# 第一章　整除理论

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

## 第一节　数的整除性

**定义 1**　设 $a$，$b$ 是整数，$b\neq 0$，如果存在整数 $c$，使得

$$a=bc$$

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

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

被 2 整除的整数称为偶数，不被 2 整除的整数称为奇数。

**定理 1**　下面的结论成立：

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

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

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

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

(ⅴ)　$b\mid a$，$a\neq 0\Longrightarrow |b|\leq |a|$；$b\mid a$ 且 $|a|<|b|\Longrightarrow a=0$。

**证明**　留作习题。

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

以后在本书中若无特别说明，素数总是指正素数。

**定理 2**　任何大于 1 的整数 $a$ 都至少有一个素约数。

**证明**　若 $a$ 是素数，则定理是显然的。



若 $a$ 不是素数，那么它有两个以上的正的非平凡约数，设它们是 $d_1,d_2,\cdots,d_k$。不妨设 $d_1$ 是其中最小的。若 $d_1$ 不是素数，则存在 $e_1>1$，$e_2>1$，使得 $d_1=e_1e_2$，因此，$e_1$ 和 $e_2$ 也是 $a$ 的正的非平凡约数。这与 $d_1$ 的最小性矛盾。所以 $d_1$ 是素数。证毕。

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

**证明**　使用定理 2 中的记号，有 $a=d_1d_2$，其中 $d_1>1$ 是最小的素约数，所以 ${d_1}^2\leq a$。证毕。

**例 1**　设 $r$ 是正奇数，证明：对任意的正整数 $n$，有

$$n+2\nmid 1^r+2^r+\cdots+n^r。$$

**解**　对于任意的正整数 $a$，$b$ 以及正奇数 $k$，有

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

其中 $q$ 是整数。记 $s=1^r+2^r+\cdots+n^r$，则

$$2s=2+(2^r+n^r)+(3^r+(n-1)^r)+\cdots+(n^r+2^r)=2+(n+2)Q,$$

其中 $Q$ 是整数。若 $n+2\mid s$，由上式知 $n+2\mid 2$，因为 $n+2>2$，这是不可能的，所以 $n+2\nmid s$。

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

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

也是 $n$ 的所有约数的集合。

**解**　由以下三点理由可以证得结论：

(ⅰ)　$A$ 和 $B$ 的元素个数相同；

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

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

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

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

是否为偶数？

**解**　对于 $n$ 的每个约数 $d$，都有 $n=d\cdot\frac{n}{d}$，因此，$n$ 的正约数 $d$ 与

$\frac{n}{d}$ 是成对地出现的。只有当 $d=\frac{n}{d}$，即 $n=d^2$ 时，$d$ 和 $\frac{n}{d}$ 才是同一个数。故当且仅当 $n$ 是完全平方数时，$d(n)$是奇数。

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

**例 4** 设凸 $2n$ 边形 $M$ 的顶点是 $A_1, A_2, \cdots, A_{2n}$，点 $O$ 在 $M$ 的内部，用 $1, 2, \cdots, 2n$ 将 $M$ 的 $2n$ 条边分别编号，又将 $OA_1, OA_2, \cdots, OA_{2n}$ 也同样进行编号，若把这些编号作为相应的线段的长度，证明：无论怎么编号，都不能使得三角形 $OA_1A_2, OA_2A_3, \cdots, OA_{2n}A_1$ 的周长都相等。

**解** 假设这些三角形的周长都相等，记为 $s$。则

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

即

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

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

**例 5** 设整数 $k\geq 1$，证明：

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

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

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

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

**例 6** 写出不超过 100 的所有的素数。

**解** 将不超过 100 的正整数排列如下：

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ~~1~~ | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| ~~21~~ | ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ |
| 31 | ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ |
| 41 | ~~42~~ | 43 | ~~44~~ | ~~45~~ | ~~46~~ | 47 | ~~48~~ | ~~49~~ | ~~50~~ |
| ~~51~~ | ~~52~~ | 53 | ~~54~~ | ~~55~~ | ~~56~~ | ~~57~~ | ~~58~~ | 59 | ~~60~~ |
| 61 | ~~62~~ | ~~63~~ | ~~64~~ | ~~65~~ | ~~66~~ | 67 | ~~68~~ | ~~69~~ | ~~70~~ |



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 71 | ~~72~~ | 73 | ~~74~~ | ~~75~~ | ~~76~~ | ~~77~~ | ~~78~~ | 79 | ~~80~~ |
| ~~81~~ | ~~82~~ | 83 | ~~84~~ | ~~85~~ | ~~86~~ | ~~87~~ | ~~88~~ | 89 | ~~90~~ |
| ~~91~~ | ~~92~~ | ~~93~~ | ~~94~~ | ~~95~~ | ~~96~~ | 97 | ~~98~~ | ~~99~~ | ~~100~~ |

按以下步骤进行：

(ⅰ) 删去 1，剩下的后面的第一个数是 2，2 是素数；

(ⅱ) 删去 2 后面的被 2 整除的数，剩下的 2 后面的第一个数是 3，3 是素数；

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

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

…… ……

照以上步骤可以依次得到素数 $2, 3, 5, 7, 11, \cdots$。

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

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

**例 7** 证明：存在无穷多个正整数 $a$，使得

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

都是合数。

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

$$n^4+4k^4=(n^2+2k^2)^2-4n^2k^2=(n^2+2k^2+2nk)(n^2+2k^2-2nk)。$$

因为

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

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

**例 8** 设 $a_1, a_2, \cdots, a_n$ 是整数，且

$$a_1+a_2+\cdots+a_n=0，\ a_1a_2\cdots a_n=n,$$

则 $4\mid n$。

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

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

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

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

**例 9** 若 $n$ 是奇数，则 $8 \mid n^2 - 1$。

**解** 设 $n = 2k + 1$，则

$$n^2 - 1 = (2k+1)^2 - 1 = 4k(k+1)。$$

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

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

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

**例 10** 证明：方程

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

无整数解。

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

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

于是

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

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

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

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

于是

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

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

综上证得所需要的结论。



## 习 题 一

**1.** 证明定理 1。

**2.** 证明：若 $m - p \mid mn + pq$，则 $m - p \mid mq + np$。

**3.** 证明：任意给定的连续 39 个自然数，其中至少存在一个自然数，使得这个自然数的数字和能被 11 整除。

**4.** 设 $p$ 是 $n$ 的最小素约数，$n = pn_1$，$n_1 > 1$，证明：若 $p > \sqrt[3]{n}$，则 $n_1$ 是素数。

**5.** 证明：存在无穷多个自然数 $n$，使得 $n$ 不能表示为

$$a^2 + p（a > 0 是整数，p 为素数）$$

的形式。

# 第二节 带余数除法

在本节中，我们要介绍带余数除法及其简单应用。

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

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

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

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

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

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

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

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

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

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

则

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

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

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

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

以后在本书中，除特别声明外，在谈到带余数除法时总是假定 $b$ 是正整数。

**例 1** 设 $a$，$b$，$x$，$y$ 是整数，$k$ 和 $m$ 是正整数，并且

$$a = a_1m + r_1,\ 0 \le r_1 < m,$$
$$b = b_1m + r_2,\ 0 \le r_2 < m,$$

则 $ax + by$ 和 $ab$ 被 $m$ 除的余数分别与 $r_1x + r_2y$ 和 $r_1r_2$ 被 $m$ 除的余数相同。特别地，$a^k$ 与 $r_1^k$ 被 $m$ 除的余数相同。

**解** 由

$$ax + by = (a_1m + r_1)x + (b_1m + r_2)y = (a_1x + b_1y)m + r_1x + r_2y$$

可知，若 $r_1x + r_2y$ 被 $m$ 除的余数是 $r$，即

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

则

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

即 $ax + by$ 被 $m$ 除的余数也是 $r$。

同样方法可以证明其余结论。

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

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

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

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

$$y = qy_0 + r_0,\ 0 \le r_0 < y_0\ 。$$

因此

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

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



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

**例 3** 任意给出的五个整数中，必有三个数之和被 3 整除。

**解** 设这五个数是 $a_i$，$i = 1, 2, 3, 4, 5$，记

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

分别考虑以下两种情形：

(ⅰ) 若在 $r_1, r_2, \cdots, r_5$ 中数 0，1，2 都出现，不妨设 $r_1 = 0$，$r_2 = 1$，$r_3 = 2$，此时

$$a_1 + a_2 + a_3 = 3(q_1 + q_2 + q_3) + 3$$

可以被 3 整除；

(ⅱ) 若在 $r_1, r_2, \cdots, r_5$ 中数 0，1，2 至少有一个不出现，这样至少有三个 $r_i$ 要取相同的值，不妨设 $r_1 = r_2 = r_3 = r$（$r = 0$，1 或 2），此时

$$a_1 + a_2 + a_3 = 3(q_1 + q_2 + q_3) + 3r$$

可以被 3 整除。

**例 4** 设 $a_0, a_1, \cdots, a_n \in \mathbf{Z}$，$f(x) = a_nx^n + \cdots + a_1x + a_0$，已知 $f(0)$与 $f(1)$都不是 3 的倍数，证明：若方程 $f(x) = 0$ 有整数解，则

$$3 \mid f(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^n a_n\ 。$$

**解** 对任何整数 $x$，都有

$$x = 3q + r,\ r = 0,\ 1\ 或\ 2,\ q \in \mathbf{Z}。$$

(ⅰ) 若 $r = 0$，即 $x = 3q$，$q \in \mathbf{Z}$，则

$$f(x) = f(3q) = a_n(3q)^n + \cdots + a_1(3q) + a_0 = 3Q_1 + a_0 = 3Q_1 + f(0),$$

其中 $Q_1 \in \mathbf{Z}$，由于 $f(0)$不是 3 的倍数，所以 $f(x) \ne 0$；

(ⅱ) 若 $r = 1$，即 $x = 3q + 1$，$q \in \mathbf{Z}$，则

$$\begin{aligned} f(x) &= f(3q + 1) = a_n(3q + 1)^n + \cdots + a_1(3q + 1) + a_0 \\ &= 3Q_2 + a_n + \cdots + a_1 + a_0 = 3Q_2 + f(1), \end{aligned}$$

其中 $Q_2 \in \mathbf{Z}$。由于 $f(1)$不是 3 的倍数，所以 $f(x) \ne 0$。

因此若 $f(x) = 0$ 有整数解 $x$，则必是 $x = 3q + 2 = 3q' - 1$，$q' \in \mathbf{Z}$，于是

$$\begin{aligned} 0 = f(x) &= f(3q' - 1) = a_n(3q' - 1)^n + \cdots + a_1(3q' - 1) + a_0 \\ &= 3Q_3 + a_0 - a_1 + a_2 - \cdots + (-1)^n a_n = 3Q_3 + f(-1), \end{aligned}$$

其中 $Q_3 \in \mathbf{Z}$。所以 $3 \mid f(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$ 。

**例 5** 证明：对于任意的整数 $n$，$f(n) = 3n^5 + 5n^3 + 7n$ 被 15 整除。

**解** 对于任意的正整数 $n$，记

$$n = 15q + r,\ 0 \le r < 15。$$

由例 1，

$$n^2 = 15Q_1 + r_1,\ n^4 = 15Q_2 + r_2,$$

其中 $r_1$ 与 $r_2$ 分别是 $r^2$ 与 $r^4$ 被 15 除的余数。

以 $R$ 表示 $3n^4 + 5n^2 + 7$ 被 15 除的余数，则 $R$ 就是 $3r_2 + 5r_1 + 7$ 被 15 除的余数，而且 $f(n)$被 15 除的余数就是 $rR$ 被 15 除的余数，记为 $R'$。

当 $r = 0$ 时，显然 $R' = 0$，即 $15 \mid 3n^5 + 5n^3 + 7n$。

对于 $r = 1, 2, 3, \cdots, 14$ 的情形，通过计算列出下表：

| $r =$ | 1, 14 | 2, 13 | 3, 12 | 4, 11 | 5, 10 | 6, 9 | 7, 8 |
|---|---|---|---|---|---|---|---|
| $r_1 =$ | 1 | 4 | 9 | 1 | 10 | 6 | 4 |
| $r_2 =$ | 1 | 1 | 6 | 1 | 10 | 6 | 1 |
| $R =$ | 0 | 0 | 10 | 0 | 12 | 10 | 0 |
| $R' =$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

这证明了结论。

**例 6**　设 $n$ 是奇数，则 $16 \mid n^4 + 4n^2 + 11$。

**解**　我们有

$$n^4 + 4n^2 + 11 = (n^2 - 1)(n^2 + 5) + 16。$$

由第一节例题 9，有 $8 \mid n^2 - 1$，由此及 $2 \mid n^2 + 5$ 得到 $16 \mid (n^2 - 1)(n^2 + 5)$。

**例 7**　证明：若 $a$ 被 9 除的余数是 3，4，5 或 6，则方程 $x^3 + y^3 = a$ 没有整数解。

**解**　对任意的整数 $x$，$y$，记

$$x = 3q_1 + r_1,\ y = 3q_2 + r_2,\ 0 \le r_1, r_2 < 3。$$

则存在 $Q_1, R_1, Q_2, R_2 \in \mathbf{Z}$，使得

$$x^3 = 9Q_1 + R_1,\ y^3 = 9Q_2 + R_2\ ,$$

其中 $R_1$ 和 $R_2$ 被 9 除的余数分别与 ${r_1}^3$ 和 ${r_2}^3$ 被 9 除的余数相同，即

$$R_1 = 0，1 \text{ 或 } 8，R_2 = 0，1 \text{ 或 } 8。 \tag{4}$$

因此

$$x^3 + y^3 = 9(Q_1 + Q_2) + R_1 + R_2\ 。$$

又由式(4)可知，$R_1 + R_2$ 被 9 除的余数只可能是 0，1，2，7 或 8，所以，$x^3 + y^3$ 不可能等于 $a$ 。



## 习 题 二

**1.**　证明：$12 \mid n^4 + 2n^3 + 11n^2 + 10n$，$n \in \mathbf{Z}$。

**2.**　设 $3 \mid a^2 + b^2$，证明：$3 \mid a$ 且 $3 \mid b$。

**3.**　设 $n$，$k$ 是正整数，证明：$n^k$ 与 $n^{k+4}$ 的个位数字相同。

**4.**　证明：对于任何整数 $n$，$m$，等式 $n^2 + (n+1)^2 = m^2 + 2$ 不可能成立。

**5.**　设 $a$ 是自然数，问 $a^4 - 3a^2 + 9$ 是素数还是合数？

**6.**　证明：对于任意给定的 $n$ 个整数，必可以从中找出若干个作和，使得这个和能被 $n$ 整除。

# 第三节　最大公约数

**定义 1**　整数 $a_1, a_2, \cdots, a_k$ 的公共约数称为 $a_1, a_2, \cdots, a_k$ 的公约数。不全为零的整数 $a_1, a_2, \cdots, a_k$ 的公约数中最大的一个叫做 $a_1, a_2, \cdots, a_k$ 的最大公约数（或最大公因数），记为$(a_1, a_2, \cdots, a_k)$。

由于每个非零整数的约数的个数是有限的，所以最大公约数是存在的，并且是正整数。

如果$(a_1, a_2, \cdots, a_k) = 1$，则称 $a_1, a_2, \cdots, a_k$ 是互素的（或互质的）；如果

$$(a_i, a_j) = 1，\ 1 \le i, j \le k，\ i \ne j,$$

则称 $a_1, a_2, \cdots, a_k$ 是两两互素的（或两两互质的）。

显然，$a_1, a_2, \cdots, a_k$ 两两互素可以推出$(a_1, a_2, \cdots, a_k) = 1$，反之则不然，例如$(2, 6, 15) = 1$，但$(2, 6) = 2$。

**定理 1**　下面的等式成立：

(ⅰ)　$(a_1, a_2, \cdots, a_k) = (|a_1|, |a_2|, \cdots, |a_k|)$；

(ⅱ)　$(a, 1) = 1$，$(a, 0) = |a|$，$(a, a) = |a|$；

(ⅲ)　$(a, b) = (b, a)$；

(ⅳ)　若 $p$ 是素数，$a$ 是整数，则$(p, a) = 1$ 或 $p \mid a$；

(ⅴ)　若 $a = bq + r$，则$(a, b) = (b, r)$。

**证明**　(ⅰ)–(ⅳ)留作习题。

（ⅴ） 由第一节定理 1 可知，如果 $d|a$，$d|b$，则有 $d|r=a-bq$，反之，若 $d|b$，$d|r$，则 $d|a=bq+r$。因此 $a$ 与 $b$ 的全体公约数的集合就是 $b$ 与 $r$ 的全体公约数的集合，这两个集合中的最大正数当然相等，即$(a, b)=(b, r)$。证毕。

由定理 1 可知，在讨论$(a_1, a_2, \cdots, a_n)$时，不妨假设 $a_1, a_2, \cdots, a_n$ 是正整数，以后我们就维持这一假设。

**定理 2** 设 $a_1, a_2, \cdots, a_k \in \mathbf{Z}$，记

$$A=\{y;\ y=\sum_{i=1}^{k} a_i x_i\ ,\ x_i\in\mathbf{Z},\ 1\le i\le k\}。$$

如果 $y_0$ 是集合 $A$ 中最小的正数，则 $y_0=(a_1, a_2, \cdots, a_k)$。

**证明** 设 $d$ 是 $a_1, a_2, \cdots, a_k$ 的一个公约数，则 $d|y_0$，所以 $d\le y_0$。另一方面，由第二节例 2 知，$y_0$ 也是 $a_1,\ a_2,\ \cdots,\ a_k$ 的公约数。因此 $y_0$ 是 $a_1, a_2, \cdots, a_k$ 的公约数中的最大者，即 $y_0=(a_1, a_2, \cdots, a_k)$。证毕。

**推论 1** 设 $d$ 是 $a_1, a_2, \cdots, a_k$ 的一个公约数，则 $d|(a_1, a_2, \cdots, a_k)$。

这个推论对最大公约数的性质做了更深的刻划：最大公约数不但是公约数中的最大的，而且是所有公约数的倍数。

**推论 2** $(ma_1, ma_2, \cdots, ma_k)=|m|(a_1, a_2, \cdots, a_k)$。

**推论 3** 记$\delta=(a_1, a_2, \cdots, a_k)$，则

$$\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \cdots, \frac{a_k}{\delta}\right)=1,$$

特别地，$\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right)=1$。

**定理 3** $(a_1, a_2, \cdots, a_k)=1$ 的充要条件是存在整数 $x_1, x_2, \cdots, x_k$，使得

$$a_1x_1+a_2x_2+\cdots+a_kx_k=1。\tag{1}$$

**证明** 必要性 由定理 2 得到。

充分性 若式(1)成立，如果 $(a_1, a_2, \cdots, a_k)=d>1$，那么由 $d|a_i$（$1\le i\le k$）推出 $d|a_1x_1+a_2x_2+\cdots+a_kx_k=1$，这是不可能的。所以有$(a_1, a_2, \cdots, a_k)=1$。证毕。

**定理 4** 对于任意的整数 $a$，$b$，$c$，下面的结论成立：

（ⅰ） 由 $b|ac$ 及$(a, b)=1$ 可以推出 $b|c$；

（ⅱ） 由 $b|c$，$a|c$ 及$(a, b)=1$ 可以推出 $ab|c$。



**证明** （ⅰ） 若$(a, b)=1$，由定理 2，存在整数 $x$ 与 $y$，使得

$$ax+by=1。$$

因此

$$acx+bcy=c。\tag{2}$$

由上式及 $b|ac$ 得到 $b|c$。结论（ⅰ）得证；

（ⅱ） 若$(a, b)=1$，则存在整数 $x$，$y$ 使得式(2)成立。由 $b|c$ 与 $a|c$ 得到 $ab|ac$，$ab|bc$，再由式(2)得到 $ab|c$。结论（ⅱ）得证。证毕。

**推论 1** 若 $p$ 是素数，则下述结论成立：

（ⅰ） $p|ab\Longrightarrow p|a$ 或 $p|b$；

（ⅱ） $p|a^2\Longrightarrow p|a$。

**证明** 留作习题。

**推论 2** 若 $(a, b)=1$，则$(a, bc)=(a, c)$。

**证明** 设 $d$ 是 $a$ 与 $bc$ 的一个公约数，则 $d|a$，$d|bc$，由式（2）得到，$d|c$, 即 $d$ 是 $a$ 与 $c$ 的公约数。另一方面，若 $d$ 是 $a$ 与 $c$ 的公约数，则它也是 $a$ 与 $bc$ 的公约数。因此，$a$ 与 $c$ 的公约数的集合，就是 $a$ 与 $bc$ 的公约数的集合，所以$(a, bc)=(a, c)$。证毕。

**推论 3** 若 $(a, b_i)=1$，$1\le i\le n$，则$(a, b_1b_2\cdots b_n)=1$。

**证明** 留作习题。

**定理 5** 对于任意的 $n$ 个整数 $a_1, a_2, \cdots, a_n$，记

$(a_1, a_2)=d_2$，$(d_2, a_3)=d_3$，$\cdots$，$(d_{n-2}, a_{n-1})=d_{n-1}$，$(d_{n-1}, a_n)=d_n$，

则

$$d_n=(a_1, a_2, \cdots, a_n)。$$

**证明** 由定理 2 的推论，我们有

$$\begin{aligned}
d_n=(d_{n-1}, a_n)&\Longrightarrow d_n|a_n,\ d_n|d_{n-1},\\
d_{n-1}=(d_{n-2}, a_{n-1})&\Longrightarrow d_{n-1}|a_{n-1},\ d_{n-1}|d_{n-2},\\
&\Longrightarrow d_n|a_n,\ d_n|a_{n-1},\ d_n|d_{n-2},\\
d_{n-2}=(d_{n-3}, a_{n-2})&\Longrightarrow d_{n-2}|a_{n-2},\ d_{n-2}|d_{n-3}\\
&\Longrightarrow d_n|a_n,\ d_n|a_{n-1},\ d_n|a_{n-2},\ d_n|d_{n-3},\\
&\cdots\cdots\\
d_2=(a_1, a_2)&\Longrightarrow d_n|a_n,\ d_n|a_{n-1},\ \cdots,\ d_n|a_2,\ d_n|a_1,
\end{aligned}$$

即 $d_n$ 是 $a_1, a_2, \cdots, a_n$ 的一个公约数。

另一方面，对于 $a_1, a_2, \cdots, a_n$ 的任何公约数 $d$，由定理 2 的推论及

$d_2, \cdots, d_n$ 的定义，依次得出

$$d \mid a_1,\ d \mid a_2 \Longrightarrow d \mid d_2,$$
$$d \mid d_2,\ d \mid a_3 \Longrightarrow d \mid d_3,$$
$$\cdots\cdots$$
$$d \mid d_{n-1},\ d \mid a_n \Longrightarrow d \mid d_n,$$

因此 $d_n$ 是 $a_1, a_2, \cdots, a_n$ 的公约数中的最大者，即 $d_n = (a_1, a_2, \cdots, a_n)$。证毕。

**例 1**　证明：若 $n$ 是正整数，则 $\dfrac{21n+4}{14n+3}$ 是既约分数。

**解**　由定理 1 得到

$$(21n+4, 14n+3) = (7n+1, 14n+3) = (7n+1, 1) = 1。$$

**注**：一般地，若 $(x, y) = 1$，那么，对于任意的整数 $a$，$b$，有

$$(x, y) = (x - ay, y) = (x - ay, y - b(x - ay)) = (x - ay, (ab+1)y - bx),$$

因此，$\dfrac{x-ay}{(ab+1)y-bx}$ 是既约分数。

**例 2**　证明：$121 \nmid n^2 + 2n + 12$，$n \in \mathbf{Z}$。

**解**　由于 $121 = 11^2$，$n^2 + 2n + 12 = (n+1)^2 + 11$，所以，若

$$11^2 \mid (n+1)^2 + 11, \tag{3}$$

则 $11 \mid (n+1)^2$，因此，由定理 4 的推论 1 得到

$$11 \mid n+1,\ 11^2 \mid (n+1)^2。$$

再由式(3)得到

$$11^2 \mid 11,$$

这是不可能的。所以式(3)不能成立。

**注**：这个例题的一般形式是：

设 $p$ 是素数，$a$，$b$ 是整数，则

$$p^k \nmid (an+b)^k + p^{k-1}c,$$

其中 $c$ 是不被 $p$ 整除的任意整数，$k$ 是任意的大于 1 的整数。

**例 3**　设 $a$，$b$ 是整数，且

$$9 \mid a^2 + ab + b^2, \tag{4}$$

则 $3 \mid (a, b)$。

**解**　由式(4)得到

$$9 \mid (a-b)^2 + 3ab \Longrightarrow 3 \mid (a-b)^2 + 3ab$$



$$\Longrightarrow 3 \mid (a-b)^2 \Longrightarrow 3 \mid a-b \tag{5}$$
$$\Longrightarrow 9 \mid (a-b)^2。$$

再由式(4)得到

$$9 \mid 3ab \Longrightarrow 3 \mid ab。$$

因此，由定理 4 的推论 1，得到

$$3 \mid a \text{ 或 } 3 \mid b。$$

若 $3 \mid a$，由式(5)得到 $3 \mid b$；若 $3 \mid b$，由(5)式也得到 $3 \mid a$。因此，总有 $3 \mid a$ 且 $3 \mid b$。

由定理 2 的推论推出 $3 \mid (a, b)$。

**例 4**　设 $a$ 和 $b$ 是正整数，$b > 2$，则 $2^b - 1 \nmid 2^a + 1$。

**解**　(ⅰ)　若 $a < b$，且

$$2^b - 1 \mid 2^a + 1。 \tag{6}$$

成立，则

$$2^b - 1 \le 2^a + 1 \Longrightarrow 2^b - 2^a \le 2 \Longrightarrow 2^a(2^{b-a} - 1) \le 2,$$

于是 $a = 1$，$b - a = 1$，即 $b = 2$，这是不可能的，所以式(6)不成立。

(ⅱ)　若 $a = b$，且式(6)成立，则由式(6)得到

$$2^a - 1 \mid (2^a - 1) + 2 \Longrightarrow 2^a - 1 \mid 2 \Longrightarrow 2^a - 1 \le 2 \Longrightarrow 2^a \le 3,$$

于是 $b = a = 1$，这是不可能的，所以式(6)不成立。

(ⅲ)　若 $a > b$，记 $a = kb + r$，$0 \le r < b$，此时

$$2^{kb} - 1 = (2^b - 1)(2^{(k-1)b} + 2^{(k-2)b} + \cdots + 1) = (2^b - 1)Q,$$

其中 $Q$ 是整数。所以

$$2^a + 1 = 2^{kb+r} + 1 = 2^r(2^{kb} - 1 + 1) + 1$$
$$= 2^r((2^b - 1)Q + 1) + 1 = (2^b - 1)Q' + (2^r + 1),$$

其中 $Q'$ 是整数。因此

$$2^b - 1 \mid 2^a + 1 \Longrightarrow 2^b - 1 \mid 2^r + 1,$$

在(ⅰ)中已经证明这是不可能的，所以式(6)不能成立。

综上证得 $2^b - 1 \nmid 2^a + 1$。

## 习 题 三

**1.**　证明定理 1 中的结论(ⅰ)—(ⅳ)。

**2.**　证明定理 2 的推论 1，推论 2 和推论 3。

**3.** 证明定理 4 的推论 1 和推论 3。

**4.** 设 $x$，$y\in\mathbf{Z}$，$17\mid 2x+3y$，证明：$17\mid 9x+5y$。

**5.** 设 $a$，$b$，$c\in\mathbf{N}$，$c$ 无平方因子，$a^2\mid b^2c$，证明：$a\mid b$。

**6.** 设 $n$ 是正整数，求 $C_{2n}^{1},C_{2n}^{3},\cdots,C_{2n}^{2n-1}$ 的最大公约数。

## 第四节　最小公倍数

**定义 1**　整数 $a_1, a_2, \cdots, a_k$ 的公共倍数称为 $a_1, a_2, \cdots, a_k$ 的公倍数。$a_1, a_2, \cdots, a_k$ 的正公倍数中的最小的一个叫做 $a_1, a_2, \cdots, a_k$ 的最小公倍数，记为$[a_1, a_2, \cdots, a_k]$。

**定理 1**　下面的等式成立：

(ⅰ)　$[a, 1]=|a|$，$[a, a]=|a|$；

(ⅱ)　$[a, b]=[b, a]$；

(ⅲ)　$[a_1, a_2, \cdots, a_k]=[|a_1|, |a_2| \cdots, |a_k|]$；

(ⅳ)　若 $a\mid b$，则$[a, b]=|b|$。

**证明**　留作习题。

由定理 1 中的结论(ⅲ)可知，在讨论 $a_1, a_2, \cdots, a_k$ 的最小公倍数时，不妨假定它们都是正整数。在本节中总是维持这一假定。

最小公倍数和最大公约数之间有一个很重要的关系，即下面的定理。

**定理 2**　对任意的正整数 $a$，$b$，有

$$[a, b]=\frac{ab}{(a,b)}。$$

**证明**　设 $m$ 是 $a$ 和 $b$ 的一个公倍数，那么存在整数 $k_1$，$k_2$，使得 $m=ak_1$，$m=bk_2$，因此

$$ak_1=bk_2。\tag{1}$$

于是

$$\frac{a}{(a,b)}k_1=\frac{b}{(a,b)}k_2。$$

由于$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$，所以由第三节定理 4 得到



$$\frac{b}{(a,b)}\mid k_1，\text{ 即 } k_1=\frac{b}{(a,b)}t，$$

其中 $t$ 是某个整数。将上式代入式(1)得到

$$m=\frac{ab}{(a,b)}t。\tag{2}$$

另一方面，对于任意的整数 $t$，由式(2)所确定的 $m$ 显然是 $a$ 与 $b$ 的公倍数，因此 $a$ 与 $b$ 的公倍数必是式(2)中的形式，其中 $t$ 是整数。当 $t=1$ 时，得到最小公倍数

$$[a, b]=\frac{ab}{(a,b)}。$$

证毕。

**推论 1**　两个整数的任何公倍数可以被它们的最小公倍数整除。

**证明**　由式(2)可得证。证毕。

这个推论说明：两个整数的最小公倍数不但是最小的正倍数，而且是另外的公倍数的约数。

**推论 2**　设 $m$，$a$，$b$ 是正整数，则$[ma, mb]=m[a, b]$。

**证明**　由定理 2 及第三节定理 2 的推论得到

$$[ma, mb]=\frac{m^2ab}{(ma,mb)}=\frac{m^2ab}{m(a,b)}=\frac{mab}{(a,b)}=m[a, b]。$$

证毕。

**定理 3**　对于任意的 $n$ 个整数 $a_1, a_2, \cdots, a_n$，记

$[a_1, a_2]=m_2$，$[m_2, a_3]=m_3$，$\cdots$，$[m_{n-2}, a_{n-1}]=m_{n-1}$，$[m_{n-1}, a_n]=m_n$，

则

$$[a_1, a_2, \cdots, a_n]=m_n。$$

**证明**　我们有

$$\begin{aligned}
m_n=[m_{n-1}, a_n] &\Longrightarrow m_{n-1}\mid m_n，\ a_n\mid m_n，\\
m_{n-1}=[m_{n-2}, a_{n-1}] &\Longrightarrow m_{n-2}\mid m_{n-1}\mid m_n，\ a_n\mid m_n，\ a_{n-1}\mid m_{n-1}\mid m_n，\\
m_{n-2}=[m_{n-3}, a_{n-2}] &\Longrightarrow m_{n-3}\mid m_{n-2}\mid m_n，\ a_n\mid m_n，\ a_{n-1}\mid m_n，\ a_{n-2}\mid m_n，\\
&\cdots\cdots\\
m_2=[a_1, a_2] &\Longrightarrow a_n\mid m_n，\ \cdots，\ a_2\mid m_n，\ a_1\mid m_n，
\end{aligned}$$

即 $m_n$ 是 $a_1, a_2, \cdots, a_n$ 的一个公倍数。

另一方面，对于 $a_1, a_2, \cdots, a_n$ 的任何公倍数 $m$，由定理 2 的推论及

$m_2, \cdots, m_n$ 的定义，得

$$m_2 \mid m，\ m_3 \mid m，\ \cdots，\ m_n \mid m。$$

即 $m_n$ 是 $a_1, a_2, \cdots, a_n$ 最小的正的公倍数。证毕。

**推论**　若 $m$ 是整数 $a_1, a_2, \cdots, a_n$ 的公倍数，则 $[a_1, a_2, \cdots, a_n] \mid m$ 。

**证明**　留作习题。

**定理 4**　整数 $a_1, a_2, \cdots, a_n$ 两两互素，即

$$(a_i, a_j) = 1，\ 1 \le i, j \le n，\ i \ne j$$

的充要条件是

$$[a_1, a_2, \cdots, a_n] = a_1 a_2 \cdots a_n 。 \tag{3}$$

**证明**　必要性　因为 $(a_1, a_2) = 1$，由定理 2 得到

$$[a_1, a_2] = \frac{a_1 a_2}{(a_1, a_2)} = a_1 a_2 。$$

由 $(a_1, a_3) = (a_2, a_3) = 1$ 及第三节定理 4 推论 3 得到

$$(a_1 a_2, a_3) = 1，$$

由此及定理 3 得到

$$[a_1, a_2, a_3] = [[a_1, a_2], a_3] = [a_1 a_2, a_3] = a_1 a_2 a_3 。$$

如此继续下去，就得到式(3)。

充分性　用归纳法证明。当 $n = 2$ 时，式(3)成为 $[a_1, a_2] = a_1 a_2$。由定理 2

$$a_1 a_2 = [a_1, a_2] = \frac{a_1 a_2}{(a_1, a_2)} \Longrightarrow (a_1, a_2) = 1，$$

