得 $n = 4k$. 代入不定方程 (6.5.1) 得到

$$(x^k)^4 + (y^k)^4 = (z^k)^4 \quad (6.5.2)$$

由定理 6.14 知方程 (6.5.2) 没有正整数解, 即方程 (6.5.1) 没有正整数解.

若 n 能被某个奇素数 p 整除, 则存在某个奇素数 p 和某个正整数 $k \geq 1$ 使得 $n = pk$, 于是, 不定方程 (6.5.1) 可变形为

$$(x^k)^p + (y^k)^p = (z^k)^p$$

因此, 如果能证明对任意奇素数 p , $u^p + v^p = w^p$ 没有正整数解, 那么, 也就证明了 Fermat 最后定理.

Euler 在 1753 年 8 月写信给 Goldbach 说他证明了 $p = 3$ 的情况. 该证明于 1770 年发表在代数杂志上, 但是, Euler 的证明有一个漏洞, 后来 Legendre 弥补了该漏洞. $p = 5$ 情形的完整证明由 Dirichlet 在 1825 年 7 月发表的论文中的工作与 Legendre 在 1825 年 9 月发表的论文中的工作所组成. 1839 年, Lamé 证明了 $p = 7$ 的情形. 此后虽然有许多人对 Fermat 最后定理的证明做出了贡献, 如在 1993 年人们采用德国数学家 Kummer 的方法, 借助计算机证明了 Fermat 最后定理对 $n \leq 4000000$ 成立, 但直到 1994 年这个困惑了数学家或数学爱好者 360 多年的世界难题才由英国数学家 Wiles 获得了比较彻底的突破——Wiles 利用模椭圆曲线理论彻底证明了 Fermat 最后定理^①.

练 习 6.5

1. 证明不定方程 $\frac{1}{x^4} + \frac{1}{y^4} = \frac{1}{z^4}$ 无整数解.

2. 证明有无限组勾股数 x, y, z , 使 x 不仅是偶数, 且是一个完全平方数 (提示: 对于任意的正整数 n , 考虑 $4n^2, n^4 - 4, n^4 + 4$).

3. 证明不定方程 $x^2 + y^2 = z^3$ 有无穷多个正整数解 (提示: 对任意的整数 $n > 3$, 令 $x = n(n^2 - 3), y = 3n^2 - 1$).

4. 证明正整数 x, y, z 是不定方程 $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$ 的满足 $(x, y, z) = 1$ 的解当且仅当

^① Wiles 关于 Fermat 最后定理的完整证明于 1994 年 10 月投稿, 后于 1995 年 5 月发表在美国的《数学年刊》上.

$$x = 2st(s^2 + t^2), \quad y = s^4 - t^4, \quad z = 2st(s^2 - t^2)$$

其中, $s > t > 0$ 是互素的正整数, 且一奇一偶.

5. 证明正整数 x, y, z 是不定方程 $x^2 + 2y^2 = z^2$ 的满足 $(x, y, z) = 1$ 的解当且仅当

$$x = \pm(2s^2 - t^2), \quad y = 2st, \quad z = 2s^2 + t^2$$

其中, s, t 是任意的非负整数.

6. 证明下列方程无正整数解.

(1) $x^4 + 4y^4 = z^2$ (提示: 可采用类似于引理 6.5 的证法).

(2) $x^4 - y^4 = 2z^2$.

7. 证明对任意正整数 n , 不定方程

$$x^2 + y^2 = z^n$$

有正整数解(提示: 若 r, s, t 是方程组 $x^2 + y^2 = z^2$ 的一组正整数解, 则 $r \cdot t^{n-1}, s \cdot t^{n-1}, t^2$ 就是该不定方程的一组解).

6.6 用 Maple 解不定方程

在 Maple 中, 函数 `isolve(eqns)` 表示求不定方程或方程组“eqns”的整数解. 如下所示:

```
> isolve(7 * x + 4 * y = 100);
      {x = 4, _Z1, y = 25 - 7_Z1}
```

表示解得不定方程 $3x - 4y = 7$ 的通解为

$$x = 4_Z1, \quad y = 25 - 7_Z1 \quad (_Z1 \text{ 表示自由整数参数})$$

又如

```
> isolve(9 * x + 24 * y - 5 * z = 1000);
      {x = _Z1, z = -200 + 21_Z1 + 24_Z2, y = 4_Z1 + 5_Z2}
```

表示 $9x + 24y - 5z = 1000$ 的通解为

$$x = _Z1, \quad y = 4_Z1 + 5_Z2, \quad z = -200 + 21_Z1 + 24_Z2$$

其中, $_Z1$ 与 $_Z2$ 表示自由整数参数. 注意到, 此处通解的形式与本章例 6.4 求得的通解不一样, 但它们实际上是等价的.

用函数 `isolve(eqns)` 解不定方程组也非常快. 如下所示:

```
> isolve({x + y + z = 100, x + 2 * y + 3 * z = 200});
      {y = 100 - 2_Z1, x = _Z1, z = _Z1}
```

即不定方程组 $\begin{cases} x + y + z = 100 \\ x + 2y + 3z = 200 \end{cases}$ 的通解为

$$x = _Z1, \quad y = 100 - 2_Z1, \quad z = _Z1$$

又如利用函数

```
isolve({x+y+z+w=100,x+2*y+3*z+4*w=300,x+4*y+9*z+16*w=1000})
```

解不定方程组

$$\begin{cases} x+y+z+w=100 \\ x+2y+3z+4w=300 \\ x+4y+9z+16w=1000 \end{cases}$$

得其通解为

$$x=50-_{Z1}, \quad y=-100+3_{Z1}, \quad z=150-3_{Z1}, \quad w=_{Z1}$$

利用函数 `isolve(eqns)` 也可解高次不定方程或不定方程组. 例如解高次不定方程 $3x^3-4y=7$ 与 $y^4-z^2y^2-3xzy^2-x^3z=0$ 如下:

```
>isolve(3*x^3-4*y=7);
```

$$\{y = -1 - 9_{Z1} + 36_{Z1}^2 - 48_{Z1}^3, x = 1 - 4_{Z1}\}$$

```
>isolve(y^4-z^2*y^2-3*x*z*y^2-x^3*z=0);
```

$$\left\{ \begin{aligned} z &= -\frac{_{Z3}_{Z2}^4}{\text{igcd}(-_{Z2}^4, -(-_{Z2}^2 + _{Z1}^2)_{Z1}^2, _{Z1}^3, _{Z2})}, \\ x &= -\frac{_{Z3}(-_{Z2}^2 + _{Z1}^2)_{Z1}^2}{\text{igcd}(-_{Z2}^4, -(-_{Z2}^2 + _{Z1}^2)_{Z1}^2, _{Z1}^3, _{Z2})}, \\ y &= \frac{_{Z3}, _{Z1}^3, _{Z2}}{\text{igcd}(-_{Z2}^4, -(-_{Z2}^2 + _{Z1}^2)_{Z1}^2, _{Z1}^3, _{Z2})}, \end{aligned} \right\}$$

又如,解不定方程组 $\begin{cases} 3x^3-4y-2z=7 \\ x^4-2y+z=11 \end{cases}$ 如下:

```
>isolve({3*x^3-4*y-2*z=7,x^4-2*y+z=11});
```

$$\left\{ y = \frac{(1+8_{Z1})^4}{4} + \frac{3(1+8_{Z1})^3}{8} - \frac{29}{8}, z = \frac{3(1+8_{Z1})^3}{4} - \frac{(1+8_{Z1})^4}{2} + \frac{15}{4}, x = 1+8_{Z1} \right\}$$

注意,这里得到的通解是整数形式的,因为通解中

$$y = \frac{(1+8_{Z1})^4}{4} + \frac{3(1+8_{Z1})^3}{8} - \frac{29}{8}$$

与

$$z = \frac{3(1+8_{Z1})^3}{4} - \frac{(1+8_{Z1})^4}{2} + \frac{15}{4}$$

其实分别是整数形式,即

$$y = -3 + 17_{Z1} + 168_{Z1}^2 + 704_{Z1}^3 + 1024_{Z1}^4$$

$$z = 4 + 2_{Z1} - 48_{Z1}^2 - 640_{Z1}^3 - 2048_{Z1}^4$$

如果给出的不定方程或不定方程组无解,那么,函数 `isolve(eqns)` 判断出无解后将不返回任何值. 如下所示:

```

>isolve(x+2*y+3*z=4);
isolve({x+2*y+3*z=4,2*x+4*y+6*z=5});
isolve(x^3-8=0);
isolve(x^4-8=0);
isolve(x^5+y-8=0);
      {z=_Z1,x=4-3_Z1-2_Z2,y=_Z2}
      {x=2}
      {y=-_Z1^5+8,x=_Z1}

```

在函数 `isolve(eqns)` 解上面的 5 个不定方程时, 只得到第一、第三及第五个不定方程的解, 其余两个不定均无解, 因此没有返回值。

利用函数 `isolve(eqns)`, 也可以判断一个给定的整数是否是两个整数的平方和。如下所示:

```

>isolve(x^2+y^2=2008);
isolve(x^2+y^2=20089);
isolve(x^2+y^2=1234567891234);
{x=80,y=117},{x=-117,y=-80},{x=117,y=-80},{x=-80,y=117},
{x=-117,y=80},{y=-117,x=80},{y=-117,x=-80},{x=117,y=80}
{x=942603,y=588275},{x=588275,y=942603},{y=-942603,x=-588275},
{y=-588275,x=-942603},{y=942603,x=-588275},
{x=588275,y=-942603},{x=942603,y=-588275},
{y=588275,x=-942603}

```

上面的解过程说明不定方程 $x^2+y^2=2008$ 无整数, 所以没有输出值。而 $x^2+y^2=20089$ 有解, 且从解的结果可以看出, 20089 表示成两个正整数平方和的形式是唯一的。事实上, 20089 是一个形如 $4k+1$ 的素数。1234567891234 虽不是一个素数, 但其表示成两个正整数的平方和的形式仍是唯一的。

对于勾股不定方程 $x^2+y^2=z^2$ 的求解, 用函数 `isolve(eqns)` 可解得

```

>isolve(x^2+y^2=z^2);

```

$$\left\{ \begin{aligned} x &= -\frac{2_Z3_Z1_Z2}{\text{igcd}(-2_Z1_Z2, _Z1^2 - _Z2^2, _Z1^2 + _Z2^2)}, \\ y &= \frac{_Z3(_Z1^2 - _Z2^2)}{\text{igcd}(-2_Z1_Z2, _Z1^2 - _Z2^2, _Z1^2 + _Z2^2)}, \\ z &= \frac{_Z3(_Z1^2 + _Z2^2)}{\text{igcd}(-2_Z1_Z2, _Z1^2 - _Z2^2, _Z1^2 + _Z2^2)}. \end{aligned} \right.$$

这里给出的解是勾股不定方程的一般整数解的形式。如只要求本原解(即解是本原勾股数), 则显然解的形式可简化成

$$\{x=2_Z1_Z2, y=_Z1^2 - _Z2^2, z=_Z1^2 + _Z2^2\}$$

且此处的正整数参数 $_Z1$ 与 $_Z2$ 是互素的. 这与定理 6.13 得到的解是一致的.

但函数 `isolve(eqns)` 不能求解次数大于二次齐次的不定方程, 因而也就不求解次数大于二的 Fermat 方程. 例如, 三次齐次不定方程

$$x^3 + (y-1)^3 = (z-2)^3$$

有一个整数解 $(0, 1, 2)$, 但用 `isolve(eqns)` 求解时却不返回任何值.

利用 `isolve(eqns)` 可求解 Pell 方程, 如可求得 Pell 方程 $x^2 - 2y^2 = 1$ 有 4 组解.

`> isolve(x^2 - 2 * y^2 = 1);`

$$\left\{ \begin{aligned} x &= \frac{(3+2\sqrt{2})^{-z1}}{2} + \frac{(3-2\sqrt{2})^{-z1}}{2}, y = \frac{\sqrt{2}((3+2\sqrt{2})^{-z1} - (3-2\sqrt{2})^{-z1})}{4} \end{aligned} \right\},$$

$$\left\{ \begin{aligned} y &= \frac{\sqrt{2}((3+2\sqrt{2})^{-z1} - (3-2\sqrt{2})^{-z1})}{4}, x = -\frac{(3+2\sqrt{2})^{-z1}}{2} - \frac{(3-2\sqrt{2})^{-z1}}{2} \end{aligned} \right\},$$

$$\left\{ \begin{aligned} x &= -\frac{(3+2\sqrt{2})^{-z1}}{2} - \frac{(3-2\sqrt{2})^{-z1}}{2}, y = -\frac{\sqrt{2}((3+2\sqrt{2})^{-z1} - (3-2\sqrt{2})^{-z1})}{4} \end{aligned} \right\},$$

$$\left\{ \begin{aligned} x &= \frac{(3+2\sqrt{2})^{-z1}}{2} + \frac{(3-2\sqrt{2})^{-z1}}{2}, y = -\frac{\sqrt{2}((3+2\sqrt{2})^{-z1} - (3-2\sqrt{2})^{-z1})}{4} \end{aligned} \right\}$$

但为正整数的通解只有一组, 即

$$x = \frac{(3+2\sqrt{2})^{-z1}}{2} + \frac{(3-2\sqrt{2})^{-z1}}{2}, y = \frac{\sqrt{2}((3+2\sqrt{2})^{-z1} - (3-2\sqrt{2})^{-z1})}{4}$$

Rosen 的 *Elementary Number Theory and Its Applications* 一书中第 13.4 节的定理 13.11 是关于求 Pell 方程 $x^2 - dy^2 = 1$ 的正整数解的, 即是下面的定理 6.15. 这里不给出其证明.

定理 6.15 设 d 是一个非完全平方的正整数, $\frac{p_k}{q_k}$ 是 \sqrt{d} 的简单连分数, $k=1, 2, \dots, n$ 是该连分数的周期长度. 那么, 当 n 是偶数时, Pell 方程 $x^2 - dy^2 = 1$ 的全部正整数解是

$$x = p_{j-1}, \quad y = q_{j-1}, \quad j = 1, 2, 3, \dots$$

当 n 是奇数时, $x^2 - dy^2 = 1$ 的全部正整数解是

$$x = p_{2j-1}, \quad y = q_{2j-1}, \quad j = 1, 2, 3, \dots$$

利用此定理, 可以给出一个非常简单的求 Pell 方程的最小正整数解的 Maple 程序算法.

由于 $\frac{p_k}{q_k}$ 是 \sqrt{d} 的简单连分数, 正整数序列 p_1, p_2, p_3, \dots 与 q_1, q_2, q_3, \dots 均是递增序列, 所以, 当 n 是偶数时, $x=p_{n-1}, y=q_{n-1}$ 是 Pell 方程 $x^2 - dy^2 = 1$ 的最小正整数解; 而当 n 是奇数时, $x=p_{2n-1}, y=q_{2n-1}$ 是 $x^2 - dy^2 = 1$ 的最小正整数解. 因此, 可得到下面的求 Pell 方程的最小正整数解的 Maple 程序算法.

```

>with(numtheory):
PellEqMinSolve:=proc(d:posint)
local cf,n,r,s;
  cf:=cffrac(sqrt(d),periodic,quotients);
  n:=nops(cf[2]);
  if modp(n,2)=0 then
    r:=numer(nthconver(cf,n-1));
    s:=denom(nthconver(cf,n-1));
  else
    r:=numer(nthconver(cf,2*n-1));
    s:=denom(nthconver(cf,2*n-1));
  fi;
printf("Pell 方程"):
print(x^2-d*y^2=1):
printf("的最小正整数解是"):
print(x=r,y=s):
end;

```

例如,用上面的 Maple 程序函数 PellEqMinSolve()解 Pell 方程 $x^2 - 13y^2 = 1$ 得到其最小正整数解是 $x=649, y=180$.

```
>PellEqMinSolve(13);
```

Pell 方程

$$x^2 - 13y^2 = 1$$

的最小正整数解是

$$x = 649, \quad y = 180$$

再如

```
>PellEqMinSolve(109); PellEqMinSolve(2008); PellEqMinSolve(200888);
```

Pell 方程

$$x^2 - 109y^2 = 1$$

的最小正整数解是

$$x = 158070671986249, \quad y = 15140424455100$$

Pell 方程

$$x^2 - 2008y^2 = 1$$

的最小正整数解是

$$x = 3832352837, \quad y = 85523139$$

Pell 方程

$$x^2 - 200888y^2 = 1$$

的最小正整数解是

$x=85033223777331337959206159934693022438518035327261458682870970853\backslash$
 056287041807614944419983

$y=18971935820829125224863291647689797597374563635384910398743580963\backslash$
 2070139915672958857526

第 6 章综合例题

例 1 把 $\frac{17}{60}$ 表示成分母两两互素的三个既约分数之和.

证 由于 $60=3\times 4\times 5$, 不妨可设

$$\frac{17}{60} = \frac{x}{3} + \frac{y}{4} + \frac{z}{5}$$

于是得

$$20x + 15y + 12z = 17 \quad (6.1)$$

令 $4x+3y=t$, 则式(6.1)变为

$$5t + 12z = 17 \quad (6.2)$$

易知方程(6.2)有一组特解为 $\begin{cases} t_0=1 \\ z_0=1 \end{cases}$ (利用辗转相除法可求得该特解), 于是,

由定理 6.2 得式(6.2)的所有解为 $\begin{cases} t=12k+1 \\ z=1-5k \end{cases}, k=0, \pm 1, \pm 2, \dots$.

再解不定方程 $4x+3y=1+12k$. 易知 $\begin{cases} x_0=1+12k \\ y_0=-(1+12k) \end{cases}$ 是其一个解, 从而由

定理 6.2 便得式(6.1)的所有解为

$$\begin{cases} x = 1 + 12k + 3l \\ y = -(1 + 12k) - 4l, \quad k = 0, \pm 1, \pm 2, \dots, \quad l = 0, \pm 1, \pm 2, \dots \\ z = 1 - 5k \end{cases}$$

为求满足题设条件要求的解, 则必需 $x < 3, y < 4, z < 5$. 因此, 上式中需要 $k=l=0$, 即 $x=1, y=-1, z=1$. 因此, $\frac{17}{60} = \frac{1}{3} - \frac{1}{4} + \frac{1}{5}$.

例 2 证明不定方程 $ax+by=c (a, b, c \in \mathbb{N}, (a, b)=1)$ 的非负整数解的解数为

$$\left[\frac{c}{ab} \right] \quad \text{或} \quad \left[\frac{c}{ab} \right] + 1$$

证 设 x_0, y_0 是方程的一组整数解. 由定理 6.2 可知, 不定方程 $ax+by=c$ 的所有整数解为

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases}$$

其中, t 为整数.

为了使 x, y 非负, 则必需 $x = x_0 + bt \geq 0, y = y_0 - at \geq 0$ 同时成立, 即

$$-x_0/b \leq t \leq y_0/a \quad (6.3)$$

(1) 若 $\frac{-x_0}{b} \in \mathbb{Z}$, 则满足(6.3)的整数值 t 的个数是

$$\left[\frac{y_0}{a} - \frac{-x_0}{b} \right] + 1, \text{ 即 } \left[\frac{y_0}{a} - \frac{-x_0}{b} \right] + 1 = \left[\frac{by_0 + ax_0}{ab} \right] + 1 = \left[\frac{c}{ab} \right] + 1$$

(2) 若 $\frac{-x_0}{b} \notin \mathbb{Z}$, 则可设

$$\frac{-x_0}{b} = \left[\frac{-x_0}{b} \right] + \alpha, \quad 0 < \alpha < 1$$

此时, t 满足

$$\left[\frac{-x_0}{b} \right] + 1 \leq t \leq y_0/a$$

因此, 整数 t 的个数是

$$\begin{aligned} & \left[\frac{y_0}{a} - \left(\left[\frac{-x_0}{b} \right] + 1 \right) \right] + 1 = \left[\frac{y_0}{a} - \left(\frac{-x_0}{b} - \alpha + 1 \right) \right] + 1 \\ & = \left[\frac{by_0 + ax_0}{ab} + \alpha - 1 \right] + 1 = \left[\frac{c}{ab} + \alpha \right] \end{aligned}$$

假设 $\left[\frac{c}{ab} \right] = \frac{c}{ab} - \beta$ ($0 < \beta < 1$), 那么

$$\left[\frac{c}{ab} + \alpha \right] = \left[\left[\frac{c}{ab} \right] + \alpha + \beta \right] = \left[\frac{c}{ab} \right] + [\alpha + \beta]$$

由于 $0 < \alpha < 1, 0 < \beta < 1$, 因而 $0 < \alpha + \beta < 2$. 故当 $1 \leq \alpha + \beta < 2$ 时, $t = \left[\frac{c}{ab} \right] + 1$;

当 $0 < \alpha + \beta < 1$, $t = \left[\frac{c}{ab} \right]$.

综上所述, 命题成立.

例3 设 a_1, a_2 是正整数且 $(a_1, a_2) = 1$, 则当 $n > a_1 a_2$ 时, 方程 $a_1 x + a_2 y = n$ 有正整数解; 当 $n = a_1 a_2$ 时, 方程 $a_1 x + a_2 y = n$ 无正整数解.

证 由定理 6.2 可知 $a_1 x + a_2 y = n$ 有解, 且其全部解可表示为 $x = x_0 - a_2 t$, $y = y_0 + a_1 t$, 其中, x_0, y_0 是方程的一组特解, $t = 0, \pm 1, \pm 2, \dots$. 取 t_0 满足

$$0 < y = y_0 + a_1 t_0 \leq a_1$$

由 $n > a_1 a_2$ 可得

$$(x_0 - a_2 t_0) a_1 = n - (y_0 + a_1 t_0) a_2 > a_1 a_2 - a_1 a_2 = 0$$

故对上述 t_0 有

$$x = x_0 - a_2 t_0 > 0$$

这就证明了当 $n > a_1 a_2$ 时, 方程 $a_1 x + a_2 y = n$ 有正整数解.

如果 $n = a_1 a_2$ 且 $a_1 x + a_2 y = n$ 有正整数解 $x_0 > 0, y_0 > 0$, 则

$$a_1 x_0 + a_2 y_0 = a_1 a_2$$

因为 $(a_1, a_2) = 1$, 所以, $a_1 \mid y_0, a_2 \mid x_0$, 故 $a_1 \leq y_0, a_2 \leq x_0$. 因此有

$$a_1 a_2 = a_1 x_0 + a_2 y_0 \geq 2a_1 a_2$$

这不可能.

例 4 证明 Diophantine 方程 $x^4 - 4y^4 = z^2$ 没有正整数解.

证 将方程两端同时平方可得

$$\begin{aligned} z^4 &= (x^4 - 4y^4)^2 = x^8 - 8x^4 y^4 + 16y^8 \\ &= x^8 + 8x^4 y^4 + 16y^8 - 16x^4 y^4 = (x^4 + 4y^4)^2 - (4xy)^4 \end{aligned}$$

即有

$$(4xy)^4 + z^4 = (x^4 + 4y^4)^2$$

由引理 6.5 知, $(4xy)^4 + z^4 = (x^4 + 4y^4)^2$ 无整数解, 因此, $x^4 - 4y^4 = z^2$ 无整数解.

例 5 证明 Diophantine 方程 $x^4 - y^4 = z^2$ 无正整数解.

证法一 假设 x_0, y_0, z_0 是方程 $x^4 - y^4 = z^2$ 的所有正整数解中使 x_0 取值最小的一组整数解.

不失一般性, 设 $(x_0, y_0) = 1$. 否则, 若 $(x_0, y_0) = d > 1$, 记 $x_0 = dx_1, y_0 = dy_1$, 则有 $d^4(x_1^4 - y_1^4) = z_0^2$. 于是, 存在某个正整数 z_1 使得 $z_0 = d^2 z_1$, 即得到方程 $x^4 - y^4 = z^2$ 的另一组正整数解 x_1, y_1, z_1 , 且 $0 < x_1 < x_0$, 这与 x_0 的最小性矛盾.

下面分 y_0 的奇偶性讨论解的情况.

(1) 设 y_0 是奇数. 将 $x_0^4 - y_0^4 = z_0^2$ 变形为 $z_0^2 + (y_0^2)^2 = (x_0^2)^2$. 由 $(x_0, y_0) = 1$ 可知 z_0, y_0^2, x_0^2 是一组本原勾股数. 由定理 6.13 可知存在互素且一奇一偶的正整数 $s > t > 0$, 满足

$$z_0 = 2st, \quad y_0^2 = s^2 - t^2, \quad x_0^2 = s^2 + t^2$$

因此

$$s^4 - t^4 = (s^2 + t^2)(s^2 - t^2) = x_0^2 y_0^2 = (x_0 y_0)^2$$

从而得到 $x^4 - y^4 = z^2$ 的一组正整数解 $s, t, x_0 y_0$, 且

$$0 < s < \sqrt{s^2 + t^2} = x_0$$

这与 x_0 的最小性矛盾.

(2) 设 y_0 是偶数. 把 $x_0^4 - y_0^4 = z_0^2$ 变形为 $z_0^2 + (y_0^2)^2 = (x_0^2)^2$. 由 $(x_0, y_0) = 1$ 可知 x_0, y_0^2, z_0^2 是一组本原勾股数. 由定理 6.13 可知存在互素且一奇一偶的正整数 $s > t > 0$ (不妨设 s 为偶数, t 为奇数), 满足

$$y_0^2 = 2st, \quad z_0 = s^2 - t^2, \quad x_0^2 = s^2 + t^2$$

由于 $y_0^2 = 2st$, 且 $(2s, t) = 1$. 据引理 6.4 可知, 存在正整数 w, v 使得 $w^2 = 2s$, $v^2 = t$. 而 w 必须是偶数, 设 $w = 2u$, 那么 $s = 2u^2$. 因而

$$x_0^2 = s^2 + t^2 = 4u^4 + v^4, \quad \text{且 } (2u^2, v^2) = 1$$

从而 $2u^2, v^2, x_0$ 是一组本原勾股数. 再由定理 6.13 可知, 存在互素的正整数 $a > b > 0$, 使得

$$2u^2 = 2ab, \quad v^2 = a^2 - b^2, \quad x_0 = a^2 + b^2$$

由于 $2u^2 = 2ab$, 即 $u^2 = ab$, 据引理 6.4 可知, 存在正整数 c, d , 使得 $a = c^2, b = d^2$. 因此

$$v^2 = a^2 - b^2 = c^4 - d^4$$

于是, 就得到 $x^4 - y^4 = z^2$ 的另一组正整数解 c, d, v , 且满足

$$0 < c = \sqrt{a} < a^2 + b^2 = x_0$$

这与 x_0 的最小性矛盾.

综上所述, 方程 $x^4 - y^4 = z^2$ 无正整数解.

证法二 将方程两端平方可得

$$\begin{aligned} z^4 &= (x^4 - y^4)^2 = x^8 - 2x^4y^4 + y^8 \\ &= x^8 + 2x^4y^4 + y^8 - 4x^4y^4 = (x^4 + y^4)^2 - 4(xy)^4 \end{aligned}$$

即

$$z^4 + 4(xy)^4 = (x^4 + y^4)^2$$

类似于引理 6.5 的证法, 可证明 $z^4 + 4(xy)^4 = (x^4 + y^4)^2$ 无整数解, 所以, 方程 $x^4 - y^4 = z^2$ 无正整数解.

例 6 证明若直角三角形的三边都是正整数, 那么, 它的面积不可能是平方数.

证 设勾股数 x, y, z 是直角三角形的三边, 则 $x^2 + y^2 = z^2$, 且三角形的面积为 $\frac{1}{2}xy$. 假若 $\frac{1}{2}xy$ 是一个平方数, 设为 u^2 , 那么, $2xy = 4u^2$. 于是得

$$(x + y)^2 = z^2 + 4u^2, \quad (x - y)^2 = z^2 - 4u^2$$

将上面的两个等式相乘得

$$(x^2 - y^2)^2 = z^4 - 16u^4 = z^4 - (2u)^4$$

即

$$z^4 - (2u)^4 = (x^2 - y^2)^2 \tag{6.4}$$

由上面的例 5 知式 (6.4) 没有整数解. 因此, 不存在 u^2 使得 $\frac{1}{2}xy = u^2$.

例 7 证明不定方程 $x^2 + y^2 = z^4$ 的满足条件 $(x, y) = 1$ 的一切正整数解均可以表示成

$$x = 4st(s^2 - t^2), \quad y = 6s^2t^2 - s^4 - t^4, \quad z = s^2 + t^2 \quad (6.5)$$

或

$$x = 6s^2t^2 - s^4 - t^4, \quad y = 4st(s^2 - t^2), \quad z = s^2 + t^2 \quad (6.6)$$

其中, $s > t > 0$, $(t, s) = 1$, 且 $s \not\equiv t \pmod{2}$.

证 将不定方程 $x^2 + y^2 = z^4$ 变形为

$$x^2 + y^2 = (z^2)^2 \quad (6.7)$$

由定理 6.13 可知, 当 $2 \mid x$ 时, 存在正整数 $m > n > 0$, $(m, n) = 1$, 且 $m \not\equiv n \pmod{2}$ 使得

$$x = 2mn, \quad y = m^2 - n^2, \quad z^2 = m^2 + n^2 \quad (6.8)$$

是不定方程(6.7)的通解.

不妨设 $2 \mid m$, 则再次由定理 6.13 可知, 存在正整数 $s > t > 0$, $(t, s) = 1$, 且 $s \not\equiv t \pmod{2}$, 使得不定方程

$$z^2 = m^2 + n^2 \quad (6.9)$$

的通解可表示为

$$m = 2st, \quad n = s^2 - t^2, \quad z = s^2 + t^2 \quad (6.10)$$

将式(6.10)代入式(6.8), 可得式(6.5)是不定方程 $x^2 + y^2 = z^4$ 的通解.

对于 $2 \mid y$ 的情况, 可类似证明式(6.6)是不定方程 $x^2 + y^2 = z^4$ 的通解.

思考题、研究题六

1. 将一个正整数乘 3 减 2 后, 再将得到的数乘 3 减 2, 如此继续. 证明这种运算一定可以进行到某有限次后, 得到的数能被 2008 整除.

2. 对任意给定的正整数 n , 证明存在一个直角三角形, 其内切圆的半径等于 n .

3. 对任意给定的正整数 n , 证明如果 n 不能表示成两个整数的平方和, 那么, n 也不能表示成两个有理数的平方和.