即当 $n = 2$ 时，充分性成立。

假设充分性当 $n = k$ 时成立，即

$$[a_1, a_2, \cdots, a_k] = a_1 a_2 \cdots a_k \Longrightarrow (a_i, a_j) = 1，\ 1 \le i, j \le k，\ i \ne j。$$

对于整数 $a_1, a_2, \cdots, a_k, a_{k+1}$，使用定理 3 中的记号，由定理 3 可知

$$[a_1, a_2, \cdots, a_k, a_{k+1}] = [m_k, a_{k+1}]。 \tag{4}$$

其中 $m_k = [a_1, a_2, \cdots, a_k]$。因此，如果

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

那么，由此及式(4)得到

$$[a_1, a_2, \cdots, a_k, a_{k+1}] = [m_k, a_{k+1}] = \frac{m_k a_{k+1}}{(m_k, a_{k+1})} = a_1 a_2 \cdots a_k a_{k+1}，$$



即

$$\frac{m_k}{(m_k, a_{k+1})} = a_1 a_2 \cdots a_k \ ，$$

显然 $m_k \le a_1 a_2 \cdots a_k$，$(m_k, a_{k+1}) \ge 1$。所以若使上式成立，必是

$$(m_k, a_{k+1}) = 1， \tag{5}$$

并且

$$m_k = a_1 a_2 \cdots a_k 。 \tag{6}$$

由式(6)与式(5)推出

$$(a_i, a_{k+1}) = 1，\ 1 \le i \le k； \tag{7}$$

由式(6)及归纳假设推出

$$(a_i, a_j) = 1，\ 1 \le i, j \le k，\ i \ne j 。 \tag{8}$$

综合式(7)与式(8)，可知当 $n = k + 1$ 时，充分性成立。由归纳法证明了充分性。证毕。

定理 4 有许多应用。例如，如果 $m_1, m_2, \cdots, m_k$ 是两两互素的整数，那么，要证明 $m = m_1 m_2 \cdots m_k$ 整除某个整数 $Q$，只需证明对于每个 $i$，$1 \le i \le k$，都有 $m_i \mid Q$。这一点在实际计算中是很有用的。对于函数 $f(x)$，要验证命题“$m \mid f(n)$，$n \in \mathbf{Z}$”是否成立，可以用第二节例 5 中的方法，验证“$m \mid f(r)$，$r = 0, 1, \cdots, m - 1$”是否成立。这需要做 $m$ 次除法。但是，若分别验证“$m_i \mid f(r_i)$，$r_i = 0, 1, \cdots, m_i - 1$，$1 \le i \le k$”是否成立，则总共需要做 $m_1 + m_2 + \cdots + m_k$ 次除法。后者的运算次数显然少于前者。

**例 1**　设 $a$，$b$，$c$ 是正整数，证明：$[a, b, c](ab, bc, ca) = abc$ 。

**解**　由定理 3 和定理 2 有

$$[a, b, c] = [[a, b], c] = \frac{[a, b]c}{([a, b], c)}， \tag{9}$$

由第三节定理 5 和定理 2 的推论，

$$\begin{aligned}(ab, bc, ca) &= (ab, (bc, ca)) = (ab, c(a, b)) \\ &= \left(ab, \frac{abc}{[a, b]}\right) = \frac{(ab[a, b], abc)}{[a, b]} = \frac{ab([a, b], c)}{[a, b]}。\end{aligned} \tag{10}$$

联合式(9)与式(10)得到所需结论。

**例 2**　对于任意的整数 $a_1, a_2, \cdots, a_n$ 及整数 $k$，$1 \le k \le n$，证明：

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

**解** 因为$[a_1, a_2, \cdots, a_n]$是 $a_1, \cdots, a_k, a_{k+1}, \cdots, a_n$的公倍数，所以由定理 2 推论，推出

$$[a_1, \cdots, a_k] \mid [a_1, a_2, \cdots, a_n],$$
$$[a_{k+1}, \cdots, a_n] \mid [a_1, a_2, \cdots, a_n],$$

再由定理 3 推论知

$$[[a_1, \cdots, a_k], [a_{k+1}, \cdots, a_n]] \mid [a_1, a_2, \cdots, a_n]。 \tag{11}$$

另一方面，对于任意的 $a_i$（$1 \le i \le n$），显然

$$a_i \mid [[a_1, \cdots, a_k], [a_{k+1}, \cdots, a_n]],$$

所以由定理 3 推论可知

$$[a_1, a_2, \cdots, a_n] \mid [[a_1, \cdots, a_k], [a_{k+1}, \cdots, a_n]],$$

联合上式与式(11)得证。

**例 3** 设 $a$，$b$，$c$ 是正整数，证明：

$$[a, b, c][ab, bc, ca] = [a, b][b, c][c, a]。$$

**解** 由定理 2 推论 2 及例 2，有

$$\begin{aligned}[a, b, c][ab, bc, ca] &= [[a, b, c]ab, [a, b, c]bc, [a, b, c]ca] \\ &= [[a^2b, ab^2, abc], [abc, b^2c, bc^2], [a^2c, abc, ac^2]] \\ &= [a^2b, ab^2, abc, abc, b^2c, bc^2, a^2c, abc, ac^2] \\ &= [abc, a^2b, a^2c, b^2c, b^2a, c^2a, c^2b]\end{aligned}$$

以及

$$\begin{aligned}[a, b][b, c][c, a] &= [[a, b]b, [a, b]c][c, a] \\ &= [ab, b^2, ac, bc][c, a] \\ &= [ab[c, a], b^2[c, a], ac[c, a], bc[c, a]] \\ &= [abc, a^2b, b^2c, b^2a, ac^2, a^2c, bc^2, bca] \\ &= [abc, a^2b, a^2c, b^2c, b^2a, c^2a, c^2b],\end{aligned}$$

由此得证。

## 习 题 四

**1.** 证明定理 1。

**2.** 证明定理 3 的推论。

**3.** 设 $a$，$b$ 是正整数，证明：$(a + b)[a, b] = a[b, a + b]$。

**4.** 求正整数 $a$，$b$，使得 $a + b = 120$，$(a, b) = 24$，$[a, b] = 144$。

**5.** 设 $a$，$b$，$c$ 是正整数，证明：



$$\frac{[a, b, c]^2}{[a, b][b, c][c, a]} = \frac{(a, b, c)^2}{(a, b)(b, c)(c, a)}。$$

**6.** 设 $k$ 是正奇数，证明：$1 + 2 + \cdots + 9 \mid 1^k + 2^k + \cdots + 9^k$。

# 第五节 辗转相除法

本节要介绍一个计算最大公约数的算法——辗转相除法，又称 Euclid 算法。它是数论中的一个重要方法，在其他数学分支中也有广泛的应用。

**定义 1** 下面的一组带余数除法，称为辗转相除法。

设 $a$ 和 $b$ 是整数，$b \neq 0$，依次做带余数除法：

$$\begin{aligned}a &= bq_1 + r_1, && 0 < r_1 < |b|, \\ b &= r_1q_2 + r_2, && 0 < r_2 < r_1, \\ &\cdots\cdots \\ r_{k-1} &= r_kq_{k+1} + r_{k+1}, && 0 < r_{k+1} < r_k, \\ &\cdots\cdots \\ r_{n-2} &= r_{n-1}q_n + r_n, && 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_{n+1}。\end{aligned} \tag{1}$$

由于 $b$ 是固定的，而且

$$|b| > r_1 > r_2 > \cdots,$$

所以式(1)中只包含有限个等式。

下面，我们要对式(1)所包含的等式的个数，即要做的带余数除法的次数进行估计。

**引理 1** 用下面的方式定义 Fibonacci 数列$\{F_n\}$：

$$F_1 = F_2 = 1，F_n = F_{n-1} + F_{n-2}，n \ge 3，$$

那么对于任意的整数 $n \ge 3$，有

$$F_n > \alpha^{n-2}, \tag{2}$$

其中$\alpha = \dfrac{1 + \sqrt{5}}{2}$。

**证明** 容易验证

$$\alpha^2 = \alpha + 1。$$

当 $n=3$ 时，由

$$F_3=2>\frac{1+\sqrt{5}}{2}=\alpha$$

可知式(2)成立。

假设式(2)对于所有的整数 $k\le n$（$n\ge 3$）成立，即

$$F_k>\alpha^{k-2},\ k\le n,$$

则

$$F_{n+1}=F_n+F_{n-1}>\alpha^{n-2}+\alpha^{n-3}=\alpha^{n-3}(\alpha+1)=\alpha^{n-3}\alpha^2=\alpha^{n-1},$$

即当 $k=n+1$ 时式(2)也成立。由归纳法知式(2)对一切 $n\ge 3$ 成立。证毕。

**定理 1**(Lame)　设 $a, b\in\mathbf{N}$，$a>b$，使用在式(1)中的记号，则

$$n<5\log_{10}b。$$

**证明**　在式(1)中，$r_n\ge 1$，$q_{n+1}\ge 2$，$q_i\ge 1$（$1\le i\le n$），因此

$$\begin{aligned}
&r_n\ge 1=F_2\ ,\\
&r_{n-1}\ge 2r_n\ge 2=F_3\ ,\\
&r_{n-2}\ge r_{n-1}+r_n\ge F_3+F_2=F_4\ ,\\
&\quad\cdots\cdots\\
&b\ge r_1+r_2\ge F_{n+1}+F_n=F_{n+2}\ ,
\end{aligned}$$

由此及式(2)得

$$b\ge\alpha^n=\left(\frac{1+\sqrt{5}}{2}\right)^n,$$

即

$$\log_{10}b\ge n\log_{10}\frac{1+\sqrt{5}}{2}>\frac{1}{5}n\ ,$$

这就是定理结论。证毕。

**定理 2**　使用式(1)中的记号，记

$$\begin{aligned}
&P_0=1,\ P_1=q_1,\ P_k=q_kP_{k-1}+P_{k-2},\ k\ge 2,\\
&Q_0=0,\ Q_1=1,\ Q_k=q_kQ_{k-1}+Q_{k-2},\ k\ge 2,
\end{aligned}$$

则

$$aQ_k-bP_k=(-1)^{k-1}r_k,\ k=1, 2, \cdots, n\ 。\qquad (3)$$

**证明**　当 $k=1$ 时，式(3)成立。

当 $k=2$ 时，有



$$Q_2=q_2Q_1+Q_0=q_2,\ P_2=q_2P_1+P_0=q_2q_1+1,$$

此时由式(1)得到

$$aQ_2-bP_2=aq_2-b(q_2q_1+1)=(a-bq_1)q_2-b=r_1q_2-b=-r_2,$$

即式(3)成立。

假设对于 $k<m$（$1\le m\le n$）式(3)成立，由此假设及式(1)得到

$$\begin{aligned}
aQ_m-bP_m&=a(q_mQ_{m-1}+Q_{m-2})-b(q_mP_{m-1}+P_{m-2})\\
&=(aQ_{m-1}-bP_{m-1})q_m+(aQ_{m-2}-bP_{m-2})\\
&=(-1)^{m-2}r_{m-1}q_m+(-1)^{m-3}r_{m-2}\\
&=(-1)^{m-1}(r_{m-2}-r_{m-1}q_m)=(-1)^{m-1}r_m\ ,
\end{aligned}$$

即式(3)当 $k=m$ 时也成立。定理由归纳法得证。证毕。

**定理 3**　使用式(1)中的记号，有 $r_n=(a, b)$。

**证明**　由第三节定理 1，从式(1)可见

$$r_n=(r_{n-1}, r_n)=(r_{n-2}, r_{n-1})=\cdots=(r_1, r_2)=(b, r_1)=(a, b)。$$

证毕。

现在我们已经知道，利用辗转相除法可以求出整数 $x$，$y$，使得

$$ax+by=(a, b)\ 。\qquad (4)$$

为此所需要的除法次数是 $O(\log_{10}b)$。但是如果只需要计算$(a, b)$而不需要求出使式(4)成立的整数 $x$ 与 $y$，则所需要的除法次数还可更少一些。

**例 1**　设 $a$ 和 $b$ 是正整数，那么只使用被 2 除的除法运算和减法运算就可以计算出$(a, b)$。

**解**　下面的四个基本事实给出了证明：

(ⅰ)　若 $a\mid b$，则$(a, b)=a$；

(ⅱ)　若 $a=2^{\alpha}a_1$，$2\nmid a_1$，$b=2^{\beta}b_1$，$2\nmid b_1$，$\alpha\ge\beta\ge 1$，则

$$(a, b)=2^{\beta}(2^{\alpha-\beta}a_1, b_1);$$

(iii)　若 $2\nmid a$，$b=2^{\beta}b_1$，$2\nmid b_1$，则$(a, b)=(a, b_1)$；

(iv)　若 $2\nmid a$，$2\nmid b$，则 $(a, b)=\left(\left|\frac{a-b}{2}\right|, b\right)$。

在实际计算过程中，若再灵活运用最大公约数的性质（例如第三节定理 4 的推论），则可使得求最大公约数的过程更为简单。

**例 2**　用辗转相除法求(125, 17)，以及 $x$，$y$，使得

$$125x+17y=(125, 17)。$$

**解**　做辗转相除法：

$$125 = 7\cdot 17 + 6,\quad q_1 = 7,\quad r_1 = 6,$$
$$17 = 2\cdot 6 + 5,\quad q_2 = 2,\quad r_2 = 5,$$
$$6 = 1\cdot 5 + 1,\quad q_3 = 1,\quad r_3 = 1,$$
$$5 = 5\cdot 1,\quad q_4 = 5。$$

由定理 4，$(125, 17) = r_3 = 1$。

利用定理 2 计算（$n = 3$）

$$P_0 = 1,\ P_1 = 7,\ P_2 = 2\cdot 7 + 1 = 15,\ P_3 = 1\cdot 15 + 7 = 22,$$
$$Q_0 = 0,\ Q_1 = 1,\ Q_2 = 2\cdot 1 + 0 = 2,\ Q_3 = 1\cdot 2 + 1 = 3,$$

取 $x = (-1)^{3-1}Q_3 = 3$，$y = (-1)^3 P_3 = -22$，则

$$125\cdot 3 + 17\cdot(-22) = (125, 17) = 1。$$

**例 3** 求$(12345, 678)$。

**解** $(12345, 678) = (12345, 339) = (12006, 339) = (6003, 339)$
$= (5664, 339) = (177, 339) = (177, 162) = (177, 81)$
$= (96, 81) = (3, 81) = 3$。

**例 4** 在 $m$ 个盒子中放若干个硬币，然后以下述方式往这些盒子里继续放硬币：每一次在 $n$（$n < m$）个盒子中各放一个硬币。证明：若$(m, n) = 1$，那么无论开始时每个盒子中有多少硬币，经过若干次放硬币后，总可使所有盒子含有同样数量的硬币。

**解** 由于$(m, n) = 1$，所以存在整数 $x$，$y$，使得 $mx + ny = 1$。因此对于任意的自然数 $k$，有

$$1 + m(-x + kn) = n(km + y),$$

这样，当 $k$ 充分大时，总可找出正整数 $x_0$，$y_0$，使得

$$1 + mx_0 = ny_0 。$$

上式说明，如果放 $y_0$ 次（每次放 $n$ 个），那么在使 $m$ 个盒子中各放 $x_0$ 个后，还多出一个硬币。把这个硬币放入含硬币最少的盒子中（这是可以做到的），就使它与含有最多硬币的盒子所含硬币数量之差减少 1。因此经过若干次放硬币后，必可使所有盒子中的硬币数目相同。

## 习 题 五

**1.** 说明例 1 证明中所用到的四个事实的依据。

**2.** 用辗转相除法求整数 $x$，$y$，使得 $1387x - 162y = (1387, 162)$。



**3.** 计算：$(27090, 21672, 11352)$。

**4.** 使用引理 1 中的记号，证明：$(F_{n+1}, F_n) = 1$。

**5.** 若四个整数 2836，4582，5164，6522 被同一个大于 1 的整数除所得的余数相同，且不等于零，求除数和余数各是多少？

**6.** 记 $M_n = 2^n - 1$，证明：对于正整数 $a$，$b$，有$(M_a, M_b) = M_{(a, b)}$。

# 第六节 算术基本定理

在本节中，我们要介绍整数与素数的一个重要关系，即任何大于 1 的正整数都可以表示成素数的乘积。

**引理 1** 任何大于 1 的正整数 $n$ 可以写成素数之积，即

$$n = p_1 p_2 \cdots p_m, \tag{1}$$

其中 $p_i$（$1 \le i \le m$）是素数。

**证明** 当 $n = 2$ 时，结论显然成立。

假设对于 $2 \le n \le k$，式(1)成立，我们来证明式(1)对于 $n = k + 1$ 也成立，从而由归纳法推出式(1)对任何大于 1 的整数 $n$ 成立。

如果 $k + 1$ 是素数，式(1)显然成立。

如果 $k + 1$ 是合数，则存在素数 $p$ 与整数 $d$，使得 $k + 1 = pd$。由于 $2 \le d \le k$，由归纳假定知存在素数 $q_1, q_2, \cdots, q_l$，使得 $d = q_1 q_2 \cdots q_l$，从而 $k + 1 = pq_1 q_2 \cdots q_l$。证毕。

**定理 1**(算术基本定理) 任何大于 1 的整数 $n$ 可以唯一地表示成

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\ , \tag{2}$$

其中 $p_1, p_2, \cdots, p_k$ 是素数，$p_1 < p_2 < \cdots < p_k$，$\alpha_1, \alpha_2, \cdots, \alpha_k$ 是正整数。

**证明** 由引理 1，任何大于 1 的整数 $n$ 可以表示成式(2)的形式，因此，只需证明表示式(2)的唯一性。

假设 $p_i$（$1 \le i \le k$）与 $q_j$（$1 \le j \le l$）都是素数，

$$p_1 \le p_2 \le \cdots \le p_k,\ \ q_1 \le q_2 \le \cdots \le q_l, \tag{3}$$

并且

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l\ , \tag{4}$$

则由第三节定理 4 推论 1，必有某个 $q_j$（$1 \le j \le l$），使得 $p_1 \mid q_j$，所以 $p_1 = q_j$；又有某个 $p_i$（$1 \le i \le k$），使得 $q_1 \mid p_i$，所以 $q_1 = p_i$。于是，由式

(3)可知 $p_1 = q_1$，从而由式(4)得到

$$p_2 \cdots p_k = q_2 \cdots q_l \text{。}$$

重复上述这一过程，得到

$$k = l,\ p_i = q_i,\ 1 \le i \le k \text{。}$$

证毕。

**定义 1** 使用定理 1 中的记号，称

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

是 $n$ 的标准分解式，其中 $p_i$（$1 \le i \le k$）是素数，$p_1 < p_2 < \cdots < p_k$，$\alpha_i$（$1 \le i \le k$）是正整数。

**推论 1** 使用式(2)中的记号，有

(ⅰ) $n$ 的正因数 $d$ 必有形式

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k},\ \gamma_i \in \mathbf{Z},\ 0 \le \gamma_i \le \alpha_i,\ 1 \le i \le k;$$

(ⅱ) $n$ 的正倍数 $m$ 必有形式

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} M,\ M \in \mathbf{N},\ \beta_i \in \mathbf{N},\ \beta_i \ge \alpha_i,\ 1 \le i \le k\text{。}$$

**证明** 留作习题。

**推论 2** 设正整数 $a$ 与 $b$ 的标准分解式是

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\gamma_1} \cdots q_l^{\gamma_l},\ b = p_1^{\beta_1} \cdots p_k^{\beta_k} r_1^{\delta_1} \cdots r_s^{\delta_s},$$

其中 $p_i$（$1 \le i \le k$），$q_i$（$1 \le i \le l$）与 $r_i$（$1 \le i \le s$）是两两不相同的素数，$\alpha_i$，$\beta_i$（$1 \le i \le k$），$\gamma_i$（$1 \le i \le l$）与 $\delta_i$（$1 \le i \le s$）都是非负整数，则

$$(a, b) = p_1^{\lambda_1} \cdots p_k^{\lambda_k},\quad \lambda_i = \min\{\alpha_i, \delta_i\},\ 1 \le i \le k,$$

$$[a, b] = p_1^{\mu_1} \cdots p_k^{\mu_k} q_1^{\beta_1} \cdots q_l^{\beta_l} r_1^{\gamma_1} \cdots r_s^{\gamma_s},\ \mu_i = \max\{\alpha_i, \delta_i\},\ 1 \le i \le k\text{。}$$

**证明** 留作习题。

为了方便，推论 2 常叙述为下面的形式：

**推论 2′** 设正整数 $a$ 与 $b$ 的标准分解式是

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ b = p_1^{\beta_1} p_2^{\beta_1} \cdots p_k^{\beta_k},$$

其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$\alpha_i$，$\beta_i$（$1 \le i \le k$）都是非负整数，则



$$(a, b) = p_1^{\lambda_1} p_2^{\lambda_1} \cdots p_k^{\lambda_k},\quad \lambda_i = \min\{\alpha_i, \beta_i\},\quad 1 \le i \le k,$$

$$[a, b] = p_1^{\mu_1} p_2^{\mu_1} \cdots p_k^{\mu_k},\quad \mu_i = \max\{\alpha_i, \beta_i\},\quad 1 \le i \le k\text{。}$$

**推论 3** 设 $a$，$b$，$c$，$n$ 是正整数，

$$ab = c^n,\ (a, b) = 1, \tag{5}$$

则存在正整数 $u$，$v$，使得

$$a = u^n,\ b = v^n,\ c = uv,\ (u, v) = 1\text{。}$$

**证明** 设 $c = p_1^{\gamma_1} p_2^{\gamma_1} \cdots p_k^{\gamma_k}$，其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$\gamma_i$（$1 \le i \le k$）是正整数。又设

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ b = p_1^{\beta_1} p_2^{\beta_1} \cdots p_k^{\beta_k},$$

其中 $\alpha_I$，$\beta_i$（$1 \le i \le k$）都是非负整数。由式(5)及推论 2′可知

$$\min\{\alpha_i, \beta_i\} = 0,\ \alpha_i + \beta_i = n\gamma_i,\ 1 \le i \le k,$$

因此，对于每个 $i$（$1 \le i \le k$），等式

$$\alpha_i = n\gamma_i,\ \beta_i = 0 \text{ 与 } \alpha_i = 0,\ \beta_i = n\gamma_i$$

有且只有一个成立。这就证明了推论。证毕。

**例 1** 写出 51480 的标准分解式。

**解** 我们有

$$\begin{aligned} 51480 &= 2 \cdot 25740 = 2^2 \cdot 12870 = 2^3 \cdot 6435 \\ &= 2^3 \cdot 5 \cdot 1287 = 2^3 \cdot 5 \cdot 3 \cdot 429 \\ &= 2^3 \cdot 5 \cdot 3^2 \cdot 143 = 2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13\text{。} \end{aligned}$$

**例 2** 设 $a$，$b$，$c$ 是整数，证明：

(ⅰ) $(a, b)[a, b] = ab$；

(ⅱ) $(a, [b, c]) = [(a, b), (a, c)]$。

**解** 为了叙述方便，不妨假定 $a$，$b$，$c$ 是正整数。

(ⅰ) 设

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ b = p_1^{\beta_1} p_2^{\beta_1} \cdots p_k^{\beta_k},$$

其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$\alpha_i$，$\beta_i$（$1 \le i \le k$）都是非负整数。由定理 1 推论 2′，有

$$(a, b) = p_1^{\lambda_1} p_2^{\lambda_1} \cdots p_k^{\lambda_k},\quad \lambda_i = \min\{\alpha_i, \beta_i\},\quad 1 \le i \le k,$$

$$[a, b] = p_1^{\mu_1} p_2^{\mu_1} \cdots p_k^{\mu_k},\quad \mu_i = \max\{\alpha_i, \beta_i\},\quad 1 \le i \le k\text{。}$$

由此知

$$(a,b)[a,b]=\prod_{i=1}^{k}p_i^{\lambda_i+\mu_i}=\prod_{i=1}^{k}p_i^{\min\{\alpha_i,\beta_i\}+\max\{\alpha_i,\beta_i\}}=\prod_{i=1}^{k}p_i^{\alpha_i+\beta_i}=ab;$$

(ii) 设

$$a=\prod_{i=1}^{k}p_i^{\alpha_i},\quad b=\prod_{i=1}^{k}p_i^{\beta_i},\quad c=\prod_{i=1}^{k}p_i^{\gamma_i},$$

其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$\alpha_i$，$\beta_i$，$\gamma_i$（$1\le i\le k$）都是非负整数。由定理 1 推论 2′，有

$$(a,[b,c])=\prod_{i=1}^{k}p_i^{\lambda_i},\quad [(a,b),(a,c)]=\prod_{i=1}^{k}p_i^{\mu_i},$$

其中，对于 $1\le i\le k$，有

$$\lambda_i=\min\{\alpha_i,\max\{\beta_i,\gamma_i\}\},$$
$$\mu_i=\max\{\min\{\alpha_i,\beta_i\},\min\{\alpha_i,\gamma_i\}\},$$

不妨设$\beta_i\le\gamma_i$，则

$$\min\{\alpha_i,\beta_i\}\le\min\{\alpha_i,\gamma_i\},$$

所以

$$\mu_i=\min\{\alpha_i,\gamma_i\}=\lambda_i,$$

即$(a,[b,c])=[(a,b),(a,c)]$。

**注**：利用定理 1 可以容易地处理许多像例 2 这样的问题。

**例 3** 证明：$N=1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n-1}$（$n\ge 2$）不是整数。

**解** 设

$$3^k\le 2n-1<3^{k+1}。$$

对于任意的 $1\le i\le n$，$2i-1\ne 3^k$，记

$$2i-1=3^{\alpha_i}Q_i,\quad Q_i\in\mathbf{Z},$$

由第一节例 5，知$\alpha_i\le k-1$。因为 $3^{k-1}Q_1Q_2\cdots Q_{2n-1}$ 是整数，所以，如果 $N$ 是整数，则存在整数 $Q$，使得

$$3^{k-1}Q_1Q_2\cdots Q_{2n-1}N=Q+3^{k-1}Q_1Q_2\cdots Q_{2n-1}\frac{1}{3^k}。$$

由于 $3\nmid Q_1Q_2\cdots Q_{2n-1}$，所以上式右端不是整数，这个矛盾说明 $N$ 不能是整数。



## 习 题 六

**1.** 证明定理 1 的推论 1。

**2.** 证明定理 1 的推论 2。

**3.** 写出 22345680 的标准分解式。

**4.** 证明：在 $1, 2, \cdots, 2n$ 中任取 $n+1$ 数，其中至少有一个能被另一个整除。

**5.** 证明：$1+\frac{1}{2}+\cdots+\frac{1}{n}$（$n\ge 2$）不是整数。

**6.** 设 $a$，$b$ 是正整数，证明：存在 $a_1$，$a_2$，$b_1$，$b_2$，使得

$$a=a_1a_2,\quad b=b_1b_2,\quad (a_2,b_2)=1,$$

并且$[a,b]=a_2b_2$。

# 第七节　函数[x]与{x}

本节中要介绍函数[x]，它在许多数学问题中有广泛的应用。

**定义 1** 设 $x$ 是实数，以[x]表示不超过 $x$ 的最大整数，称它为 $x$ 的整数部分，又称$\{x\}=x-[x]$为 $x$ 的小数部分。

**定理 1** 设 $x$ 与 $y$ 是实数，则

(i) $x\le y\Longrightarrow [x]\le[y]$;

(ii) 若 $m$ 是整数，则$[m+x]=m+[x]$;

(iii) 若 $0\le x<1$，则$[x]=0$;

(iv) $[x+y]=\begin{cases}[x]+[y] & \text{若 } \{x\}+\{y\}<1\\ [x]+[y]+1 & \text{若 } \{x\}+\{y\}\ge 1\end{cases}$;

(v) $[-x]=\begin{cases}-[x] & \text{若 } x\in\mathbf{Z}\\ -[x]-1 & \text{若 } x\notin\mathbf{Z}\end{cases}$;

(vi) $\{-x\}=\begin{cases}0 & \text{若 } x\in\mathbf{Z}\\ 1-\{x\} & \text{若 } x\notin\mathbf{Z}\end{cases}$。

**证明** 留作习题。

**定理 2** 设 $a$ 与 $b$ 是正整数，则在 $1, 2, \cdots, a$ 中能被 $b$ 整除的整数

有$[\frac{a}{b}]$个。

**证明** 能被 $b$ 整除的正整数是 $b, 2b, 3b, \cdots$，因此，若数 $1, 2, \cdots, a$ 中能被 $b$ 整除的整数有 $k$ 个，则

$$kb \le a < (k+1)b \Longrightarrow k \le \frac{a}{b} < k+1 \Longrightarrow k = [\frac{a}{b}]。$$

证毕。

由定理 2 我们看到，若 $b$ 是正整数，那么对于任意的整数 $a$，有

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

即在带余数除法

$$a = bq + r,\ 0 \le r < b$$

中有 $q = [\frac{a}{b}]$，$r = b\{\frac{a}{b}\}$。

**定理 3** 设 $n$ 是正整数，$n! = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 是 $n!$的标准分解式，则

$$\alpha_i = \sum_{r=1}^{\infty} [\frac{n}{p_i^r}]。 \tag{1}$$

**证明** 对于任意固定的素数 $p$，以 $p(k)$表示在 $k$ 的标准分解式中的 $p$ 的指数，则

$$p(n!) = p(1) + p(2) + \cdots + p(n)。$$

以 $n_j$ 表示 $p(1), p(2), \cdots, p(n)$中等于 $j$ 的个数，那么

$$p(n!) = 1\cdot n_1 + 2\cdot n_2 + 3\cdot n_3 + \cdots\ , \tag{2}$$

显然，$n_j$ 就是在 $1, 2, \cdots, n$ 中满足 $p^j \mid a$ 并且 $p^{j+1} \nmid a$ 的整数 $a$ 的个数，所以，由定理 2 有

$$n_j = [\frac{n}{p^j}] - [\frac{n}{p^{j+1}}]。$$

将上式代入式(2)，得到

$$p(n!) = 1([\frac{n}{p}] - [\frac{n}{p^2}]) + 2([\frac{n}{p^2}] - [\frac{n}{p^3}]) + 3([\frac{n}{p^3}] - [\frac{n}{p^4}]) + \cdots$$

$$= \sum_{r=1}^{\infty} [\frac{n}{p^r}]。$$



即式(1)成立。证毕。

**推论** 设 $n$ 是正整数，则

$$n! = \prod_{p \le n} p^{\sum_{r=1}^{\infty} [\frac{n}{p^r}]},$$

其中 $\prod_{p \le n}$ 表示对不超过 $n$ 的所有素数 $p$ 求积。

**定理 4** 设 $n$ 是正整数，$1 \le k \le n-1$，则

$$C_n^k = \frac{n!}{k!(n-k)!} \in \mathbf{N}。 \tag{3}$$

若 $n$ 是素数，则 $n \mid C_n^k$，$1 \le k \le n-1$。

**证明** 由定理 3，对于任意的素数 $p$，整数 $n!$，$k!$与$(n-k)!$的标准分解式中所含的 $p$ 的指数分别是

$$\sum_{r=1}^{\infty} [\frac{n}{p^r}],\ \sum_{r=1}^{\infty} [\frac{k}{p^r}] \text{ 与 } \sum_{r=1}^{\infty} [\frac{n-k}{p^r}]。$$

利用定理 1 可知

$$\sum_{r=1}^{\infty} [\frac{n}{p^r}] \ge \sum_{r=1}^{\infty} [\frac{k}{p^r}] + \sum_{r=1}^{\infty} [\frac{n-k}{p^r}],$$