4. 证明存在无限组勾股数 x, y, z , 使 x, y 是连续的正整数.

5. 求不定方程 $x_1^4 + x_2^4 + \cdots + x_7^4 = 2008$ 的所有整数解.

6. 证明方程 $x^2 + y^2 = z^3$ 有无限个正整数解.

7. 证明任意 4 个连续的整数, 至少有一个整数不能表示成两个整数的平方和.

8. 证明下列诸结论.

(1) 如果一个素数 p 能表示成两个或四个不同的素数的平方和, 那么, 其中的一个素数必等于 2.

(2) 如果一个素数 p 能表示成三个不同的素数的平方和, 那么, 其中的一个素

数必等于 3.

(3) 如果 n 是两个互素的素数的平方和, 那么, n 的任意一个正因子都可以表示成两个整数的平方和.

9. 对于给定的正整数 n , 证明至少有 n 组勾股数, 它们的第一个数相同.

10. 证明 $x^2 + (x+1)^2 = x^3$ 没有正整数解.

11. 求方程 $x^4 + 4y^4 = 2(z^4 + 4u^4)$ 的正整数解.

12. 证明存在任意大的整数, 它不能表示成 4 个正整数的平方和.

13. 证明对于每个正整数 m , 方程

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

存在解 x_1, x_2, x_3, x_4 使得 $x_i \geq m, i=1, 2, 3, 4$.

14. 对于正整数 n , 用 $M(n)$ 表示满足如下条件的最大整数: 对每个正整数 $k \leq M(n), n^2$ 均可以表示成 k 个正整数的平方和. 证明

(1) 对每个 $n \geq 4$, 有 $M(n) \leq n^2 - 14$.

(2) 试求出一个正整数 n , 使得 $M(n) = n^2 - 14$. 进而证明存在无限多个正整数 n , 使得 $M(n) = n^2 - 14$ (此题为 1992 年第 33 届国际数学奥林匹克竞赛题).

15. 求不定方程

$$1 + 2^x + 2^{2x+1} = y^2$$

所有的整数解 (此题为 2006 年的第 47 届国际数学奥林匹克竞赛题).

第 7 章 初等数论在密码学中的应用

密码学是研究信息及信息系统安全与保密的科学,是数学科学与计算机科学相结合的产物. 数学理论是密码学的基础. 密码学中涉及的数学理论知识主要有初等数论、代数学、组合数学及概率论.

在密码体制中,传递者要传递的信息叫做明文,传递者用密钥把明文加密变成密文,然后把密文传给消息的合法接收者,最后消息的合法接受者用同一个密钥(或另外一个密钥)解密密文得到明文.

因使用密钥个数及方式的不同,密码学可分为单钥密码学与双钥密码学,相应的密码体制或算法则称为单钥密码体制与双钥密码体制. 单钥密码学又称为私钥密码学或对称密码学. 在私钥密码体制中,只有信息的传递者和信息的合法接收者知道密钥. 如果攻击者能找到密钥或者截获密文,那么,他也可能计算出密钥并且恢复出明文.

双钥密码学又称公钥密码学或非对称密码学,其概念是由 Diffie 和 Hellman 于 1976 年首次提出的. 双钥密码体制与单钥密码体制的主要区别在于:单钥密码体制中加密算法与解密算法使用同一个密钥或等价的一对密钥,而双钥密码体制中加密算法与解密算法则使用完全不同的密钥. 也就是说,从加密密钥中解出解密密钥是不可行的,反之亦然.

本章介绍初等数论的一些理论知识在古典密码术与公钥密码学上的应用.

7.1 古典密码术

古典密码的特征主要是以纸和笔进行加密与解密操作的密码术时代,这时,密码还远没有成为一门科学,而仅仅是一门技艺或技术. 古典密码的基本技巧都是较简单的代替、置换或二者混合使用.

古典密码的历史最早可追溯到 4000 多年前雕刻在古埃及法老纪念碑上的奇特的象形文字. 不过,这些奇特象形文字纪录可能并不是用于严格意义上秘密通信的,而更可能仅是为了神秘、娱乐等目的.

下面介绍同余理论在一些比较典型的古典密码术中的应用例子.

(1) Caesar 密码. Caesar 密码大约出现于公元前 100 年的高卢战争期间,是古罗马统治者 Caesar 为了秘密传达战争计划或命令. Caesar 密码就是以 Caesar 的名字命名的. Caesar 密码的规则是将明文信息中的每个字母,用它在字母表中位

置的右边的第 k 个位置上的字母代替,从而获得相应的密文. 如 $k=3$ 时,明文字母与密文字母的对应关系可用置换表表示如下:

$$\begin{pmatrix} A B C D E F G H I J K L M N O P Q R S T U V W X Y Z \\ D E F G H I J K L M N O P Q R S T U V W X Y Z A B C \end{pmatrix}$$

于是,对于明文信息 secret message,可得其相应的密文为 vhfuhw phvjh.

在 Caesar 密码中,参数 k 就是密钥. 如果 26 个字母用 0 至 25 的整数替代,即 1 代 a, 2 代 b, ..., 25 代 y, 0 代 z. 那么, Caesar 加密运算其实就是计算同余式

$$c = m + k \pmod{26}$$

其中, m 是明文字母对应的数, c 就是对应的密文字母代表的数, 密钥 k 是 1 至 25 内的任何一个确定的数.

Caesar 密码属于单表代换密码.

(2) Vigenère 密码. Vigenère 密码是由法国密码家、外交家 Vigenère 在 1586 年提出的一种多表代换密码,其代换原则基于下列字母对应表,每行都对应于一个 Caesar 密码代换表,即第 t ($0 \leq t \leq 26$) 行对应于密钥 $k=t$ 的 Caesar 密码代换表:

	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

每次在加密信息时,需要利用此表及一个关键词,即密钥.具体地说,加密一条明文信息时,须对每一个明文的字母,先从表的顶端找出明文字母所在得列,然后再从最左边找出相应的密钥字母所在的行,那么,对应该明文字母的密文字母就是表中此列与此行交叉位置上的字母.解密时,在最左边找出相应的密钥字母所在的行,然后沿着此行找出密文字母,那么,密文字母所对应的最顶端的字母就是相应的明文字母.一般来说,使用的密钥比明文短,所以,密钥一般是周期性地重复使用,即将加长到与明文相同的长度.

例如,假设明文信息为

$$m = \text{Please keep this message in secret}$$

密钥为 computer,那么,加密后的密文为

$$c = \text{RZQPMX OVGD FWCL QVUGMVY BR JGQDTN}$$

如果像上面一样将 26 个字母 A 至 Z 分别用 0 至 25 的 26 个数字代替,那么, Vigenère 密码的加密计算同样可用数学式子来表示. 设 $m = m_1 m_2 \cdots m_t$ (每个 m_i 代表一个字母) 是明文, $k = k_1 k_2 \cdots k_t$ (每个 k_i 代表一个字母) 是密钥. 记加密后的密文为 $c = c_1 c_2 \cdots c_t$, 则

$$c_i = m_i + k_i \pmod{26}$$

这里作模运算时 m_i 与 k_i 分别取对应的数字.

所以, Vigenère 密码可以看成 Caesar 密码的推广.

(3) Hill 密码. Hill 密码是在 1929 年由 Hill 发明的,其主要思想是基于同余类环 \mathbb{Z}_n 上的线性变换.

在 Hill 密码中,首先将字母集编码称数字,如将 26 个英文字母 A, B, \cdots , Z 分别编码成 0, 1, 2, \cdots , 25. 密钥就是剩余类环 \mathbb{Z}_{26} 上的一个方阵,可称为密钥矩阵. 在加密前,明文则需要先按字母分组成若干个长度为密钥矩阵阶数的明文组. 设密钥矩阵为 n 阶方阵 $\mathbf{K} = (k_{i,j})_{n \times n}$, 那么,明文 \mathbf{M} 就按字母分成若干个长度为 n 的明文组(看成一个 n 元向量), 记为 $\mathbf{M} = \mathbf{M}_1 \mathbf{M}_2 \cdots \mathbf{M}_t$, 其中, $\mathbf{M}_i = (m_{i,1}, m_{i,2}, \cdots, m_{i,n})$ ($i = 1, 2, \cdots, t$), 则加密后的密文为 $\mathbf{C} = \mathbf{C}_1 \mathbf{C}_2 \cdots \mathbf{C}_t$, 其中

$$C_i = M_i K = (m_{i,1}, m_{i,2}, \dots, m_{i,n}) \begin{pmatrix} k_{1,1} & k_{1,2} & \dots & k_{1,n} \\ k_{2,1} & k_{2,2} & \dots & k_{2,n} \\ \vdots & \vdots & & \vdots \\ k_{n,1} & k_{n,2} & \dots & k_{n,n} \end{pmatrix} \pmod{26}, i=1, 2, \dots, t$$

这里的矩阵运算为剩余类环 \mathbb{Z}_{26} 上的矩阵乘积, 即须对乘积后的每个矩阵元作取模 26 运算.

如果将明文 M 记成

$$M = \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_t \end{pmatrix}$$

则加密运算可表示成剩余类环 \mathbb{Z}_{26} 上的矩阵乘积: $C = MK = (m_{i,s})_{t \times n} (k_{i,j})_{n \times n} \pmod{26}$.

由线性代数知识可知, 如果密钥矩阵不可逆, 那么, 不同明文的密文可能会相同, 因此, 密钥矩阵须取为可逆矩阵. 由密文恢复出明文的运算为 $M = CK^{-1} \pmod{26}$, 其中, K^{-1} 为 K 的逆矩阵.

7.2 RSA 公钥密码体制

RSA 是公钥密码体制, 它是由 Rivest、Shamir 及 Adleman 在 1977 年共同发明的, 其安全性是建立在大整数素因子分解问题的困难性基础上. 大整数素因子分解问题是一个公认的计算上困难的问题, 即是一个 NP 问题. RSA 的私钥是一对大素数 (150 位以上的十进制数), 从密文和公钥中恢复出明文的难度等价于分解两个大素数的乘积.

RSA 公钥加密算法如下.

(1) 密钥生成.

① 用户 Alice 选择两个大素数 p, q (150 位以上的十进制数), 计算出 $n = pq$, $\varphi(n) = (p-1)(q-1)$.

② Alice 随机选择与 $\varphi(n)$ 互素的整数 e ($1 < e < \varphi(n)$), 用 Euclid 扩展算法计算出解密密钥 d , 使得 $ed \equiv 1 \pmod{\varphi(n)}$.

③ Alice 把公钥 $k_1 = (n, e)$ 公开, 把私钥 $k_2 = (p, q, d)$ 保密.

(2) 加密运算.

① 用户 Bob 若想给 Alice 发送消息. 那么, Bob 得到 Alice 的真实公钥 $k_1 = (n, e)$.

② Bob 把消息 m 分成比 n 小的数据组 (采用二进制数, 选取小于 n 的 2 的最

大次幂). 也就是说, 如果 p, q 为 150 位的素数, 那么, n 将为 300 位. 每个明文消息单元, 即明文消息分组 m_i 应小于 300 位长的十进制数. 如果需要加密固定的消息分组, 那么, 可以在它的左边填充一些 0 并确保该数比 n 小.

③ Bob 计算 $c_i = m_i^e \pmod{n}$.

④ Bob 把由相同长度的分组密文 c_i 组成的密文 c 发送给 Alice.

(3) 解密运算.

当 Alice 收到密文 c 或分组密文 c_i 后, 计算 $c_i^d \pmod{n}$ 就可恢复出明文 m_i , 进而恢复明文消息 m . 这是因为

$$c_i^d = (m_i^e)^d = m_i^{ed} = m_i^{1+k\varphi(n)} \equiv m_i \pmod{n}$$

假设明文与密文均是有 N 个字母的字母表的字母构成的消息. 选择适当的正整数 $k < l$, 使得 N^k 和 N^l 大约都是 300 位的十进制数. 设明文消息单元都是 k 字母块, 即明文消息单元可看成以整数 N 为基的 k 重数组 (即 k 比特数组). 也就是说, 每个明文消息单元组看成是 0 到 N^k 之间的某个数值. 同样, 设密文消息单元是 l 字母块, 那么, 每个密文消息单元看成是 0 到 N^l 之间的某个数值.

用户 Alice 选择大素数 p_A 和 q_A , 使得 $n_A = p_A \cdot q_A$ 满足 $N^k < n_A < N^l$. 那么, 任意的明文消息单元均与 \mathbb{Z}_{n_A} 中的某个元素对应. 并且由于 $n_A < N^l$, 密文消息单元就是唯一的 l 字母块.

例 7.1 为了便于说明, 选择比较小的数字 $N=26, k=3, l=4$, 即明文消息单元是由通常字母表 (也就是 A~Z 共 26 个字母, 它们分别对应于 0~25 个数字) 中的三字母块组成, 密文消息单元是由通常字母表中的四字母块组成. 假设用户 Alice 的公钥为 $k_A = (n_A, e_A) = (46927, 39423)$, 若用户 Bob 想要给 Alice 发送明文消息 'YES'. 那么, Bob 首先找到 Alice 的公钥 $k_A = (n_A, e_A) = (46927, 39423)$ (即加密密钥); 其次, 计算出 'YES' 所对应的数值, 即 $24 \times 26^2 + 5 \times 26 + 18 = 16346$; 再次, 计算 $16346^{39423} \pmod{46927} = 21166$; 最后, 把 21166 表示为 $21166 = 1 \times 26^3 + 5 \times 26^2 + 8 \times 26 + 2 = \text{'BFIC'}$, 并把 'BFIC' 发送给用户 Alice.

例 7.2 设 RSA 算法中公钥为 (3337, 79), 私钥为 (47, 71, 1019), 应用 RSA 算法加密 $m=882326879666683$.

解 首先把 m 按三位数字一分组就可以进行加密, 消息 m 将分成 6 个分组 m_i 进行加密.

$$m_1 = 688, \quad m_2 = 232, \quad m_3 = 687, \quad m_4 = 966, \quad m_5 = 668, \quad m_6 = 003$$

对于第一分组, 加密为

$$688^{79} \pmod{3337} = 1571 = c_1$$

对其他分组进行同样的加密之后得到密文

$$c = 1570 \ 2756 \ 2091 \ 2276 \ 2423 \ 158$$

解密消息时, 需要用解密密钥 $d=1019$ 进行相同的指数运算, 因而

$$1571^{1019} \pmod{3337} = 688 = m_1$$

消息的其余部分用同样的方法恢复出来.

在 RSA 公钥密码系统中,解密时需要整数 d, n , 计算 d 时,必须知道 $e, \varphi(n)$. 由于 $\varphi(n) = (p-1)(q-1)$, 因此,必须能够因子分解 n . 下面定理说明了求 $\varphi(n)$ 和把 n 分解成 $n = pq$ 是同等困难的问题.

定理 7.1 设 n 是两个不同的奇素数的乘积, n 的素因子是一元二次方程

$$x^2 - (n+1 - \varphi(n))x + n = 0$$

的根,即 $\varphi(n)$ 决定着 n 的素因子分解.

证 如果 $n = pq$, 那么

$$\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - \frac{n}{p} + 1$$

因此

$$p - (n+1 - \varphi(n)) + \frac{n}{p} = 0$$

即

$$p^2 - (n+1 - \varphi(n))p + n = 0$$

同理可得

$$q^2 - (n+1 - \varphi(n))q + n = 0$$

所以, p, q 是一元二次方程 $x^2 - (n+1 - \varphi(n))x + n = 0$ 的两个根.

例如,如果 $n = 221$, $\varphi(n) = 192$, 那么,一元二次方程 $x^2 - 30x + 221 = 0$ 的两个根为 $x_1 = 13, x_2 = 17$. 因此, $n = 221 = 13 \times 17$.

在本节的最后,我们介绍在 RSA 公钥加密算法中的主要运算,即求幂的算法(平方-乘法),以及扩展 Euclid 算法.

算法 7.1 求幂的模指数算法(平方-乘法).

假设要计算 a^m , 其中, a 和 m 都是正整数,若将 m 表示为二进制数 $b_k b_{k-1} \cdots b_0$,

则有 $m = \sum_{b_i \neq 0} 2^i$, 因此, $a^m = a \sum_{b_i \neq 0} 2^i = \prod_{b_i \neq 0} a^{2^i}$, 故

$$a^m \pmod{n} = \left(\prod_{b_i \neq 0} a^{2^i} \pmod{n} \right) \pmod{n}$$

所以,有下面的模指数算法.

输入: 正整数 $a (0 \leq a < n), m (0 \leq m < n)$.

输出: $a^m \pmod{n}$.

(1) m 转化成二进制表示 $m = (b_k b_{k-1} \cdots b_0)_2$.

(2) (初始化) $c \leftarrow 0, d \leftarrow 1$.

(3) 对 i 从 k 依次减小到 0 , 执行

① $c \leftarrow 2c$;

② $d \leftarrow d \times d \pmod{n}$;

③ 如果 $b_i = 1$, 执行:

(i) $c \leftarrow c + 1$;

(ii) $d \leftarrow d \times a \pmod{n}$.

(4) 输出 d .

例 7.3 求 $7^{560} \pmod{561}$.

解 由于 $560 = (1000110000)_2$, 为了便于理解, 用表 7.1 解释.

表 7.1

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
d	7	49	157	526	160	241	298	166	67	1

因此, $7^{560} \pmod{561} = 1$.

实际求 $a^m \pmod{n}$ 的值时, 可将计算 c 的步骤去掉, 即改成

输入: 正整数 $a (0 \leq a < n)$, $m (0 \leq m < n)$.

输出: $a^m \pmod{n}$.

(1) m 转化成二进制表示 $m = (b_k b_{k-1} \cdots b_0)_2$.

(2) $P \leftarrow 1$.

(3) 对 i 从 k 依次减小到 0, 执行

① $P \leftarrow P \times P \pmod{n}$;

② 如果 $b_i = 1$, 执行 $P \leftarrow P \times a \pmod{n}$.

(4) 输出 d .

将上述算法用 Maple 编程算法如下:

```
>power:=proc(a,m,n)
local L,l,i,P;
L:=convert(m,base,2):
l:=nops(L)-1:
P:=1:
for i from l+1 by -1 to 1 do
P:=P*P mod n:
if L[i]=1 then P:=P*a mod n
fi:
od:
print(P):
end:
```

利用该 Maple 算法计算例 6.3 可得 $\text{power}(7, 560, 561) = 1$. 当然, 可利用 Maple 函数 $\text{modp}()$ 直接进行模指数运算, 如 $\text{modp}(7^{560}, 561) = 1$.

算法 7.2 扩展 Euclid 算法.

输入: 非负整数 $a, b (a > b)$.

输出: $d = (a, b)$ 和满足等式 $as + bt = d$ 的整数 s 和 t .

- (1) $u = a, v = b$.
- (2) $s \leftarrow -1, s_1 \leftarrow 0, t \leftarrow 0, t_1 \leftarrow -1$.
- (3) 如果 $v = 0$, 那么, $d \leftarrow u$, 返回 (d, s, t) .
- (4) 如果 $v > 0$, 执行
 - ① $q \leftarrow \left[\frac{u}{v} \right], r \leftarrow u - qv$;
 - ② $u \leftarrow v, v \leftarrow r$;
 - ③ $s_0 \leftarrow s - qs_1, t_0 \leftarrow t - qt_1$;
 - ④ $s \leftarrow s_1, s_1 \leftarrow s_0, t \leftarrow t_1, t_1 \leftarrow t_0$.
- (5) 输出 (u, s, t) .

例 7.4 用扩展 Euclid 算法求 $(4864, 3458)$, 及满足

$$4864 \cdot s + 3458 \cdot t = (4864, 3458)$$

的 s, t .

解 为了便于理解, 用表 7.2 解释.

表 7.2

q	s_0	t_0	u	v	s	s_1	t	t_1
			4864	3458	1	0	0	1
1	1	-1	3458	1406	0	1	1	-1
2	-2	3	1406	646	1	-2	-1	3
2	5	-7	646	114	-2	5	3	-7
5	-27	38	114	76	5	-27	-7	38
1	32	-45	76	38	-27	32	38	-45
2	-91	128	38	0	32	-91	-45	128

可得 $(4864, 3458) = 38, s = 32, t = -45$.

可用 Maple 编程实现扩展 Euclid 算法如下:

```
> Ex_Euclid: = proc(a, b)
  local u, v, d, q, r, s, s0, s1, t, t0, t1;
  u: = a; v: = b;
  s: = 1; s1: = 0; t: = 0; t1: = 1;
  while v > 0 do
```



```

q:= floor(u/v); r:= u-q*v;
u:= v; v:= r;
s0:= s-q*s1; t0:= t-q*t1;
s:= s1; s1:= s0; t:= t1; t1:= t0

od;
d:= u;
printf("( %d, %d) = %d = %d* %d + %d* %d", a, b, d, a, s, b, t);
end:

```

如例 7.4, 用 Ex_Euclid() 计算可得

```

> Ex_Euclid(4864, 3458);
(4864, 3458) = 38 = 4864 * 32 + 3458 * -45

```

在 Maple 中, 其实有一个实现扩展 Euclid 算法的函数 igcdex(). 如求例 7.4 中最大公约数及 s 与 t .

```

> igcdex(4864, 3458, 's', 't');
                                     38
> s, t;
                                     32, -45

```

练 习 7.2

1. 说明文和密文都是用下面的 40 个字母构成的消息. 英文字母表. A~Z 分别依次对应于 0~25, 数字 0~9 分别依次对应于 30~39, 而符号“空格”、“.”、“?”及“\$”则分别对应于 26、27、28 及 29. 说明文消息单元是两字母块, 密文消息单元是三字母块, 也就是 $k=2, l=3, 40^2 < n_A < 40^3$.

(1) 已知用户 Alice 的公钥是 $(n_A, e_A) = (2047, 179)$, 若想给用户 Alice 发送明文消息“SEND \$7500”, 需要发送的密文是什么?

(2) 请通过因子分解 n_A 破译出公钥 (n_A, e_A) 所对应的私钥 (n_A, d_A) .

2. 试着把 RSA 密码系统中加密公钥 $(n_A, e_A) = (536813567, 3602561)$ 所对应的私钥破译出来. 若已经知道明文消息单元是通常的英文字母表 (A~Z 共 26 个字母) 的六字母块, 且加密之后的密文为“BNBPPKZAVQZLBJ”, 所对应的明文是什么?

3. 说明文和密文的消息单元都是三字母块, 且明文用下面的 27 个字母的字母表. A~Z 对应于 0~25, 符号“空格”对应 26. 密文用上面的 27 个字母外加一个符号“/”(其数值等于 27). 并且要求每一个用户 Alice 选择 n_A 时满足 $27^3 < n_A < 28^3$, 这样, 每一个明文块对应于唯一的一个 $P \pmod{n_A}$, 并且 $C = P^{e_A} \pmod{n_A}$ 与 28 个字母的字母表中的三字母块唯一对应.

(1) 若解密密钥是 $k_D = (n, d) = (21583, 20787)$, 解密消息“YSNAUOZHXXH”;

(2) 如果在(1)中已经知道 $\varphi(n) = 21280$, 求

① $e \equiv d^{-1} \pmod{\varphi(n)}$;

② 因式分解 n .

(3) 设 n 是一个无平方根的整数(即 n 是不同的素因子的乘积), d, e 都是正整数且满足 $p-1$ 整除 $de-1$ (p 是 n 的任意的素因子, 也就是说, $de \equiv 1 \pmod{\varphi(n)}$), 证明对于任意的正整数 a , 都有 $a^{de} \equiv a \pmod{n}$.

7.3 ElGamal 公钥密码系统

ElGamal 公钥密码体制是 1985 年 7 月由 ElGamal 发明的, 它是建立在解有限乘法群上的离散对数问题的困难性基础之上的一种公钥密码体制, 其既可以用于数字签名, 也可以用于加解密. 该密码体制至今仍被认为是一个安全性能较好的公钥密码体制, 目前被广泛应用于许多密码协议中.

定义 7.1 如果 G 是一个 n 阶循环群, $y \in G$, 且 g 是 G 的一个生成元, 那么, y 对底数 g 的离散对数就是使得 $y = g^x$ 成立的唯一整数 x ($0 \leq x \leq n-1$). 记作 $x = L_g(y)$ 或 $x = L_{n,g}(y)$.

例 7.5 设 $G = \mathbb{Z}_{19}^*$, 2 是 G 的一个生成元. 求 7 对底数 2 的离散对数.

解 因为 2 是 19 的一个生成元, 所以, $G = \mathbb{Z}_{19}^*$ 中任意一个元素都可以表示成 2 的方幂的形式. 而且, $7 \equiv 2^6 \pmod{19}$. 因此, 7 对底数 2 的离散对数是 6, 即 $L_{19,2}(7) = 6$.

例 7.6 设 $G = \mathbb{Z}_9^*$ 且 $\alpha \in \mathbb{Z}_9^*$ 是方程 $x^2 - x - 1$ 的一个根, 求 -1 对底数 α 的离散对数.

解 因为 $x^2 - x - 1$ 是 $\mathbb{Z}_3[x]$ 的一个本原(不可约)多项式, 且 α 是方程 $x^2 - x - 1$ 的一个根, 所以, α 是 $G = \mathbb{Z}_9^*$ 中的一个生成元, 即 $G = \mathbb{Z}_9^*$ 的任意一个元素都可以表示成 α 的方幂的形式, 而

$\alpha^1 = \alpha$, $\alpha^2 = \alpha + 1$, $\alpha^3 = (\alpha + 1)\alpha = -\alpha + 1$, $\alpha^4 = (-\alpha + 1)\alpha = -\alpha^2 + \alpha = -1$
因此, -1 对底数 α 的离散对数是 4, 即 $L_\alpha(-1) = 4$.

基于乘法群 \mathbb{Z}_p^* 的 ElGamal 公钥密码算法如下.

(1) 公开参数.

假定用户 Alice 希望接收用 ElGamal 加密系统加密的消息. 那么, 用户 Alice 首先选取一个大素数 p (目前一般认为 p 应为 160 位以上的十进制素数), 并取 g 是乘法群 $\mathbb{Z}_p^* = \{1, \dots, p-1\}$ 的一个生成元.

(2) 密钥生成.

用户 Alice 随机选取整数 d : $0 < d < p-1$, 并计算 $\beta = g^d \pmod{p}$. 这里, p 与 g 是公开参数, β 是公开的加密密钥(公钥), d 是保密的解密密钥(私钥).

(3) 加密运算.

假定用户 Bob 要发送明文 P 给 Alice, 那么, Bob 执行下列步骤: ① 获得 Alice 的真实公钥 β , 以及公开参数 p 与 g ; ② 把明文信息 M 表示成 $\mathbb{Z}_p = \{0, 1, \dots, p\}$ 中的一个数据 m ; ③ 随机选择一个秘密数 k , 满足 $1 \leq k \leq p-2$; ④ 计算出 $c_1 \equiv g^k \pmod{p}$, $c_2 \equiv m\beta^k \pmod{p}$; ⑤ 将密文 $c = (c_1, c_2)$ 发送给用户 Alice.

(4) 解密运算.

Alice 对接收到的密文 $c = (c_1, c_2)$, 先验证 $c_i \in \mathbb{Z}_p^*$ 是否成立? 若不成立, 则拒绝接受 c 为 Bob 发送的真实密文, 否则, 执行下列大素数模运算:

$$m \equiv c_2 (c_1^d)^{-1} \pmod{p}$$

然后, 用户 Alice 从明文数据 m 恢复出明文信息 M .

下面验证从解密运算中得到的明文确实是原明文数据 m . 设 $c_2 (c_1^d)^{-1} \pmod{p} = m'$, 则

$$\begin{aligned} m' &\equiv c_2 (c_1^d)^{-1} \pmod{p} \equiv m\beta^k ((g^k)^d)^{-1} \pmod{p} \\ &\equiv m(g^{dk})(g^{-kd}) \pmod{p} \equiv m(g^{dk})(g^{-kd}) \pmod{p} \\ &\equiv m \pmod{p} \end{aligned}$$

即有 $m' = m$.

例 7.7 已知用户 Alice 选择的素数 $p = 2357$, \mathbb{Z}_{2357}^* 的一个生成元 $g = 2 \in \mathbb{Z}_{2357}^*$. Alice 的一个为私钥 $a_A = 1751$. 若用户 Bob 想发给 Alice 的消息为 $m = 2035$, 那么, Bob 需要发给 Alice 的密文是什么? Alice 如何恢复出明文消息 m (假若用户 Bob 选择的整数 $k = 1520$)?

解 由于 $\beta \equiv g^{a_A} \pmod{p} \equiv 2^{1751} \pmod{2357} = 1185$, 所以, Alice 的公开信息为

$$k_A = (p, g, \beta) = (2357, 2, 1185)$$

由于 Bob 选择的整数 $k = 1520$, 可以计算出

$$c_1 \equiv g^k \pmod{p} \equiv 2^{1520} \pmod{2357} = 1430$$

$$c_2 \equiv m\beta^k \pmod{p} \equiv 2035 \times 1185^{1520} \pmod{2357} = 697$$

因此, Bob 发给 Alice 的密文为 $c = (1430, 697)$.

Alice 收到密文 $c = (1430, 697)$ 之后计算

$$c_2 \cdot (c_1)^{-a_A} \equiv c_2 \cdot (c_1)^{p-1-a_A} \pmod{p} \equiv 697 \cdot 1430^{2357-1-1751} \pmod{2357} = 2035$$

这样, 就恢复出明文消息 $m = 2035$.

上面介绍的是基于乘法群 $\mathbb{Z}_p^* = \{1, 2, \dots, p\}$ 上建立的 ElGamal 公钥加密算法. 实际上, 可推广在任意有限循环群 G 上实现 ElGamal 公钥密码算法.

ElGamal 公钥加密算法的安全性是基于有限乘法群 \mathbb{Z}_p^* 上的离散对数问题, 即设 g 是模数 p 的一个原根, 已知 $b \in \mathbb{Z}_p^*$, 求解同余方程 $g^x \equiv b \pmod{p}$.

由于 g 是模数 p 的一个原根, 也即是乘法群 \mathbb{Z}_p^* 的生成元, 所以, $g^x \equiv b \pmod{p}$ 在 \mathbb{Z}_p^* 中一定有解. 若 $a_1, a_2 \in \mathbb{Z}_p^*$ 是该方程的解, 则有 $g^{a_1} \equiv g^{a_2} \pmod{p}$, 即得

$g^{a_1 - a_2} \equiv 1 \pmod{p}$, 于是 $a_1 - a_2 \equiv 0 \pmod{p-1}$, 亦即 $a_1 \equiv a_2 \pmod{p-1}$. 这说明 $g^x \equiv b \pmod{p}$ 在 \mathbb{Z}_p^* 中有唯一解.