因此 $C_n^k$ 是整数。

若 $n$ 是素数，则对于 $1 \le k \le n-1$，有

$$(n, k!) = 1,\ (n, (n-k)!) = 1 \Longrightarrow (n, k!(n-k)!) = 1,$$

由此及

$$C_n^k = \frac{n\cdot(n-1)!}{k!(n-k)!} \in \mathbf{N},$$

推出 $k!(n-k)! \mid (n-1)!$，从而 $n \mid C_n^k$。证毕。

**例 1** 求最大的正整数 $k$，使得 $10^k \mid 199!$。

**解** 由定理 3，199!的标准分解式中所含的 5 的幂指数是

$$[\frac{199}{5}] + [\frac{199}{5^2}] + [\frac{199}{5^3}] + \cdots = 47,$$

所以，所求的最大整数是 $k = 47$。

**例 2** 设 $x$ 与 $y$ 是实数，则

$$[2x]+[2y]\geq[x]+[x+y]+[y]。\tag{4}$$

**解** 设 $x=[x]+\alpha$，$0\leq\alpha<1$，$y=[y]+\beta$，$0\leq\beta<1$，则

$$[x]+[x+y]+[y]=2[x]+2[y]+[\alpha+\beta],\tag{5}$$

$$[2x]+[2y]=2[x]+2[y]+[2\alpha]+[2\beta]。\tag{6}$$

如果$[\alpha+\beta]=0$，那么显然有$[\alpha+\beta]\leq[2\alpha]+[2\beta]$；

如果$[\alpha+\beta]=1$，那么$\alpha$与$\beta$中至少有一个不小于$\frac{1}{2}$，于是

$$[2\alpha]+[2\beta]\geq1=[\alpha+\beta]。$$

因此无论$[\alpha+\beta]=0$ 或 1，都有$[\alpha+\beta]\leq[2\alpha]+[2\beta]$，由此及式(5)和式(6)可以推出式(4)。

**例 3** 设 $n$ 是正整数，则

$$[\sqrt{n}+\sqrt{n+1}]=[\sqrt{4n+2}]。\tag{7}$$

**解** 首先，我们有

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

$$<\sqrt{2n+1+2n+1}=\sqrt{4n+2}\,,$$

所以

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

若上式中的等号不成立，即

$$[\sqrt{n}+\sqrt{n+1}]<[\sqrt{4n+2}]\,,\tag{8}$$

则存在整数 $a$，使得

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

因此

$$2n+1+2\sqrt{n(n+1)}<a^2\leq4n+2\,,$$

$$2\sqrt{n^2+n}<a^2-2n-1\leq2n+1\,,$$

$$(2n+1)^2-1<(a^2-2n-1)^2\leq(2n+1)^2,$$

所以

$$a^2-2n-1=2n+1\Longrightarrow a^2=4n+2。\tag{9}$$

但是，无论 $2\mid a$ 或 $2\nmid a$，式(9)都不能成立，这个矛盾说明式(8)不能成立，即式(7)成立。

**例 4** 设 $x$ 是正数，$n$ 是正整数，则



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

**解** 设 $x=[x]+\alpha$，$\frac{i}{n}\leq\alpha<\frac{i+1}{n}$，$0\leq i\leq n-1$，则

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

$$=n[x]+i=n[x]+[n\alpha]=[n([x]+\alpha)]=[nx]。$$

**例 5** 求$[(\sqrt{3}+\sqrt{2})^{1992}]$的个位数。

**解** 由 $(\sqrt{3}\pm\sqrt{2})^2=5\pm2\sqrt{6}$ 得

$$(\sqrt{3}+\sqrt{2})^{1992}+(\sqrt{3}-\sqrt{2})^{1992}$$

$$=(5+2\sqrt{6})^{996}+(5-2\sqrt{6})^{996}$$

$$=2(5^{996}+\mathrm{C}_{996}^2\cdot5^{994}2^2\cdot6+\cdots+2^{996}6^{498})$$

$$=10A+2^{997}\cdot6^{498}=10A+2\cdot24^{498}=10A+2(25-1)^{498}$$

$$=10B+2,\tag{10}$$

其中 $A$ 和 $B$ 都是整数。由于 $0<5-2\sqrt{6}<1$，所以，由式(10)可知$[(\sqrt{3}+\sqrt{2})^{1996}]$的个位数是 1。

**注**：一般地，如果 $A$，$B\in\mathbf{N}$，$A^2>B$，$A-\sqrt{B}<1$，则由

$$(A+\sqrt{B})^k+(A-\sqrt{B})^k=2(A^k+\mathrm{C}_k^2A^{k-2}B+\cdots)$$

可以求出$[(A+\sqrt{B})^k]$。

**例 6** 设 $x$ 和 $y$ 是正无理数，$\frac{1}{x}+\frac{1}{y}=1$，证明：数列

$$[x],[2x],\cdots,[kx],\cdots\ \text{与}\ [y],[2y],\cdots,[my],\cdots\tag{11}$$

联合构成了整个正整数集合，而且，两个数列中的数互不相同。

**解** 显然 $x>1$，$y>1$，并且 $x\neq y$。因此，在数列(11)中至多有一个数等于给定的正整数 $n$，否则存在正整数 $k$ 与 $m$，使得

$$n=[kx]=[my]。$$

因为 $x$ 与 $y$ 都是无理数，所以我们有

$$n<kx<n+1,\ n<my<n+1,$$

$$\frac{k}{n+1}<\frac{1}{x}<\frac{k}{n},\quad \frac{m}{n+1}<\frac{1}{y}<\frac{m}{n},$$

$$\frac{k+m}{n+1}<\frac{1}{x}+\frac{1}{y}=1<\frac{k+m}{n},$$

$$n<k+m<n+1,$$

这是不可能的。

下面证明，对于任意给定的正整数 $n$，总可找到某个正整数 $k$，使得 $n$ 等于$[kx]$或者$[ky]$。假设不然，则存在 $p, q\in\mathbf{N}$，使得

$$[px]<n<[(p+1)x],\ [qy]<n<[(q+1)y]。$$

于是（因为 $x$ 和 $y$ 是无理数），

$$px<n<n+1\le[(p+1)x]<(p+1)x,$$

$$qy<n<n+1\le[(q+1)y]<(q+1)y,$$

$$\frac{p+q}{n}<\frac{1}{x}+\frac{1}{y}=1<\frac{p+q+2}{n+1},$$

$$p+q<n<n+1<p+q+2,$$

这是不可能的。

## 习 题 七

**1.** 证明定理 1。

**2.** 求使 12347!被 $35^k$ 整除的最大的 $k$ 值。

**3.** 设 $n$ 是正整数，$x$ 是实数，证明：$\sum_{r=1}^{\infty}\left[\frac{n+2^{r-1}}{2^r}\right]=n$。

**4.** 设 $n$ 是正整数，求方程

$$x^2-[x^2]=(x-[x])^2$$

在$[1, n]$中的解的个数。

**5.** 证明：方程

$$f(x)=[x]+[2x]+[2^2x]+[2^3x]+[2^4x]+[2^5x]=12345$$

没有实数解。

**6.** 证明：在 $n!$的标准分解式中，2 的指数 $h=n-k$，其中 $k$ 是 $n$ 的二进制表示的位数码之和。



# 第八节　素　数

在第六节中我们已经证明了：每个正整数可以表示成素数幂的乘积。这就引出了一个问题：素数是否有无穷多个？如果有无穷多个，那么，作为无穷大量，素数个数具有怎样的性状？这是数论研究中的一个中心课题。本节要对这一问题作初步的研究。

**定义 1**　对于正实数 $x$，以$\pi(x)$表示不超过 $x$ 的素数个数。

例如，$\pi(15)=6$，$\pi(10.4)=4$，$\pi(50)=15$。

**定理 1**　素数有无限多个。

**证明**　我们给出三个证明方法。

**证法Ⅰ**　假设只有 $k$ 个素数，设它们是 $p_1, p_2, \cdots, p_k$。记

$$N=p_1p_2\cdots p_k+1。$$

由第一节定理 2 可知，$N$ 有素因数 $p$，我们要说明 $p\ne p_i$，$1\le i\le k$，从而得出矛盾。

事实上，若有某个 $i$，$1\le i\le k$，使得 $p=p_i$，则由

$$p\mid N=p_1p_2\cdots p_k+1$$

推出 $p\mid 1$，这是不可能的。因此在 $p_1, p_2, \cdots, p_k$ 之外又有一个素数 $p$，这与假设是矛盾的。所以素数不可能是有限个。

**证法Ⅱ**　我们证明整数

$$2+1,\ 2^2+1,\ 2^{2^2}+1,\ \cdots,\ 2^{2^n}+1,\ \cdots$$

是两两互素的，从而由第六节引理 1 可知素数有无限多个。

事实上，若 $m$ 和 $n$ 是整数，$m>n\ge 0$，则

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

此处 $Q$ 是整数。因此

$$2^{2^m}+1=Q(2^{2^n}+1)+2,$$

故

$$(2^{2^m}+1, 2^{2^n}+1)=(2, 2^{2^n}+1)=1。$$

**证法Ⅲ** 假设只有有限个素数 $p_1, p_2, \cdots, p_k$。由第六节定理 1，每个正整数可以写成

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}，\ \alpha_i\geq 1，\ 1\leq i\leq k。$$

由于

$$\left(1-\frac{1}{p}\right)^{-1}=\sum_{\alpha=0}^{\infty}\frac{1}{p^{\alpha}}，$$

所以，对于任何正整数 $N$，有

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{N}\leq\left(1-\frac{1}{p_1}\right)^{-1}\left(1-\frac{1}{p_2}\right)^{-1}\cdots\left(1-\frac{1}{p_k}\right)^{-1}。$$

当 $N\to\infty$ 时，上式左端是一个无穷大量，右端是有限的，这个矛盾说明素数不能是有限多个。证毕。

**注 1**：形如 $2^{2^n}+1$（$n$ = 0, 1, 2, …）的数称为 Fermat 数。Fermat 曾经猜测它们都是素数。这是错误的，因为尽管 $F_0$，$F_1$，$F_2$，$F_3$，$F_4$ 都是素数，$F_5=2^{2^5}+1=641\cdot 6700417$ 却是合数。

**注 2**：将全体素数按大小顺序排列为

$$p_1=2，\ p_2=3，\ p_3=5，\ p_4，\ \cdots，\ p_n，\ \cdots，$$

那么由第一个证明方法可以看出

$$p_{n+1}\leq p_1p_2\cdots p_n+1，\ n\geq 1。$$

**定理 2** 对于 $n\geq 1$，

（ⅰ） $\pi(n)\geq\frac{1}{2}\log_2 n$;

（ⅱ） $p_n\leq 2^{2n}$。

**证明** （ⅰ） 设 $n$ 是大于 1 的正整数。由算术基本定理，对于任意的整数 $k$，$1\leq k\leq n$，都有整数 $a$ 和 $b$，使得 $k=a^2b$，其中整数 $b$ 不能被任何大于 1 的整数的平方整除。现在，我们来看使得

$$k=a^2b，\ 1\leq k\leq n \tag{1}$$

即 $1\leq a^2b\leq n$ 成立的整数 $a$，$b$ 有多少对。首先，整数 $a$ 的个数 $\leq\sqrt{n}$；其次，由于 $b\leq n$ 并且不含有平方因数，所以，整数 $b$ 的因数只可能是不超过 $n$ 的不同的素数的乘积，因此，整数 $b$ 的个数 $\leq 2^{\pi(n)}$。这样，



使得式(1)成立的整数 $a$ 和 $b$ 至多是 $\sqrt{n}\,2^{\pi(n)}$ 对，所以，$n\leq\sqrt{n}\,2^{\pi(n)}$，即 $\pi(n)\geq\frac{1}{2}\log_2 n$。

（ⅱ） 以 $p_m$ 表示第 $m$ 个素数，在结论（ⅰ）中取 $n=p_m$，我们得到 $m\geq\frac{1}{2}\log_2 p_m$，由此即可得到结论（ⅱ）。证毕。

**注**：定理 2 对于无穷大量 $\pi(x)$ 的下界估计是相当粗糙的。下面的定理是已经知道的（由于其证明较繁，故本书中不予证明）。

**定理 3**(素数定理) 我们有

$$\pi(x)\sim\frac{x}{\log x}，\ (x\to\infty)，$$

此处 $\log x$ 是以 $e$ 为底的 $x$ 的对数。

**推论** 以 $p_n$ 表示第 $n$ 个素数，则

$$p_n\sim n\log n\ (n\to\infty)。$$

**证明** 由定理 3，当 $n\to\infty$ 时，有

$$n\sim\frac{p_n}{\log p_n}。 \tag{2}$$

因此

$$n\log p_n\sim p_n，$$
$$\log n+\log\log p_n\sim\log p_n，$$
$$\log n\sim\log p_n。$$

由上式与式(2)得 $p_n\sim n\log n$（$n\to\infty$）。证毕。

**例 1** 若 $a>1$，$a^n-1$ 是素数，则 $a=2$，并且 $n$ 是素数。

**解** 若 $a>2$，则由

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

可知 $a^n-1$ 是合数。所以 $a=2$。

若 $n$ 是合数，则 $n=xy$，$x>1$，$y>1$，于是由

$$2^{xy}-1=(2^x-1)(2^{x(y-1)}+2^{x(y-2)}+\cdots+1)$$

以及 $2^x-1>1$ 可知 $2^n-1$ 是合数，所以 $2^n-1$ 是素数时，$n$ 必是素数。

**注**：若 $n$ 是素数，则称 $2^n-1$ 是 Mersenne 数。

**例 2** 形如 $4n+3$ 的素数有无限多个。

**解** 若不然，假设只有 $k$ 个形如 $4n+3$ 的素数 $p_1, p_2, \cdots, p_k$。记

$$N = 4p_1p\cdots p_k - 1。$$

由第六节引理 1，正整数 $N$ 可以写成若干个素数之积。我们指出，这些素因数中至少有一个是 $4n+3$ 形式。否则，若它们都是 $4n+1$ 的形式，则 $N$ 也是 $4n+1$ 的形式，这与 $N$ 的定义矛盾。以 $p$ 表示这个素因数，则 $p \neq p_i$，$1 \le i \le k$。否则若有某个 $i$，$1 \le i \le k$，使得 $p = p_i$，则由 $p \mid N$ 推出 $p \mid 1$，这是不可能的。因此在 $p_1, p_2, \cdots, p_k$ 之外又存在一个形如 $4n+3$ 的素数 $p$，这与原假设矛盾，所以形如 $4n+3$ 的素数有无限多个。

**例 3**　设 $f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_0$ 是整系数多项式，那么，存在无穷多个正整数 $n$，使得 $f(n)$是合数。

**解**　不妨假定 $a_k > 0$。于是 $f(x) \to +\infty$（$x \to +\infty$），因此，存在正整数 $N$，使得当 $n > N$ 时，有 $f(n) > 1$。取整数 $x > N$，记

$$y = f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_0,$$

又设 $r$ 是任意的正整数，$n = ry + x$，则

$$\begin{aligned} f(n) = f(ry+x) &= a_k(ry+x)^k + a_{k-1}(ry+x)^{k-1} + \cdots + a_0 \\ &= yQ + f(x) = y(Q+1) \end{aligned}$$

是合数。

## 习 题 八

**1.**　证明：若 $2^n + 1$ 是素数，则 $n$ 是 2 的乘幂。

**2.**　证明：若 $2^n - 1$ 是素数，则 $n$ 是素数。

**3.**　证明：形如 $6n+5$ 的素数有无限多个。

**4.**　设 $d$ 是正整数，$6 \nmid d$，证明：在以 $d$ 为公差的等差数列中，连续三项都是素数的情况最多发生一次。

**5.**　证明：对于任意给定的正整数 $n$，必存在连续的 $n$ 个自然数，使得它们都是合数。

**6.**　证明：级数 $\sum\limits_{n=1}^{\infty} \dfrac{1}{p_n}$ 发散，此处使用了定理 1 注 2 中的记号。



# 第二章　同 余

同余是数论中的一个基本概念。本章除介绍同余的基础知识外，还要介绍它的一些应用。

## 第一节　同余的基本性质

**定义 1**　给定正整数 $m$，如果整数 $a$ 与 $b$ 之差被 $m$ 整除，则称 $a$ 与 $b$ 对于模 $m$ 同余，或称 $a$ 与 $b$ 同余，模 $m$，记为

$$a \equiv b \pmod{m},$$

此时也称 $b$ 是 $a$ 对模 $m$ 的同余。

如果整数 $a$ 与 $b$ 之差不能被 $m$ 整除，则称 $a$ 与 $b$ 对于模 $m$ 不同余，或称 $a$ 与 $b$ 不同余，模 $m$，记为 $a \not\equiv b \pmod{m}$。

**定理 1**　下面的三个叙述是等价的：

（ⅰ）　$a \equiv b \pmod{m}$；

（ⅱ）　存在整数 $q$，使得 $a = b + qm$；

(ⅲ)　存在整数 $q_1$，$q_2$，使得 $a = q_1m + r$，$b = q_2m + r$，$0 \le r < m$。

**证明**　留作习题。

**定理 2**　同余具有下面的性质：

（ⅰ）　$a \equiv a \pmod{m}$；

（ⅱ）　$a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$；

(ⅲ)　$a \equiv b$，$b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$。

**证明**　留作习题。

**定理 3**　设 $a$，$b$，$c$，$d$ 是整数，并且

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}, \tag{1}$$

则

（ⅰ）　$a + c \equiv b + d \pmod{m}$；

（ⅱ）　$ac \equiv bd \pmod{m}$。

**证明** (ⅰ) 由式(1)及定义 1 可知

$$m \mid a-b,\ m \mid c-d,$$

因此

$$m \mid (a+c)-(b+d),$$

此即结论(ⅰ);

(ⅱ) 由式(1)及定理 1 可知，存在整数 $q_1$ 与 $q_2$ 使得

$$a=b+q_1m,\ c=d+q_2m,$$

因此

$$ac=bd+(q_1q_2m+q_1d+q_2b)m,$$

再利用定理 1，推出结论(ⅱ)。证毕。

**定理 4** 设 $a_i$，$b_i$（$0 \le i \le n$）以及 $x$，$y$ 都是整数，并且

$$x \equiv y \pmod m,\ a_i \equiv b_i \pmod m,\ 0 \le i \le n,$$

则

$$\sum_{i=0}^{n} a_i x^i \equiv \sum_{i=0}^{n} b_i y^i \pmod m。 \tag{2}$$

**证明** 留作习题。

**定理 5** 下面的结论成立:

(ⅰ) $a \equiv b \pmod m,\ d \mid m,\ d>0 \Longrightarrow a \equiv b \pmod d$;

(ⅱ) $a \equiv b \pmod m,\ k>0,\ k \in \mathbf{N} \Longrightarrow ak \equiv bk \pmod{mk}$;

(ⅲ) $a \equiv b \pmod{m_i},\ 1 \le i \le k \Longrightarrow a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$;

(ⅳ) $a \equiv b \pmod m \Longrightarrow (a, m)=(b, m)$;

(ⅴ) $ac \equiv bc \pmod m,\ (c, m)=1 \Longrightarrow a \equiv b \pmod m$。

**证明** 结论(ⅰ)—(ⅳ)的证明，留作习题。

(ⅴ) 由

$$ac \equiv bc \pmod m$$

得到 $m \mid c(a-b)$，再由 $(c, m)=1$ 和第一章第三节定理 4 得到 $m \mid a-b$，即

$$a \equiv b \pmod m。$$

证毕。

**例 1** 设 $N=\overline{a_n a_{n-1} \cdots a_0}$ 是整数 $N$ 的十进制表示，即

$$N=a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0,$$

则



(ⅰ) $3 \mid N \Longleftrightarrow 3 \mid \sum_{i=0}^{n} a_i$;

(ⅱ) $9 \mid N \Longleftrightarrow 9 \mid \sum_{i=0}^{n} a_i$;

(ⅲ) $11 \mid N \Longleftrightarrow 11 \mid \sum_{i=0}^{n} (-1)^i a_i$;

(ⅳ) $13 \mid N \Longleftrightarrow 13 \mid \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots$。

**解** 由

$$10^0 \equiv 1,\ 10^1 \equiv 1,\ 10^2 \equiv 1,\ \cdots \pmod 3$$

及式(2)可知

$$N=\sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \pmod 3,$$

由上式可得到结论(ⅰ)。

结论(ⅱ)，(ⅲ)用同样方法证明。

为了证明结论(ⅳ)，只需利用式(2)及

$$10^0 \equiv 1,\ 10^1 \equiv -3,\ 10^2 \equiv -4,\ 10^3 \equiv -1,\ \cdots \pmod{13}$$

和

$$N=\overline{a_{n-1} a_{n-2} \cdots a_1 a_0}=\overline{a_2 a_1 a_0} \cdot 10^0 + \overline{a_5 a_4 a_3} \cdot 10^3 + \cdots \ 。$$

**注**：一般地，在考虑使 $N=\overline{a_{n-1} a_{n-2} \cdots a_1 a_0}$ 被 $m$ 除的余数时，首先是求出正整数 $k$，使得

$$10^k \equiv -1 \text{ 或 } 1 \pmod m,$$

再将 $N=\overline{a_{n-1} a_{n-2} \cdots a_1 a_0}$ 写成

$$N=\overline{a_{k-1} a_{k-2} \cdots a_1 a_0} \cdot 10^0 + \overline{a_{2k-1} a_{2h-2} \cdots a_k} \cdot 10^k + \cdots$$

的形式，再利用式(2)。

**例 2** 求 $N=\overline{a_{n-1} a_{n-2} \cdots a_1 a_0}$ 被 7 整除的条件，并说明 1123456789 能否被 7 整除。

**解** $10^0 \equiv 1,\ 10^1 \equiv 3,\ 10^2 \equiv 2,\ 10^3 \equiv -1 \pmod 7$，因此

$$\begin{aligned} N &= \overline{a_{n-1} a_{n-2} \cdots a_1 a_0}=\overline{a_2 a_1 a_0} \cdot 10^0 + \overline{a_5 a_4 a_3} \cdot 10^3 + \cdots \\ &\equiv \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \cdots \pmod 7, \end{aligned}$$

即

$$7 \mid N \Leftrightarrow 7 \mid \overline{a_2a_1a_0} - \overline{a_5a_4a_3} + \overline{a_8a_7a_6} - \cdots 。$$

由于

$$789 - 456 + 123 - 1 = 455，\ 7 \mid 455，$$

所以 $7 \mid 1123456789$。

**例 3**　说明 $2^{2^5}+1$ 是否被 641 整除。

**解**　依次计算同余式

$2^2 \equiv 4$，$2^4 \equiv 16$，$2^8 \equiv 256$，$2^{16} \equiv 154$，$2^{32} \equiv -1 \pmod{641}$。

因此

$$2^{2^5}+1 \equiv 0 \pmod{641}，$$

即 $641 \mid 2^{2^5}+1$。

**注**：一般地，计算 $a^b \pmod m$ 常是一件比较繁复的工作。但是，如果利用 Euler 定理或 Fermat 定理（见第四节）就可以适当简化。

**例 4**　求 $(257^{33}+46)^{26}$ 被 50 除的余数。

**解**　利用定理 4 有

$$\begin{aligned}(257^{33}+46)^{26} &\equiv (7^{33}-4)^{26} = [7\cdot(7^2)^{16}-4]^{26}\\ &\equiv [7\cdot(-1)^{16}-4]^{26} = (7-4)^{26}\\ &\equiv 3^{26} = 3\cdot(3^5)^5 \equiv 3\cdot(-7)^5 = -3\cdot 7\cdot(7^2)^2\\ &\equiv -21 \equiv 29 \pmod{50}，\end{aligned}$$

即所求的余数是 29。

**例 5**　求 $n = 7^{7^7}$ 的个位数。

**解**　我们有

$$7^1 \equiv -3，\ 7^2 \equiv -1，\ 7^4 \equiv 1 \pmod{10}，$$

因此，若

$$7^7 \equiv r \pmod 4，$$

则

$$n = 7^{7^7} \equiv 7^7 \pmod{10}。 \tag{3}$$

现在 $7^7 \equiv (-1)^7 \equiv -1 \equiv 3 \pmod 4$，所以由式(3)得到

$$n = 7^{7^7} \equiv 7^3 \equiv (-3)^3 \equiv -7 \equiv 3 \pmod{10}，$$

即 $n$ 的个位数是 3。

**注**：一般地，若求 $a^{b^c}$ 对模 $m$ 的同余，可分以下步骤进行：



(ⅰ)　求出整数 $k$，使 $a^k \equiv 1 \pmod m$；

(ⅱ)　求出正整数 $r$，$r < k$，使得 $b^c \equiv r \pmod k$；

(ⅲ)　$a^{b^c} \equiv a^r \pmod m$。

**例 6**　证明：若 $n$ 是正整数，则 $13 \mid 4^{2n+1} + 3^{n+2}$。

**解**　由

$$\begin{aligned}4^{2n+1} + 3^{n+2} &= 4\cdot 4^{2n} + 9\cdot 3^n = 4\cdot 16^n + 9\cdot 3^n\\ &\equiv 4\cdot 3^n + 9\cdot 3^n = 13\cdot 3^n \equiv 0 \pmod{13}\end{aligned}$$

得证。

**例 7**　证明：若 $2 \nmid a$，$n$ 是正整数，则

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}。 \tag{4}$$

**解**　设 $a = 2k+1$，当 $n = 1$ 时，有

$$a^2 = (2k+1)^2 = 4k(k+1) + 1 \equiv 1 \pmod{2^3}，$$

即式(4)成立。

设式(4)对于 $n = k$ 成立，则有

$$a^{2^k} \equiv 1 \pmod{2^{k+2}} \Rightarrow a^{2^k} = 1 + q2^{k+2}，$$

其中 $q \in \mathbf{Z}$，所以

$$a^{2^{k+1}} = (1 + q2^{k+2})^2 = 1 + q'2^{k+3} \equiv 1 \pmod{2^{k+3}}，$$

其中 $q'$ 是某个整数。这说明式(4)当 $n = k+1$ 也成立。

由归纳法知式(4)对所有正整数 $n$ 成立。

**例 8**　设 $p$ 是素数，$a$ 是整数，则由 $a^2 \equiv 1 \pmod p$ 可以推出

$$a \equiv 1 \text{ 或 } a \equiv -1 \pmod p。$$

**解**　由

$$a^2 \equiv 1 \pmod p \Rightarrow p \mid a^2 - 1 = (a+1)(a-1)，$$

所以必是

$$p \mid a+1 \text{ 或 } p \mid a-1，$$

即 $a \equiv -1 \pmod p$ 或 $a \equiv 1 \pmod p$。

**例 9**　设 $n$ 的十进制表示是 $\overline{13xy45z}$，若 $792 \mid n$，求 $x$，$y$，$z$。

**解**　因为 $792 = 8\cdot 9\cdot 11$，故

$$792 \mid n \Leftrightarrow 8 \mid n，\ 9 \mid n \text{ 及 } 11 \mid n。$$

我们有

$$8 \mid n \Leftrightarrow 8 \mid \overline{45z} \Rightarrow z = 6，$$

以及

$$9 \mid n \Leftrightarrow 9 \mid 1+3+x+y+4+5+z=19+x+y \Leftrightarrow 9 \mid x+y+1, \quad (5)$$

$$11 \mid n \Leftrightarrow 11 \mid z-5+4-y+x-3+1=3-y+x \Leftrightarrow 11 \mid 3-y+x。 \quad (6)$$

由于 $0 \le x, y \le 9$，所以由式(5)与式(6)分别得出

$$x+y+1=9 \text{ 或 } 18,$$

$$3-y+x=0 \text{ 或 } 11。$$

这样得到四个方程组：

$$\begin{cases} x+y+1=a \\ 3-y+x=b \end{cases},$$

其中 $a$ 取值 9 或 18，$b$ 取值 0 或 11。在 $0 \le x, y \le 9$ 的条件下解这四个方程组，得到 $x=8$，$y=0$，$z=6$。

## 习 题 一

**1.** 证明定理 1 和定理 2。

**2.** 证明定理 4。

**3.** 证明定理 5 中的结论(ⅰ)—(ⅳ)。

**4.** 求 $8^{1234}$ 被 13 除的余数。

**5.** 设 $f(x)$是整系数多项式，并且 $f(1), f(2), \cdots, f(m)$都不能被 $m$ 整除，则 $f(x)=0$ 没有整数解。

**6.** 已知 $99 \mid \overline{62\alpha\beta427}$，求$\alpha$与$\beta$。

# 第二节　完全剩余系

由带余数除法我们知道，对于给定的正整数 $m$，可以将所有的整数按照被 $m$ 除的余数分成 $m$ 类。本节将对此作进一步的研究。

**定义 1**　给定正整数 $m$，对于每个整数 $i$，$0 \le i \le m-1$，称集合

$$R_i(m)=\{\, n;\ n \equiv i \pmod m,\ n \in \mathbf{Z} \,\}。$$

是模 $m$ 的一个剩余类。

显然，每个整数必定属于且仅属于某一个 $R_i(m)$（$0 \le i \le m-1$），



而且，属于同一剩余类的任何两个整数对模 $m$ 是同余的，不同剩余类中的任何两个整数对模 $m$ 是不同余的。

例如，模 5 的五个剩余类是

$$R_0(5)=\{\cdots, -10, -5, 0, 5, 10, \cdots\},$$

$$R_1(5)=\{\cdots, -9, -4, 1, 6, 11, \cdots\},$$

$$R_2(5)=\{\cdots, -8, -3, 2, 7, 12, \cdots\},$$

$$R_3(5)=\{\cdots, -7, -2, 3, 8, 13, \cdots\},$$

$$R_4(5)=\{\cdots, -6, -1, 4, 9, 14, \cdots\}。$$

**定义 2**　设 $m$ 是正整数，从模 $m$ 的每一个剩余类中任取一个数 $x_i$（$0 \le i \le m-1$），称集合$\{x_0, x_1, \cdots, x_{m-1}\}$是模 $m$ 的一个完全剩余系（或简称为完全系）。

由于 $x_i$的选取是任意的，所以模 $m$ 的完全剩余系有无穷多个，通常称

(ⅰ)　$\{0, 1, 2, \cdots, m-1\}$是模 $m$ 的最小非负完全剩余系；

(ⅱ)　$\left\{-\frac{m}{2}+1, \cdots, -1, 0, 1, \cdots, \frac{m}{2}\right\}$（当$2 \mid m$）或

$$\left\{-\frac{m-1}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-1}{2}\right\}（当 2 \nmid m）$$

是模 $m$ 的绝对最小完全剩余系。

例如，集合$\{0, 6, 7, 13, 24\}$是模 5 的一个完全剩余系，集合$\{0, 1, 2, 3, 4\}$是模 5 的最小非负完全剩余系。

**定理 1**　整数集合 $A$ 是模 $m$ 的完全剩余系的充要条件是

(ⅰ)　$A$ 中含有 $m$ 个整数；

(ⅱ)　$A$ 中任何两个整数对模 $m$ 不同余。

**证明**　留作习题。

**定理 2**　设 $m \ge 1$，$a$，$b$ 是整数，$(a, m)=1$，$\{x_1, x_2, \cdots, x_m\}$是模 $m$ 的一个完全剩余系，则$\{ax_1+b, ax_2+b, \cdots, ax_m+b\}$也是模 $m$ 的一个完全剩余系。

**证明**　由定理 1，只需证明：若 $x_i \ne x_j$，则

$$ax_i+b \not\equiv ax_j+b \pmod m。 \quad (1)$$

事实上，若

$$ax_i+b \equiv ax_j+b \pmod m,$$

则

$$ax_i \equiv ax_j \pmod m,$$

由此及第一节定理 5 得到

$$x_i \equiv x_j \pmod m,$$

因此 $x_i = x_j$。所以式(1)必定成立。证毕。

**定理 3** 设 $m_1, m_2 \in \mathbf{N}$，$A \in \mathbf{Z}$，$(A, m_1) = 1$，又设

$$X = \{x_1, x_2, \cdots, x_{m_1}\},\quad Y = \{y_1, y_2, \cdots, y_{m_2}\},$$

分别是模 $m_1$ 与模 $m_2$ 的完全剩余系，则

$$R = \{\, Ax + m_1 y;\ x \in X,\ y \in Y \,\}$$

是模 $m_1 m_2$ 的一个完全剩余系。

**证明** 由定理 1 只需证明：若 $x', x'' \in X$，$y', y'' \in Y$，并且

$$Ax' + m_1 y' \equiv Ax'' + m_1 y'' \pmod{m_1 m_2}, \tag{2}$$

则

$$x' = x'',\ y' = y''。$$

事实上，由第一节定理 5 及式(2)，有

$$Ax' \equiv Ax'' \pmod{m_1} \Longrightarrow x' \equiv x'' \pmod{m_1} \Longrightarrow x' = x'',$$

再由式(2)，又推出

$$m_1 y' \equiv m_1 y'' \pmod{m_1 m_2} \Longrightarrow y' \equiv y'' \pmod{m_2} \Longrightarrow y' = y''\ 。$$

证毕。

**推论** 若 $m_1, m_2 \in \mathbf{N}$，$(m_1, m_2) = 1$，则当 $x_1$ 与 $x_2$ 分别通过模 $m_1$ 与模 $m_2$ 的完全剩余系时，$m_2 x_1 + m_1 x_2$ 通过模 $m_1 m_2$ 的完全剩余系。

**定理 4** 设 $m_i \in \mathbf{N}$（$1 \le i \le n$），则当 $x_i$ 通过模 $m_i$（$1 \le i \le n$）的完全剩余系时，

$$x = x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 m_2 \cdots m_{n-1} x_n$$