我们简单地讨论一下此离散对数问题 $g^x \equiv b \pmod{p}$ 的求解.

首先, 由 Fermat 小定理可知

$$(g^{(p-1)/2})^2 = g^{p-1} \equiv 1 \pmod{p}$$

而 $\text{ord}_p(g) = p-1$, 因此必有

$$g^{(p-1)/2} \equiv -1 \pmod{p}$$

对于 $b \equiv g^x \pmod{p}$, 等号两边做 $(p-1)/2$ 次幂可得

$$b^{(p-1)/2} = g^{x(p-1)/2} \equiv (-1)^x \pmod{p}$$

因此, 如果 $b^{(p-1)/2} \equiv 1 \pmod{p}$, 则 x 是偶数. 如果 $b^{(p-1)/2} \equiv -1 \pmod{p}$, 则 x 是奇数.

例如, 要求解 $6^x \equiv 9 \pmod{11}$, 那么计算

$$9^{(p-1)/2} = 9^5 \equiv 1 \pmod{11}$$

因而 x 是偶数, 因此, x 可能为 2, 4, 6, 8 或 10, 经简单验算得知 $x=4$, 即 $L_6(9) = 4$.

从上例看出, 当判断出解 x 的奇偶性后, 再通过 $(p-1)/2$ 次验算来最后获得其确切值, 这等价于穷搜索法. 当 p 是一个比较大的素数时, 这种方法几乎是无效的. 下面介绍两个求解 \mathbb{Z}_p^* 上离散对数问题比较有效的算法, 即 Pohlig-Hellman 算法及指数演算法. 虽然这两算法比穷搜索法有效, 但它们的运行时间也至少是亚指数的. 所以, \mathbb{Z}_p^* 上的离散对数问题被认为是计算上困难的问题.

算法 7.3 Pohlig-Hellman 算法.

设 g 是素数 p 的一个原根, 已知 $b \in \mathbb{Z}_p^*$, 求解同余方程 $g^x \equiv b \pmod{p}$.

假设 $p-1$ 的标准分解式为

$$p-1 = \prod_i p_i^{r_i}$$

对于 $b \equiv g^x \pmod{p}$, 解出 $x \pmod{p_i^{r_i}}$, $i = 1, 2, \dots$. 若对每一个 i 都能求出 $x \pmod{p_i^{r_i}}$, 那么, 根据中国剩余定理就可以求出该离散对数.

可设

$$x = x_0 + x_1 \cdot p_i + x_2 \cdot p_i^2 + \dots + x_{r_i-1} \cdot p_i^{r_i-1}, 0 \leq x_i \leq p_i - 1$$

如果计算出系数 $x_0, x_1, \dots, x_{r_i-1}$, 则可求得 $x \pmod{p_i^{r_i}}$, $i = 1, 2, \dots$. 因为

$$\begin{aligned} x \cdot \frac{p-1}{p_i} &= x_0 \cdot \frac{p-1}{p_i} + (p-1)(x_1 + x_2 \cdot p_i + \dots + x_{r_i-1} \cdot p_i^{r_i-2}) \\ &= x_0 \cdot \frac{p-1}{p_i} + (p-1)n \end{aligned}$$

其中, $n = x_1 + x_2 \cdot p_i + \dots + x_{r_i-1} \cdot p_i^{r_i-2}$.

将 $b \equiv g^x \pmod{p}$ 等号两边作 $(p-1)/p_i$ 次幂运算, 得

$$b^{(p-1)/p_i} \equiv g^{x \cdot (p-1)/p_i} \equiv g^{x_0 \cdot (p-1)/p_i} (g^{p-1})^n \equiv g^{x_0 \cdot (p-1)/p_i} \pmod{p}$$

为了求 x_0 , 只需要计算下列幂运算:

$$g^{k \cdot (p-1)/p_i} \pmod{p}, \quad k = 0, 1, 2, \dots, p_i - 1$$

若 $g^{x_1} \equiv g^{x_2} \pmod{p}$, 则 $x_1 \equiv x_2 \pmod{p-1}$. 因此, $k(p-1)/p_i$ 对模数 $p-1$ 两两不同余. 所以, 存在唯一的 $k_0 \in \{0, 1, 2, \dots, p_i - 1\}$ 使得

$$g^{k_0 \cdot (p-1)/p_i} \equiv b^{(p-1)/p_i} \pmod{p}$$

这样, 就可以得到 $x_0 = k_0$.

为了求 x_1 , 令 $b_1 = b/g^{x_0}$, 则

$$b_1 = b/g^{x_0} \equiv g^{p_i \cdot (x_1 + x_2 \cdot p_i + \dots + x_{r_i-1} \cdot p_i^{r_i-2})} \pmod{p}$$

将等号两端作 $(p-1)/p_i^2$ 次幂, 得到

$$b_1^{(p-1)/p_i^2} \equiv g^{x_1 \cdot (p-1)/p_i} (g^{p-1})^{x_2 \cdot p_i + x_3 \cdot p_i + \dots + x_{r_i-1} \cdot p_i^{r_i-3}} \equiv g^{x_1 \cdot (p-1)/p_i} \pmod{p}$$

类似于求 x_0 , 存在唯一的 $k_1 \in \{0, 1, 2, \dots, p_i - 1\}$ 使得

$$g^{k_1 \cdot (p-1)/p_i} \equiv b_1^{(p-1)/p_i^2} \pmod{p}$$

这样, 就可以得到 $x_1 = k_1$.

同理, 可得系数 $x_2, x_3, \dots, x_{r_i-1}$, 所以得到 $x \pmod{p_i^{r_i}}$. 这样, 就可以确定 x 的值.

显然, 当 $p-1$ 的某个素因子 p_i 比较大时, 上述算法的计算复杂度等价于 $O(p_i)$, 因此等价于穷搜索法. 所以, Pohlig-Hellman 算法只当 $p-1$ 的所有素因子较小时才是一个比较有效的算法.

例 7.8 解离散对数问题

$$7^x \equiv 12 \pmod{41}$$

解 把 $p-1=41-1=40$ 因子分解成 $40=2^3 \times 5$.

首先, 设 $p_1=2$, 求 $x \pmod{2^3}$. 记 $x=x_0+2x_1+4x_2 \pmod{8}$, 由于

$$b^{(p-1)/2} = 12^{20} \equiv -1 \pmod{41}$$

且

$$g^{(p-1)/2} = 7^{20} \equiv -1 \pmod{41}$$

因为

$$b^{(p-1)/2} \equiv g^{x_0 \cdot (p-1)/2} \pmod{p}$$

所以, $x_0=1$.

其次, 令 $b_1 = b/g^{x_0} = 12/7 \equiv 31 \pmod{41}$, 由于

$$b_1^{(p-1)/2^2} = 31^{10} \equiv 1 \pmod{41}$$

且

$$g^{(p-1)/2} = 7^{20} \equiv -1 \pmod{41}$$

因为

$$b_1^{(p-1)/2^2} \equiv g^{x_1 \cdot (p-1)/2} \pmod{p}$$

所以, $x_1=0$. 继续计算, 可得

$$b_2 = b_1/g^{2x_1} \equiv 31 \pmod{41}$$

由

$$b_2^{(p-1)/2^3} \equiv g^{k_2 \cdot (p-1)/2} \pmod{p}$$

可得 $x_2=1$. 因此

$$x = x_0 + 2x_1 + 4x_2 \equiv 5 \pmod{8}$$

对于 $p_2=5$, 求 $x \pmod{5}$, 已知

$$b^{(p-1)/5} = 12^8 \equiv 18 \pmod{41}$$

且

$$g^{(p-1)/5} = 7^8 \equiv 37 \pmod{41}$$

依次计算

$$37^0 = 1, \quad 37^1 = 37, \quad 37^2 = 16, \quad 37^3 = 18$$

因此, $x \equiv 3 \pmod{5}$.

由于 $x \equiv 5 \pmod{8}$, 且 $x \equiv 3 \pmod{5}$. 根据中国剩余定理可得

$$x \equiv 13 \pmod{40}$$

即 $L_{41,7}(12) = 13$.

下面用实现 Pohlig-Hellman 算法的 Maple 程序.

```
>Pohlig_Hellman = proc(p, g, b)
local M, H, a, c, d, x, i, j, n, k, u, v, t;
M := ifactors(p-1)[2]:
for i from 1 to nops(M) do
H[i] := [seq(n, n=0..M[i][1]-1)];
for k in H[i] do
if modp(g^(k*(p-1)/M[i][1]) - b^((p-1)/M[i][1]), p) = 0 then
x[i, 0] := k;
break:
fi:
od:
d[i, 0] := b;
for j from 1 to M[i][2]-1 do
d[i, j] := modp(d[i, j-1]/g^((M[i][1])^(j-1) * x[i, j-1]), p):
for k in H[i] do
if modp(g^(k*(p-1)/M[i][1]) - d[i, j]^((p-1)/(M[i][1]^(j+1))), p)
= 0 then
x[i, j] := k;
```

```

        break;
      fi;
    od;
  od;
c[i] := add(x[i, j] * M[i][1]^j, j = 0..M[i][2] - 1);
od:
u := [seq(c[i], i = 1..nops(M))];
v := [seq(M[i][1]^M[i][2], i = 1..nops(M))];
a := chrem(u, v);
print(L[p, g](b) = a);
end:

```

如求例 7.8 中的离散对数 $L_{41,7}(12)$.

```
>Pohlig_Hellman(41, 7, 12);
```

$$L_{41,7}(12) = 13$$

又如求离散对数 $L_{32605967,5}(12)$ (32605967 是第 2008888 个素数).

```
>Pohlig_Hellman(32605967, 5, 12);
```

$$L_{32605967,5}(12) = 12397382$$

算法 7.4 指数演算法.

已知 p 是素数, b 是整数, g 是模数 p 的一个原根, 要求解同余方程 $b \equiv g^x \pmod{p}$.

首先, 有一个预备计算. 设 B 是上限值, p_1, p_2, \dots, p_n 是小于 B 的素数, 这些素数的集合称之为因子基. 选取一些不同的 k 值, 计算 $g^k \pmod{p}$. 对于计算出的每一个值, 试着表示为小于 B 的素数的乘积, 如果不能表示, 就将 $g^k \pmod{p}$ 舍弃. 如果

$$g^k \equiv \prod p_i^{r_i} \pmod{p}$$

那么

$$k \equiv \sum r_i L_g(p_i) \pmod{p-1}$$

当得到足够多的这样的关系后, 就能对每一个 i 求出 $L_g(p_i)$.

任取一个整数 s , 计算 $b \cdot g^s \pmod{p}$. 对每一个这样的数, 试着将其表示成小于 B 的素数的乘积. 如果能够写成这样的形式, 则有

$$b \cdot g^s \pmod{p} \equiv \prod p_i^{t_i} \pmod{p}$$

即

$$L_g(b) \equiv -s + \sum t_i L_g(p_i) \pmod{p-1}$$

当 p 比较大的时候, 这种算法的效率很高.

例 7.9 解同余式

$$2^x \equiv 37 \pmod{131}$$

解 假设取上限值 $B=10$, 用素数 $2, 3, 5, 7$ 进行计算, 分别选取 $k=1, 8, 12, 14, 34$, 计算 $2^k \pmod{131}$, 得到

$$2^1 \equiv 2 \pmod{131}$$

$$2^8 \equiv 5^3 \pmod{131}$$

$$2^{12} \equiv 5 \times 7 \pmod{131}$$

$$2^{14} \equiv 3^2 \pmod{131}$$

$$2^{34} \equiv 3 \times 5^2 \pmod{131}$$

因此

$$1 \equiv L_2(2) \pmod{130}$$

$$8 \equiv 3L_2(5) \pmod{130}$$

$$12 \equiv L_2(5) + L_2(7) \pmod{130}$$

$$14 \equiv 2L_2(3) \pmod{130}$$

$$34 \equiv L_2(3) + 2L_2(5) \pmod{130}$$

根据上面的同余式可得

$$L_2(3) \equiv 72 \pmod{130}, \quad L_2(5) \equiv 46 \pmod{130}, \quad L_2(7) \equiv 96 \pmod{130}$$

用试探法随机选择一些指数可以得到

$$37 \times 2^{43} \equiv 3 \times 5 \times 7 \pmod{131}$$

因此得

$$L_2(37) \equiv -43 + L_2(3) + L_2(5) + L_2(7) \equiv 41 \pmod{130}$$

故 $L_2(37) = 41$.

练习 7.3

1. 设 $p=19$, 那么, 2 是 19 的一个原根, 用 Pohlig-Hellman 算法计算 $L_2(14)$.
2. 设 g 是 p 的一个原根, 证明

$$L_g(y_1 \cdot y_2) = L_g(y_1) + L_g(y_2) \pmod{p-1}$$

3. 在 F_{181}^* 中用 Pohlig-Hellman 算法计算 $L_2(153)$ (已知 2 是 181 的一个原根).

4. 用户 A 接收用 ElGamal 公钥密码系统加密的消息, 它选择素数 $p=65537$ 和私钥 $a=13908, g=5$ 是 $p=65537$ 的一个原根. 若用户 B (用 A 的公钥 g^a 加密) 发给用户 A 的密文是 (29095, 23846). 假设用户 A 把 F_p 上的整数与 31 个字母的字母表 (A~Z 对应 0~25, blank=26, . =27, ? =28, ! =29, ' =30) 中的 3 字母块对应, 那么用户 A 解密恢复出的明文是什么?

5. 设你的明文消息单元是常用的字母表 (A~Z) 中的 18 字母块, 其中, 这些

字母块对应于基为 26 的 18 比特的整数. 若你收到基于素数 $p = 297262705009139006771611927$ 的乘法群上的 ElGamal 公钥密码系统, 且用你的公钥 g^a 加密而成的密文是

(82746592004375034872957717, 164063768437915425954819351)

如果你的私钥是 $a = 1038475684394756438549809$, 请恢复出明文消息.

6. 编写实现指数演算法的 Maple 程序.

7.4 MH 背包公钥密码系统

MH 背包公钥密码系统是 Merkle 与 Hellman 在 1978 年提出的, 该密码系统的安全性是基于背包问题(又称子集和问题)的难解性.

假设你有一个为将要远足旅行而准备的容积为 V 的大背包, 有一些体积为 $v_i (i=0, 1, \dots, k-1)$ 的 k 个物品打算放到你的背包里面. 假设你是一个经验丰富的背包包装师, 能把背包装满而不浪费一点空间. 也就是说, 你想找到集合 $\{0, 1, \dots, k-1\}$ 的子集 I (如果存在的话), 使得 $\sum_{i \in I} v_i = V$. 这就是通常所说的背包问题. 若假定 V 及所有的 $v_i (i=0, 1, \dots, k-1)$ 都是正整数, 则得下列背包问题的等价定义 7.2.