通过模 $m_1 m_2 \cdots m_n$ 的完全剩余系。

**证明** 对 $n$ 施行归纳法。

当 $n = 2$ 时，由定理 3 知定理结论成立。

假设定理结论当 $n = k$ 时成立，即当 $x_i$（$2 \le i \le k+1$）分别通过模 $m_i$ 的完全剩余系时，

$$y = x_2 + m_2 x_3 + m_2 m_3 x_4 + \cdots + m_2 \cdots m_k x_{k+1}$$

通过模 $m_2 m_3 \cdots m_{k+1}$ 的完全剩余系。由定理 3，当 $x_1$ 通过模 $m_1$ 的完全剩余系，$x_i$（$2 \le i \le k+1$）通过模 $m_i$ 的完全剩余系时，



$$\begin{aligned} x_1 + m_1 y &= x_1 + m_1(x_2 + m_2 x_3 + \cdots + m_2 \cdots m_k x_{k+1}) \\ &= x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 m_2 \cdots m_k x_{k+1} \end{aligned}$$

通过模 $m_1 m_2 \cdots m_{k+1}$ 的完全剩余系。即定理结论对于 $n = k+1$ 也成立。定理由归纳法得证。证毕。

**定理 5** 设 $m_i \in \mathbf{N}$，$A_i \in \mathbf{Z}$（$1 \le i \le n$），并且满足下面的条件：

(ⅰ) $(m_i, m_j) = 1$，$1 \le i, j \le n$，$i \ne j$；

(ⅱ) $(A_i, m_i) = 1$，$1 \le i \le n$；

(ⅲ) $m_i \mid A_j$，$1 \le i, j \le n$，$i \ne j$ 。

则当 $x_i$（$1 \le i \le n$）通过模 $m_i$ 的完全剩余系 $X_i$ 时，

$$y = A_1 x_1 + A_2 x_2 + \cdots + A_n x_n$$

通过模 $m_1 m_2 \cdots m_n$ 的完全剩余系。

**证明** 由定理 1 只需证明：若 $x_i', x_i'' \in X_i$，$1 \le i \le n$，则由

$$A_1 x_1' + A_2 x_2' + \cdots + A_n x_n' \equiv A_1 x_1'' + A_2 x_2'' + \cdots + A_n x_n'' \pmod{m_1 \cdots m_n} \tag{3}$$

可以得到 $x_i' = x_i''$，$1 \le i \le n$。

事实上，由条件(ⅲ)及式(3)易得，对于任意的 $i$，$1 \le i \le n$，有

$$A_i x_i' \equiv A_i x_i'' \pmod{m_i}。$$

由此并利用条件(ⅱ)和第一节定理 5 推得

$$x_i' \equiv x_i'' \pmod{m_i},$$

因此 $x_i' = x_i''$。证毕。

**例 1** 设 $A = \{x_1, x_2, \cdots, x_m\}$ 是模 $m$ 的一个完全剩余系，以 $\{x\}$ 表示 $x$ 的小数部分，证明：若 $(a, m) = 1$，则

$$\sum_{i=1}^{m} \left\{\frac{ax_i + b}{m}\right\} = \frac{1}{2}(m-1)。$$

**解** 当 $x$ 通过模 $m$ 的完全剩余系时，$ax + b$ 也通过模 $m$ 的完全剩余系，因此对于任意的 $i$（$1 \le i \le m$），$ax_i + b$ 一定与且只与某个整数 $j$（$1 \le j \le m$）同余，即存在整数 $k$，使得

$$ax_i + b = km + j,\ (1 \le j \le m)$$

从而

$$\begin{aligned} \sum_{i=1}^{m} \left\{\frac{ax_i + b}{m}\right\} &= \sum_{j=1}^{m} \left\{k + \frac{j}{m}\right\} = \sum_{j=1}^{m} \left\{\frac{j}{m}\right\} = \sum_{j=1}^{m-1} \left\{\frac{j}{m}\right\} \\ &= \sum_{j=1}^{m-1} \frac{j}{m} = \frac{1}{m} \cdot \frac{m(m-1)}{2} = \frac{m-1}{2}。 \end{aligned}$$

**例 2**　设 $p \geq 5$ 是素数，$a \in \{2, 3, \cdots, p-2\}$，则在数列

$$a，2a，3a，\cdots，(p-1)a，pa \tag{4}$$

中有且仅有一个数 $b$，满足

$$b \equiv 1 \pmod{p}。 \tag{5}$$

此外，若 $b = ka$，则 $k \neq a$，$k \in \{2, 3, \cdots, p-2\}$。

**解**　因为$(a, p) = 1$，所以由定理 2，式(4)中的数构成模 $p$ 的一个完全剩余系，因此必有数 $b$ 满足式(5)。

设 $b = ka$，那么

(ⅰ)　$k \neq a$，否则，$b = a^2 \equiv 1 \pmod{p}$，即 $p \mid (a+1)(a-1)$，因此 $p \mid a-1$ 或 $p \mid a+1$，这与 $2 \leq a \leq p-2$ 矛盾；

(ⅱ)　$k \neq 1$，否则，$b = 1 \cdot a \equiv 1 \pmod{p}$，这与 $2 \leq a \leq p-2$ 矛盾；

(ⅲ)　$k \neq -1$，否则，$b = -a \equiv 1 \pmod{p}$，这与 $2 \leq a \leq p-2$ 矛盾。

若又有 $k'$，$2 \leq k' \leq p-2$，使得 $b \equiv k'a \pmod{p}$，则

$$k'a \equiv ka \pmod{p}。$$

因$(a, p) = 1$，所以 $k \equiv k' \pmod{p}$，从而 $p \mid k - k'$，这是不可能的。这证明了唯一性。

**例 3**(Wilson 定理)　设 $p$ 是素数，则

$$(p-1)! \equiv -1 \pmod{p}。$$

**解**　不妨设 $p \geq 5$。由例 2 容易推出对于 $2, 3, \cdots, p-2$，中的每个整数 $a$，都存在唯一的整数 $k$，$2 \leq k \leq p-2$，使得

$$ka \equiv 1 \pmod{p}。 \tag{6}$$

因此，整数 $2, 3, \cdots, p-2$ 可以两两配对使得式(6)成立。所以

$$2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p}，$$

从而

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2)(p-1) \equiv p-1 \equiv -1 \pmod{p}。$$

**例 4**　设 $m > 0$ 是偶数，$\{a_1, a_2, \cdots, a_m\}$与$\{b_1, b_2, \cdots, b_m\}$都是模 $m$ 的完全剩余系，证明：$\{a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m\}$不是模 $m$ 的完全剩余系。

**解**　因为$\{1, 2, \cdots, m\}$与$\{a_1, a_2, \cdots, a_m\}$都是模 $m$ 的完全剩余系，所以

$$\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} i = \frac{m(m+1)}{2} \equiv \frac{m}{2} \pmod{m}。 \tag{7}$$



同理

$$\sum_{i=1}^{m} b_i \equiv \frac{m}{2} \pmod{m}。 \tag{8}$$

如果$\{a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m\}$是模 $m$ 的完全剩余系，那么也有

$$\sum_{i=1}^{m} (a_i + b_i) \equiv \frac{m}{2} \pmod{m}。$$

联合上式与式(7)和式(8)，得到

$$0 \equiv \frac{m}{2} + \frac{m}{2} \equiv \frac{m}{2} \pmod{m}，$$

这是不可能的，所以$\{a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m\}$不能是模 $m$ 的完全剩余系。

## 习 题 二

**1.**　证明定理 1。

**2.**　证明：若 $2p + 1$ 是奇素数，则

$$(p!)^2 + (-1)^p \equiv 0 \pmod{2p+1}。$$

**3.**　证明：若 $p$ 是奇素数，$N = 1 + 2 + \cdots + (p-1)$，则

$$(p-1)! \equiv p - 1 \pmod{N}。$$

**4.**　证明 Wilson 定理的逆定理：若 $n > 1$，并且

$$(n-1)! \equiv -1 \pmod{n}，$$

则 $n$ 是素数。

**5.**　设 $m$ 是整数，$4 \mid m$，$\{a_1, a_2, \cdots, a_m\}$与$\{b_1, b_2, \cdots, b_m\}$是模 $m$ 的两个完全剩余系，证明：$\{a_1b_1, a_2b_2, \cdots, a_mb_m\}$不是模 $m$ 的完全剩余系。

**6.**　设 $m_1, m_2, \cdots, m_n$ 是两两互素的正整数，$\delta_i$（$1 \leq i \leq n$）是整数，并且

$$\delta_i \equiv 1 \pmod{m_i}，\qquad 1 \leq i \leq n，$$

$$\delta_i \equiv 0 \pmod{m_j}，\ i \neq j，\ 1 \leq i, j \leq n。$$

证明：当 $b_i$ 通过模 $m_i$（$1 \leq i \leq n$）的完全剩余系时，

$$b_1\delta_1 + b_2\delta_2 + \cdots + b_n\delta_n$$

通过模 $m = m_1m_2 \cdots m_n$ 的完全剩余系。

# 第三节　简化剩余系

在模 $m$ 的完全剩余系中，与 $m$ 互素的整数所成的集合有一些特殊的性质，我们要在这一节中对它们做些研究。

**定义 1**　设 $R$ 是模 $m$ 的一个剩余类，若有 $a\in R$，使得$(a, m) = 1$，则称 $R$ 是模 $m$ 的一个简化剩余类。

显然，若 $R$ 是模的简化剩余类，则 $R$ 中的每个整数都与 $m$ 互素。

例如，模 4 的简化剩余类有两个：

$$R_1(4) = \{ \cdots, -7 , -3, 1 , 5 , 9 , \cdots \},$$

$$R_3(4) = \{ \cdots, -5 , -1 , 3 , 7 , 11 , \cdots \}。$$

**定义 2**　对于正整数 $k$，令函数$\varphi(k)$的值等于模 $k$ 的所有简化剩余类的个数，称$\varphi(k)$为 Euler 函数，或 Euler—$\varphi$函数。

例如，容易验证$\varphi(2) = 1$，$\varphi(3) = 2$，$\varphi(4) = 2$，$\varphi(7) = 6$。

显然，$\varphi(m)$就是在 $m$ 的一个完全剩余系中与 $m$ 互素的整数的个数。

**定义 3**　对于正整数 $m$，从模 $m$ 的每个简化剩余类中各取一个数 $x_i$，构成一个集合$\{x_1, x_2, \cdots, x_{\varphi(m)}\}$，称为模 $m$ 的一个简化剩余系（或简称为简化系）。

显然，由于选取方式的任意性，模 $m$ 的简化剩余系有无穷多个。

例如，集合{9, –5, –3, –1}是模 8 的简化剩余系，集合{1, 3, 5, 7}也是模 8 的简化剩余系，通常称最小非负简化剩余系。

**定理 1**　整数集合 $A$ 是模 $m$ 的简化剩余系的充要条件是

(ⅰ)　$A$ 中含有$\varphi(m)$个整数；

(ⅱ)　$A$ 中的任何两个整数对模 $m$ 不同余；

(ⅲ)　$A$ 中的每个整数都与 $m$ 互素。

**证明**　留作习题。

**定理 2**　设 $a$ 是整数，$(a, m) = 1$，$B = \{x_1, x_2, \cdots, x_{\varphi(m)}\}$是模 $m$ 的简化剩余系，则集合 $A = \{ax_1, ax_2, \cdots, ax_{\varphi(m)}\}$也是模 $m$ 的简化剩余系。

**证明**　显然，集合 $A$ 中有$\varphi(m)$个整数。其次，由于$(a, m) = 1$，所以，对于任意的 $x_i$（$1 \le i \le \varphi(m)$），$x_i\in B$，有$(ax_i, m) = (x_i, m) = 1$。因此，$A$ 中的每一个数都与 $m$ 互素。最后，我们指出，$A$ 中的任何两个不同的整数对模 $m$ 不同余。事实上，若有 $x', x''\in B$，使得

$$a x' \equiv ax'' \pmod m,$$



那么，因为$(a, m) = 1$，所以 $x' \equiv x'' \pmod m$，于是 $x' = x''$。由以上结论及定理 1 可知集合 $A$ 是模 $m$ 的一个简化系。证毕。

**注**：在定理 2 的条件下，若 $b$ 是整数，集合

$$\{ax_1 + b, ax_2 + b,, \cdots, ax_{\varphi(m)} + b\}$$

不一定是模 $m$ 的简化剩余系。例如，取 $m = 4$，$a = 1$，$b = 1$，以及模 4 的简化剩余系{1, 3}。

**定理 3**　设 $m_1, m_2\in\mathbf{N}$，$(m_1, m_2) = 1$，又设

$$X = \{x_1, x_2, \cdots, x_{\varphi(m_1)}\} 与 Y = \{y_1, y_2, \cdots, y_{\varphi(m_2)}\}$$

分别是模 $m_1$ 与 $m_2$ 的简化剩余系，则

$$A = \{ m_1y + m_2x；\ x\in X，\ y\in Y \}$$

是模 $m_1m_2$ 的简化剩余系。

**证明**　由第二节定理 3 推论可知，若以 $X'$与 $Y'$分别表示模 $m_1$ 与 $m_2$ 的完全剩余系，使得 $X\subset X'$，$Y\subset Y'$，则

$$A' = \{ m_1y + m_2x；\ x\in X'，\ y\in Y' \}$$

是模 $m_1m_2$ 的完全剩余系。因此只需证明 $A'$中所有与 $m_1m_2$ 互素的整数的集合 $R$ 是集合 $A$。显然，$A\subseteq A'$。

若 $m_1y + m_2x\in R$，则$(m_1y + m_2x, m_1m_2) = 1$，所以$(m_1y + m_2x, m_1) = 1$，于是

$$(m_2x, m_1) = 1，(x, m_1) = 1，\ x\in X。$$

同理可得到 $y\in Y$，因此 $m_1y + m_2x\in A$。这说明 $R\subseteq A$。

另一方面，若 $m_1y + m_2x\in A$，则 $x\in X$，$y\in Y$，即

$$(x, m_1) = 1，(y, m_2) = 1。$$

由此及$(m_1, m_2) = 1$ 得到

$$(m_2x + m_1y, m_1) = (m_2x, m_1) = 1$$

以及

$$(m_2x + m_1y, m_2) = (m_1y, m_2) = 1。$$

因为 $m_1$ 与 $m_2$ 互素，所以$(m_2x + m_1y, m_1m_2) = 1$，于是 $m_2x + m_1y\in R$。因此 $A\subseteq R$。

综合以上，得到 $A = R$。证毕。

**定理 4**　设 $m, n\in\mathbf{N}$，$(m, n) = 1$，则$\varphi(mn) = \varphi(m)\varphi(n)$。

**证明**　这是定理 3 的直接推论。证毕。

**定理 5**　设 $n$ 是正整数，$p_1, p_2, \cdots, p_k$ 是它的全部素因数，则

$$\varphi(n)=n\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdots\Big(1-\frac{1}{p_k}\Big)=n\prod_{p\mid n}\Big(1-\frac{1}{p}\Big)。$$

**证明**　设 $n$ 的标准分解式是 $n=\prod_{i=1}^{k}p_i^{\alpha_i}$，由定理 4 得到

$$\varphi(n)=\prod_{i=1}^{k}\varphi(p_i^{\alpha_i})。\tag{1}$$

对任意的素数 $p$，$\varphi(p^\alpha)$等于数列 $1, 2, \cdots, p^\alpha$中与 $p^\alpha$（也就是与 $p$）互素的整数的个数，因此

$$\varphi(p^\alpha)=p^\alpha-\Big[\frac{p^\alpha}{p}\Big]=p^\alpha-p^{\alpha-1}=p^\alpha\Big(1-\frac{1}{p}\Big),$$

将上式与式(1)联合，证明了定理。证毕。

由定理 5 可知，$\varphi(n)=1$ 的充要条件是 $n=1$ 或 2。

**例 1**　设整数 $n\ge 2$，证明：

$$\sum_{\substack{1\le i\le n\\(i,n)=1}} i=\frac{1}{2}n\varphi(n),$$

即在数列 $1, 2, \cdots, n$ 中，与 $n$ 互素的整数之和是 $\frac{1}{2}n\varphi(n)$。

**解**　设在 $1, 2, \cdots, n$ 中与 $n$ 互素的$\varphi(n)$个数是

$$a_1, a_2, \cdots, a_{\varphi(n)},\ (a_i, n)=1,\ 1\le a_i\le n-1,\ 1\le i\le\varphi(n),$$

则

$$(n-a_i, n)=1,\ 1\le n-a_i\le n-1,\ 1\le i\le\varphi(n),$$

因此，集合$\{a_1, a_2, \cdots, a_{\varphi(n)}\}$与集合$\{n-a_1, n-a_2, \cdots, n-a_{\varphi(n)}\}$是相同的，于是

$$a_1+a_2+\cdots+a_{\varphi(n)}=(n-a_1)+(n-a_2)+\cdots+(n-a_{\varphi(n)}),$$
$$2(a_1+a_2+\cdots+a_{\varphi(n)})=n\varphi(n),$$

因此

$$a_1+a_2+\cdots+a_{\varphi(n)}=\frac{1}{2}n\varphi(n)。$$

**例 2**　设 $n$ 是正整数，则

$$\sum_{d\mid n}\varphi(d)=n,$$



此处$\sum_{d\mid n}$是对 $n$ 的所有正约数求和。

**解**　将正整数 $1, 2, \cdots, n$ 按它们与整数 $n$ 的最大的公约数分类，则

$$n=\sum_{i=1}^{n}1=\sum_{d\mid n}\sum_{\substack{(i,n)=d\\1\le i\le n}}1=\sum_{d\mid n}\sum_{\substack{(\frac{i}{d},\frac{n}{d})=1\\1\le\frac{i}{d}\le\frac{n}{d}}}1=\sum_{d\mid n}\varphi(\frac{n}{d})=\sum_{d\mid n}\varphi(d)。$$

**例 3**　设 $n\in\mathbf{N}$，证明：

(ⅰ)　若 $n$ 是奇数，则$\varphi(4n)=2\varphi(n)$；

(ⅱ)　$\varphi(n)=\frac{1}{2}n$ 的充要条件是 $n=2^k$，$k\in\mathbf{N}$；

(ⅲ)　$\varphi(n)=\frac{1}{3}n$ 的充要条件是 $n=2^k3^l$，$k, l\in\mathbf{N}$；

(ⅳ)　若 $6\mid n$，则$\varphi(n)\le\frac{1}{3}n$；

(ⅴ)　若 $n-1$ 与 $n+1$ 都是素数，$n>4$，则$\varphi(n)\le\frac{1}{3}n$。

**解**　(ⅰ)　我们有

$$\varphi(4n)=\varphi(2^2n)=\varphi(2^2)\varphi(n)=2\varphi(n);$$

(ⅱ)　若 $n=2^k$，则

$$\varphi(2^k)=2^k\Big(1-\frac{1}{2}\Big)=2^{k-1}=\frac{1}{2}n,$$

若$\varphi(n)=\frac{1}{2}n$，设 $n=2^kn_1$，$2\nmid n_1$，则由

$$\frac{1}{2}n=\varphi(n)=\varphi(2^kn_1)=\varphi(2^k)\varphi(n_1)=2^{k-1}\varphi(n_1)$$
$$=\frac{1}{2}2^k n_1\frac{\varphi(n_1)}{n_1}=\frac{1}{2}n\frac{\varphi(n_1)}{n_1}$$

推出$\varphi(n_1)=n_1$，所以 $n_1=1$，即 $n=2^k$；

(ⅲ)　若 $n=2^k3^l$，则

$$\varphi(n)=\varphi(2^k)\varphi(3^l)=2^k\Big(1-\frac{1}{2}\Big)3^l\Big(1-\frac{1}{3}\Big)=\frac{1}{3}n。$$

若$\varphi(n)=\frac{1}{3}n$，设$n=2^k3^ln_1$，$6\nmid n_1$，则由

$$\frac{1}{3}n=\varphi(n)=\varphi(2^k3^ln_1)=\varphi(2^k)\varphi(3^l)\varphi(n_1)=\frac{1}{3}n\frac{\varphi(n_1)}{n_1}$$

推出$\varphi(n_1)=n_1$，所以$n_1=1$，即$n=2^k3^l$；

(iv) 设$n=2^k3^ln_1$，$6\nmid n_1$，则

$$\varphi(n)=\varphi(2^k)\varphi(3^l)\varphi(n_1)=\frac{1}{3}2^k3^l\varphi(n_1)\le\frac{1}{3}2^k3^ln_1=\frac{1}{3}n;$$

(v) 因为$n>4$，所以$n-1$与$n+1$都是奇素数，所以$n$是偶数。

因为$n-1>3$，所以$n-1$与$n+1$都不等于3，当然不被3整除，所以$3\mid n$，因此$6\mid n$。再由上面已经证明的结论(iv)，即可得到结论(v)。

**例 4** 证明：若$m, n\in\mathbf{N}$，则$\varphi(mn)=(m,n)\varphi([m,n])$；

**解** 显然$mn$与$[m,n]$有相同的素因数，设它们是$p_i$（$1\le i\le k$），则

$$\varphi(mn)=mn\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right),$$

$$\varphi([m,n])=[m,n]\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)。$$

由此两式及$mn=(m,n)[m,n]$即可得证。

## 习 题 三

**1.** 证明定理1。

**2.** 设$m_1, m_2, \cdots, m_n$是两两互素的正整数，$x_i$分别通过模$m_i$的简化剩余系（$1\le i\le n$），$m=m_1m_2\cdots m_n$，$M_i=\frac{m}{m_i}$，则

$$M_1x_1+M_2x_2+\cdots+M_nx_n$$

通过模$m$的简化剩余系。

**3.** 设$m>1$，$(a,m)=1$，$x_1, x_2, \ldots, x_{\varphi(m)}$是模$m$的简化剩余系，证明：



$$\sum_{i=1}^{\varphi(m)}\left\{\frac{ax_i}{m}\right\}=\frac{1}{2}\varphi(m)。$$

其中$\{x\}$表示$x$的小数部分。

**4.** 设$m$与$n$是正整数，证明：

$$\varphi(mn)\varphi((m,n))=(m,n)\varphi(m)\varphi(n)。$$

**5.** 设$a$，$b$是任意给定的正整数，证明：存在无穷多对正整数$m$与$n$，使得

$$a\varphi(m)=b\varphi(n)。$$

**6.** 设$n$是正整数，证明：

(i) $\varphi(n)>\frac{1}{2}\sqrt{n}$；

(ii) 若$n$是合数，则$\varphi(n)\le n-\sqrt{n}$。

## 第四节 Euler 定理

本节中所介绍的 Euler 定理，在理论和应用两个方面都是很重要的。

**定理 1**(Euler) 设$m$是正整数，$(a,m)=1$，则

$$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m)。$$

**证明** 由第三节定理2，设$\{x_1, x_2, \cdots, x_{\varphi(m)}\}$是模$m$的一个简化剩余系，则$\{ax_1, ax_2, \cdots, ax_{\varphi(m)}\}$也是模$m$的简化剩余系，因此

$$ax_1ax_2\cdots ax_{\varphi(m)}\equiv x_1x_2, \cdots x_{\varphi(m)}\ (\mathrm{mod}\ m),$$

$$a^{\varphi(m)}x_1x_2\cdots x_{\varphi(m)}\equiv x_1x_2, \cdots x_{\varphi(m)}\ (\mathrm{mod}\ m)。\qquad(1)$$

由于$(x_1x_2\cdots x_{\varphi(m)}, m)=1$，所以由式(1)得出

$$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m)。$$

证毕。

**定理 2**(Fermat) 设$p$是素数，则对于任意的整数$a$，有

$$a^p\equiv a\ (\mathrm{mod}\ p)。$$

**证明** 若$(a,p)=1$，则由定理1得到

$$a^{p-1}\equiv 1\ (\mathrm{mod}\ p)\Longrightarrow a^p\equiv a\ (\mathrm{mod}\ p)。$$

若$(a,p)>1$，则$p\mid a$，所以

$$a^p \equiv 0 \equiv a \pmod{p}。$$

证毕。

**例 1**　设 $n$ 是正整数，则 $5 \nmid 1^n + 2^n + 3^n + 4^n$ 的充要条件是 $4 \mid n$。

**解**　因为 $\varphi(5) = 4$，所以，由定理 2

$$k^4 \equiv 1 \pmod{5}，\ 1 \le k \le 4。$$

因此，若 $n = 4q + r$，$0 \le r \le 3$，则

$$1^n + 2^n + 3^n + 4^n \equiv 1^r + 2^r + 3^r + 4^r \equiv 1^r + 2^r + (-2)^r + (-1)^r \pmod{5}，\quad (2)$$

用 $r = 0$，1，2，3，4 分别代入式(2)即可得出所需结论。

**例 2**　设 $\{x_1, x_2, \cdots, x_{\varphi(m)}\}$ 是模 $m$ 的简化剩余系，则

$$(x_1 x_2 \cdots x_{\varphi(m)})^2 \equiv 1 \pmod{m}。$$

**解**　记 $P = x_1 x_2 \cdots x_{\varphi(m)}$，则 $(P, m) = 1$。又记

$$y_i = \frac{P}{x_i}，\ 1 \le i \le \varphi(m)，$$

则 $\{y_1, y_2, \cdots, y_{\varphi(m)}\}$ 也是模 $m$ 的简化剩余系，因此

$$\prod_{i=1}^{\varphi(m)} x_i \equiv \prod_{i=1}^{\varphi(m)} \frac{P}{x_i} \pmod{m}，$$

再由 Euler 定理，推出

$$P^2 \equiv P^{\varphi(m)} \equiv 1 \pmod{m}。$$

**例 3**　设 $(a, m) = 1$，$d_0$ 是使

$$a^d \equiv 1 \pmod{m}$$

成立的最小正整数，则

(ⅰ)　$d_0 \mid \varphi(m)$；

(ⅱ)　对于任意的 $i$，$j$，$0 \le i, j \le d_0 - 1$，$i \ne j$，有

$$a^i \not\equiv a^j \pmod{m}。\quad (3)$$

**解**　(ⅰ)　由 Euler 定理，$d_0 \le \varphi(m)$，因此，由带余数除法，有

$$\varphi(m) = q d_0 + r，\ q \in \mathbf{Z}，\ q > 0，\ 0 \le r < d_0。$$

因此，由上式及 $d_0$ 的定义，利用定理 1，我们得到

$$1 \equiv a^{\varphi(m)} = a^{q d_0 + r} \equiv a^r \pmod{m}，$$

即整数 $r$ 满足

$$a^r \equiv 1 \pmod{m}，\ 0 \le r < d_0 。$$

由 $d_0$ 的定义可知必是 $r = 0$，即 $d_0 \mid \varphi(m)$；

(ⅱ)　若式(3)不成立，则存在 $i$，$j$，$0 \le i, j \le d_0 - 1$，$i \ne j$，使得



$$a^i \equiv a^j \pmod{m}。$$

不妨设 $i > j$。因为 $(a, m) = 1$，所以

$$a^{i-j} \equiv 0 \pmod{m}，\ 0 < i - j < d_0。$$

这与 $d_0$ 的定义矛盾，所以式(3)必成立。

**例 4**　设 $a$，$b$，$c$，$m$ 是正整数，$m > 1$，$(b, m) = 1$，并且

$$b^a \equiv 1 \pmod{m}，\ b^c \equiv 1 \pmod{m}，\quad (4)$$

记 $d = (a, c)$，则 $b^d \equiv 1 \pmod{m}$。

**解**　利用辗转相除法可以求出整数 $x$，$y$，使得 $ax + cy = d$，显然 $xy < 0$。

若 $x > 0$，$y < 0$，由式(4)知

$$1 \equiv b^{ax} = b^d b^{-cy} = b^d (b^c)^{-y} \equiv b^d \pmod{m}。$$

若 $x < 0$，$y > 0$，由式(4)知

$$1 \equiv b^{cy} = b^d b^{-ax} = b^d (b^a)^{-x} \equiv b^d \pmod{m}。$$

**例 5**　设 $p$ 是素数，$p \mid b^n - 1$，$n \in \mathbf{N}$，则下面的两个结论中至少有一个成立：

(ⅰ)　$p \mid b^d - 1$ 对于 $n$ 的某个因数 $d < n$ 成立；

(ⅱ)　$p \equiv 1 \pmod{n}$。

若 $2 \nmid n$，$p > 2$，则(ⅱ)中的 mod $n$ 可以改为 mod $2n$。

**解**　记 $d = (n, p - 1)$，由 $b^n \equiv 1$，$b^{p-1} \equiv 1 \pmod{p}$，及例题 4，有

$$b^d \equiv 1 \pmod{p}。$$

若 $d < n$，则结论(ⅰ)得证。

若 $d = n$，则 $n \mid p - 1$，即 $p \equiv 1 \pmod{n}$，这就是结论(ⅱ)。

若 $2 \nmid n$，$p > 2$，则 $p \equiv 1 \pmod{2}$。由此及结论(ⅱ)，并利用同余的基本性质，得到 $p \equiv 1 \pmod{2n}$。

**注**：例 5 提供了一个求素因数的方法，就是说，整数 $b^n - 1$ 的素因数 $p$，是 $b^d - 1$（当 $d \mid n$ 时）的素因数，或者是形如 $kn + 1$ 的数（当 $2 \nmid n$，$p > 2$ 时，是形如 $2kn + 1$ 的数）。

**例 6**　将 $2^{11} - 1 = 2047$ 分解因数。

**解**　由例 5，若 $p \mid 2^{11} - 1$，则 $p \equiv 1 \pmod{22}$，即 $p$ 只能在数列

$$23，45，67，\cdots，22k + 1，\cdots$$

中。逐个用其中的素数去除 2047，得到

$$23 \mid 2047，\ 2047 = 23 \cdot 89。$$

**例 7**　将 $2^{35}-1=34359738367$ 分解因数。

**解**　由例 5，若 $p\mid 2^{35}-1$，则 $p$ 是 $2^5-1=31$ 或 $2^7-1=127$ 的素因数，或者 $p\equiv 1 \pmod{70}$。由于 31 和 127 是素数，并且

$$2^{35}-1=31\cdot 127\cdot 8727391,$$

所以，$2^{35}-1$ 的另外的素因数 $p$ 只可能在数列

$$71，211，281，\cdots \tag{5}$$

中。经检验，得到 $8727391=71\cdot 122921$。

显然，122921 的素因数也在 31，127 或者数列(5)中。简单的计算说明，122921 不能被 31 和 127 整除，也不能被数列(5)中的不超过 $\sqrt{122921}<351$ 的数整除，所以 122921 是素数，于是

$$2^{35}-1=31\cdot 127\cdot 71\cdot 122921。$$

**例 8**　设 $n$ 是正整数，记 $F_n=2^{2^n}+1$，则 $2^{F_n}\equiv 2 \pmod{F_n}$。

**解**　容易验证，当 $n\le 4$ 时 $F_n$ 是素数，所以，由 Fermat 定理可知结论显然成立。

当 $n\ge 5$ 时，有 $n+1<2^n$，$2^{n+1}\mid 2^{2^n}$。记 $2^{2^n}=k2^{n+1}$，则

$$\begin{aligned}2^{F_n}-2&=2^{2^{2^n}+1}-2=2(2^{2^{2^n}}-1)=2(2^{k2^{n+1}}-1)\\&=2((2^{2^{n+1}})^k-1)=2Q_1(2^{2^{n+1}}-1)=Q_2(2^{2^n}+1),\end{aligned}$$

其中 $Q_1$ 与 $Q_2$ 是整数。上式即是 $2^{F_n}\equiv 2 \pmod{F_n}$。

**注 1**：我们已经知道，$F_5$ 是合数，因此，例 8 说明，一般地，Fermat 定理的逆定理不成立。即若有整数 $a$，$(a,n)=1$，使得

$$a^{n-1}\equiv 1 \pmod{n}, \tag{6}$$

并不能保证 $n$ 是素数。习题 3 说明，即使所有的与 $n$ 互素的整数都满足式(6)，也不能保证 $n$ 是素数。

**注 2**：设 $n$ 是合数，若存在整数 $a$，$(a,n)=1$，使得式(6)成立，则称 $n$ 是关于基数 $a$ 的伪素数。

**例 9**　对于任意的正整数 $a\ge 3$，存在无穷多个关于基数 $a$ 的伪素数。

**解**　取奇素数 $p$，$(p,a(a^2-1))=1$，令

$$m=\frac{a^p-1}{a-1}\cdot\frac{a^p+1}{a+1}=\frac{a^{2p}-1}{a^2-1},$$

则 $m$ 显然是合数。由于 $p-1$ 是偶数，所以，$a^2-1\mid a^{p-1}-1$；由 Euler



定理，又有 $p\mid a^{p-1}-1$。但是$(p,a^2-1)=1$，所以 $p(a^2-1)\mid a^{p-1}-1$。此外，由于 $a$ 和 $a^p$ 有相同的奇偶性，所以 $2\mid a+a^p$。注意到

$$(a^2-1)(m-1)=a^{2p}-a^2=a(a^{p-1}-1)(a^p+a),$$

我们得到

$$2p(a^2-1)\mid(a^2-1)(m-1)\Longrightarrow 2p\mid m-1,$$

即存在整数 $t$，使得 $m=1+2pt$。

由 $m$ 的定义，有

$$a^{2p}=1+m(a^2-1)\equiv 1 \pmod{m},$$

因此

$$a^{m-1}=a^{2pt}\equiv 1 \pmod{m}$$

并且$(a,m)=1$，这说明 $m$ 是关于基数 $a$ 的伪素数。由于满足条件的素数 $p$ 有无穷多个，所以，关于基数 $a$ 的伪素数 $m$ 也有无穷多个。