定义 7.2(背包问题) 已知有 k 个正整数的集合 $\{v_0, v_1, \dots, v_{k-1}\}$ 和一个整数 V . 如果存在一个 k 比特的整数(二进制数) $n = (\epsilon_{k-1}, \epsilon_{k-2}, \dots, \epsilon_1, \epsilon_0)_2$, 其中, $\epsilon_i = 0, 1$, 使得

$$\sum_{i=0}^{k-1} \epsilon_i v_i = V$$

依据定义, 背包问题又可称为子集和问题, 一般的背包问题是一个 NP-完全问题, 目前还没有找到它的多项式时间解法. 但对某些较“容易”的背包问题, 已经有很有效的解决方法. MH 背包公钥密码系统是利用一类超递增序列的背包问题来实现的.

一个正整数序列 (a_1, a_2, \dots, a_n) 称为超递增序列, 当且仅当对任意 $j > 1$, 有

$$a_j > \sum_{i=1}^{j-1} a_i$$

例如, $\{1, 3, 6, 13, 27, 52\}$, $\{2, 3, 7, 15, 31\}$ 都是超递增序列, 而 $\{1, 3, 4, 8, 16, 20\}$ 则不是.

超递增序列的背包问题可用穷搜索法在时间 $O(n)$ 内解决, 具体算法可描述如下.

算法 7.5 超递增序列的背包问题求解算法.

输入: 超递增序列 (a_1, a_2, \dots, a_n) 及一个正整数 S .

输出: 一个 n 元的 0-1 向量 $X = \{x_1, \dots, x_n\}$, 或“无解”.

(1) 对 i 自 n 递减到 1, 执行

如果 $S \geq a_i$, 那么, 令 $x_i = 1$; $S = S - a_i$, 否则, 令 $x_i = 0$.

(2) 如果 $\sum_{i=1}^n x_i a_i = S$, 那么, 输出 $X = \{x_1, \dots, x_n\}$, 否则, 输出“无解”.

该算法用 Maple 语言实现如下:

```
>Uknapp: = proc(A, S)
local T, X, n, i;
T: = S;
n: = nops(A);
for i from n by -1 to 1 do
  if T >= A[i] then X[i]: = 1: T: = T - A[i]
  else X[i]: = 0
  fi;
od;
if add(X[i] * A[i], i = 1..n) = S
  then print(X = seq(X[n - i], i = 0..n - 1));
  else printf("No solution!");
fi;
end;
```

例如, $\{2, 3, 7, 15, 33\}$ 与 $\{2, 3, 7, 16, 33\}$ 均是超递增序列, 它们对于 $S = 24$ 分别有解 $X = (0, 1, 1, 0, 1)$ 和无解.

```
>Uknapp([2, 3, 7, 15, 33], 24);
X = (0, 1, 1, 0, 1)
>Uknapp([2, 3, 7, 16, 33], 24);
No solution!
```

MH 背包公钥密码系统描述如下.

(1) 参数选定.

① Alice 秘密选定一个超递增序列 $A = \{a_1, a_2, \dots, a_n\}$, 并选定整数 M 与 W

满足 $M > \sum_{i=1}^n a_i$ 及 $\gcd(W, M) = 1$;

② 选择 $\{1, 2, \dots, n\}$ 上的一个置换 π , 并计算 $b_i \equiv W a_{\pi(i)} \pmod{M}$;

③ $B = \{b_1, b_2, \dots, b_n\}$ 是 Alice 的公开钥, 而 (A, π, W, M) 或 (π, W, M) 或 (W, M) 是她的私钥.

(2) 加密运算.

设 Bob 有信息明文 $m = m_1 m_2 \dots m_n$ (m 的二进制表示) 要秘密发送给 Alice. Bob 利用 Alice 的公钥 B 计算出密文 c , 并发送给 Alice

$$c = b_1 m_1 + b_2 m_2 + \cdots + b_n m_n$$

(3) 解密运算.

Alice 收到密文 c 后, 计算

$$S \equiv cW^{-1} \pmod{M}$$

对超递增序列 $A = \{a_1, a_2, \dots, a_n\}$ 及整数 S 利用超递增序列背包问题求解算法, 求得 r_1, r_2, \dots, r_n . 对 $i = 1, \dots, n$, 令 $m_i = r_{\pi(i)}$, 则恢复出明文 $m = m_1 m_2 \cdots m_n$.

(4) 验证运算.

$$\begin{aligned} cW^{-1} &\equiv (b_1 m_1 + b_2 m_2 + \cdots + b_n m_n)W^{-1} \pmod{M} \\ &\equiv ((b_1 W^{-1})m_1 + (b_2 W^{-1})m_2 + \cdots + (b_n W^{-1})m_n) \pmod{M} \\ &\equiv (a_{\pi(1)} m_1 + a_{\pi(2)} m_2 + \cdots + a_{\pi(n)} m_n) \pmod{M} \end{aligned}$$

这说明解密运算中求得的 $r_{\pi(1)}, r_{\pi(2)}, \dots, r_{\pi(n)}$ 的确为 m_1, m_2, \dots, m_n , 即准确地恢复出明文 $r_{\pi(1)} r_{\pi(2)} \cdots r_{\pi(n)} = m_1 m_2 \cdots m_n = m$.

在实际运用 MH 背包公钥密码系统时, 为节约运行时间, 可选 M 为素数, 置换 π 为单位置换.

关于 MH 背包公钥密码系统的安全性问题, 1983 年, Shamir 利用所谓的“陷门对”及公钥成功地破解了密钥, 即 MH 背包公钥密码系统已被破解. 此外, 还存在一个称为“格基约化”(lattice base reduction.) 的破解算法.

例 7.10 设明文消息单元是与从 $0 = (00000)_2$ 到 $25 = (11001)_2$ 的 5 比特的整数相对应的单个字母. 设 Alice 秘密选取的超递增序列是 $\{2, 3, 7, 15, 31\}$, 若取 $M = 61, W = 17$, 那么, Alice 的公钥是什么? 如果 Bob 想要秘密发送明文消息“WHY”给 Alice, 他需要传送的密文是什么?

解 由 $b_i = 17a_i \pmod{61}$ 可得 $B = \{34, 51, 58, 11, 39\}$, 故 Alice 的公钥为 $\{34, 51, 58, 11, 39\}$.

当 Bob 想要秘密发送明文消息‘WHY’时, 首先计算出对应的密文.

$$'W' = (10110)_2 \rightarrow 51 + 58 + 39 = 148$$

$$'H' = (00111)_2 \rightarrow 34 + 51 + 58 = 143$$

$$'Y' = (11000)_2 \rightarrow 11 + 39 = 50$$

然后将密文(148, 143, 50)发送给 Alice. Alice 收到密文(148, 143, 50)后, 可进行验证. 先计算出

$$148 \times 18 \pmod{61} \equiv 41, \quad 143 \times 18 \pmod{61} = 12, \quad 50 \times 18 \pmod{61} = 46$$

然后, 利用算法 7.5 分别对 $S = 41, 12$ 及 46 求解超递增序列问题的解, 可得 $(10110)_2, (00111)_2, (11000)_2$, 它们对应的明文即是“WHY”.

练习 7.4

1. 对于下列每一个序列和背包容量,判断是否为超递增背包问题?如是,则求其超递增背包问题的解.

$$(1) A_1 = \{2, 3, 7, 20, 35, 69\}, S_1 = 45.$$

$$(2) A_2 = \{1, 2, 5, 9, 20, 49\}, S_2 = 73.$$

$$(3) A_3 = \{2, 3, 6, 11, 21, 40\}, S_3 = 39.$$

$$(4) A_4 = \{4, 5, 10, 30, 50, 101\}, S_4 = 186.$$

2. 证明对任意一个序列,若对所有的 i , 都有 $v_{i+1} \geq 2v_i$, 那么, 该序列为超递增序列.

3. 设明文消息单元是通常的 26 个字母 A~Z 对应于 0~25 的单个字母. 已知用于加密的公钥是 $K_E = \{57, 14, 3, 24, 8\}$, 用于解密的私钥是 $(W^{-1}, M) = (23, 61)$. 假若你收到的消息单元是 14, 25, 89, 3, 65, 24, 3, 49, 89, 24, 41, 25, 68, 41, 71, 求出相应的明文消息.

4. 设明文消息单元是 A~Z 对应于 0~25, blank=26, ? =27, · =29, ' =30, \$ =31 的三字母词, 已知公钥是 $\{24038, 29756, 34172, 34286, 38334, 1824, 18255, 19723, 143, 17146, 35366, 11204, 32395, 12958, 6479\}$, 私钥是 $(W, M) = (6479, 47107)$; 若你收到密文消息是 152472, 116116, 68546, 165420, 168261, 请恢复出明文.

7.5 Rabin 公钥加密系统

1979 年, MIT 计算机科学实验室的 Rabin 提出了一种变形的 RSA 算法, 称之为 Rabin 算法.

Rabin 公钥密码体制是第一个可证明安全的公钥密码体制的例子. 也就是说, 破解该体制的困难性已被证明等价于大整数的素因数分解. 而破解 RSA 公钥密码体制的难度则不超过大整数的素因数分解, 且未被证明是与大整数的素因数分解等价的. 所以在理论上说, Rabin 公钥密码体制比 RSA 公钥密码体制具有更好的安全性. Rabin 公钥密码体制的一个缺点是接收者面临着需要从 4 个可能的明文中选择出正确的明文的问题. 在实际应用中, 解决此问题的一条途径是加密前在明文添加一些标识冗余码.

Rabin 公钥密码系统描述如下.

(1) 密钥生成.

假若用户 Alice 希望接收用 Rabin 公钥密码系统加密的消息, 那么, Alice 随机选择两个大素数 p 和 q (最好是 p, q 差不多一样大), 并计算 $n = pq$. Alice 的私钥

是 (p, q) , 公钥是 $k_A = n$.

(2) 加密运算.

如果用户 Bob 想发送明文消息 P 给 Alice, 那么, Bob 完成下列工作:

- ① 获得用户 Alice 的真实公钥 $k_A = n$;
- ② 把明文消息 P 表示成 $\{0, 1, \dots, n-1\}$ 中的某个整数 m ;
- ③ 计算 $c \equiv m^2 \pmod{n}$, 并将计算结果作为明文消息 P 的密文发送给 Alice.

(3) 解密运算.

Alice 收到 Bob 发来的密文消息 c 之后, 完成下列工作:

- ① 分别求出 $c \pmod{p}$ 的两个平方根, 可设为 r 与 $p-r$, 及 $c \pmod{q}$ 的两个平方根, 设为 s 与 $q-s$;
- ② 利用算法 7.2 (扩展 Euclid 算法) 求出满足 $ap + bq = 1$ 的 a 与 b ;
- ③ 计算 $m_1 = (aps + bqr) \pmod{n}$, $m_2 = (aps + bq(p-r)) \pmod{n}$, $m_3 = (ap(q-s) + bqr) \pmod{n}$, $m_4 = (ap(q-s) + bq(p-r)) \pmod{n}$;
- ④ 在 m_1, m_2, m_3, m_4 中必有一个等于 m .

所以, 要确定出有效的明文, 必须在要加密的明文中加入一些额外的信息, 如发送者的 ID、时间等信息.

当 $p, q \equiv 3 \pmod{4}$ 时, 因已知 c 是模 p 的平方剩余, 设 $r^2 = c \pmod{p}$, 则 $c^{(p-1)/2} = r^{p-1} = 1 \pmod{p}$. 于是, 由 $(p+1)/4$ 是整数, 可计算出

$$(c^{(p+1)/4})^2 = c^{(p+1)/2} = c^{(p-1)/2} \cdot c = c \pmod{p}$$

从而 $c^{(p+1)/4}$ 及 $p - c^{(p+1)/4}$ 是

$$x^2 = c \pmod{p}$$

的两个解. 同理可证, $c^{(q+1)/4}$ 及 $q - c^{(q+1)/4}$ 是

$$x^2 = c \pmod{q}$$

的两个解.

例 7.11 已知用户 A 选择公钥是 $k_A = 91687$ (即私钥是素数 $p = 277, q = 331$), 若用户 B 希望发给用户 A 的消息是 $P = 1001111001$ (二进制数), 为了易于解密, 假定用户 B 把消息的最后 6 比特串添加到消息的最后面, 那么, 用户 B 发给用户 A 的密文是什么? 用户 A 怎么恢复出明文消息?

解 首先, 用户 B 需要把 $P = 1001111001$ 变为 $P' = 1001111001111001$; 其次, 用户 B 把 $P' = 1001111001111001$ 表示成十进制数 $m = 40569$; 再次, 用户 B 计算 $c = m^2 \pmod{n} = 40569^2 \pmod{91689} = 62111$; 最后, 用户 B 把密文 $c = 62111$ 发给用户 A. 当用户 A 收到密文 $c = 62111$ 后: 首先, 结合上面的 Rabin 解密算法与下面的算法 7.6 可以计算出 62111 模数 91689 的 4 个平方根.

$$m_1 = 69654, \quad m_2 = 22033, \quad m_3 = 40569, \quad m_4 = 51118$$

其次, 分别把 m_1, m_2, m_3, m_4 表示成二进制数为

$$m_1 = 10001000000010110, \quad m_2 = 101011000010001$$

$$m_3 = 1001111001111001, \quad m_4 = 1100011110101110$$

由于只有 m_3 满足最后 6 比特是前面最后 6 比特的重复,故明文就是 m_3 ,进而可得明文消息就是 $P=1001111001$.

下面介绍求素数模的平方根算法.

算法 7.6 素数模的平方根算法.

输入:一个素数 p 和一个整数 $a(1 \leq a \leq p-1)$.

输出: a 模素数 p 的两个平方根(假设存在的话).

(1) 如果 $\left(\frac{a}{p}\right) = -1$,那么,整数 a 关于模 p 无平方根,否则,执行下列步骤.

(2) 随机选择整数 $b(1 \leq b \leq p-1)$ 使得 $\left(\frac{b}{p}\right) = -1$ (若 $\left(\frac{b}{p}\right) = 1$,则重新选择 b).

(3) 将 $p-1$ 表示成 $p-1=2^s t$,其中, t 是奇数.

(4) 利用扩展 Euclid 算法求出 $a^{-1} \pmod{p}$.

(5) 令 $c \leftarrow b^t \pmod{p}$, $r \leftarrow a^{(t+1)/2} \pmod{p}$.

(6) 对 i 从 0 到 $s-2$ 执行

① 计算 $d \equiv (r^2 \cdot a^{-1})^{2^{s-i-2}} \pmod{p}$;

② 如果 $d \equiv -1 \pmod{p}$,那么,令 $r \leftarrow r \cdot c \pmod{p}$;

③ 令 $c \leftarrow c^2 \pmod{p}$;

(7) 输出 $(r, p-r)$.

上面的算法来源于 Koblitz 的思想.

用 Maple 语言实现该算法如下:

```
>with(numtheory):
SqRoot:=proc(a,p)
local L,l,b,s,t,c,d,r,i:
if legendre(a,p)=-1 then
printf("%d has no square roots modulo %d!",a,p);
else
L:= [seq(k,k=1..p-1)];
for l in L do
if legendre(l,p)=-1 then
b:=l;
break;
fi;
od;
s:=1:t:=(p-1)/2:
```

```

while igcd(2, (p-1)/2^s) <> 1 do
  s := s + 1; t := t/2;
od;
c := modp(bt, p);
r := modp(a^((t+1)/2), p);
for i from 0 to s-2 do
  d := mods(((r^2)/a)^(2^(s-i-2)), p);
  if d = -1 then r := modp(r * c, p)
  fi;
  c := modp(c^2, p);
od;
if legendre(a, p) = -1 then
  printf("%d has no square roots modulo %d!", a, p);
else print(r, p-r);
fi;
fi;
end:

```

例如, 由于 $\left(\frac{186}{401}\right) = 1$, $\left(\frac{2008}{17467}\right) = -1$, 故 186 关于模 401 有平方根, 2008 关于模 17467 无平方根. 利用程序函数 SqRoot() 可得

```

> SqRoot(186, 401);
                                     304, 97
> SqRoot(2008, 17467);
2008 has no square roots modulo 17467!