## 习 题 四

**1.**　证明：$1978^{103}-1978^3$ 能被 $10^3$ 整除。

**2.**　求 $313^{159}$ 被 7 除的余数。

**3.**　证明：对于任意的整数 $a$，$(a,561)=1$，都有 $a^{560}\equiv 1 \pmod{561}$，但 561 是合数。

**4.**　设 $p$，$q$ 是两个不同的素数，证明：

$$p^{q-1}+q^{p-1}\equiv 1 \pmod{pq}。$$

**5.**　将 $6^{12}-1$ 分解成素因数之积。

**6.**　设 $n\in\mathbf{N}$，$b\in\mathbf{N}$，对于 $b^n+1$ 的素因数，你有甚麼与例 6 相似的结论？

# 第五节　数论函数

定义在整数集合上的函数，称为数论函数，或算术函数。例如，函数

$$y=x^2，\ y=\sin x，\ y=e^x$$

都可称为数论函数。但是，通常在使用数论函数这个词时，仅指那些

只在整数集合或正整数集合上有定义的函数，或者只与数论研究有特殊关系的函数，例如，在前面所遇到过的欧拉函数$\varphi(n)$，整数部分函数$[x]$。本节中还要介绍几个数论函数。

**定义 1**　设$f(n)$是定义在整数集合$A$上的函数，若

$$f(mn)=f(m)f(n) \tag{1}$$

对所有的整数$m,n\in A$，$(m,n)=1$成立，则称$f(n)$是$A$上的积性函数，或者，在不引起误会的情况下，简称为积性函数。

如果式(1)对于$A$中的任何$m$，$n$都成立，则称$f(n)$是$A$上的完全积性函数，简称为完全积性函数。

以下，我们总假定$A$是由全体正整数所成的集合，即$A=\mathbf{N}$。

**例 1**　函数$\varphi(n)$是积性函数，但不是完全积性函数。事实上，由第三节定理 4 我们知道$\varphi(n)$是积性函数。由

$$2=\varphi(4)\neq\varphi(2)\varphi(2)=1$$

可知$\varphi(n)$不是完全积性函数。

**例 2**　以$d(n)$表示正整数$n$的正约数的个数，则$d(n)$是积性函数，但不是完全积性函数。

**例 3**　函数

$$\mu(n)=\begin{cases}1 & \text{当 } n=1\\ (-1)^r & \text{当 } n=p_1p_2\cdots p_r,\ \ p_1,p_2,\cdots,p_r\text{是互异的素数}\\ 0 & \text{其他情形}\end{cases},$$

是积性函数，但不是完全积性函数。事实上，容易看出$\mu(n)$是积性函数。由

$$1=\mu(2)\mu(2)\neq\mu(4)=0$$

可知$\mu(n)$不是完全积性函数。

**定理 1**　设函数$f(n)$是不恒等于零的数论函数，则$f(n)$是积性函数的充要条件是：$f(1)=1$并且对任意的$n\in\mathbf{N}$，$n>1$，有

$$f(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k})=f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_k^{\alpha_k}), \tag{2}$$

其中$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$是$n$的标准分解式。

**证明**　必要性　若$f(n)$是不恒等于零的积性函数，则有某个$n_0\in\mathbf{N}$，使得$f(n_0)\neq0$，于是有$f(n_0)=f(1)f(n_0)$，所以$f(1)=1$。由积性函数的性质可知式(2)成立。

充分性　设$m\in\mathbf{N}$，$n\in\mathbf{N}$，$(m,n)=1$。若$m$与$n$中有一个是 1，则



由$f(1)=1$易知式(1)成立。若$m>1$，$n>1$，设$m$与$n$的标准分解式分别是

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\ \text{与}\ n=q_1^{\beta_1}q_2^{\beta_2}\cdots q_r^{\beta_r},$$

其中$p_i$（$1\le i\le k$）与$q_j$（$1\le j\le r$）是互不相同的素数，则由式(2)得到

$$\begin{aligned}f(mn)&=f(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\cdots q_r^{\beta_r})\\&=f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_k^{\alpha_k})f(q_1^{\beta_1})f(q_2^{\beta_2})\cdots f(q_r^{\beta_r})\\&=f(m)f(n),\end{aligned}$$

即$f(n)$是积性函数。证毕。

**定理 2**　设函数$f(n)$是不恒为零的数论函数，则$f(n)$是完全积性函数的充要条件是：$f(1)=1$并且对任意的$n\in\mathbf{N}$，$n>1$，有

$$f(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k})=f(p_1)^{\alpha_1}f(p_2)^{\alpha_2}\cdots f(p_k)^{\alpha_k},$$

其中$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$是$n$的标准分解式。

**证明**　留作习题。

**定义 2**　设$f(n)$是数论函数，称函数

$$F(n)=\sum_{d|n}f(d),\ \ n\in\mathbf{N} \tag{3}$$

是$f(n)$的 Mobius 变换，$f(n)$是$F(n)$的 Mobius 逆变换，其中$\sum_{d|n}$表示对$n$的所有正约数$d$求和。

例如，取$f(n)=1$，则$F(n)=\sum_{d|n}1=d(n)$；取$f(n)=n$，则$F(n)=\sum_{d|n}d$是$n$的所有正约数$d$之和，通常记为$\sigma(n)$。

以下，我们用$n=\prod_{i=1}^{k}p_i^{\alpha_i}$或$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$表示正整数$n$的标准分解式。

**定理 3**　(ⅰ)　设$F(n)$是$f(n)$的 Mobius 变换，则

$$F(n)=\sum_{i_1=0}^{\alpha_1}\cdots\sum_{i_k=0}^{\alpha_k}f(p_1^{i_1}\cdots p_k^{i_k});$$

(ⅱ)　设$F(n)$是积性函数$f(n)$的 Mobius 变换，则

$$F(n)=\sum_{i_1=0}^{\alpha_1} f(p_1^{i_1})\cdots\sum_{i_k=0}^{\alpha_k} f(p_k^{i_k})=\prod_{i=1}^{k}(1+f(p_i)+\cdots+f(p_i^{\alpha_i}))\ ,$$

从而 $F(n)$也是积性函数。

**证明**　因为 $n$ 的正约数具有

$$p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k}\quad(0\le i_1\le\alpha_1,0\le i_2\le\alpha_2,\cdots,0\le i_k\le\alpha_k)$$

的形式，所以结论(ⅰ)成立。由结论(ⅰ)与定理 1 推出结论(ⅱ)。证毕。

**引理 1**　对任意的正整数 $n$，有

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{当 } n=1\\ 0 & \text{其他情形}\end{cases}。$$

**证明**　$\mu(n)$是积性函数，因此，由$\mu(n)$的定义及定理 3 得到

$$\sum_{d|n}\mu(d)=\prod_{p^{\alpha}\|n}(1+\mu(p)+\mu(p^2)+\cdots+\mu(p^{\alpha}))=\prod_{p|n}(1+\mu(p))\,,$$

其中 $p^{\alpha}\|n$ 表示 $p^{\alpha}\mid n$，同时 $p^{\alpha+1}\nmid n$。由上式即可得出引理结论。证毕。

**定理 4**　设 $f(n)$是数论函数，则式(3)与下式是等价的：

$$f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right),\ n\in\mathbf{N}。\tag{4}$$

**证明**　若式(3)成立，则

$$\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)\sum_{m|\frac{n}{d}}f(m)=\sum_{d|n}\mu(d)\sum_{md|n}f(m)$$

$$=\sum_{m|n}f(m)\sum_{d|\frac{n}{m}}\mu(d)\,,$$

由引理 1，我们知道上式右端等于 $f(n)$，即式(4)成立。

若式(4)成立，则

$$\sum_{d|n}f(d)=\sum_{d|n}\sum_{m|d}\mu(m)F\left(\frac{d}{m}\right)=\sum_{m|n}\mu(m)\sum_{m|d,d|n}F\left(\frac{d}{m}\right)。$$

在第二个和式中，令 $d=mk$，则上式成为



$$\sum_{d|n}f(d)=\sum_{m|n}\mu(m)\sum_{mk|n}F(k)=\sum_{m|n}\mu(m)\sum_{k|\frac{n}{m}}F(k)$$

$$=\sum_{k|n}F(k)\sum_{m|\frac{n}{k}}\mu(m)=F(n)。$$

证毕。

**例 4**　对于正整数 $n$，若它的标准分解式是 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，定义

$$\omega(n)=\begin{cases}k & \text{当 } n>1\\ 0 & \text{当 } n=1\end{cases};$$

与

$$\Omega(n)=\begin{cases}\alpha_1+\cdots+\alpha_k & \text{当 } n>1\\ 0 & \text{当 } n=1\end{cases}。$$

则$\omega(n)$与$\Omega(n)$满足下面的等式：

$\omega(mn)=\omega(m)+\omega(n)$，$(m,n)=1$，$m,n\in\mathbf{N}$，

$\Omega(mn)=\Omega(m)+\Omega(n)$，　　$m,n\in\mathbf{N}$。

**例 5**　数论函数$\nu(n)=(-1)^{\omega(n)}$是积性函数，数论函数$\lambda(n)=(-1)^{\Omega(n)}$是完全积性函数。

**例 6**　对于正整数 $n$。以$\sigma(n)$表示 $n$ 的所有正约数之和，即

$$\sigma(n)=\sum_{d|n}d\ 。$$

若 $n$ 的标准分解式是 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\sigma(n)=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}。\tag{5}$$

**解**　由定理 3，$\sigma(n)$是积性函数，并且

$$\sigma(n)=\prod_{i=1}^{k}(1+p_i+p_i^2+\cdots+p_i^{\alpha_i})。\tag{6}$$

对于固定的 $p^{\alpha}$，有

$$\sigma(p^{\alpha})=1+p+p^2+\cdots+p^{\alpha}=\frac{p^{\alpha+1}-1}{p-1}。$$

由此及式(6)得到式(5)。

**例 7**　求 $\dfrac{\mu^2(n)}{\varphi(n)}$ 的 Mobius 变换。

**解**　设 $n$ 的标准分解式是 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$,则由$\mu(n)$的定义及定理 3，得到

$$\begin{aligned}F(n)&=\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}=\prod_{i=1}^{k}\left(1+\frac{\mu^2(p_i)}{\varphi(p_i)}+\cdots+\frac{\mu^2(p_i^{\alpha_i})}{\varphi(p_i^{\alpha_i})}\right)\\&=\prod_{i=1}^{k}\left(1+\frac{1}{\varphi(p_i)}\right)=\prod_{i=1}^{k}\left(1+\frac{1}{p_i-1}\right)\\&=\prod_{i=1}^{k}\frac{p_i}{p_i-1}=\prod_{i=1}^{k}\frac{p_i^{\alpha_i}}{p_i^{\alpha_i-1}(p_i-1)}=\frac{n}{\varphi(n)}。\end{aligned}$$

## 习 题 五

**1.** 证明例 2 中的结论。

**2.** 证明定理 2。

**3.** 求 $\sum\limits_{d|n}\dfrac{1}{d}$。

**4.** 设 $f(n)$是积性函数，证明：

(ⅰ) $\sum\limits_{d|n}\mu(d)f(d)=\prod\limits_{p|n}(1-f(p))$

(ⅱ) $\sum\limits_{d|n}\mu^2(d)f(d)=\prod\limits_{p|n}(1+f(p))$。

**5.** 求$\varphi(n)$的 Mobius 变换。



# 第三章　数的表示

对于数的十进制表示，我们已经是很熟悉的了。本章主要介绍实数的 $b$ 进制表示和连分数表示，以及一些基本知识。

## 第一节　实数的 $b$ 进制表示法

本节介绍实数的 $b$ 进制表示法。

**定理 1**　设 $b$ 是大于 1 的整数，则任何正整数 $a$ 都可以写成

$$a=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0$$

的形式，其中 $a_k\neq 0$，$a_i$（$0\le i\le k$）是在 0 与 $b-1$ 之间唯一确定的整数。

**证明**　由带余数除法，有整数 $k$，使得

$$\begin{aligned}&a=q_1b+a_0,\quad 0\le a_0\le b-1,\quad q_1\ge b,\\&q_1=q_2b+a_1,\quad 0\le a_1\le b-1,\quad q_2\ge b,\\&\cdots\cdots\\&q_{k-1}=q_kb+a_{k-1},\ 0\le a_{k-1}\le b-1,\ 0<q_k\le b-1,\end{aligned}$$

其中诸 $a_i$ 与 $q_i$ 都是唯一确定的。记 $q_k=a_k$，则 $0<a_k\le b-1$，并且

$$\begin{aligned}a&=q_1b+a_0=(q_2b+a_1)b+a_0=q_2b^2+a_1b+a_0\\&=(q_3b+a_2)b^2+a_1b+a_0=q_3b^3+a_2b^2+a_1b+a_0\\&=\cdots\\&=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0\ 。\end{aligned}$$

证毕。

**定理 2**　设 $b$ 是大于 1 的整数，则任何小于 1 的正实数$\alpha$都可以写成

$$\alpha=\sum_{i=1}^{\infty}\frac{a_i}{b_i}\ ,\ 0\le a_i\le b-1,\ i\ge 1。\tag{1}$$

如果对于任意的正整数 $m$，都有某个 $n>m$，使得 $a_n\neq b-1$，则$\alpha$的表

示式(1)是唯一的。

**证明** 记 $a_1=[b\alpha]$，则

$$0\le a_1\le b-1。$$

记$\alpha_1=b\alpha-a_1$，则 $0\le\alpha_1<1$，并且

$$\alpha=\frac{a_1}{b}+\frac{\alpha_1}{b}。$$

如果$\alpha_1=0$，则定理得证。如果 $0<\alpha_1<1$，则重复上述过程，有

$$\alpha_1=\frac{a_2}{b}+\frac{\alpha_2}{b}，\ 0\le a_2\le b-1，\ 0\le\alpha_2<1。$$

将这样的过程进行 $k$ 次之后，我们得到

$$\alpha=\frac{a_1}{b}+\frac{a_2}{b^2}+\cdots+\frac{a_k}{b^k}+\frac{\alpha_k}{b^k}，\tag{2}$$

其中 $0\le a_i\le b-1$（$0\le i\le k$），$0\le\alpha_k<1$。如果$\alpha_k=0$，则定理得证。如果总是$\alpha_k\ne0$（$k\ge1$），不断进行以上过程，我们就得到了一个无穷级数

$$\sum_{i=1}^{\infty}\frac{a_i}{b^i}，\ 0\le a_i\le b-1，\ i\ge1。$$

因为

$$\frac{\alpha_k}{b^k}\to0\ (k\to\infty)，$$

所以，由式(2)可知

$$\alpha=\sum_{i=1}^{\infty}\frac{a_i}{b^i}。$$

下面证明式(1)的唯一性。设

$$\alpha=\sum_{i=1}^{\infty}\frac{a_i}{b^i}=\sum_{i=1}^{\infty}\frac{c_i}{b^i}，\ 0\le a_i,c_i\le b-1，\ i\ge1。\tag{3}$$

此时，若有正整数 $k$，使得 $a_i=c_i$，（$1\le i\le k-1$），$a_k\ne c_k$，那么，不妨设 $a_k>c_k$，于是，由式(3)得到

$$\frac{a_k-c_k}{b^k}=\sum_{i=k+1}^{\infty}\frac{c_i-a_i}{b^i}。\tag{4}$$

显然



$$\frac{a_k-c_k}{b^k}\ge\frac{1}{b^k}。$$

另一方面，由式(3)，有

$$\Big|\sum_{i=k+1}^{\infty}\frac{c_i-a_i}{b^i}\Big|\le\sum_{i=k+1}^{\infty}\frac{b-1}{b^i}=(b-1)\frac{\frac{1}{b^{k+1}}}{1-\frac{1}{b}}=\frac{1}{b^k}，$$

在上式中，当且仅当

$$a_i=b-1，\ c_i=0\ 或\ c_i=b-1，\ a_i=0\ (i\ge k+1)\tag{5}$$

时等号成立。因此，若使式(4)成立，必是式(5)成立。这说明，在定理的假设条件下，表达式(1)是唯一的。证毕。

**定理 3** 设 $b$ 是大于 1 的整数，则任何正实数$\alpha$都可以唯一地写成

$$\alpha=\sum_{i=-\infty}^{k}a_ib^i，\ 0\le a_i\le b-1，\ i\le k\tag{6}$$

的形式，其中，对于任何正整数 $m$，都存在 $n>m$，使得 $a_{-n}<b-1$。

**证明** 留做习题。

**定义 1** 设$\alpha$是正实数，若式(6)成立，则记为

$$\alpha=(a_ka_{k-1}\cdots a_1a_0.a_{-1}a_{-2}\cdots)_b，\tag{7}$$

并称它是$\alpha$的 $b$ 进制表示，称 $a_i$（$i\le k$）是$\alpha$的 $b$ 进制表示的位数码。当 $b=10$ 时，就是通常的十进制记数法，此时常略去式(7)中的括号和下标 $b=10$。

此外，称$(a_ka_{k-1}\cdots a_1a_0)_b$ 与 $(0.a_{-1}a_{-2}\cdots)_b$ 分别是$\alpha$的 $b$ 进制表示的整数部分和小数部分。

**定义 2** 设$\alpha$是实数，$0<\alpha<1$，$\alpha$的 $b$ 进制表示是

$$\alpha=(0.c_1c_2c_3\cdots)_b，\tag{8}$$

则称它是一个 $b$ 进制小数。若存在整数 $s\ge0$，$t>0$，使得

$$c_{s+i}=c_{s+i+kt}，\ i=1,2,\cdots,t，\ k=0,1,2,\cdots\tag{9}$$

成立，则称式(8)中的 $b$ 进制小数是循环小数，并记作

$$\alpha=(0.c_1\cdots c_s\dot{c}_{s+1}\cdots\dot{c}_{s+t})_b。$$

若使式(9)成立的最小的 $s$ 和 $t$ 分别是 $s_0$ 和 $t_0$，则称$\{c_{s_0+1},\cdots,c_{s_0+t_0}\}$是循环节；若 $s_0=0$，则称式(8)中的小数是（$b$ 进制）纯循环小数。

下面，我们讨论数的十进制表示的小数的循环性。为方便计，将使用记号 $\overline{a_n a_{n-1}\cdots a_1 a_0}$ 表示整数$(a_n a_{n-1}\cdots a_1 a_0)_{10}$，用 $0.a_1 a_2\cdots$表示小数$(0.a_1 a_2\cdots)_{10}$。

**定理 4**　循环小数表示有理数。

**证明**　不妨只考察小于 1 的正循环小数。设有循环小数

$$\alpha = 0.a_1\cdots a_s b_1\cdots b_t b_1\cdots b_t\cdots ,$$

记 $\overline{a_1\cdots a_s} = A$，$\overline{b_1\cdots b_t} = B$，则

$$\begin{aligned}\alpha &= \overline{a_1\cdots a_s}\cdot\frac{1}{10^s} + \overline{b_1\cdots b_t}\left(\frac{1}{10^{s+t}} + \frac{1}{10^{s+2t}} + \cdots\right)\\ &= \frac{1}{10^s}\left(A + B\left(\frac{1}{10^t} + \frac{1}{10^{2t}} + \cdots\right)\right)\\ &= \frac{1}{10^s}\left(A + B\frac{1}{10^t - 1}\right) = \frac{A(10^t - 1) + B}{10^s(10^t - 1)}\end{aligned}$$

是有理数。证毕。

**推论**　纯循环小数表示有理数 $\frac{a}{b}$；若$(a, b) = 1$，则$(b, 10) = 1$。

**证明**　在定理 4 的证明中，取 $s = 0$，则

$$\frac{a}{b} = \frac{B}{10^t - 1},$$

所以 $a(10^t - 1) = bB$。但是$(a, b) = 1$，所以 $b \mid 10^t - 1$，于是$(b, 10) = 1$。证毕。

**定理 5**　设 $a$ 与 $b$ 是正整数，$0 < a < b$，$(a, b) = 1$，并且$(b, 10) = 1$，则 $\frac{a}{b}$ 的十进制表示是纯循环小数。

**证明**　因为 $(b, 10) = 1$，由 Euler 定理可知，有正整数 $k$，使得

$$10^k \equiv 1 \pmod b),\quad 0 < k \le \varphi(b),$$

因此存在整数 $q$ 使得

$$10^k a = qb + a,\quad 10^k\frac{a}{b} = q + \frac{a}{b}, \tag{10}$$

其中 $0 < q = (10^k - 1)\frac{a}{b} < 10^k - 1$，即 $q$ 具有 $\overline{a_k a_{k-1}\cdots a_1}$ 的形式，而且



$a_k, \cdots, a_1$ 不能都等于 0，也不能都等于 9。由式(10)，有

$$(10^k - 1)\frac{a}{b} = q = \overline{a_k a_{k-1}\cdots a_1},$$

$$\begin{aligned}\frac{a}{b} &= \overline{a_k a_{k-1}\cdots a_1}\,\frac{1}{10^k - 1} = \overline{a_k a_{k-1}\cdots a_1}\left(\frac{1}{10^k} + \frac{1}{10^{2k}} + \cdots\right)\\ &= 0.a_k a_{k-1}\cdots a_1 a_k a_{k-1}\cdots a_1\cdots .\end{aligned}$$

证毕。

**定理 6**　设 $a$ 与 $b$ 是正整数，$0 < a < b$，$(a, b) = 1$，并且

$$b = 2^\alpha 5^\beta b_1,\ (b_1, 10) = 1,\ b_1 \ne 1,$$

此处$\alpha$与$\beta$是不全为零的正整数，则 $\frac{a}{b}$ 可以表示成循环小数，其中不循环的位数码个数是$\mu = \max\{\alpha, \beta\}$。

**证明**　不妨假设$\mu = \beta \ge \alpha$，则

$$10^\mu\,\frac{a}{b} = \frac{2^{\beta-\alpha}a}{b_1} = M + \frac{a_1}{b_1}, \tag{11}$$

其中 $0 < a_1 < b_1$，$0 \le M < 10^\mu$，并且

$$(a_1, b_1) = (2^{\alpha-\beta}a - Mb_1, b_1) = (2^{\alpha-\beta}a, b_1) = (a, b_1) = 1。$$

因此，由定理 5，$\frac{a_1}{b_1}$ 可以表示成纯循环小数：

$$\frac{a_1}{b_1} = 0.c_1\cdots c_k c_1\cdots c_k\cdots = 0.\dot c_1\cdots\dot c_k。 \tag{12}$$

记 $M = m_1 10^{\mu-1} + m_2 10^{\mu-2} + \cdots + m_\mu$（$0 \le m_i \le 9$，$1 \le i \le \mu$），则由式(11)及(12)得到

$$\begin{aligned}\frac{a}{b} &= \frac{1}{10^\mu}M + \frac{1}{10^\mu}\frac{a_1}{b_1}\\ &= 0.m_1\cdots m_\mu + \frac{1}{10^\mu}\cdot 0.\dot c_1\cdots\dot c_k = 0.m_1\cdots m_\mu\dot c_1\cdots\dot c_k。\end{aligned} \tag{13}$$

下面要说明，上式中的$\mu$是最小的不循环位数码的个数。若不然，设又有正整数$\lambda$，使得

$$\frac{a}{b} = 0.m'_1\cdots m'_\lambda\dot c'_1\cdots\dot c'_l\ ,$$

于是

$$10^{\lambda}\frac{a}{b}=\overline{m_1'\cdots m_\lambda'}+0.\dot{c}_1'\cdots\dot{c}_l'\ 。$$

由定理 4 推论，有

$$0.\dot{c}_1'\cdots\dot{c}_l'=\frac{a_1'}{b_1'},$$

其中$(b_1', 10)=1$，因此，

$$10^{\lambda}\frac{a}{b}=\overline{m_1'\cdots m_\lambda'}+\frac{a_1'}{b_1'}=\frac{a'}{b_1'},$$

$$10^{\lambda}ab_1'=ba'。$$

上式右端可以被 $5^{\mu}$ 整除，但是$(a, 10)=1$，$(b_1', 10)=1$，所以 $5^{\mu}\mid 10^{\lambda}$，$\mu\le\lambda$。这就证明了，式(13)中的不循环位数码个数不能再少了。证毕。

**例 1**　写出 1235 的七进制表示和九进制表示。

**解**　(ⅰ)　由

$$\begin{aligned}1235&=176\cdot 7+3,\\176&=25\cdot 7+1,\\25&=3\cdot 7+4,\end{aligned}$$

得到 $1235=(3413)_7$。

(ⅱ)　由

$$\begin{aligned}1235&=137\cdot 9+2,\\137&=15\cdot 9+2,\\15&=1\cdot 9+6,\end{aligned}$$

得到 $1235=(1622)_9$。

**例 2**　将整数$(1212)_3$用十进制表示。

**解**　$(1212)_3=1\cdot 3^3+2\cdot 3^2+1\cdot 3^1+2\cdot 3^0=27+18+3+2=50$。

**例 3**　设 $n$ 是正整数，证明：在$-\frac{1}{2}(3^n-1)$与$\frac{1}{2}(3^n-1)$之间的任意整数 $k$，可以唯一地表示成

$$k=\sum_{i=0}^{n-1}b_i3^i,\ b_i=-1,\ 0\text{ 或 }1,\ 0\le i\le n-1。$$

**解**　由定理 1 容易看出，对任意的整数 $m$，$0\le m\le 3^n-1$，有

$$m=\sum_{i=0}^{n-1}a_i3^i,\ 0\le a_i\le 2,\ 0\le i\le n-1。$$

当

$$-\frac{1}{2}(3^n-1)\le k\le\frac{1}{2}(3^n-1)$$

时，有

$$0\le k+\frac{1}{2}(3^n-1)\le 3^n-1,$$

因此，存在唯一的整数 $a_{n-1}, a_{n-2}, \cdots, a_1, a_0$，使得

$$k+\sum_{i=0}^{n-1}3^i=\sum_{i=0}^{n-1}a_i3^i,\ 0\le a_i\le 2,\ 0\le i\le n-1,$$

$$k=\sum_{i=0}^{n-1}(a_i-1)3^i,\ -1\le a_i-1\le 1,\ 0\le i\le n-1。$$

这个例子表明，用重量分别是 $1, 3, 3^2, \cdots, 3^{n-1}$ 的砝码，可以在天平上称量出不超过$\frac{1}{2}(3^n-1)$的任何整数值的重量。

## 习 题 一

**1.**　证明定理 3。

**2.**　写出 789 的二进制表示和五进制表示。

**3.**　求$\frac{8}{21}$的小数的循环节。

**4.**　证明：七进制表示的整数是偶数的充要条件是它的各位数字之和为偶数。

**5.**　证明：既约正分数$\frac{m}{n}$的 $b$ 进制小数$(0.a_{-1}a_{-2}a_{-3}\cdots)_b$为有限小数的充要条件是 $n$ 的每个素因数都是 $b$ 的素因数。

# 第二节　连分数的基本性质

本节及以下几节都讨论实数的连分数表示。

**定义 1**　设$\alpha_1, \alpha_2, \cdots, \alpha_n$是不为零的实数，当分数

$$\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\alpha_3 + \cfrac{1}{\ddots + \cfrac{1}{\alpha_n}}}}$$

有意义时，称为有限连分数，简记为

$$\alpha_1 + \frac{1}{\alpha_2 +}\ \frac{1}{\alpha_3 +}\ \cdots\ \frac{1}{+\alpha_n}$$

或

$$\langle\, \alpha_1, \alpha_2, \cdots, \alpha_n \,\rangle\ 。$$

**定义 2**　设$\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots$是不为零的无限的实数列，记

$$\frac{p_n}{q_n} = \langle\, \alpha_1, \alpha_2, \cdots, \alpha_n \,\rangle\ 。$$

若$\dfrac{p_n}{q_n}$（$n \geq 1$）都有意义并且

$$\lim_{n\to\infty} \frac{p_n}{q_n} = A \neq \infty\ ,$$

则称$\langle\, \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \,\rangle$是无限连分数，并称连分数$\langle\, \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \,\rangle$等于 $A$，或称它的值是 $A$。也称它是 $A$ 的连分数，或者称它表示 $A$，记为

$$A = \langle\, \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \,\rangle = \alpha_1 + \frac{1}{\alpha_2 +}\ \frac{1}{\alpha_3 +}\ \cdots\ \frac{1}{+\alpha_n +}\ \cdots\ 。$$

称$\dfrac{p_n}{q_n}$（$n \geq 1$）是连分数$\langle\, \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \,\rangle$的第 $n$ 个渐近分数。

**定理 1**　连分数$\langle\, \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \,\rangle$的第 $k$ 个渐近分数为$\dfrac{p_k}{q_k}$，则



$$\begin{aligned} &p_1 = \alpha_1,\ p_2 = \alpha_2\alpha_1 + 1,\ p_k = \alpha_k p_{k-1} + p_{k-2},\quad (k \geq 3) \\ &q_1 = 1,\quad q_2 = \alpha_2,\qquad\ q_k = \alpha_k q_{k-1} + q_{k-2},\quad (k \geq 3) \end{aligned} \tag{1}$$

**证明**　容易计算

$$\frac{p_1}{q_1} = \frac{\alpha_1}{1},\ \ \frac{p_2}{q_2} = \frac{\alpha_2\alpha_1 + 1}{\alpha_2},\ \ \frac{p_3}{q_3} = \frac{\alpha_3(\alpha_2\alpha_1 + 1) + \alpha_1}{\alpha_3\alpha_2 + 1}\ ,$$

因此，当 $k = 1$，2，3 时，式(1)成立。

假设当 $k \leq n$ 时，式(1)成立。则由

$$\frac{p_{n+1}}{q_{n+1}} = \langle \alpha_1, \alpha_2, \cdots, \alpha_{n+1} \rangle = \langle \alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n + \frac{1}{\alpha_{n+1}} \rangle$$

和归纳假设，有

$$\frac{p_{n+1}}{q_{n+1}} = \frac{(\alpha_n + \dfrac{1}{\alpha_{n+1}})p_{n-1} + p_{n-2}}{(\alpha_n + \dfrac{1}{\alpha_{n+1}})q_{n-1} + q_{n-2}} = \frac{(\alpha_{n+1}\alpha_n + 1)p_{n-1} + \alpha_{n+1}p_{n-2}}{(\alpha_{n+1}\alpha_n + 1)q_{n-1} + \alpha_{n+1}q_{n-2}}$$

$$= \frac{\alpha_{n+1}(\alpha_n p_{n-1} + p_{n-2}) + p_{n-1}}{\alpha_{n+1}(\alpha_n q_{n-1} + q_{n-2}) + q_{n-1}} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}\ 。$$

这说明式(1)当 $k = n + 1$ 时也成立。由归纳法知式(1)对任意的 $k \geq 1$ 成立。证毕。

**推论**　在定理 1 中，若$\alpha_i \geq 1$（$i \geq 1$），则 $q_n \geq n - 1$（$n \geq 2$）。

**定理 2**　设$\dfrac{p_k}{q_k}$是连分数$\langle\, \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \,\rangle$的渐近分数，则

（ⅰ）　$p_k q_{k-1} - p_{k-1} q_k = (-1)^k$，（$k \geq 2$）；

（ⅱ）　$p_k q_{k-2} - p_{k-2} q_k = (-1)^{k-1}\alpha_k$，（$k \geq 3$）；

**证明**　（ⅰ）　当 $k = 2$ 时，由式(1)，有

$$p_2 q_1 - p_1 q_2 = (\alpha_1\alpha_2 + 1)\cdot 1 - \alpha_1\alpha_2 = 1,$$

即结论(ⅰ)成立。假设结论(ⅰ)对于 $k = n$ 成立，即

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^n,$$

此时，由式(1)，有

$$\begin{aligned} p_{n+1}q_n - p_n q_{n+1} &= (\alpha_{n+1}p_n + p_{n-1})q_n - p_n(\alpha_{n+1}q_n + q_{n-1}) \\ &= p_{n-1}q_n - p_n q_{n-1} = (-1)^{n+1}, \end{aligned}$$

即结论(ⅰ)当 $k = n + 1$ 时成立。由归纳法证明了结论(ⅰ)。

(ⅱ) 由式(1)及结论(ⅰ)，我们有

$$p_kq_{k-2}-p_{k-2}q_k=(\alpha_kp_{k-1}+p_{k-2})q_{k-2}-p_{k-2}(\alpha_kq_{k-1}+q_{k-2})$$
$$=\alpha_k(p_{k-1}q_{k-2}-p_{k-2}q_{k-1})=\alpha_k(-1)^{k-1}。$$

证毕。

**定义 3** 设 $a_1$ 是整数，$a_2, a_3, \cdots, a_n, \cdots$ 是正整数，则称连分数

$$\langle a_1, a_2, \cdots, a_n, \cdots \rangle$$

是简单连分数。

以后，在本章中，除特别声明外，在谈到连分数时，都是指简单连分数。

**定理 3** 设$\langle a_1, a_2, \cdots, a_n, \cdots \rangle$是简单连分数，$\frac{p_k}{q_k}$（$k\geq 1$）是它的渐近分数，则

(ⅰ) $\frac{p_{2(k-1)}}{q_{2(k-1)}}>\frac{p_{2k}}{q_{2k}}$，$\frac{p_{2k-1}}{q_{2k-1}}>\frac{p_{2k-3}}{q_{2k-3}}$，$\frac{p_{2k}}{q_{2k}}>\frac{p_{2k-1}}{q_{2k-1}}$；

(ⅱ) 对任意的正整数 $k$，$p_k$ 与 $q_k$ 互素。

**证明** (ⅰ) 由定理 2，得到

$$\frac{p_{2k}}{q_{2k}}-\frac{p_{2(k-1)}}{q_{2(k-1)}}=\frac{(-1)^{2k-1}a_{2k}}{q_{2k}q_{2k-2}}<0,$$

$$\frac{p_{2k-1}}{q_{2k-1}}-\frac{p_{2k-3}}{q_{2k-3}}=\frac{(-1)^{2k-2}a_{2k-1}}{q_{2k-1}q_{2k-3}}>0,$$

以及

$$\frac{p_{2k}}{q_{2k}}-\frac{p_{2k-1}}{q_{2k-1}}=\frac{(-1)^{2k}}{q_{2k}q_{2k-1}}>0。$$

结论(ⅰ)得证。

(ⅱ) 由定理 2 的结论(ⅰ)即可得出$(p_k, q_k)=1$。证毕。

**定理 4** 任何简单连分数都表示一个实数。

**证明** 以 $\frac{p_n}{q_n}$ 表示这个连分数的第 $n$ 个渐近分数。由定理 3，

$$\frac{p_1}{q_1}, \frac{p_3}{q_3}, \cdots 与 \frac{p_2}{q_2}, \frac{p_4}{q_4}, \cdots$$



分别是有界的递增数列和有界的递减数列，因此，下面的极限存在：

$$\lim_{n\to\infty}\frac{p_{2n-1}}{q_{2n-1}}=A<\infty,\quad \lim_{n\to\infty}\frac{p_{2n}}{q_{2n}}=B<\infty,\tag{2}$$

利用定理 1 推论，得到

$$0<\frac{p_{2k}}{q_{2k}}-\frac{p_{2k-1}}{q_{2k-1}}=\frac{1}{q_{2k}q_{2k-1}}\leq\frac{1}{(2k-1)(2k-2)}\to 0\quad(k\to\infty),$$

所以，$A=B$，并且 $\lim_{n\to\infty}\frac{p_n}{q_n}=A$。证毕。

**例 1** 设 $a$ 与 $b$ 是正整数，$b>1$，$\langle a_1, a_2, \cdots, a_n \rangle$是 $\frac{a}{b}$ 的有限简单连分数，证明

$$aq_{n-1}-bp_{n-1}=(-1)^n(a, b),$$

其中$(a, b)$是 $a$ 与 $b$ 的最大公约数。

**解** 由渐近分数定义，

$$\frac{a}{b}=\langle a_1, a_2, \cdots, a_n \rangle=\frac{p_n}{q_n}。$$

记 $a=(a, b)A$，$b=(a, b)B$，则$(A, B)=1$。由定理 2 可知$(p_n, q_n)=1$，因此，

$$p_n=A，\ q_n=B，\ a=p_n(a, b)，\ b=q_n(a, b)。\tag{3}$$

再利用定理 2，有

$$p_nq_{n-1}-p_{n-1}q_n=(-1)^n,$$
$$aq_{n-1}-bp_{n-1}=(-1)^n(a, b)。$$

**注**：例 1 给出了求不定方程 $ax+by=c$ 的特解的一个方法。

**例 2** 求不定方程

$$13x+17y=5\tag{4}$$

的解。

**解** 容易验证 $\frac{13}{17}=\frac{1}{1+\frac{4}{13}}=\frac{1}{1+\frac{1}{3+\frac{1}{4}}}=\langle 0, 1, 3, 4 \rangle$，于是

$$p_1=0，\ p_2=1\cdot 0+1=1，\ p_3=3\cdot 1+0=3，$$
$$q_1=1，\ q_2=1，\qquad q_3=3\cdot 1+1=4。$$

由例 1 有 $13\cdot4-17\cdot3=(-1)^4=1$，因此 $13\cdot4\cdot5-17\cdot3\cdot5=5$，即 $x=20$，$y=-15$ 是方程(4)的特解，所以方程(4)的一般解是

$$\begin{cases} x=20+17t \\ y=-15-13t \end{cases},\quad t\in\mathbf{Z}。$$

**例 3**　设 $\dfrac{p_n}{q_n}$ 是$\langle a_1, a_2, \cdots, a_n, \cdots\rangle$的第 $n$ 个渐近分数，则

$$\frac{q_n}{q_{n-1}}=\langle a_n, a_{n-1}, \cdots, a_2\rangle\ (n\geq 2)。\tag{5}$$

**解**　用归纳法证明。当 $n=2$ 时，由式(1)，有

$$\frac{q_2}{q_1}=a_2=\langle a_2\rangle,$$

即式(5)成立。

假设式(5)当 $n=k$（$k\geq 2$）时成立，即

$$\frac{q_k}{q_{k-1}}=\langle a_k, a_{k-1}, \cdots, a_2\rangle,\tag{6}$$

则由式(1)，有

$$\frac{q_{k+1}}{q_k}=\frac{a_{k+1}q_k+q_{k-1}}{q_k}=a_{k+1}+\frac{q_{k-1}}{q_k},$$

由此及式(6)，得到

$$\frac{q_{k+1}}{q_k}=a_{k+1}+\frac{1}{\langle a_k, a_{k-1}, \cdots, a_2\rangle}=\langle a_{k+1}, a_k, \cdots, a_2\rangle,$$

即式(5)当 $n=k+1$ 时也成立。由归纳法证得到所需结论。

**例 4**　求连分数$\langle 0, 1, 2, 1, 2, \cdots\rangle$的值。

**解**　设

$$x=\langle 0,1,2,1,2,\cdots\rangle=\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\ddots}}}},$$



则 $x=\dfrac{1}{1+\dfrac{1}{2+x}}$，解这个方程，并注意 $0<x<1$，得到 $x=\sqrt{3}-1$。

## 习 题 二

**1.** 设连分数$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots\rangle$的第 $k$ 个渐近分数为 $\dfrac{p_k}{q_k}$，证明：

$$p_k=\begin{vmatrix} a_1 & -1 & 0 & \cdots & \cdots & 0 & 0 \\ 1 & a_2 & -1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & a_3 & -1 & 0 & \cdots & 0 \\ & \cdots & & & & \cdots & \\ & \cdots & & & & \cdots & \\ 0 & \cdots & \cdots & 0 & 1 & a_{k-1} & -1 \\ 0 & 0 & \cdots & \cdots & 0 & 1 & a_k \end{vmatrix},\quad q_k=\begin{vmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & a_2 & -1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & a_3 & -1 & 0 & \cdots & 0 \\ & \cdots & & & & \cdots & \\ & \cdots & & & & \cdots & \\ 0 & \cdots & \cdots & 0 & 1 & a_{k-1} & -1 \\ 0 & 0 & \cdots & \cdots & 0 & 1 & a_k \end{vmatrix},$$

**2.** 设连分数$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots\rangle$的第 $k$ 个渐近分数为 $\dfrac{p_k}{q_k}$，证明：

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix},\ k\geq 2。$$

**3.** 求连分数$\langle 1, 2, 3, 4, 5, \cdots\rangle$的前三个渐近分数。

**4.** 求连分数$\langle 2, 3, 2, 3, \cdots\rangle$的值。

**5.** 解不定方程：$7x-9y=4$。

# 第三节　实数的连分数表示

现在，我们来讨论连分数表示实数的问题。

**定理 1**　任一有理数$\alpha$可以表示成有限简单连分数。

**证明**　设$\alpha=\dfrac{a}{b}$，$a$ 与 $b$ 是整数，$b>0$，$(a, b)=1$，由辗转相除法，有

$$a = bq_1 + r_1,\ 0 < r_1 < b,\ \frac{a}{b} = q_1 + \frac{r_1}{b},\ 0 < \frac{r_1}{b} < 1,$$

$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1,\ \frac{b}{r_1} = q_2 + \frac{r_2}{r_1},$$

$$0 < \frac{r_2}{r_1} < 1,\ q_2 \geq 1,$$

……

$$r_{n-2} = r_{n-1}q_n + r_n,\ 0 < r_n < r_{n-1},\ \frac{r_{n-2}}{r_{n-1}} = q_n + \frac{r_n}{r_{n-1}},$$

$$0 < \frac{r_n}{r_{n-1}} < 1,\ q_n \geq 1,$$

$$r_{n-1} = r_nq_{n+1},\ \frac{r_{n-1}}{r_n} = q_{n+1},\ q_{n+1} > 1,$$

因此$\frac{a}{b} = \langle q_1, q_2, \cdots, q_{n+1} \rangle$。证毕。

**定理 2**　任一无理数可以表示成无限简单连分数。

**证明**　对于任意的无理数$\beta$，总有无理数$\beta_1$，使得

$$\beta = [\beta] + \frac{1}{\beta_1},\quad \beta_1 = \frac{1}{\beta - [\beta]} > 1。$$

由此，对于任意的无理数α，我们依次得到：

$$\alpha = a_1 + \frac{1}{\alpha_1},\ a_1 = [\alpha],\ \alpha_1 = \frac{1}{\alpha - a_1} > 1,$$

$$\alpha_1 = a_2 + \frac{1}{\alpha_2},\ a_2 = [\alpha_1],\ \alpha_2 = \frac{1}{\alpha_1 - a_2} > 1, \tag{1}$$

……

$$\alpha_n = a_{n+1} + \frac{1}{\alpha_{n+1}},\ a_{n+1} = [\alpha_n],\ \alpha_{n+1} = \frac{1}{\alpha_n - a_{n+1}} > 1,$$

……

下面证明$\alpha = \langle a_1, a_2, \cdots, a_n, \cdots \rangle$。



由上面的等式及第二节定理 1 可见，对于任意的正整数 $n > 1$，有

$$\alpha = \langle a_1, a_2, \cdots, a_n, \alpha_n \rangle = \frac{\alpha_n p_n + p_{n-1}}{\alpha_n q_n + q_{n-1}},\tag{2}$$

其中$\frac{p_i}{q_i}$（$i \geq 1$）是$\langle a_1, a_2, \cdots, a_n, \cdots \rangle$的渐近分数。因此，由式(2)及第二节定理 2，得到

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha_n p_n + p_{n-1}}{\alpha_n q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1}}{q_n(\alpha_n q_n + q_{n-1})}。\tag{3}$$

再利用式(1)及第二节定理 1 推论，得到

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{(n-1)(n-1+1)} \to 0,\ n \to \infty,$$

即$\alpha = \langle a_1, a_2, \cdots, a_n, \cdots \rangle$。证毕。

**推论**　设$\alpha$是实无理数，那么，对于任意的正整数 $n$，存在$\delta_n$与$\eta_n$，$0 < \delta_n, \eta_n < 1$，使得

$$\alpha = \frac{p_n}{q_n} + \frac{(-1)^{n-1}\delta_n}{q_nq_{n+1}} = \frac{p_n}{q_n} + \frac{(-1)^{n-1}\eta_n}{{q_n}^2}。$$

**证明**　由定理 2 的证明，有$\alpha_n > a_{n+1}$，因此，

$$\alpha_n q_n + q_{n-1} > a_{n+1}q_n + q_{n-1} = q_{n+1} > q_n,$$

$$0 < \frac{1}{\alpha_n q_n + q_{n-1}} < \frac{1}{q_{n+1}} < \frac{1}{q_n},$$

所以，必有$\delta_n$，$\eta_n$，$0 < \delta_n, \eta_n < 1$，使得

$$\frac{1}{\alpha_n q_n + q_{n-1}} = \frac{\delta_n}{q_{n+1}} = \frac{\eta_n}{q_n},$$

由此及(3)式得证。证毕。

**定理 3**　无理数的连分数表示是唯一的。

**证明**　设

$$\alpha = \langle a_1, a_2, \cdots, a_n, \cdots \rangle = \langle b_1, b_2, \cdots, b_n, \cdots \rangle。\tag{4}$$

我们用归纳法证明

$$a_i = b_i,\ i \geq 1。\tag{5}$$

对于正整数 $i$，记

$$\alpha_i = \langle a_i, a_{i+1}, \cdots, a_n, \cdots \rangle,\ \beta_i = \langle b_i, b_{i+1}, \cdots, b_n, \cdots \rangle,$$

则

$$\alpha = a_1 + \frac{1}{\alpha_2} = b_1 + \frac{1}{\beta_2},$$

其中 $a_1$ 与 $b_1$ 是整数，$\alpha_2$ 与 $\beta_2$ 是大于 1 的无理数。因此，$a_1 = b_1$，即式(5)当 $i = 1$ 时成立。

假设式(5)对于 $i < k+1$ 成立，即 $a_1 = b_1$，$a_2 = b_2$，…，$a_k = b_k$，则由式(4)得到

$$\langle a_{k+1}, a_{k+2}, \cdots \rangle = \langle b_{k+1}, b_{k+2}, \cdots \rangle,$$

于是，$a_{k+1} = b_{k+1}$，即式(5)当 $i = k+1$ 时成立。

定理由归纳法得证。证毕。

**定理 4** 设 $a$ 与 $b$ 是整数，$\langle a_1, a_2, \cdots, a_n \rangle$与$\langle b_1, b_2, \cdots, b_m \rangle$是$\frac{a}{b}$的两个简单连分数表示，

(ⅰ) 若 $a_n > 1$，$b_m > 1$，则 $n = m$，$a_i = b_i$（$1 \le i \le n$）；

(ⅱ) 若 $a_n$ 是大于 1 的整数，则有理数 $\frac{a}{b}$ 仅有两种表示成简单连分数的方法，即$\langle a_1, a_2, \cdots, a_n \rangle = \langle a_1, a_2, \cdots, a_n - 1, 1 \rangle$。

**证明** 留做习题。

**定理 5** 设 $\frac{p_n}{q_n}$（$n$ = 1, 2, …）是实数$\alpha$的连分数的渐近分数，则对于任意的正整数 $q \le q_n$及整数 $p$，有

$$\left|\alpha - \frac{p_n}{q_n}\right| \le \left|\alpha - \frac{p}{q}\right| \quad (6)$$

**证明** 若$\alpha = \frac{p_n}{q_n}$，则式(6)是显然的。

若 $\alpha \ne \frac{p_n}{q_n}$，则 $\alpha$ 有第 $n+1$ 个渐近分数 $\frac{p_{n+1}}{q_{n+1}}$，并且 $\frac{p_{n+1}}{q_{n+1}} \ne \frac{p_n}{q_n}$。不妨设 $\frac{p_{n+1}}{q_{n+1}} > \frac{p_n}{q_n}$，于是

$$\frac{p_n}{q_n} < \alpha \le \frac{p_{n+1}}{q_{n+1}}. \quad (7)$$



分别以下情况讨论：

(ⅰ) 若 $\frac{p}{q} \le \frac{p_n}{q_n}$，则由式(7)可知式(6)成立。

(ⅱ) 若 $\frac{p}{q} > \frac{p_{n+1}}{q_{n+1}}$，则由式(7)得到

$$\left|\alpha - \frac{p}{q}\right| \ge \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p}{q}\right| \ge \frac{1}{qq_{n+1}} \ge \frac{1}{q_n q_{n+1}}.$$

由上式及定理 2 推论得到式(6)。

(iii) 若 $\frac{p}{q} = \frac{p_{n+1}}{q_{n+1}}$，则 $pq_{n+1} = qp_{n+1}$，因此，由第二节定理 3 得到 $q_{n+1} \mid q$，$q \ge q_{n+1} > q_n$，这与假设矛盾。因此，这一情况不出现。

(iv) 若 $\frac{p_n}{q_n} < \frac{p}{q} < \frac{p_{n+1}}{q_{n+1}}$，则容易看出

$$\frac{p}{q} - \frac{p_n}{q_n} \ge \frac{1}{qq_n}, \quad \frac{p_{n+1}}{q_{n+1}} - \frac{p}{q} \ge \frac{1}{qq_{n+1}},$$

于是

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \ge \frac{q_n + q_{n+1}}{qq_n q_{n+1}} > \frac{1}{q_n q_{n+1}},$$

这与第二节定理 2 矛盾。因此，这一情况不出现。证毕。

定理 5 说明，在分母不超过 $q_n$ 的分数中，$\frac{p_n}{q_n}$ 是$\alpha$的最佳有理逼近。这是渐近分数的一个非常重要的性质。

**定理 6**(Hurwitz) 设$\alpha$是无理数，那么，在它的连分数的任何两个相邻渐近分数中，至少有一个满足不等式

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}. \quad (8)$$

**证明** 设 $\frac{p_n}{q_n}$ 与 $\frac{p_{n+1}}{q_{n+1}}$ 是$\alpha$的两个相邻的渐近分数，不妨设

$$\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}.$$

于是，由第二节定理 2，

$$\frac{1}{q_n q_{n+1}}=\left|\frac{p_{n+1}}{q_{n+1}}-\frac{p_n}{q_n}\right|=\left|\alpha-\frac{p_n}{q_n}\right|+\left|\alpha-\frac{\beta_{n+1}}{q_{n+1}}\right|。\qquad(9)$$

若 $\frac{p_n}{q_n}$ 与 $\frac{p_{n+1}}{q_{n+1}}$ 都不使式(8)成立，则

$$\left|\alpha-\frac{p_n}{q_n}\right|\geq\frac{1}{2{q_n}^2},\quad\left|\alpha-\frac{p_{n+1}}{q_{n+1}}\right|\geq\frac{1}{2{q_{n+1}}^2},\qquad(10)$$

于是

$$\left|\alpha-\frac{p_n}{q_n}\right|+\left|\alpha-\frac{p_{n+1}}{q_{n+1}}\right|\geq\frac{{q_n}^2+{q_{n+1}}^2}{2{q_n}^2{q_{n+1}}^2},\qquad(11)$$

但是 $q_{n+1}\neq q_n$，所以 ${q_n}^2+{q_{n+1}}^2>2q_nq_{n+1}$，因此，由式(11)得到

$$\left|\alpha-\frac{p_n}{q_n}\right|+\left|\alpha-\frac{p_{n+1}}{q_{n+1}}\right|>\frac{1}{q_n q_{n+1}},$$

这与式(9)矛盾。所以式(10)中至少有一个不等式不成立。证毕。

**推论**　对于任意的无理数$\alpha$，存在无穷多个有理数 $\frac{p}{q}$ 满足

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}。$$

**例 1**　写出 $\sqrt{8}$ 的连分数

**解**　由

$$\sqrt{8}=2+\sqrt{8}-2=2+\frac{1}{\frac{\sqrt{8}+2}{4}},$$

$$\frac{\sqrt{8}+2}{4}=1+\frac{\sqrt{8}-2}{4}=1+\frac{1}{\sqrt{8}+2},$$

$$\sqrt{8}+2=4+\sqrt{8}-2=4+\frac{1}{\frac{\sqrt{8}+2}{4}},$$

…… 



得到 $\sqrt{8}=\langle 2, 1, 4, 1, 4, 1, \cdots\rangle$。

**例 2**　求 $\sqrt{8}$ 的误差不超过 $10^{-4}$ 的有理近似值。

**解**　由定理 2 推论，只需求正整数 $n$，使得 $\frac{1}{q_n q_{n+1}}\leq 10^{-4}$。

利用例 1 及第二节定理 1，有下表

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $a_n$ | 2 | 1 | 4 | 1 | 4 | 1 | 4 | 1 |
| $p_n$ | 2 | 3 | 14 | 17 | 82 | 99 | 478 | 577 |
| $q_n$ | 1 | 1 | 5 | 6 | 29 | 35 | 169 | 204 |

由于 $q_7q_8>10^4$，因此取 $n=7$。即所求的 $\sqrt{8}$ 的有理近似是 $\frac{p_7}{q_7}=\frac{478}{169}$。

## 习 题 三

**1.**　证明定理 4。

**2.**　求 $\sqrt{13}$ 的连分数。

**3.**　求 $2+\sqrt{3}$ 的误差$\leq 10^{-5}$的有理逼近。

**4.**　求 sin18°的误差$\leq 10^{-5}$的有理逼近。

**5.**　已知圆周率$\pi=\langle 3, 7, 15, 1, 292, 1, 1, 1, 21, \cdots\rangle$，求$\pi$的误差$\leq 10^{-6}$的有理逼近。

**6.**　证明：$\frac{1+\sqrt{5}}{2}$ 连分数展开的第 $k$ 个渐近分数为 $\frac{F_{k+1}}{F_k}$。此处$\{F_n\}$是 Fibonacci 数列。

# 第四节　循环连分数

本节要讨论整系数二次方程的实无理根的连分数。

**定义 1**　设$\langle a_1, a_2, \cdots, a_n, \cdots \rangle$是无限简单连分数。如果存在正整数 $s$ 与 $t$，使得

$$a_{s+i} = a_{s+kt+i},\ i = 1, 2, \cdots, t;\ k = 0, 1, 2, \cdots ,$$

则称$\langle a_1, a_2, \cdots, a_n, \cdots \rangle$是循环连分数,并记为

$$\langle a_1, \cdots, a_s, \dot{a}_{s+1}, \cdots, \dot{a}_{s+t} \rangle 。$$

如果 $s = 0$，则称它是纯循环连分数。

**定理 1**　任何循环连分数表示一个不可约整系数二次方程的实根。

**证明**　设$\alpha = \langle a_1, \cdots, a_s, \dot{b}_1, \cdots, \dot{b}_t \rangle = \langle a_1, a_2, \cdots, a_n, \cdots \rangle$是循环连分数。

记$\alpha_n = \langle a_{n+1}, a_{n+2}, \cdots \rangle$，以 $\dfrac{p_n}{q_n}$（$n = 1, 2, \cdots$）表示$\alpha$的渐近分数。

（ⅰ）　若 $s = 0$，则$\alpha = \langle \dot{b}_1, \cdots, \dot{b}_t \rangle = \langle b_1, \cdots, b_t, \alpha \rangle$，因此，由第二节定理 1 得到

$$\alpha = \frac{\alpha p_t + p_{t-1}}{\alpha q_t + q_{t-1}},$$

即$\alpha$满足整系数二次方程

$$q_t x^2 + (q_{t-1} - p_t)x - p_{t-1} = 0。 \tag{1}$$

（ⅱ）　若 $s \neq 0$，则$\alpha = \langle a_1, \cdots, a_s, b_1, \cdots, b_t, b_1, \cdots, b_t, \cdots \rangle$，由第二节定理可知，

$$\alpha = \frac{\alpha_s p_s + p_{s-1}}{\alpha_s q_s + q_{s-1}} = \frac{\alpha_s p_{s+t} + p_{s+t-1}}{\alpha_s q_{s+t} + q_{s+t-1}},$$

于是

$$\alpha_s = \frac{p_{s-1} - \alpha q_{s-1}}{q_s \alpha - p_s} = \frac{p_{s+t-1} - \alpha q_{s+t-1}}{q_{s+t}\alpha - p_{s+t}},$$

由此得到

$$(q_{s+t}\alpha - p_{s+t})(p_{s-1} - \alpha q_{s-1}) = (q_s \alpha - p_s)(p_{s+t-1} - \alpha q_{s+t-1}),$$

即$\alpha$满足整系数二次方程

$$Ax^2 + Bx + C = 0, \tag{2}$$

其中

$$A = q_s q_{s+t-1} - q_{s+t} q_{s-1},$$



$$B = q_{s+t} p_{s-1} + q_{s+t} p_{s-1} - p_s q_{s+t-1} - q_s p_{s+t-1},$$

$$C = p_s p_{s+t-1} - p_{s+t} p_{s-1}。$$

由于$\alpha$是无限连分数，所以是实无理数，因此方程(1)和(2)都是不可约的。证毕。

**定理 2**　设$\alpha = \langle \dot{a}_1, \cdots, \dot{a}_t \rangle$是纯循环连分数，则它所满足的二次方程的另一个根在–1 与 0 之间。

**证明**　从定理 1 的证明中可知，$\alpha$满足方程(1)。记

$$f(x) = q_t x^2 + (q_{t-1} - p_t)x - p_{t-1} = 0,$$

则由 $a_t \geq 1$ 及 $p_i > 0$，$q_i > 0$（$i \geq 1$）可知

$$f(0) = -p_{t-1} < 0,$$

$$f(-1) = q_t - (q_{t-1} - p_t) - p_{t-1} = (q_t - q_{t-1}) + (p_t - p_{t-1})$$

$$= (a_t - 1)(q_{t-1} + p_{t-1}) + q_{t-2} + p_{t-2} > 0 ,$$

因此，方程(1)必有一根在–1 与 0 之间。由于 $a_1, a_2, \cdots, a_n, \cdots$都是正整数，所以$\alpha > 0$，即这个根不是$\alpha$。证毕。

**定理 3**　设$\alpha$是二次不可约整系数方程

$$Ax^2 + Bx + C = 0 \tag{3}$$

的实根，则$\alpha$的简单连分数是循环连分数。

**证明**　因为方程(3)是不可约的，所以$\alpha$是无理数，因此，由第三节定理 2，它可以表示成无限简单连分数，设

$$\alpha = \langle a_1, a_2, \cdots, a_n, \cdots \rangle。$$

记$\alpha_n = \langle a_{n+1}, a_{n+2}, \cdots \rangle$，则

$$\alpha = \langle a_1, a_2, \cdots, a_n, \alpha_n \rangle ,$$

由第二节定理 1，得到

$$\alpha = \frac{\alpha_n p_n + p_{n-1}}{\alpha_n q_n + q_{n-1}},$$

将此式代入式(3)，可知$\alpha_n$满足方程

$$A_n x^2 + B_n x + C_n = 0, \tag{4}$$

其中

$$\begin{cases} A_n = A p_n^2 + B p_n q_n + C q_n^2 \\ B_n = 2A p_n p_{n-1} + B(p_n q_{n-1} + p_{n-1} q_n) + 2C q_n q_{n-1} 。 \\ C_n = A p_{n-1}^2 + B p_{n-1} q_{n-1} + C q_{n-1}^2 = A_{n-1} \end{cases} \tag{5}$$

由第三节定理 2 推论，

$$p_n = \alpha q_n + \frac{\delta_n}{q_n},\quad |\delta_n| < 1\text{。}$$

因此，由于$\alpha$满足方程(3)，有

$$A_n = A\left(\alpha q_n + \frac{\delta_n}{q_n}\right)^2 + B\left(\alpha q_n + \frac{\delta_n}{q_n}\right)q_n + C{q_n}^2$$

$$= {q_n}^2(A\alpha^2 + B\alpha + C) + 2A\alpha\delta_n + A\frac{{\delta_n}^2}{{q_n}^2} + B\delta_n$$

$$= 2A\alpha\delta_n + A\frac{{\delta_n}^2}{{q_n}^2} + B\delta_n\text{，}$$

$$|A_n| \le |A|(2|\alpha| + 1) + |B|\text{。} \tag{6}$$

由式(5)又推出

$$|C_n| \le |A|(2|\alpha| + 1) + |B|\text{。} \tag{7}$$

此外，容易验证

$$B_n^2 - 4A_nC_n = (B^2 - 4AC)(p_nq_{n-1} - p_{n-1}q_n)^2 = B^2 - 4AC,$$

我们看到，存在只与 $A$，$B$，$C$ 及$\alpha$有关的 $M$，使得

$$|B_n| \le M\text{。} \tag{8}$$

由式(6)，式(7)，式(8)可知，对于 $n = 1, 2, 3, \cdots$，数组$\{A_n, B_n, C_n\}$只有有限多个不同的取法，因此，至少有三组是相同的，即存在正整数 $n_1$，$n_2$，$n_3$，$n_1 < n_2 < n_3$，使得

$$A_{n_1} = A_{n_2} = A_{n_3} = A_0\text{，}$$

$$B_{n_1} = B_{n_2} = B_{n_3} = B_0\text{，}$$

$$C_{n_1} = C_{n_2} = C_{n_3} = C_0\text{。}$$

这样，$\alpha_{n_1}, \alpha_{n_2}, \alpha_{n_3}$ 满足同一个方程

$$A_0x^2 + B_0x + C_0 = 0\text{。} \tag{9}$$

但是方程(9)至多有两个不同的解，所以 $\alpha_{n_1}, \alpha_{n_2}, \alpha_{n_3}$ 中必有两个相同，设是 $\alpha_{n_1} = \alpha_{n_2}$，则

$$\langle a_{n_1+1}, a_{n_1+2}, \cdots\rangle = \langle a_{n_2+1}, a_{n_2+2}, \cdots\rangle\text{。} \tag{10}$$

由于 $\alpha_{n_1}$ 和 $\alpha_{n_2}$ 都是无限简单连分数，所以，由式(10)及第三节定理 3，



得到

$$a_{n_1+i} = a_{n_2+i}\text{，}\quad i = 1, 2, \cdots\text{。}$$

因此

$$\langle a_{n_1+1}, a_{n_1+2}, \cdots\rangle = \langle \dot{a}_{n_1+1}, a_{n_1+2}, \cdots, \dot{a}_{n_2}\rangle\text{。}$$

这说明$\alpha = \langle a_1, a_2, \cdots a_{n_1}, a_{n_1+1}, \cdots\rangle$是循环连分数。证毕。

**例 1**　设 $a$，$b$，$c$ 是正整数，$b = ac$，求连分数

$$x = b + \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{a + \cdots}}} = \langle \dot{b}, \dot{a}\rangle$$

的值。

**解**　由

$$x = \langle b, a, x\rangle = b + \cfrac{1}{a + \cfrac{1}{x}} = b + \frac{x}{ax + 1}\text{，}$$

得到

$$ax^2 - abx - b = 0\text{，}$$

即

$$x^2 - bx - c = 0\text{，}$$

于是

$$x = \frac{b + \sqrt{b^2 + 4c}}{2}\text{。}$$

**例 2**　求$\alpha = \langle \dot{1}, 2, \dot{3}\rangle$之值。

**解**　由定理 1 的证明可知，$\alpha$满足方程

$$q_3x^2 + (q_2 - p_3)x - p_2 = 0\text{，} \tag{11}$$

其中，由第二节定理 1，有

$$a_1 = 1\text{，}\ a_2 = 2\text{，}\ a_3 = 3\text{，}$$

$$p_1 = 1\text{，}\ p_2 = 3\text{，}\ p_3 = 10\text{，}$$

$$q_1 = 1\text{，}\ q_2 = 2\text{，}\ q_3 = 7\text{。}$$

将上面的数值代入方程(11)，并求解，得到

$$x = \frac{8 \pm \sqrt{64 + 4\cdot 3\cdot 7}}{14} = \frac{8 \pm \sqrt{148}}{14} = \frac{4 \pm \sqrt{37}}{7}\text{，}$$

显然$\alpha$是正数，所以$\alpha=\dfrac{4+\sqrt{37}}{7}$。

## 习 题 四

**1.** 将方程 $3x^2+2x-2=0$ 的正根写成连分数。

**2.** 求$\alpha=\langle 1,\dot{2},\dot{3}\rangle$之值。

**3.** 设 $a$ 是正整数，求$\sqrt{a^2+1}$ 的连分数。

**4.** 设无理数$\sqrt{d}=\langle a_1, a_2, \cdots, a_n, \cdots\rangle$的第 $k$ 个渐近分数为$\dfrac{p_k}{q_k}$，证明：$\sqrt{d}=\langle a_1,\dot{a}_2,\cdots,a_n,2\dot{a}_1\rangle$的充要条件是

$$p_n=a_1q_n+q_{n-1},\quad dq_n=a_1p_n+p_{n-1}。$$

**5.** 设无理数$\sqrt{d}=\langle a_1, a_2, \cdots, a_n, \cdots\rangle$的第 $k$ 个渐近分数为$\dfrac{p_k}{q_k}$，且正整数 $n$ 使得

$$p_n=a_1q_n+q_{n-1},\quad dq_n=a_1p_n+p_{n-1},$$

证明：

(ⅰ) 当 $n$ 为偶数时，$p_n$，$q_n$是不定方程 $x^2-dy^2=1$ 的解；

(ⅱ) 当 $n$ 为奇数时，$p_{2n}$，$q_{2n}$是不定方程 $x^2-dy^2=1$ 的解。



# 第四章　不定方程

本章所讨论的不定方程，是指整系数代数方程，并且限定它的解是整数。本章只讨论几类比较简单的不定方程。

## 第一节　一次不定方程

设 $a_1, a_2, \cdots, a_n$ 是非零整数，$b$ 是整数，称关于未知数 $x_1, x_2, \cdots, x_n$ 的方程

$$a_1x_1+a_2x_2+\cdots+a_nx_n=b \tag{1}$$

是 $n$ 元一次不定方程。

若存在整数 $x_1^0, x_2^0, \cdots, x_n^0$ 满足方程(1)，则称$(x_1^0, x_2^0, \cdots, x_n^0)$是方程(1)的解，或说 $x_1=x_1^0$，$x_2=x_2^0$，$\cdots$，$x_n=x_n^0$ 是方程(1)的解。