```

当然, 可用 Maple 中的函数 msolve() 来求素数模的平方根, 如下所示:

```

> msolve(x^2 = 186, 401);
                                     {x = 97}, {x = 304}
> msolve(x^2 = 2008, 17467);

```

这里, 由于同余方程 $x^2 \equiv 2008 \pmod{17467}$ 无解, 所以, 运行 msolve($x^2 = 2008, 17467$) 后没有值输出.

练习 7.5

1. 已知素数 $p=800119$, 用算法 7.6 求 126 模数 p 的平方根.
2. 用孙子定理(中国剩余定理)解同余方程组

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{156061} \end{cases}$$

3. 解同余方程 $x^2 \equiv 621 \pmod{780305}$.

4. 在 Rabin 公钥密码系统中, 公钥 $n=77$, 计算明文 $m=2$ 的密文 c , 再将 c 解密恢复出明文.

5. 在 Rabin 公钥密码系统中, 公钥 $n=1152921515344265237$, 计算明文 $m=911008$ 的密文 c , 再将 c 解密恢复出明文 (提示: 素数 $p=1073741827$ 及素数 $q=1073741831$ 的乘积为 $n=1152921515344265237$).

6. 如果 p 与 q 是满足条件 $p \equiv q \equiv 3 \pmod{4}$ 且 $p \neq q$ 的素数, 则 $n=pq$ 称为 Blum 数. 在 Rabin 公钥密码体制中, 取 Blum 数 $n=419 \times 431=180589$.

(1) 设有明文信息 $m=20052005$, 计算其相应的密文.

(2) 如果密文信息为 $c=123456$, 则可能的明文信息是什么?

(3) 一般来说, 在 Rabin 公钥密码体制下, 对一条确定的密文信息, 有四条可能的明文信息. 请问你有何方法来确定出唯一的明文?

第7章综合例题

例1 假设 m 是明文消息 (未知), 两个加密密钥是 e_1, e_2 且 $(e_1, e_2)=1$, 若在 RSA 密码系统中分别用 e_1, e_2 对共同的模数 n 取模得到的密文是

$$c_1 \equiv m^{e_1} \pmod{n} \text{ 与 } c_2 \equiv m^{e_2} \pmod{n}$$

那么, 明文消息 m 是?

解 由于 $(e_1, e_2)=1$, 由扩展 Euclid 算法可以找到 r, s 使得

$$re_1 + se_2 = 1$$

由于 r, s 必为一正一负, 不妨设 $r < 0$, 于是, 由辗转相除法可以求出 c_1^{-1} , 然后计算

$$(c_1^{-1})^{-r} \cdot c_2^s \equiv (m^{-e_1})^{-r} (m^{e_2})^s \equiv (m)^{re_1 + se_2} \equiv m \pmod{n}$$

即有 $m \equiv (c_1^{-1})^{-r} \cdot c_2^s \pmod{n}$.

例2 证明破译 ElGamal 密码系统等价于解 Diffie-Hellman 问题.

证 设 ElGamal 密码系统的私钥为 a , 公钥为 (p, g, b) . 其中, p 是素数, g 是模数 p 的一个原根, $b \equiv g^a \pmod{p}$.

对消息 $x \in \mathbb{Z}_p$ 的加密过程是: 随机选择一个整数 $k, 1 \leq k \leq p-2$, 计算 $y_1 \equiv g^k \pmod{p}, y_2 \equiv xb^k \pmod{p}$, 得密文 $c = (y_1, y_2)$.

假定有一个算法 \mathcal{A} , \mathcal{A} 能解 Diffie-Hellman 问题, 并给定一个用 ElGamal 密码系统加密的密文 $c = (y_1, y_2)$. 将 p, g, y_1, b 作为算法 \mathcal{A} 的输入, 则可以获得

$$\mathcal{A}(p, g, y_1, b) = \mathcal{A}(p, g, g^k, g^a) \equiv g^{ka} \pmod{p} \equiv b^k \pmod{p}$$

然后, 计算 $y_2 \cdot (b^k)^{-1} \pmod{p}$ 可以得到明文消息 x .

反之, 假定有一个算法 \mathcal{B} , \mathcal{B} 能完成 ElGamal 密码系统的解密过程. 也就是说, 如果将 p, g, y_1, b, y_2 作为 \mathcal{B} 的输入, 可以求得

$$\mathcal{B}(p, g, y_1, b, y_2) = x = y_2(y_1^{L_g(b)})^{-1} \pmod{p}$$

现在, 给定 p, g, b 和 t , 其中, p 是素数, g 是模数 p 的一个原根, $b, t \in \mathbb{Z}_p^*$, 则可以计算

$$\mathcal{B}(p, g, t, b, 1) = 1 \cdot (t^{L_g(b)})^{-1} \pmod{p}$$

从而得到 $t^{L_g(b)}$. 这意味着从 $g^a (\equiv b \pmod{p})$ 与 $g^k (\equiv t \pmod{p})$, 可计算出 $(g^k)^a (= t^a = t^{L_g(b)})$.

例 3 本例介绍利用特殊素数实现 Rabin 公钥密码系统的算法.

(1) 密钥生成.

假设用户 Alice 希望用户 Bob 发送给她秘密消息, 那么, Alice 执行

① 选择两个大素数 p, q (差不多一样大), 为了便于计算, 可选择 $p \equiv q \equiv 3 \pmod{4}$ (这样的素数称为 Blum 素数);

② 计算 $N = pq$;

③ 选择随机的整数 $B \in \{0, 1, \dots, N-1\}$;

④ 把 (N, B) 作为公钥公开, 把 (p, q) 作为私钥保密.

(2) 加密运算.

用户 Bob 获得用户 Alice 的真实公钥 (N, B) .

① 把明文消息 P 表示成一个整数 $m \in \{0, 1, \dots, N-1\}$;

② 计算 $c \equiv m(m+B) \pmod{N}$;

③ 把密文 c 发送给用户 Alice.

(3) 解密运算.

用户 Alice 收到 c 之后计算

$$m \equiv \sqrt{\frac{B^2}{4} + c} - \frac{B}{2} \pmod{N}$$

这样, 就恢复出整数 m , 进而恢复出明文消息 P .

上面的解密计算是有意义的. 这是因为由 $c \equiv m(m+B) \pmod{N}$ 得

$$\begin{aligned} \sqrt{\frac{B^2}{4} + c} - \frac{B}{2} &\equiv \sqrt{\frac{B^2 + 4m(m+B)}{4}} - \frac{B}{2} \pmod{N} \\ &\equiv \sqrt{\frac{4m^2 + 4mB + B^2}{4}} - \frac{B}{2} \pmod{N} \\ &\equiv \sqrt{\frac{(2m+B)^2}{4}} - \frac{B}{2} \pmod{N} \\ &\equiv \frac{2m+B}{2} - \frac{B}{2} = m \pmod{N} \end{aligned}$$

(4) 假设 Alice 希望接收上述 Rabin 公钥密码算法加密的密文, 她选择素数 $p=127, q=131$, 并随机选取 $B=12345$, 即 Alice 的公钥为 $(N, B) = (16637,$

12345),那么,若 Bob 发给 Alice 明文消息 $m=4410$,则 Bob 要发送的密文是多少? Alice 收到密文后怎样恢复出明文?

用户 Bob 首先获得用户 Alice 的真实公钥 $(N, B) = (16637, 12345)$, 并计算

$$c \equiv m(m + B) \pmod{N} \equiv 4410(4410 + 12345) \pmod{16637} \equiv 4633$$

用户 Alice 收到用户 Bob 的密文 c 之后, 计算 $\sqrt{\frac{B^2}{4} + c} - \frac{B}{2} \pmod{N}$, 即计算

$$\left(\sqrt{\frac{12345^2}{4} + 4633} - \frac{12345}{2} \right) \pmod{16637}.$$

由于求 $\sqrt{\frac{12345^2}{4} + 4633}$ 关于模 16637 的平方根, 必须先求 $\sqrt{\frac{12345^2}{4} + 4633}$ 关于模 $p=127$ 及关于模 $q=131$ 的平方根. 分别求得它们的平方根为 $\pm 22 \pmod{127}$ 与 $\pm 37 \pmod{131}$. 再利用中国剩余定理(可利用 Maple 函数 `chrem()`), 即可求得 $\sqrt{\frac{12345^2}{4} + 4633}$ 关于模 16637 的平方根的 4 个平方根是 $\pm 3705, \pm 2264$. 从而可恢复出明文的 4 个可能是 5851, 15078, 4410, 16519.

例 4 本例介绍 Chor-Rivest 背包公钥加密系统.

(1) 密钥生成.

用户 Alice 希望用户 Bob 发给她保密的消息, 那么, 用户 Alice 执行

① 选择一个特征为 p 的有限域 \mathbb{F}_q , 其中, $q = p^n$ (p, n 应满足 $p \geq n$, 且使得 $p^n - 1$ 的素数因子不要很大, 以便乘法群 \mathbb{F}_p^* 上的离散对数问题容易计算. 如可取 $p = 197, n = 24$).

② 在 \mathbb{F}_p 中随机选择一个次数为 n 、首项系数为一的不可约多项式 $f(x)$, 那么, \mathbb{F}_q 中的元素就可以表示成 $\mathbb{F}_p[x]$ 上次数小于 n 的多项式, 其加法、乘法都是模 $f(x)$ 的运算(实际上, $\mathbb{F}_q \cong \mathbb{F}_p[x]/(f(x))$), 因此, 可认为 $\mathbb{F}_q = \mathbb{F}_p[x]/(f(x))$.

③ 在 \mathbb{F}_q 上选择一个本原多项式 $g(x)$.

④ 对于 \mathbb{F}_p 中的每一个元素 k , 计算域 $\mathbb{F}_p[x]/(f(x))$ 中元素 $x+k$ 对 $g(x)$ 的离散对数 $a_k = L_{g(x)}(x+k)$.

⑤ 随机选择集合 $\{0, 1, 2, \dots, p-1\}$ 的一个置换 π .

⑥ 随机选择一个整数 d 满足 $1 \leq d \leq p^n - 2$.

⑦ 计算 $c_i = (a_{\pi(i)} + d) \pmod{p^n - 1}, 0 \leq i \leq p-1$.

⑧ Alice 的公钥是 $k_K = ((c_0, c_1, \dots, c_{p-1}), p, n)$, 私钥是 $k_D = (f(x), g(x), \pi, d)$.

(2) 加密运算.

设 Bob 要发给 Alice 的明文消息是 P , 那么, 用户 Bob

① 获得 Alice 的真实公钥 $k_{\text{pub}} = (c_0, c_1, \dots, c_{p-1}, p, n)$.

② 把消息 P 表示成长度为 $\left\lceil \lg \binom{p}{n} \right\rceil$ 的二进制数 m , 并将 m 转化成长度为 p 的恰好有 n 个 1 的二进制向量 $M=(M_0, M_1, \dots, M_{p-1})$ 如下:

a. 令 $l \leftarrow n$;

b. 对 i 自 1 到 p 执行

如果 $m \geq \binom{p-i}{l}$, 那么, 令 $M_{i-1}=1, m \leftarrow m - \binom{p-i}{l}, l \leftarrow l-1$; 否则, 令 $M_{i-1}=$

0 (对于 $n \geq 0, l \geq 1, \binom{n}{0}=1, \binom{0}{l}=0$).

③ 计算 $c \equiv \sum_{i=0}^{p-1} M_i c_i \pmod{p^n - 1}$.

④ 把密文 c 发给用户 Alice.

(3) 解密运算.

用户 Alice 收到密文 c 之后, 执行

① 计算 $r \equiv (c - nd) \pmod{p^n - 1}$.

② 计算 $u(x) \equiv g(x)^r \pmod{f(x)}$.

③ 计算 $s(x) = u(x) + f(x)$.

④ 将 $s(x)$ 因式分解成一次因式之积 $s(x) = \prod_{j=1}^n (x + t_j)$, 其中, $t_j \in \mathbb{F}_p$.

⑤ 恢复 $M=(M_0, M_1, \dots, M_{p-1})$: 对应于下标为 $\pi^{-1}(t_j) (1 \leq j \leq n)$ 的分量 $M_{\pi^{-1}(t_j)}$, 其对应值为 1, 而其余分量的取值为 0.

⑥ 从 M 恢复出 m .

a. 令 $m \leftarrow 0, l \leftarrow n$;

b. 对于 i 从 1 到 p 执行: 如果 $M_{i-1}=1$, 那么, 令 $m \leftarrow m + \binom{p-i}{l}, l \leftarrow l-1$; 否

则, 保持 m 不变.

例 5 本例介绍 Chor-Rivest 背包公钥密码系统算法的一个实例.

设 Alice 希望接收用 Chor-Rivest 背包公钥加密系统加密的密文. 假设她选定如下参数.

(1) 随机选择的整数 $p=7, n=4, d=1702$.

(2) 选择 \mathbb{Z}_7 上 4 次不可约多项式 $f(x) = x^4 + 3x^3 + 5x^2 + 6x + 2$.

(3) 选择本原多项式 $g(x) = 3x^3 + 3x^2 + 6$.

(4) 选择的置换 $\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 0 & 2 & 1 & 5 & 3 \end{pmatrix}$.

那么

(1) Alice 的公钥及私钥分别是多少?

(2) 假若 Bob 发给 Alice 明文消息 $m=22$, 则 Bob 要发送的密文是多少?

(3) Alice 收到密文后怎样恢复出明文?