**定理 1**　方程(1)有解的充要条件是

$$(a_1, a_2, \cdots, a_n)\mid b。 \tag{2}$$

**证明**　记 $d=(a_1, a_2, \cdots, a_n)$。若方程(1)有解，设为$(x_1, x_2, \cdots, x_n)$。则由 $d\mid a_i$（$1\le i\le n$）及整除的性质容易知道式(2)成立。必要性得证。

另一方面，由第一章第三节定理 2，存在整数 $y_1, y_2, \cdots, y_n$ 使得

$$a_1y_1+a_2y_2+\cdots+a_ny_n=(a_1, a_2, \cdots, a_n)=d。$$

因此，若式(2)成立，则$\left(\dfrac{b}{d}y_1,\dfrac{b}{d}y_2,\cdots,\dfrac{b}{d}y_n\right)$就是方程(1)的解，充分性得证。证毕。

**定理 2**　设 $a$，$b$，$c$ 是整数，方程

$$ax+by=c \tag{3}$$

若有解$(x_0, y_0)$，则它的一切解具有

$$\begin{cases}x=x_0+b_1t\\ y=y_0-a_1t\end{cases},\quad t\in\mathbf{Z} \tag{4}$$

的形式，其中 $a_1=\dfrac{a}{(a,b)}$，$b_1=\dfrac{b}{(a,b)}$。

**证明**　容易验证，由式(4)确定的 $x$ 与 $y$ 满足方程(3)。下面证明，方程(3)的解都可写成式(4)中的形式。

设$(x, y)$是方程(3)的解，则由

$$ax_0+by_0=ax+by=c$$

得到

$$a(x-x_0)=-b(y-y_0),$$

$$\frac{a}{(a,b)}(x-x_0)=-\frac{b}{(a,b)}(y-y_0)。$$

由此，以及

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

和第一章第三节定理 4，得到 $\dfrac{b}{(a,b)}\mid x-x_0$，因此存在整数 $t$，使得

$$x-x_0=\frac{b}{(a,b)}t,\quad y-y_0=-\frac{a}{(a,b)}t。$$

证毕。

定理 1 和定理 2 说明了解方程(3)的步骤：

(ⅰ)　判断方程是否有解，即$(a, b)\mid c$ 是否成立；

(ⅱ)　利用辗转相除法求出 $x_0$，$y_0$，使得 $ax_0+by_0=(a, b)$；

(ⅲ)　写出方程(3)的解

$$\begin{cases}x=x_0c_1+b_1t\\ y=y_0c_1-a_1t\end{cases},t\in\mathbf{Z},$$

其中$(a,b)c_1=c$，$a_1=\dfrac{a}{(a,b)}$，$b_1=\dfrac{b}{(a,b)}$。

**定理 3**　设 $a_1, a_2, \cdots, a_n, b$ 是整数，再设 $(a_1, a_2, \cdots, a_{n-1})=d_{n-1}$，$(a_1, a_2, \cdots, a_n)=d_n$，则$(x_1', x_2', \cdots, x_n')$是方程(1)的解的充分必要条件是存在整数 $t$，使得$(x_1', x_2', \cdots, x_n', t)$是方程组

$$\begin{cases}a_1x_1+a_2x_2+\cdots+a_{n-1}x_{n-1}=d_{n-1}t\\ d_{n-1}t+a_nx_n=b\end{cases}\tag{5}$$



的解。

**证明**　若有整数 $t$，使得$(x_1', x_2', \cdots, x_n', t)$是方程组(5)的解，则显然$(x_1', x_2', \cdots, x_n')$满足方程(1)。

设$(x_1', x_2', \cdots, x_n')$是方程(1)的解，则

$$a_1x_1'+a_2x_2'+\cdots+a_{n-1}x_{n-1}'+a_nx_n'=b。\tag{6}$$

令

$$a_1x_1'+a_2x_2'+\cdots+a_{n-1}x_{n-1}'=b',$$

则由定理 1

$$d_{n-1}=(a_1, a_2, \cdots, a_{n-1})\mid b'。$$

因此，存在 $t\in\mathbf{Z}$，使得

$$a_1x_1'+a_2x_2'+\cdots+a_{n-1}x_{n-1}'=d_{n-1}t,\tag{7}$$

再由式(6)，得到

$$d_{n-1}t+a_nx_n'=b,$$

即$(x_1', x_2', \cdots, x_n', t)$满足方程组(5)。证毕。

定理 3 说明了求解 $n$ 元一次不定方程的方法：先解方程组(5)中的第二个方程，再解方程组(5)中的第一个方程，于是，解 $n$ 元一次不定方程就化为解 $n-1$ 元一次不定方程。重复这个过程，最终归结为求解二元一次不定方程。由第一章第三节定理 5，记

$(a_1, a_2)=d_2$，$(d_2, a_3)=d_3$，$\cdots$，$(d_{n-2}, a_{n-1})=d_{n-1}$，$(d_{n-1}, a_n)=d_n$，

逐个地解方程

$$\begin{aligned}&d_{n-1}t_{n-1}+a_nx_n=b,\\ &d_{n-2}t_{n-2}+a_{n-1}x_{n-1}=d_{n-1}t_{n-1},\\ &\quad\cdots\cdots\\ &d_2t_2+a_3x_3=d_3t_3,\\ &a_1x_1+a_2x_2=d_2t_2,\end{aligned}$$

并且消去中间变量 $t_2, t_3, \cdots, t_{n-1}$，就可以得到方程(1)的解。

**例 1**　求不定方程 $3x+6y=15$ 的解。

**解**　$(3, 6)=3\mid 15$，所以方程有解。

由辗转相除法（或直接观察），可知 $x=-1$，$y=1$ 是

$$3x+6y=3$$

的解，所以 $x_0=-5$，$y_0=5$ 是原方程的一个解。由定理 2，所求方程的解是

$$\begin{cases} x = -5 + 2t \\ y = \ \ 5 - \ t \end{cases}, \quad t \in \mathbf{Z}。$$

**例 2**　求不定方程 $3x + 6y + 12z = 15$ 的解。

**解**　原方程等价于

$$x + 2y + 4z = 5。 \tag{8}$$

由定理 3，依次解方程

$$t + 4z = 5,$$
$$x + 2y = t,$$

分别得到

$$\begin{cases} t = 1 + 4u \\ z = 1 - \ u \end{cases}, \quad u \in \mathbf{Z}, \tag{9}$$

$$\begin{cases} x = -t + 2v \\ y = \ \ t - \ v \end{cases}, \quad v \in \mathbf{Z}。 \tag{10}$$

将式(9)与式(10)中的 $t$ 消去，得到

$$\begin{cases} x = -1 - 4u + 2v \\ y = \ \ 1 + 4u - \ v \\ z = \ \ 1 - \ u \end{cases}, \quad u, v \in \mathbf{Z}。$$

**注**：本例在解方程时，首先将原方程化为等价方程(8)，这使问题简化。对例 1 也可以如此处理。

**例 3**　设 $a$ 与 $b$ 是正整数，$(a, b) = 1$，则任何大于 $ab - a - b$ 的整数 $n$ 都可以表示成 $n = ax + by$ 的形式，其中 $x$ 与 $y$ 是非负整数，但是 $n = ab - a - b$ 不能表示成这种形式。

**解**　(ⅰ)　由定理 2，方程

$$ax + by = n \tag{11}$$

的解具有

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases}, \quad t \in \mathbf{Z} \tag{12}$$

的形式，其中 $x_0$ 与 $y_0$ 满足方程(11)。

由假设条件 $n > ab - a - b$ 及式(11)与式(12)，有

$$ax = n - by = n - b(y_0 - at) > ab - a - b - b(y_0 - at)。 \tag{13}$$

取整数 $t$，使得



$$0 \le y = y_0 - at \le a - 1,$$

则由式(13)得到

$$ax > ab - a - b - b(a - 1) = -a,$$
$$x > -1, \ x \ge 0,$$

即 $n = ax + by$，$x \ge 0$，$y \ge 0$。

(ⅱ)　设有 $x \ge 0$，$y \ge 0$，使得

$$ax + by = ab - a - b, \tag{14}$$

则

$$a(x + 1) + b(y + 1) = ab。 \tag{15}$$

所以 $a \mid b(y + 1)$。但是 $(a, b) = 1$，于是必有

$$a \mid y + 1, \ y + 1 \ge a。$$

同理可以证明 $x + 1 \ge b$，从而

$$a(x + 1) + b(y + 1) \ge 2ab,$$

这与式(15)矛盾，所以式(14)是不可能的。

**例 4**　设 $a$，$b$，$c$ 是整数，$(a, b) = 1$，则在直线 $ax + by = c$ 上，任何一个长度大于 $\sqrt{a^2 + b^2}$ 的线段上至少有一个点的坐标都是整数。

**解**　由定理 2，直线 $ax + by = c$ 上的坐标都是整数的点 $(x_t, y_t)$ 的坐标是

$$\begin{cases} x_t = x_0 + bt \\ y_t = y_0 - at \end{cases}, \quad t \in \mathbf{Z},$$

其中 $(x_0, y_0)$ 是直线 $ax + by = c$ 上的坐标都是整数的点，由定理 1，这样的点是存在的。

对于任意的 $t \in \mathbf{Z}$，记 $P_t$ 是以 $(x_t, y_t)$ 为坐标的点，则 $P_{t+1}$ 与 $P_t$ 之间的距离

$$\overline{P_{t+1}P_t} = \sqrt{(x_{t+1} - x_t)^2 + (y_{t+1} - y_t)^2} = \sqrt{a^2 + b^2}。$$

这说明，两个“相邻的”坐标是整数的点的距离是 $\sqrt{a^2 + b^2}$，从而得出所求之结论。

**例 5**　将 $\dfrac{19}{30}$ 写成三个分数之和，它们的分母分别是 2，3 和 5。

**解**　设

$$\frac{19}{30}=\frac{x}{2}+\frac{y}{3}+\frac{z}{5},$$

则

$$15x+10y+6z=19。$$

依次解方程

$$5t+6z=19,$$
$$15x+10y=5t,$$

得到

$$\begin{cases}t=-1+6u\\ z=4-5u\end{cases},\quad u\in\mathbf{Z},\tag{16}$$

$$\begin{cases}x=t+2v\\ y=-t-3v\end{cases},\quad v\in\mathbf{Z}。\tag{17}$$

从式(16)与式(17)中消去 $t$，得到

$$\begin{cases}x=-1+6u+2v\\ y=1-6u-3v\\ z=4-5u\end{cases},\quad u,v\in\mathbf{Z}。$$

取 $u=0$，$v=0$，得到 $x=-1$，$y=1$，$z=4$，因此

$$\frac{19}{30}=-\frac{1}{2}+\frac{1}{3}+\frac{4}{5}。$$

**例 6**　甲物每斤 5 元，乙物每斤 3 元，丙物每三斤 1 元，现在用 100 元买这三样东西共 100 斤，问各买几斤?

**解**　设买甲物 $x$ 斤，乙物 $y$ 斤，丙物 $z$ 斤，则

$$5x+3y+\frac{1}{3}z=100,$$
$$x+y+z=100。$$

消去 $z$，得到

$$7x+4y=100。\tag{18}$$

显然 $x=0$，$y=25$ 是方程(18)的解，因此，方程(18)的一般解是

$$\begin{cases}x=4t\\ y=25-7t\end{cases},\quad t\in\mathbf{Z}$$

因为 $x\geq 0$，$y\geq 0$，所以



$$0\leq t\leq 3。$$

即 $t$ 可以取值 $t_1=0$，$t_2=1$，$t_3=2$，$t_4=3$。相应的 $x$，$y$，$z$ 的值是 $(x,y,z)=(0,25,75)$，$(4,18,78)$，$(8,11,81)$，$(12,4,84)$。

**例 7**　求不定方程 $x+2y+3z=7$ 的所有正整数解。

**解**　依次解方程

$$t+3z=7,$$
$$x+2y=t,$$

得到

$$\begin{cases}t=1+3u\\ z=2-u\end{cases},\quad u\in\mathbf{Z},$$

$$\begin{cases}x=t+2v\\ y=-v\end{cases},\quad v\in\mathbf{Z}。$$

从上式中消去 $t$，得到

$$\begin{cases}x=1+3u+2v\\ y=-v\\ z=2-u\end{cases},\quad u,v\in\mathbf{Z}。\tag{19}$$

要使 $x\geq 1$，$y\geq 1$，$z\geq 1$，则应有

$$3u+2v\geq 0,\ -v\geq 1,\ 1-u\geq 0。\tag{20}$$

所以

$$3u\geq -2v\geq 2,\ u\leq 1\Longrightarrow\frac{2}{3}\leq u\leq 1,$$

即 $u=1$。由此及式(20)，有

$$3+2v\geq 0,\ -v\geq 1\Longrightarrow -\frac{2}{3}\leq v\leq -1,$$

所以 $v=-1$。将 $u=1$，$v=-1$ 代入式(19)，得到原方程的唯一一组正整数 $x=2$，$y=1$，$z=1$。

## 习 题 一

**1.**　将 $\frac{17}{105}$ 写成三个既约分数之和，它们的分母分别是 3，5 和 7。

**2.** 求方程 $x_1+2x_2+3x_3=41$ 的所有正整数解。

**3.** 求解不定方程组：

$$\begin{cases} x_1+2x_2+3x_3=7 \\ 2x_1-5x_2+20x_3=11 \end{cases}。$$

**4.** 甲班有学生 7 人，乙班有学生 11 人，现有 100 支铅笔分给这两个班，要使甲班的学生分到相同数量的铅笔，乙班学生也分到相同数量的铅笔，问应怎样分法？

**5.** 证明：二元一次不定方程 $ax+by=n$，$a>0$，$b>0$，$(a,b)=1$ 的非负整数解的个数为 $\left[\frac{n}{ab}\right]$ 或 $\left[\frac{n}{ab}\right]+1$。

**6.** 设 $a$ 与 $b$ 是正整数，$(a,b)=1$，证明：$1,2,\cdots,ab-a-b$ 中恰有 $\frac{(a-1)(b-1)}{2}$ 个整数可以表示成 $ax+by$（$x\geq 0$，$y\geq 0$）的形式。

## 第二节　方程 $x^2+y^2=z^2$

本节讨论二次方程

$$x^2+y^2=z^2 \quad 。 \tag{1}$$

容易看出，$(x,y,z)=(0,0,0)$，$(0,\pm a,\pm a)$以及$(\pm a,0,\pm a)$都是方程(1)的解。若$(x,y,z)$是方程(1)的解，则对于任何整数 $k$，$(kx,ky,kz)$也是方程(1)的解。此外，若$(x,y)=k$，则 $k\mid z$，$(x,y,z)=k$。因此，我们只需研究方程(1)的满足下述条件的解：

$$x>0，\ y>0，\ z>0，\ (x,y)=1。 \tag{2}$$

**定理 1**　若$(x,y,z)$是方程(1)的满足条件(2)的解，则下面的结论成立：

(ⅰ)　$x$ 与 $y$ 有不同的奇偶性；

(ⅱ)　$x$ 与 $y$ 中有且仅有一个数被 3 整除；

(ⅲ)　$x$，$y$，$z$ 中有且仅有一个数被 5 整除。

**证明**　(ⅰ)　若 $2\mid x$，$2\mid y$，则 $2\mid z$，这与$(x,y,z)=1$ 矛盾。所以 $x$ 与 $y$ 中至少有一个奇数。如果 $x$ 与 $y$ 都是奇数，则 $z$ 是偶数，因为

$$x^2\equiv 1，\ y^2\equiv 1，\ x^2+y^2\equiv 2 \pmod 8，$$



$$z^2\equiv 0 \text{ 或 } 4 \pmod 8，$$

所以 $x$，$y$，$z$ 不可能是方程(1)的解。因此，$x$ 与 $y$ 有不同的奇偶性。

(ⅱ)　显然 $x$ 与 $y$ 不能都被 3 整除。若 $x$ 与 $y$ 都不能被 3 整除，则

$$x\equiv\pm 1，\ y\equiv\pm 1 \pmod 3，$$

$$x^2\equiv 1，\ y^2\equiv 1，\ x^2+y^2\equiv 2 \pmod 3。 \tag{3}$$

但是，对任意的 $z$，总有 $z^2\equiv 0$ 或 1 (mod 3)。这与式(1)和式(3)矛盾。因此，结论(ⅱ)成立。

(ⅲ)　显然 $x$，$y$，$z$ 中不能有两个同时被 5 整除。若它们都不能被 5 整除，则

$$x，\ y，\ z\equiv\pm 1，\pm 2 \pmod 5，$$

$$x^2，\ y^2，\ z^2\equiv 1，\ 4 \pmod 5， \tag{4}$$

$$x^2+y^2\equiv 0，\ 2 \text{ 或 } 3 \pmod 5。 \tag{5}$$

式(1)，式(4)与式(5)是矛盾的，因此，结论(ⅲ)成立。证毕。

**引理**　不定方程 $xy=z^2$ 的满足条件

$$xy=z^2，\ x>0，\ y>0，\ z>0，\ (x,y)=1 \tag{6}$$

的一切正整数解，可以写成下面的形式

$$x=a^2，\ y=b^2，\ z=ab，\ (a,b)=1，\ a>0，\ b>0。 \tag{7}$$

**证明**　这是第一章第六节定理 1 推论 3 的特殊情形。证毕。

**定理 2**　方程(1)的满足式(2)和 $2\mid x$ 的一切正整数解具有下面的形式：

$$x=2ab，\ y=a^2-b^2，\ z=a^2+b^2， \tag{8}$$

其中 $a>b>0$，$(a,b)=1$，$a$ 与 $b$ 有不同的奇偶性。

**证明**　(ⅰ)　若 $x$，$y$，$z$ 由式(8)确定，容易验证它们满足方程(1)，并且 $2\mid x$。

设 $d$ 是 $(x,y)$ 的任一个素因数，则由式(1)得到 $d^2\mid z^2$，因此 $d\mid z$，于是，利用最大公约数的性质，有

$$d\mid (y,z)=(a^2-b^2,a^2+b^2)$$

$$\Longrightarrow d\mid a^2-b^2，\ d\mid a^2+b^2\Longrightarrow d\mid 2(a^2,b^2)=2。$$

所以 $d=1$ 或 2。由于 $2\nmid y$，所以 $d=1$，这说明式(2)满足。

(ⅱ)　若 $x$，$y$，$z$ 是方程(1)的满足式(2)以及 $2\mid x$ 的解，则 $2\nmid y$，$2\nmid z$，并且

$$\left(\frac{x}{2}\right)^2=\left(\frac{y+z}{2}\right)\left(\frac{y-z}{2}\right)。\tag{9}$$

记 $d=\left(\frac{y+z}{2},\frac{y-z}{2}\right)$，则有 $d\mid\frac{y+z}{2}$，$d\mid\frac{y-z}{2}$，所以 $d\mid y$，$d\mid z$，于是 $d\mid(y,z)=1$，$d=1$。因此，利用引理及式(9)得到

$$\frac{x}{2}=ab,\frac{y+z}{2}=a^2,\frac{y-z}{2}=b^2,\quad a>0,\ b>0,(a,b)=1。$$

从而

$$x=2ab,\ y=a^2-b^2,\ z=a^2+b^2。$$

由 $y>0$，可知 $a>b$；由于 $x$ 与 $y$ 有不同的奇偶性，所以 $2\nmid y$，因此，$a$ 与 $b$ 有不同的奇偶性。证毕。

**推论** 单位圆周上座标都是有理数的点（称为有理点），可以写成

$$\left(\pm\frac{2ab}{a^2+b^2},\pm\frac{a^2-b^2}{a^2+b^2}\right)\text{ 或 }\left(\pm\frac{a^2-b^2}{a^2+b^2},\pm\frac{2ab}{a^2+b^2}\right)$$

的形式，其中 $a$ 与 $b$ 是不全为零的整数。

**定理 3** 不定方程

$$x^4+y^4=z^2\tag{10}$$

没有满足 $xyz\neq0$ 的整数解。

**证明** 用反证法。不妨只考虑方程(10)的正整数解。若它有满足 $xyz\neq0$ 的正整数解，设$(x_0,y_0,z_0)$是方程(10)的有最小的 $z$ 的一组解。令 $d=(x_0,y_0)$，则由式(10)得到 $d^4\mid z_0^2$，$d^2\mid z_0$，从而 $\left(\frac{x_0}{d},\frac{y_0}{d},\frac{z_0}{d^2}\right)$ 也是方程(10)的解。因此，由 $z_0$ 的最小性，可知

$$d=(x_0,y_0)=1，(x_0^2,y_0^2)=d^2=1。$$

显然 $x_0^2$ 与 $y_0^2$ 有不同的奇偶性。不妨设 $2\mid x_0$，$2\nmid y_0$。

由定理 2，存在正整数 $a$，$b$，使得

$$(a,b)=1，\ a>b>0，\tag{11}$$

其中 $a$ 与 $b$ 有不同的奇偶性，并且

$$x_0^2=2ab，\ y_0^2=a^2-b^2，\ z_0=a^2+b^2。\tag{12}$$

下面按照 $a$ 与 $b$ 的奇偶性，考察两种情况。

（ⅰ） $2\mid$a，$2\nmid$b。此时，

$$a^2\equiv0\ (\mathrm{mod}\ 4)，\ b^2\equiv1\ (\mathrm{mod}\ 4)，$$



因此，由式(12)，

$$y_0^2=a^2-b^2\equiv-1\ (\mathrm{mod}\ 4)，$$

这与 $2\nmid y_0$，$y_0^2\equiv1\ (\mathrm{mod}\ 4)$矛盾。所以这个情况不能发生。

（ⅱ） $2\nmid a$，$2\mid b$。此时，由式(11)及式(12)，有

$$x_0^2=2ab，\ (a,2b)=1，\ a>b>0。\tag{13}$$

利用引理可知，存在正整数 $u$，$v_1$，使得

$$x_0=uv_1，\ a=u^2，\ 2b=v_1^2，\ (u,v_1)=1，\ u>0，\ v_1>0。$$

由 $2b=v_1^2$ 推出

$$2\mid v_1^2，\ 2\mid v_1，\ v_1=2v，$$

因此，存在整数 $u$，$v$，使得

$$a=u^2，\ b=2v^2，\ (u,v)=1，\ u>0，\ v>0。\tag{14}$$

代入式(12)，得到

$$y_0^2=u^4-4v^4，\ y_0^2+4v^4=u^4，\tag{15}$$

其中 $(u,v)=1$，从而 $(y_0,v)=1$。利用定理 2，可知存在正整数 $s$，$t$，$(s,t)=1$，$s$ 与 $t$ 有不同的奇偶性，使得

$$y_0=s^2-t^2，\ 2v^2=2st，\ u^2=s^2+t^2，$$

$$y_0=s^2-t^2，\ v^2=st，\ u^2=s^2+t^2，\tag{16}$$

由$(s,t)=1$，式(16)中的第二个等式，以及引理，可知存在正整数 $m$，$n$，$(m,n)=1$，使得

$$v=mn，\ s=m^2，\ t=n^2。$$

由此及式(16)中第三个等式，得到

$$m^4+n^4=u^2，\tag{17}$$

即$(m,n,u)$也满足方程(10)。

另一方面，由式(12)及式(14)，有

$$z_0=a^2+b^2=u^4+4v^4>u，$$

这样，$(m,n,u)$的存在与 $z_0$ 的最小性矛盾。这就证明了定理。证毕。

**推论** 方程 $x^4+y^4=z^4$ 没有满足 $xyz\neq0$ 的整数解。

定理 3 中使用的证明方法称为无穷递降法。常用于判定方程的可解性。

**例** 证明方程

$$x^2+y^2=x^2y^2\tag{18}$$

没有满足 $xy\neq0$ 的整数解。

**解** 用反证法。设方程(18)有满足 $xy\neq0$ 的整数解$(x,y)$。不妨设 $x$

$>0$，$y>0$。

显然 $2\mid x$，$2\mid y$。因此，由式(18)，有

$$(\frac{x}{2})^2+(\frac{y}{2})^2=4(\frac{x}{2})^2(\frac{y}{2})^2,\quad \frac{x}{2},\frac{y}{2}\in\mathbf{N}, \tag{19}$$

在上式中，$\frac{x}{2}$与$\frac{y}{2}$必都是偶数。否则，它们就都是奇数。此时，由于任何奇数的平方被 8 除的余数是 1，我们有

$$(\frac{x}{2})^2+(\frac{y}{2})^2\equiv 2(\mathrm{mod}\,8),\quad 4(\frac{x}{2})^2(\frac{y}{2})^2\equiv 4(\mathrm{mod}\,8),$$

这与式(19)矛盾。因此，$2\mid\frac{x}{2}$，$2\mid\frac{y}{2}$。由式(19)，又有

$$(\frac{x}{2^2})^2+(\frac{y}{2^2})^2=4^2(\frac{x}{2^2})^2(\frac{y}{2^2})^2,\quad \frac{x}{2^2},\frac{y}{2^2}\in\mathbf{N},$$

重复上面的讨论与分析，我们见到，对于任意的正整数 $k$，有

$$(\frac{x}{2^k})^2+(\frac{y}{2^k})^2=4^k(\frac{x}{2^k})^2(\frac{y}{2^k})^2,\quad \frac{x}{2^k},\frac{y}{2^k}\in\mathbf{N}。$$

但是，由于 $x$，$y$ 是固定的正整数，当 $k$ 充分大时，$\frac{x}{2^k}$与$\frac{y}{2^k}$不可能是正整数。这个矛盾说明方程(18)不能有满足 $xy\neq 0$ 的整数解。

## 习 题 二

**1.** 证明定理 2 推论。

**2.** 设 $x$，$y$，$z$ 是勾股数，$x$ 是素数，证明：$2z-1$，$2(x+y+1)$都是平方数。

**3.** 求整数 $x$，$y$，$z$，$x>y>z$，使 $x-y$，$x-z$，$y-z$ 都是平方数。

**4.** 解不定方程：$x^2+3y^2=z^2$，$x>0$，$y>0$，$z>0$，$(x,y)=1$。

**5.** 证明下面的不定方程没有满足 $xyz\neq 0$ 的整数解。

(ⅰ) $x^2+y^2+z^2=x^2y^2$;

(ⅱ) $x^2+y^2+z^2=2xyz$。

**6.** 求方程 $x^2+y^2=z^4$ 的满足$(x,y)=1$，$2\mid x$ 的正整数解。



# 第三节　几类特殊的不定方程

不定方程是一个内容丰富的课题，许多不定方程的解法有其特殊性。本节要介绍几类这样的方程，以及几个有普遍性的方法。

### 一、余数分析法

将不定方程的解按某个正整数 $m$ 的余数分类，或者，考察方程中的项对某个正整数的余数，再进行分析。

**例 1**　证明：若 $n=9k+t$, $t=3$, 4, 5 或 6, $k\in\mathbf{Z}$, 则方程 $x^3+y^3=n$ 没有整数解。

**解**　对任意的整数 $x$，$y$，记

$$x=3q_1+r_1,\ y=3q_2+r_2,\ 0\le r_1,r_2\le 2,\ q_1,q_2\in\mathbf{Z},$$

则

$$x^3\equiv {r_1}^3\equiv R_1\ (\mathrm{mod}\ 9),\ y^3\equiv {r_2}^3\equiv R_2\ (\mathrm{mod}\ 9),\ x^3+y^3\equiv R\ (\mathrm{mod}\ 9),$$

其中

$$R_1=0,\ 1\text{ 或 }8,\ R_2=0,\ 1\text{ 或 }8,\ \mathrm{R}=0,\ 1,\ 2,\ 7\text{ 或 }8。$$

由此得到所要证明的结论。

**例 2**　证明方程

$$3^x+1=5^y+7^z \tag{1}$$

除 $x=y=z=0$ 外没有其他整数解。

**解**　设$(x,y,z)$是方程(1)的解。容易证明：$x\ge 0$，$y\ge 0$，$z\ge 0$。

若 $x>0$，则由式(1)，有

$$5^y+7^z\equiv 1\ (\mathrm{mod}\ 3),$$

$$2^y+1\equiv 1,\ 2^y\equiv 0\ (\mathrm{mod}\ 3),$$

因此，$3\mid 2^y$，这是不可能的。所以必是 $x=0$, 于是式(1)成为

$$5^y+7^z=2。$$

由于 $y\ge 0$，$z\ge 0$，所以由上式推出 $y=z=0$。

**例 3**　证明：若实数 $x$ 与 $y$ 满足方程

$$x^2-3y^2=2, \tag{2}$$

则 $x$ 与 $y$ 不能都是有理数。

**解**　用反证法。设有理数

$$x=\frac{n}{m},\quad y=\frac{l}{m}\quad (m,n,l\in\mathbf{Z},\ (m,n,l)=1,\ m\neq 0)$$

满足方程(2)，则

$$n^2-3l^2=2m^2, \tag{3}$$

考察两种可能的情形。

(ⅰ) $3\nmid n$。此时，

$$n\equiv\pm1,\ n^2\equiv 1\ (\mathrm{mod}\ 3),$$

因此，由式(3)得到

$$2m^2\equiv 1\ (\mathrm{mod}\ 3),$$

这是不可能的，因为对于 $m\equiv 0$，1 或 2 (mod 3)，$2m^2\equiv 0$ 或 2 (mod 3)。

(ⅱ) $3\mid n$。此时，由式(3)得到 $2m^2\equiv 0$ (mod 3)，因此 $3\mid m$，再由式(3)得到 $3\mid l$，所以$(m,n,l)>1$，这与关于 $m,n,l$ 的假设矛盾。

**例 4** 求不定方程组

$$\begin{cases}x^3+y^3+z^3=3\\ x+y+z=3\end{cases} \tag{4}$$

的所有整数解。

**解** 设

$x\equiv r_1$，$y\equiv r_2$，$z\equiv r_3$ (mod 3)，$r_i=0$，1，$-1$（$i=1$，2，3），

则

$$x^3\equiv R_1,\ y^3\equiv R_2,\ z^3\equiv R_3\ (\mathrm{mod}\ 9),$$

其中 $R_i=0$，1 或 $-1$（$i=1$，2，3)。

由方程组(4)中的第一个方程，得到

$$R_1+R_2+R_3\equiv 3\ (\mathrm{mod}\ 9),$$

因此，必是

$$R_1=R_2=R_3=1,\ r_1=r_2=r_3=1,$$

即

$$x=3x_1+1,\ y=3y_1+1,\ z=3z_1+1。 \tag{5}$$

将式(5)中的 $x$，$y$，$z$ 代入方程组(4)中的第二个方程，得到

$$x_1+y_1+z_1=0。 \tag{6}$$

显然，$(x_1,y_1,z_1)=(0,0,0)$满足式(6)。

现在，假定$(x_1,y_1,z_1)\neq(0,0,0)$。

考虑两种可能的情形：



(ⅰ) 若 $x_1$，$y_1$ 与 $z_1$ 中有一个为 0，例如，$x_1=0$。由式(6)得到

$$y_1=-z_1,\ x=1,\ y=3y_1+1,\ z=-3y_1+1,$$

代入方程组(4)中的第一个方程，有

$$1+(3y_1+1)^3+(-3y_1+1)^3=3,$$

$$1+2(9y_1^2+1)=3,\ y_1=0,$$

$$x=1,\ y=1,\ z=1。$$

(ⅱ) 若 $x_1y_1z_1\neq 0$。由式(6)可知，$x_1$，$y_1$ 与 $z_1$ 三个数中有两个数符号相同。不妨设 $x_1$ 与 $y_1$ 同符号。由式(6)得到

$$z_1=-(x_1+y_1),$$

代入方程组(4)中的第一个方程，得到

$$(3x_1+1)^3+(3y_1+1)^3+(1-3(x_1+y_1))^3=3,$$

稍做整理，即是

$$3x_1y_1(x_1+y_1)-2(x_1^2+y_1^2+x_1y_1)=0,$$

$$(2x_1^2+x_1y_1)(y_1-1)+(2y_1^2+x_1y_1)(x_1-1)=0。 \tag{7}$$

由于 $x_1$ 与 $y_1$ 符号相同，所以式(7)当且仅当 $x_1=y_1=1$ 时成立，此时

$$z_1=-(x_1+y_1)=-2,$$

并且

$$x=4,\ y=4,\ z=-5。$$

综合以上讨论，注意到方程(4)中对于三个变量的对称性，得到方程组(4)的解是

$$(x,y,z)=(1,1,1),\ (4,4,-5),\ (4,-5,4),\ (-5,4,4)。$$

**例 5** 求方程$(x-1)!=x^y-1$ 的满足 $x>1$ 的正整数解。

**解** 若$(x,y)$是方程满足 $x>1$ 的正整数解，则

$$(x-1)!\equiv -1\ (\mathrm{mod}\ x)。$$

因此，由第二章第二节习题 4，$x$ 是素数。

取 $x=2$，3，5，得到方程的解

$$(x,y)=(2,1),\ (3,1),\ (5,2)。$$

设 $x>5$ 是素数，于是

$$(x-1)!\equiv 1\cdot 2\cdots\frac{x-1}{2}\cdots(x-1),$$

$$(x-1)^2\mid(x-1)!。$$

因此，若 $x$ 是方程的 $x>5$ 的解，则对于正整数 $y$，有

$$x^y-1\equiv 0\ (\mathrm{mod}\ (x-1)^2)。$$

由上式及

$$\begin{aligned} x^y-1&=((x-1)+1)^y-1\\ &=(x-1)^y+\mathrm{C}_y^1(x-1)^{y-1}+\cdots+\mathrm{C}_y^{y-2}(x-1)^2+\mathrm{C}_y^{y-1}(x-1)\\ &=(x-1)^2Q+y(x-1), \end{aligned}$$