解 (1) 由于 $g(x)=3x^3+3x^2+6$, 所以, 对 \mathbb{Z}_7 中的每一个元素 k , 计算域元素 $(x+k)$ 对 $g(x)$ 的离散对数 $a_k=L_{g(x)}(x+k)$, 得

$$a_0 = L_{g(x)}(x) = 1028$$

$$a_1 = L_{g(x)}(x+1) = 1935$$

$$a_2 = L_{g(x)}(x+2) = 2054$$

$$a_3 = L_{g(x)}(x+3) = 1008$$

$$a_4 = L_{g(x)}(x+4) = 379$$

$$a_5 = L_{g(x)}(x+5) = 1780$$

$$a_6 = L_{g(x)}(x+6) = 223$$

再根据 $\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 0 & 2 & 1 & 5 & 3 \end{pmatrix}$ 及 $d=1702$ 可得

$$c_0 = (a_6 + d) \pmod{2400} = 1925$$

$$c_1 = (a_4 + d) \pmod{2400} = 2081$$

$$c_2 = (a_0 + d) \pmod{2400} = 330$$

$$c_3 = (a_2 + d) \pmod{2400} = 1356$$

$$c_4 = (a_1 + d) \pmod{2400} = 1237$$

$$c_5 = (a_5 + d) \pmod{2400} = 1082$$

$$c_6 = (a_3 + d) \pmod{2400} = 310$$

因此, Alice 的公钥与私钥是

$$k_{\text{pub}} = ((c_0, c_1, \dots, c_{p-1}), p, n) = ((1925, 2081, 330, 1356, 1237, 1082, 310), 7, 4)$$

$$k_{\text{pri}} = (f(x), g(x), \pi, d)$$

(2) Bob 获得 Alice 的真实公钥 $k_{\text{pub}} = ((1925, 2081, 330, 1356, 1237, 1082, 310), 7, 4)$ 之后, 把 $m=22$ 表示成二进制数 $22 = (10110)_2$, 然后再按 Chor-Rivest 背包公钥加密系统中加密运算中步骤(2)将其转换成含有 4 个 1 的长度为 7 的二进制向量 $M = (1, 0, 1, 1, 0, 0, 1)$. 这样, 便得密文

$$c = (c_0 + c_2 + c_3 + c_6) \pmod{2400} = 1521$$

(3) Alice 收到密文 $c=1521$ 之后, 执行下列计算:

① 计算 $r = (c - nd) \pmod{2400} = 1913$;

② 计算 $u(x) = g(x)^{1913} \pmod{f(x)} = x^3 + 3x^2 + 2x + 5$;

③ 计算 $s(x) = u(x) + f(x) = x^4 + 4x^3 + x^2 + x$;

④ 将 $s(x)$ 分解成一次因式之积 $s(x) = x(x+2)(x+3)(x+6)$;

⑤ 由于 $\pi^{-1}(0) = 2, \pi^{-1}(2) = 3, \pi^{-1}(3) = 6, \pi^{-1}(6) = 0$, 因此, $M = (1, 0, 1,$

1,0,0,1). 进而可以恢复出 $m=10110$, 即 $m=22$.

例 6 本例介绍 Goldwasser-Micali 概率公钥加密系统.

(1) 密钥生成.

用户 Alice 希望用户 Bob 发给她保密的消息, 那么, 用户 Alice 执行

① 随机选择两个差不多一样大的大素数 p, q , 并计算 $n=pq$;

② 随机选择 $b \in \mathbb{Z}_n$, 使得 b 是模数 n 的二次非剩余, 且 Jacobi 符号 $\left(\frac{b}{n}\right)=1$;

③ 将公钥 $k_{\text{pub}}=(n, b)$ 公开, 私钥 $k_{\text{pri}}=(p, q)$ 保密.

(2) 加密运算.

假如 Bob 想发给 Alice 明文消息 m , 那么, Bob 执行

① 获得 Alice 的真实公钥 $k_{\text{pub}}=(n, b)$;

② 把消息 m 表示成二进制数 $m=(m_1 m_2 \cdots m_t)_2$;

③ 对于 i 自 1 到 t , 随机选择整数 $x_i \in \mathbb{Z}_n^*$, 如果 $m_i=1$, 令 $c_i \equiv bx_i^2 \pmod{n}$, 如果 $m_i=0$, 令 $c_i \equiv x_i^2 \pmod{n}$;

④ 将密文 $c=(c_1, c_2, \cdots, c_t)$ 发送给 Alice.

(3) 解密运算.

Alice 收到密文 $c=(c_1, c_2, \cdots, c_t)$ 之后, 计算 Legendre 符号

$$e_i = \left(\frac{c_i}{p}\right), \quad i = 1, 2, \cdots, t$$

如果 $e_i=1$, 那么, $m_i=0$; 如果 $e_i=-1$, 那么, $m_i=1$. 这样, 就恢复出明文消息

$$m = (m_1 m_2 \cdots m_t)_2$$

例 7 本例介绍 Blum-Goldwasser 概率公钥加密系统.

(1) 密钥生成.

设 Alice 希望接收用 Blum-Goldwasser 概率公钥加密系统加密的密文, 那么, Alice 执行

① 随机选择两个互异的大小相近的大素数 p, q , 且满足 $p \equiv q \equiv 3 \pmod{4}$, 并计算 $n=pq$;

② 利用扩展 Euclid 算法求得整数 a, b 满足 $ap+bq=1$;

③ 将公钥 $k_{\text{pub}}=n$ 公开, 私钥 $k_{\text{pri}}=(p, q, a, b)$ 保密.

(2) 加密运算.

假如 Bob 想发给 Alice 明文消息 m , 那么, Bob 执行

① 获得 Alice 的真实公钥 $k_{\text{pub}}=n$.

② 设 $k=\lfloor \log_2 n \rfloor, h=\lfloor \log_2 k \rfloor$. 把消息 m 表示二进制(块) $m=m_1 m_2 \cdots m_t$, 其中每一个 $m_i (i=1, 2, \cdots, t)$ 都是长为 h 的二进制串.

③ 随机选择整数 $r \in \mathbb{Z}_n^*$, 计算 $x_0 \equiv r^2 \pmod{n}$. 把 x_0 作为种子, 对 i 自 1 到 t ,

执行

- a. 计算 $x_i \equiv x_{i-1}^2 \pmod{n}$;
- b. 令 p_i 是 x_i 的二进制表示的最低的 h 位有效位串;
- c. 计算 $c_i = p_i \oplus m_i$, 这里 \oplus 是异或运算.

④ 计算 $x_{t+1} \equiv x_t^2 \pmod{n}$.

⑤ 将密文 $c = (c_1, c_2, \dots, c_t, x_{t+1})$ 发送给 Alice.

(3) 解密运算.

Alice 收到密文 $c = (c_1, c_2, \dots, c_t, x_{t+1})$ 之后, 计算

① $d_1 \equiv \left(\frac{p+1}{4}\right)^{t+1} \pmod{p-1}, d_2 \equiv \left(\frac{q+1}{4}\right)^{t+1} \pmod{q-1}$.

② $u \equiv x_{t+1}^{d_1} \pmod{p}, v \equiv x_{t+1}^{d_2} \pmod{q}$.

③ $x_0 \equiv (apv + bq u) \pmod{n}$.

④ 对 i 自 1 到 t , 令 $x_i \equiv x_{i-1}^2 \pmod{n}$.

⑤ 对于 $i=1, 2, \dots, t$, 令 p_i 是 x_i 的二进制表示的最低的 h 位有效位.

(6) 令 $m_i = p_i \oplus c_i$, 即恢复出消息 $m = m_1 m_2 \dots m_t$.

例 8 假设 Alice 希望接收用 Blum-Goldwasser 概率公钥加密系统加密的密文, 并选择的素数 $p=499, q=547$, 那么

(1) Alice 的私钥是多少?

(2) 若 Bob 发给 Alice 的明文消息是二元串 $m=10011100000100001100$, 且 Bob 随机选择整数 $r=399$, 则 Bob 要发送的密文是什么?

(3) Alice 收到密文后怎样恢复出明文?

解 (1) 因为 $p=499, q=547$, 所以, $n=pq=272953$, 由扩展 Euclid 算法求得 $a=-57, b=52$ 满足 $ap+bq=1$ (可由 Maple 函数 `igcdex(499, 547, 'a', 'b')` 求得 a, b), 因此, Alice 的私钥 $k_{\text{pri}} = (p, q, a, b) = (499, 547, -57, 52)$.

(2) 因为 Alice 的公钥 $k_{\text{pub}} = 272953$, 所以

$$k = \lfloor \log_2 n \rfloor = 18, \quad h = \lfloor \log_2 k \rfloor = 4$$

因此, Bob 把消息 $m=10011100000100001100$ 分解成 $m = m_1 m_2 m_3 m_4 m_5$, 其中, $m_1=1001, m_2=1100, m_3=0001, m_4=0000, m_5=1100$.

由于 Bob 随机选择的整数为 $r=399$, 那么, Bob 先计算出种子

$$x_0 \equiv r^2 \equiv 399^2 \pmod{272953} = 159201$$

随后 Bob 计算出密文 $c = (c_1, c_2, \dots, c_t, x_{t+1})$. 具体计算过程如表 7.3 所示.

表 7.3

i	$x_i \equiv x_{i-1}^2 \pmod{n}$	p_i	m_i	$c_i = p_i \oplus m_i$
1	180539	1011	1001	0010
2	193932	1100	1100	0000
3	245613	1101	0001	1100
4	130286	1110	0000	1110
5	40632	1000	1100	0100
6	139680			

于是, Bob 发给 Alice 的密文消息是

$$c = (0010, 0000, 1100, 1110, 0100, 139680)$$

(3) Alice 收到密文后, 计算

$$d_1 \equiv ((p+1)/4)^{t+1} \pmod{p-1} \equiv ((499+1)/4)^{5+1} \pmod{498} = 463$$

$$d_2 \equiv ((q+1)/4)^{t+1} \pmod{q-1} \equiv ((547+1)/4)^{5+1} \pmod{546} = 337$$

$$u \equiv x_{t+1}^{d_1} \pmod{p} \equiv 139680^{463} \pmod{499} = 20$$

$$v \equiv x_{t+1}^{d_2} \pmod{q} \equiv 139680^{337} \pmod{547} = 24$$

$$x_0 \equiv (apv + bqu) \pmod{n} \equiv ((-57) \times 499 \times 24 + 52 \times 547 \times 20) \pmod{272953} \\ = 159201$$

再利用 $x_0 = 159201$ 计算出 $x_i (i=1, 2, 3, 4, 5)$, 得出 $p_i (i=1, 2, 3, 4, 5)$, 进而得到 $m_i (i=1, 2, 3, 4, 5)$, 最后恢复出明文消息 m .

思考题、研究题七

1. 考虑下面的加密方法.

(1) 随机选择一个奇数 e .

(2) 随机选择两个大素数 p, q , 并使 $(p-1)(q-1)-1$ 是 e 的整数倍.

(3) 计算 $n = pq$.

(4) 计算 $d = \frac{(p-1)(q-1)(e-1)+1}{e}$.

以 (n, e) 作为加密的公钥, d 作为私钥. 分析这样的加密方法是否与 RSA 加密系统等价? 请说明理由.

2. 证明 Blum-Goldwasser 概率公钥加密系统中解密算法是有意义的.

3. 假如用户 Alice 和 Bob 用 Diffie-Hellman 密钥交换协议协商他们的会话密钥, 设他们的公共素数 $p = 32604463$, 素数 p 的一个原根是 $g = 3$.

(1) 若 Alice 的公钥是 $Pk_A = 30303238$, 则 Alice 的私钥是什么?

(2) 若 Bob 的私钥 $Sk_B = 12345678$, 则他们协商的会话密钥是什么?

4. 设 ElGmal 公钥密码系统中的公用素数 $p=32604463$, 其原根 $g=20$.

(1) 若用户 Bob 的公钥 $Pk_B = 31075535$, 用户 Alice 随机选择的整数 $k = 70251$, 则 $m=2008808$ 的密文是什么?

(2) 用户 Alice 随机选择的整数 k 值使得 $m = 2008808$ 的密文为 $c = (c_1, 15668947)$, 则整数 c_1 是多少?

5. 在 Goldwasser-Micali 概率公钥密码体制中, 取 $n=6613450787, b=65$.

(1) 计算明文 $m=2008808$ 加密后的密文 c .

(2) 如果已知私钥为 $(p, q) = (22697, 291457)$, 公钥 $(n, b) = (6615199529, 65)$. 解密密文 $c = (123, 1234, 12345, 123456, 1234567, 12345678)$.

6. 利用 Maple 编程实现 Blum-Goldwasser 概率公钥加密算法.

7. (1) 利用 Maple 编程求解例 5 中域 $\mathbb{F}_p[x]/(f(x))$ 中元素 $x+k$ 对 $g(x)$ 的离散对数 $a_k = L_{g(x)}(x+k)$.

(2) 用 Maple 编程实现 Chor-Rivest 背包公钥加密算法.

参考文献

- 陈恭亮. 2004. 信息安全数学基础. 北京: 清华大学出版社
- 陈鲁生, 沈世镒. 2002. 现代密码学. 北京: 科学出版社
- 丁存生. 2001. 公钥密码学. 单炜娟译. 北京: 国防工业出版社
- 冯克勤. 2003. 初等数论及应用. 北京: 北京师范大学出版社
- 冯克勤. 2007. 数论与密码. 北京: 科学出版社
- 何青, 王丽芬. 2006. Maple 教程. 北京: 科学出版社
- 华罗庚. 1957. 数论导引. 北京: 科学出版社
- 李世奇. 2002. 计算机代数与数论. 重庆教育学院学报, 15(3): 11—15
- 李子臣, 戴一奇. 2001. 二次剩余密码体制的安全性分析. 北京: 清华大学学报(自然科学版), 41(7): 80—82
- 闵嗣鹤, 严士健. 2003. 初等数论(第三版). 北京: 高等教育出版社
- 潘承洞, 潘承彪. 2003. 初等数论(第二版). 北京: 北京大学出版社
- 裴定一, 祝跃飞. 2002. 算法数论. 北京: 科学出版社
- 王连笑. 2002. 世界奥林匹克解题大辞典. 数论卷. 石家庄: 河北少年儿童出版社
- 肖清华, 平玲娣, 潘雪增. 2004. 基于二次剩余的安全矢量空间秘密共享方案. 浙江大学学报(工学版), 38(11): 1408—1411
- 徐茂智, 游林. 2007. 信息安全与密码学. 北京: 清华大学出版社
- 游林. 2001. Euler 函数积性的概率证明. 高等数学研究, 4(2): 31—32
- Adams P, Smith K, Vyborny R. 2005. Introduction to Mathematics with Maple. Singapore: World Scientific Publishing Company
- Diffie W, Hellman M. 1976. New direction in cryptography. IEEE Transaction on Information Theory, 22: 644—655
- Goldreich O. 2003. 密码学基础(英文影印版). 北京: 电子工业出版社
- Goldreich O. 2005. 密码学基础. 第二卷: 基础应用(英文影印版). 北京: 电子工业出版社
- Guy R K. 2003. 数论中未解决的问题(第三版). 张明尧译. 北京: 科学出版社
- Hardy G H, Wright E M. 2007. 数论导引(英文影印版)(第五版). 北京: 人民邮电出版社
- Kenneth H R. 2005. 初等数论以及应用(英文影印版)(第 5 版). 北京: 机械工业出版社
- Kim S Y. 2004. An elementary proof of the quadratic reciprocity law. The American Mathematical Monthly, 111(1): 48
- Loxton J H. 1990. Number Theory and Cryptography. Cambridge: Cambridge University Press
- Menezes A. 2005. 应用密码学手册. 胡磊译. 北京: 机械工业出版社
- Merkle R, Hellman M. 1978. Hiding information and signatures in trapdoor knapsacks. IEEE Transaction on Information Theory, 24: 525—530
- Neal Koblitz. 1987. A Course in Number Theory and Cryptography. New York: Springer-Verlag
- Schneier B. 2001. 应用密码学: 协议、算法与 C 源程序. 吴世忠等译. 北京: 机械工业出版社
- Stinson D R. 1995. Cryptography, Theory and Practice. Cambridge: CRC Press Inc.
- van Oorschot M P, Vanstone S. 1997. Handbook of Applied Cryptography. Florida: CRC Press
- Wiles A. 1995. Modular elliptic curve and fermat's last theorem. Annals of Mathematics, 142: 443—551
- Yan S Y. 2004. 计算数论(英文影印版)(第二版). 北京: 世界图书出版公司