其中 $Q$ 是某个整数，推出

$$(x-1)^2 \mid y(x-1),\ x-1 \mid y,$$

于是

$$x^y-1\geq x^{x-1}-1>(x-1)!\ (x>5)。$$

这说明当 $x>5$ 时，方程无正整数解。所以，所求的全部解是

$$(x,y)=(2,1),\ (3,1),\ (5,2)。$$

## 二、因数分析法

任何非零整数的因数个数是有限的，因此，可以对不定方程的解在有限范围内用枚举法确定。

**例 6**　求方程 $x^2y+2x^2-3y-7=0$ 的整数解。

**解**　原方程即

$$(x^2-3)(y+2)=1。$$

因此

$$\begin{cases} x^2-3=1\\ y+2=1 \end{cases}\text{或}\begin{cases} x^2-3=-1\\ y+2=-1 \end{cases},$$

解这两个联立方程组，得到所求的解是

$$\begin{cases} x_1=2\\ y_1=-1 \end{cases}\text{或}\begin{cases} x_2=-2\\ y_2=-1 \end{cases}。$$

**例 7**　求方程 $x^3+y^3=1072$ 的正整数解。

**解**　容易看出，对于任何正整数 $a$，$(x, y)=(1, a)$，$(a, 1)$及$(a, a)$都不是方程的解。所以，只需考虑 $x\geq 2$，$y\geq 2$，$x\neq y$ 的情况。于是

$$x^2-xy+y^2>xy>x+y, \tag{8}$$

$$(x+y)^2>x^2-xy+y^2。 \tag{9}$$

原方程即

$$(x+y)(x^2-xy+y^2)=2^4\cdot 67。$$

由此及式(8)与式(9)得到



$$\begin{cases} x+y=2^4\\ x^2-xy+y^2=67 \end{cases},$$

解这两个联立方程组，得到所求的解是

$$\begin{cases} x_1=7\\ y_1=9 \end{cases}\text{或}\begin{cases} x_2=9\\ y_2=7 \end{cases}。$$

## 三、不等分析法

利用量的整数性或不等关系，确定出方程解的范围。

**例 8**　求方程

$$3x^2+7xy-2x-5y-35=0$$

的正整数解。

**解**　对于正整数 $x$，$y$，由原方程得到

$$y=\frac{-3x^2+2x+35}{7x-5}。 \tag{10}$$

因此，若 $x\geq 1$，$y\geq 1$，则应有

$$\begin{cases} x\geq 1\\ -3x^2+2x+35\geq 7x-5 \end{cases},$$

解这个不等式组，得到 $1\leq x\leq 2$。

分别取 $x=1$ 和 $x=2$，由式(10)得到 $y=17$ 和 $y=3$。所以所求的解是$(x, y)=(1, 17)$，$(2, 3)$。

**例 9**　求方程 $5(xy+yz+zx)=4xyz$ 的正整数解。

**解**　原方程即

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{4}{5}。 \tag{11}$$

设 $x\leq y\leq z$，则由

$$\frac{1}{x}<\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\leq\frac{3}{x}$$

及式(11)，得到

$$\frac{1}{x}<\frac{4}{5}\leq\frac{3}{x},\ 1<x<4,\ x=2\text{ 或 }3。$$

(ⅰ)　若 $x=2$，则式(11)成为

$$\frac{1}{y}+\frac{1}{z}=\frac{3}{10}。$$

由此及

$$\frac{1}{y}<\frac{1}{y}+\frac{1}{z}\le\frac{2}{y}$$

得到

$$\frac{1}{y}<\frac{3}{10}\le\frac{2}{y}，3<y<7，y=4，5\text{ 或 }6。$$

将 $x=2$ 以及 $y=4$，5 或 6 分别代入式(11)，得到所求的解

$$(x,y,z)=(2,4,20)，(2,5,10)。$$

(ii) 若 $x=3$，同样的方法可以推出，方程(11)无解。

综合以上，注意到(11)式对于 $x$，$y$，$z$ 的对称性，得到方程的 12 个正整数解

$$\begin{aligned}(x,y,z)=&(2,4,20)，(2,5,10)，(2,20,4)，(2,10,5)，\\&(4,2,20)，(5,2,10)，(20,2,4)，(10,2,5)，\\&(20,4,2)，(10,5,2)，(4,20,2)，(5,10,2)。\end{aligned}$$

## 习 题 三

**1.** 求方程 $x^2+xy-6=0$ 的整数解。

**2.** 求方程组 $\begin{cases}x+y+z=0\\x^3+y^3+z^3=-18\end{cases}$ 的整数解。

**3.** 求方程 $2^x-3^y=1$ 的正整数解。

**4.** 求方程 $\frac{1}{x}+\frac{1}{y}=\frac{1}{z}$ 的正整数解。

**5.** 设 $p$ 是素数，求方程 $\frac{2}{p}=\frac{1}{x}+\frac{1}{y}$ 的整数解。

**6.** 设 $2n+1$ 个有理数 $a_1, a_2, \cdots, a_{2n+1}$ 满足条件 $P$：其中任意 $2n$ 个数可以分成两组，每组 $n$ 个数，两组数的和相等，证明：

$$a_1=a_1=\cdots=a_{2n+1}。$$



# 第五章　同余方程

本章主要介绍同余方程的基础知识，并介绍几类特殊的同余方程的解法。

## 第一节　同余方程的基本概念

本节要介绍同余方程的基本概念及一次同余方程。

在本章中，总假定 $m$ 是正整数。

**定义 1**　设 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是整系数多项式，称

$$f(x)\equiv 0\pmod m \tag{1}$$

是关于未知数 $x$ 的模 $m$ 的同余方程，简称为模 $m$ 的同余方程。

若 $a_n\not\equiv 0\pmod m$，则称为 $n$ 次同余方程。

**定义 2**　设 $x_0$ 是整数，当 $x=x_0$ 时式(1)成立，则称 $x_0$ 是同余方程(1)的解。凡对于模 $m$ 同余的解，被视为同一个解。同余方程(1)的解数是指它的关于模 $m$ 互不同余的所有解的个数，也即在模 $m$ 的一个完全剩余系中的解的个数。

由定义 2，同余方程(1)的解数不超过 $m$。

**定理 1**　下面的结论成立：

(i) 设 $b(x)$是整系数多项式，则同余方程(1)与

$$f(x)+b(x)\equiv b(x)\pmod m$$

等价；

(ii) 设 $b$ 是整数，$(b,m)=1$，则同余方程(1)与

$$bf(x)\equiv 0\pmod m$$

等价；

(iii) 设 $m$ 是素数，$f(x)=g(x)h(x)$，$g(x)$与 $h(x)$都是整系数多项式，又设 $x_0$ 是同余方程(1)的解，则 $x_0$ 必是同余方程

$$g(x)\equiv 0\pmod m\ \text{ 或 }\ h(x)\equiv 0\pmod m$$

的解。

**证明**　留做习题。

下面，我们来研究一次同余方程的解。

**定理 2**　设 $a$，$b$ 是整数，$a \not\equiv 0 \pmod m$。则同余方程

$$ax \equiv b \pmod m \tag{2}$$

有解的充要条件是$(a, m) \mid b$。若有解，则恰有 $d = (a, m)$个解。

**证明**　显然，同余方程(2)等价于不定方程

$$ax + my = b, \tag{3}$$

因此，第一个结论可由第四章第一节定理 1 得出。

若同余方程(2)有解 $x_0$，则存在 $y_0$，使得 $x_0$ 与 $y_0$ 是方程(3)的解，此时，方程(3)的全部解是

$$\begin{cases} x = x_0 + \dfrac{m}{(a,m)}t \\ y = y_0 - \dfrac{a}{(a,m)}t \end{cases}, \quad t \in \mathbf{Z}。 \tag{4}$$

由式(4)所确定的 $x$ 都满足方程(2)。记 $d = (a, m)$，以及

$$t = dq + r，\ q \in \mathbf{Z}，\ r = 0, 1, 2, \cdots, d-1，$$

则

$$x = x_0 + qm + \frac{m}{d}r \equiv x_0 + \frac{m}{d}r \pmod m，\ 0 \le r \le d-1。$$

容易验证，当 $r = 0, 1, 2, \cdots, d-1$ 时，相应的解

$$x_0，\ x_0 + \frac{m}{d}，\ x_0 + \frac{2m}{d}, \cdots，\ x_0 + \frac{(d-1)m}{d}$$

对于模 $m$ 是两两不同余的，所以同余方程(2)恰有 $d$ 个解。证毕。

在定理的证明中，同时给出了解方程(2)的方法，但是，对于具体的方程(2)，常常可采用不同的方法去解。

**例 1**　设$(a, m) = 1$，又设存在整数 $y$，使得 $a \mid b + ym$，则

$$x \equiv \frac{b + ym}{a} \pmod m$$

是方程(2)的解。

**解**　直接验算，有

$$ax \equiv b + ym \equiv b \pmod m。$$



**注**：例 1 说明，求方程(2)的解可以转化为求方程

$$my \equiv -b \pmod a \tag{5}$$

的解，这有两个便利之处：第一，将一个对于大模 $m$ 的同余方程转化为一个对于小模 $a$ 的同余方程，因此有可能通过对模 $a$ 的完全剩余系进行逐个验证，以求出方程(5)和(2)的解；第二，设 $m \equiv r \pmod a$，$r < a$，则又可继续转化成一个对于更小的模 $r$ 的同余方程。

**例 2**　解同余方程

$$325x \equiv 20 \pmod{161} \tag{6}$$

**解**　同余方程(6)即是

$$3x \equiv 20 \pmod{161}。$$

解同余方程

$$161y \equiv -20 \pmod 3，$$
$$2y \equiv 1 \pmod 3，$$

得到 $y \equiv 2 \pmod 3$，因此方程(6)的解是

$$x \equiv \frac{20 + 2 \cdot 161}{3} = 114 \pmod{161}。$$

**例 3**　设 $a > 0$，且$(a, m) = 1$，$a_1$ 是 $m$ 对模 $a$ 的最小非负剩余，则同余方程

$$a_1 x \equiv -b\left[\frac{m}{a}\right] \pmod m \tag{7}$$

等价于同余方程(2)。

**解**　设 $x$ 是(2)的解，则由 $m = a\left[\dfrac{m}{a}\right] + a_1$ 得到

$$a_1 x = \left(m - a\left[\frac{m}{a}\right]\right)x \equiv -ax\left[\frac{m}{a}\right] \equiv -b\left[\frac{m}{a}\right] \pmod m,$$

即 $x$ 是同余方程(7)的解。但是由假设条件可知同余方程(2)与(7)都有且只有一个解。所以这两个同余方程等价。

**注**：用本例的方法，可以将同余方程(2)转化成未知数的系数更小一些的同余方程，从而易于求解。

**例 4**　解同余方程 $6x \equiv 7 \pmod{23}$。

**解**　由例 3，依次得到

$$6x \equiv 7 \pmod{23} \iff 5x \equiv -7 \cdot 3 \equiv 2 \pmod{23}$$
$$\iff 3x \equiv -2 \cdot 4 \equiv -8 \pmod{23}$$

$$\Leftrightarrow 2x \equiv -8(-7) \equiv 10 \pmod{23}$$
$$\Leftrightarrow x \equiv 5 \pmod{23}。$$

**例 5**　设$(a, m) = 1$，并且有整数$\delta > 0$使得

$$a^{\delta} \equiv 1 \pmod{m}，$$

则同余方程(2)的解是

$$x \equiv ba^{\delta-1} \pmod{m}。$$

**解**　直接验证即可。

**注**：由例 5 及 Euler 定理可知，若$(a, m) = 1$，则

$$x \equiv ba^{\varphi(m)-1} \pmod{m}$$

总是同余方程(2)的解。

**例 6**　解同余方程

$$81x^3 + 24x^2 + 5x + 23 \equiv 0 \pmod{7}。$$

**解**　原同余方程即是

$$-3x^3 + 3x^2 - 2x + 2 \equiv 0 \pmod{7}。$$

用$x = 0$，$\pm 1$，$\pm 2$，$\pm 3$逐个代入验证，得到它的解是

$$x_1 \equiv 1，\ x_2 \equiv 2，\ x_3 \equiv -2 \pmod{7}。$$

**注**：本例使用的是最基本的解同余方程的方法，一般说来，它的计算量太大，不实用。

**例 7**　解同余方程组

$$\begin{cases} 3x + 5y \equiv 1 \pmod{7} \\ 2x - 3y \equiv 2 \pmod{7} \end{cases}。 \tag{8}$$

**解**　将(8)的前一式乘以 2 后一式乘以 3 再相减得到

$$19y \equiv -4 \pmod{7}，$$
$$5y \equiv -4 \pmod{7}，$$
$$y \equiv 2 \pmod{7}。$$

再代入(8)的前一式得到

$$3x + 10 \equiv 1 \pmod{7}，$$
$$x \equiv 4 \pmod{7}。$$

即同余方程组(8)的解是$x \equiv 4$，$y \equiv 2 \pmod{7}$。

**例 8**　设$a_1$，$a_2$是整数，$m_1$，$m_2$是正整数，证明：同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \tag{9}$$



有解的充要条件是

$$a_1 \equiv a_2 \pmod{(m_1, m_2)}。 \tag{10}$$

若有解，则对模$[m_1, m_2]$是唯一的，即若$x_1$与$x_2$都是同余方程组(9)的解，则

$$x_1 \equiv x_2 \pmod{[m_1, m_2]}。 \tag{11}$$

**解**　必要性是显然的。下面证明充分性。

若式(10)成立，由定理 2，同余方程

$$m_2 y \equiv a_1 - a_2 \pmod{m_1}$$

有解$y \equiv y_0 \pmod{m_1}$，记$x_0 = a_2 + m_2 y_0$，则

$$x_0 \equiv a_2 \pmod{m_2}$$

并且

$$x_0 = a_2 + m_2 y_0 \equiv a_2 + a_1 - a_2 \equiv a_1 \pmod{m_1}，$$

因此$x_0$是同余方程组的解。

若$x_1$与$x_2$都是方程组(9)的解，则

$$x_1 \equiv x_2 \pmod{m_1}，\ x_1 \equiv x_2 \pmod{m_2}，$$

由同余的基本性质，得到式(11)。

## 习 题 一

**1.**　证明定理 1。

**2.**　解同余方程：

(ⅰ)　$31x \equiv 5 \pmod{17}$；

(ⅱ)　$3215x \equiv 160 \pmod{235}$。

**3.**　解同余方程组：

$$\begin{cases} 3x + 5y \equiv 38 \pmod{47} \\ x - y \equiv 10 \pmod{47} \end{cases}。$$

**4.**　设$p$是素数，$0 < a < p$，证明：

$$x \equiv b(-1)^{a-1} \frac{(p-1)(p-2)\cdots(p-a+1)}{a!} \pmod{p}。$$

是同余方程$ax \equiv b \pmod{p}$的解。

**5.**　证明：同余方程$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}$有解的充要条件是

$$(a_1, a_2, \cdots, a_n, m) = d \mid b。$$

若有解，则恰有 $d \cdot m^{n-1}$ 个解，mod $m$。

**6.** 解同余方程：$2x + 7y \equiv 5 \pmod{12}$。

## 第二节　孙子定理

本节要讨论同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \cdots\cdots \\ x \equiv a_k \pmod{m_k} \end{cases} 。 \tag{1}$$

在第一节的例题中，我们已讨论了 $k = 2$ 的情形。下面考察一般情形。

**定理 1**(孙子定理)　设 $m_1, m_2, \cdots, m_k$ 是正整数，

$$(m_i, m_j) = 1，\ 1 \le i, j \le k，\ i \ne j。 \tag{2}$$

记

$$m = m_1 m_2 \cdots m_k \ ，\ M_i = \frac{m}{m_i} ，\ 1 \le i \le k,$$

则存在整数 $M_i'$（$1 \le i \le k$），使得

$$M_i M_i' \equiv 1 \pmod{m_i}, \tag{3}$$

$$M_i M_i' \equiv 0 \pmod{m_i}，\ 1 \le j \le k，\ i \ne j, \tag{4}$$

并且

$$x_0 \equiv \sum_{i=1}^{k} a_i M_i M_i' \pmod{m} \tag{5}$$

是同余方程组(1)对模 $m$ 的唯一解，即若有 $x$ 使方程组(1)成立，则

$$x \equiv x_0 \pmod{m}。 \tag{6}$$

**证明**　由式(2)，有$(M_i, m_i) = 1$，因此利用辗转相除法可以求出 $M_i'$ 与 $y_i$ ，使得

$$M_i M_i' + y_i m_i = 1,$$

即 $M_i'$满足式(3)和式(4)。由式(3)与式(4)，对于 $1 \le i \le k$，有



$$x_0 \equiv a_i M_i M_i' \equiv a_i \pmod{m_i}，\ 1 \le i \le k。$$

若 $x$ 也使式(1)成立，则

$$x \equiv x_0 \pmod{m_i}，\ 1 \le i \le k,$$

因此

$$x \equiv x_0 \pmod{[m_1, m_2, \cdots, m_k]}。$$

但是，由式(2)可知$[m_1, m_2, \cdots, m_k] = m$，这就证明了式(6)。证毕。

**定理 2**　在定理 1 的条件下，若式(1)中的 $a_1, a_2, \cdots, a_k$ 分别通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余系，则式(5)中的 $x_0$ 通过模 $m_1 m_2 \cdots m_k$ 的完全剩余系。

**证明**　这是第二章第二节习题 6 的特例。证毕。

**定理 3**　同余方程组(1)有解的充要条件是

$$a_i \equiv a_j \pmod{(m_i, m_j)}，\ 1 \le i, j \le n。 \tag{7}$$

**证明**　必要性是显然的。下面证明充分性。

当 $n = 2$ 时，由第一节例 8 可知充分性成立。

假设充分性当 $n = k$ 时成立。

假设式(7)当 $n = k + 1$ 时成立。我们来考虑同余方程组

$$x \equiv a_i \pmod{m_i}，\ 1 \le i \le k + 1。$$

由第一节例 8，存在 $b_k$，使得 $x \equiv b_k \pmod{[m_k，\ m_{k+1}]}$满足同余方程组

$$x \equiv a_k \pmod{m_k}，\ x \equiv a_{k+1} \pmod{m_{k+1}}。$$

在同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \cdots\cdots \\ x \equiv a_{k-1} \pmod{m_{k-1}} \\ x \equiv b \pmod{[m_k, m_{k+1}]} \end{cases}$$

中，由式(7)有

$$a_i \equiv a_j \pmod{(m_i, m_j)}，\ 1 \le i, j \le k - 1,$$

因此，若能证明

$$a_i \equiv b_k \pmod{(m_i, [m_k, m_{k+1}])}，\ 1 \le i \le k - 1。 \tag{8}$$

则由归纳假设就可以证明充分性。

由 $b_k$ 的定义，有

$$a_k \equiv b_k \pmod{m_k}，\ a_{k+1} \equiv b_k \pmod{m_{k+1}} \tag{9}$$

而且，由于假设式(7)当 $n=k+1$ 时成立，所以，对于 $1\le i\le k-1$ 有

$$a_i\equiv a_k \pmod{(m_i, m_k)},\quad a_i\equiv a_{k+1} \pmod{(m_i, m_{k+1})},$$

由此及式(9)得到，对于 $1\le i\le k-1$，有

$$a_i\equiv b_k \pmod{(m_i, m_k)},\quad a_i\equiv b_k \pmod{(m_i, m_{k+1})}。$$

因此

$$a_i\equiv b_k \pmod{[(m_i, m_k), (m_i, m_{k+1})]}。$$

由上式及第一章第六节例 2，就得到式(8)。证毕。

**定理 4**　设 $m=m_1m_2\cdots m_k$，其中 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，$f(x)$是整系数多项式，以 $T$ 与 $T_i$（$1\le i\le k$）分别表示同余方程

$$f(x)\equiv 0 \pmod m \tag{10}$$

与

$$f(x)\equiv 0 \pmod{m_i} \tag{11}$$

的解的个数，则 $T=T_1T_2\cdots T_k$。

**证明**　由第二章第一节定理 5 可知，同余方程(10)等价于同余方程组

$$f(x)\equiv 0 \pmod{m_i},\quad 1\le i\le k。 \tag{12}$$

对于每 $i$（$1\le i\le k$），设同余方程(11)的全部解是

$$x\equiv x_1^{(i)}, x_2^{(i)}, \cdots, x_{T_i}^{(i)} \pmod{m_i}, \tag{13}$$

则同余方程组(12)等价于下面的 $T_1T_2\cdots T_k$ 个方程组：

$$\begin{cases} x\equiv x_{j_1}^{(1)} \pmod{m_1} \\ x\equiv x_{j_2}^{(2)} \pmod{m_2} \\ \quad\cdots\cdots \\ x\equiv x_{j_k}^{(k)} \pmod{m_k} \end{cases}, \tag{14}$$

其中 $x_{j_i}^{(i)}$ 通过式(13)中的数值，即通过同余方程(11)的全部解。

由孙子定理，对于选定的每一组 $\{x_{j_1}^{(1)}, x_{j_2}^{(2)}, \cdots, x_{j_k}^{(k)}\}$，同余方程组(14)对模 $m$ 有唯一解，而且，由定理 2，当每个 $x_{j_i}^{(i)}$ 通过(13)式中的值时，所得到的 $T_1T_2\cdots T_k$ 个同余方程组(14)的解对于模 $m$ 都是两两不同余的。证毕。



由定理 4 及算术基本定理，解一般模的同余方程可以转化为解模为素数幂的同余方程。

**例 1**　求整数 $n$，它被 3，5，7 除的余数分别是 1，2，3。

**解**　$n$ 是同余方程组

$$n\equiv 1 \pmod 3,\quad n\equiv 2 \pmod 5,\quad n\equiv 3 \pmod 7$$

的解。在孙子定理中，取

$$m_1=3,\ m_2=5,\ m_3=7,\ m=3\cdot5\cdot7=105,$$
$$M_1=35,\ M_2=21,\ M_3=15,$$
$$M_1'=-1,\ M_2'=1,\ M_3'=1,$$

则

$$n\equiv 1\cdot35\cdot(-1)+2\cdot21\cdot1+3\cdot15\cdot1\equiv 52 \pmod{105},$$

因此所求的整数 $n=52+105t$，$t\in\mathbf{Z}$。

**例 2**　解同余方程

$$5x^2+6x+49\equiv 0 \pmod{60}。 \tag{15}$$

**解**　因为 $60=3\cdot4\cdot5$，所以，同余方程(15)等价于同余方程组

$$5x^2+6x+49\equiv 0 \pmod 3 \tag{16}$$
$$5x^2+6x+49\equiv 0 \pmod 4 \tag{17}$$
$$5x^2+6x+49\equiv 0 \pmod 5。 \tag{18}$$

分别解同余方程(16)，(17)，(18)得到解

$$x_1^{(1)}\equiv 1,\ x_2^{(1)}\equiv -1 \pmod 3,$$
$$x_1^{(2)}\equiv 1,\ x_2^{(2)}\equiv -1 \pmod 4,$$
$$x_1^{(3)}\equiv 1 \pmod 5,$$

这样，同余方程(15)的解 $x$ 可由下面的方程组决定：

$$x\equiv a_1 \pmod 3,\quad x\equiv a_2 \pmod 4,\quad x\equiv a_3 \pmod 5,$$

其中 $a_1=1$ 或 $-1$，$a_2=1$ 或 $-1$，$a_3=1$。利用孙子定理，取

$$m_1=3,\ m_2=4,\ m_3=5,\ m=60,$$
$$M_1=20,\ M_2=15,\ M_3=12,$$
$$M_1'=2,\ M_2'=-1,\ M_3'=3,$$

则

$$x\equiv 40a_1-15a_2+36a_3 \pmod{60}。$$

将 $a_1$，$a_2$，$a_3$ 所有可能的取值代入上式，得到方程(15)的全部解是

$$x_1\equiv 40\cdot1-15\cdot1+36\cdot1\equiv 1 \pmod{60},$$
$$x_2\equiv 40\cdot(-1)-15\cdot1+36\cdot1\equiv -19 \pmod{60},$$

$$x_3 \equiv 40\cdot 1 - 15\cdot(-1) + 36\cdot 1 \equiv 31 \pmod{60},$$
$$x_4 \equiv 40\cdot(-1) - 15\cdot(-1) + 36\cdot 1 \equiv 11 \pmod{60}。$$

## 习 题 二

**1.** 解同余方程组：$\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod 6 \\ x \equiv b_3 \pmod 7 \\ x \equiv b_4 \pmod{11} \end{cases}$。

**2.** 解同余方程组：$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 5 \pmod 8 \\ x \equiv 13 \pmod{25} \end{cases}$。

**3.** 有一队士兵，若三人一组，则余 1 人；若五人一组，则缺 2 人；若十一人一组，则余 3 人。已知这队士兵不超过 170 人，问这队士兵有几人？

**4.** 求一个最小的自然数 $n$，使得它的 $\frac{1}{2}$ 是一个平方数，它的 $\frac{1}{3}$ 是一个立方数，它的 $\frac{1}{5}$ 是一个 5 次方数。

**5.** 证明：对于任意给定的 $n$ 个不同的素数 $p_1, p_2, \cdots, p_n$，必存在连续 $n$ 个整数，使得它们中的第 $k$ 个数能被 $p_k$ 整除。

**6.** 解同余方程：$3x^2 + 11x - 20 \equiv 0 \pmod{105}$。

# 第三节　模 $p^\alpha$ 的同余方程

在第二节中，我们已经看到，求解模 $m$ 的同余方程可以转化为对模 $p^\alpha$ 的同余方程的求解。本节要对模 $p^\alpha$ 的同余方程做进一步讨论。

容易看出，若 $x_0$ 是同余方程

$$f(x) \equiv 0 \pmod{p^\alpha} \tag{1}$$

的解，则它必是方程



$$f(x) \equiv 0 \pmod{p^{\alpha-1}} \tag{2}$$

的解，因此，必有与 $x_0$ 相应的方程(2)的某个解 $x_1$，使

$$x_0 \equiv x_1 \pmod{p^{\alpha-1}},\quad x_0 = x_1 + p^{\alpha-1}t_0,$$

此处，$t_0$ 是某个适当的整数。

这提示我们：可以从方程(2)的解中去求方程(1)的解。于是，现在的问题是，对于方程(2)的每个解 $x_1$，是否必有方程(1)的解 $x_0$ 与之对应？若有，如何去确定它？

**定理**　设 $p$ 是素数，$\alpha \geq 2$ 是整数，$f(x) = a_n x^n + \cdots + a_1 x + a_0$ 是整系数多项式，又设 $x_1$ 是同余方程(2)的一个解。以 $f'(x)$ 表示 $f(x)$ 的导函数。

（ⅰ）　若 $f'(x_1) \not\equiv 0 \pmod p$，则存在整数 $t$，使得

$$x = x_1 + p^{\alpha-1}t \tag{3}$$

是同余方程(1)的解。

（ⅱ）　若 $f'(x_1) \equiv 0 \pmod p$，并且 $f(x_1) \equiv 0 \pmod{p^\alpha}$，则对于 $t = 0, 1, 2, \cdots, p-1$，式(3)中的 $x$ 都是方程(1)的解。

**证明**　我们来说明，如何确定式(3)中的 $t$，使 $x_1 + p^{\alpha-1}t$ 满足同余方程(1)，即要使

$$a_n(x_1+p^{\alpha-1}t)^n + a_{n-1}(x_1+p^{\alpha-1}t)^{n-1} + \cdots + a_1(x_1+p^{\alpha-1}t) + a_0 \equiv 0 \pmod{p^\alpha}, \tag{4}$$

即

$$f(x_1) + p^{\alpha-1}tf'(x_1) \equiv 0 \pmod{p^\alpha},$$

$$tf'(x_1) \equiv -\frac{f(x_1)}{p^{\alpha-1}} \pmod p。 \tag{5}$$

下面考虑两种情形。

（ⅰ）　若 $f'(x) \not\equiv 0 \pmod p$，则关于 $t$ 的同余方程(5)有唯一解 $t \equiv t_0 \pmod p$，即 $t = t_0 + pk$（$k \in \mathbf{Z}$），于是

$$x \equiv x_1 + p^{\alpha-1}t_0 \pmod{p^\alpha}$$

是同余方程(1)的解。

（ⅱ）　若 $f'(x_1) \equiv 0 \pmod p$，并且 $f(x_1) \equiv 0 \pmod{p^\alpha}$，则式(5)对于任意的整数 $t$ 成立，即同余方程(5)有 $p$ 个解

$$t \equiv i \pmod p,\quad 0 \leq i \leq p-1。$$

于是 $x \equiv x_1 + p^{\alpha-1}i \pmod{p^\alpha}$，$0 \leq i \leq p-1$，都是同余方程(1)的解。证毕。

在定理中，没有对 $f'(x_1) \equiv 0 \pmod p$ 并且 $f(x_1) \not\equiv 0 \pmod{p^\alpha}$ 的情形

进行讨论。事实上，此时，同余方程(5)无解。即，我们无法从同余方程(2)的解 $x_1$ 出发去求得同余方程(1)的解。

由定理，可以把解同余方程(1)，转化为解同余方程

$$f(x) \equiv 0 \pmod{p}。 \tag{6}$$

事实上，由方程(6)的解，利用定理，可以求出方程 $f(x) \equiv 0 \pmod{p^2}$的解，再利用定理，又可以求出方程 $f(x) \equiv 0 \pmod{p^3}$的解，……，直到求出方程(1)的解。

**推论** 使用定理的记号，

(ⅰ) 若 $x \equiv a \pmod{p}$是同余方程(6)的解，并且 $f'(a) \not\equiv 0 \pmod{p}$，则存在 $x_\alpha$，$x_\alpha \equiv a \pmod{p}$，使得 $x \equiv x_\alpha \pmod{p^\alpha}$是同余方程(1)的解。

(ⅱ) 若 $f'(x) \equiv 0 \pmod{p}$与同余方程(6)没有公共解，则对于任意的整数 $\alpha \geq 1$，同余方程(1)与(6)的解数相同。

**证明** 留做习题。

**例 1** 解同余方程

$$x^3 + 3x - 14 \equiv 0 \pmod{45}。$$

**解** 原同余方程等价于同余方程组

$$x^3 + 3x - 14 \equiv 0 \pmod{9}, \tag{7}$$

$$x^3 + 3x - 14 \equiv 0 \pmod{5}。 \tag{8}$$

先解同余方程(7)。容易验证，同余方程 $x^3 + 3x - 14 \equiv 0 \pmod{3}$的解是 $x \equiv 2 \pmod{3}$。

令 $x = 2 + 3t$ 并代入方程(7)，得到

$$(2 + 3t)^3 + 3(2 + 3t) - 14 \equiv 0 \pmod{9}, \tag{9}$$

容易看出，这是一个对于任何整数 $t$ 都成立的同余式，所以，方程(9)的解是 $t \equiv 0$，1，2 (mod 3)，于是方程(7)的解是

$$x \equiv 2，5，8 \pmod{9}。 \tag{10}$$

再解同余方程(8)。用 $x = 0$，1，2，3，4 去验证，得到(8)的解是

$$x \equiv 1，2 \pmod{5}。$$

因此，原同余方程的解是下面六个同余方程组的解：

$$x \equiv a_1 \pmod{9}，\quad a_1 = 2，5，8，$$

$$x \equiv a_2 \pmod{5}，\quad a_2 = 1，2。$$

利用孙子定理解这六个方程组，记

$m_1 = 9$，$m_2 = 5$，$m = 45$，$M_1 = 5$，$M_2 = 9$，$M_1' = 2$，$M_2' = -1$，

则



$$x \equiv 10a_1 - 9a_2 \pmod{45}。$$

将 $a_1$ 和 $a_2$ 的不同取值代入，得到所求的解是

$$x_1 \equiv 10\cdot 2 - 9\cdot 1 \equiv 11 \pmod{45},$$

$$x_2 \equiv 10\cdot 2 - 9\cdot 2 \equiv 2 \pmod{45},$$

$$x_3 \equiv 10\cdot 5 - 9\cdot 1 \equiv 41 \pmod{45},$$

$$x_4 \equiv 10\cdot 5 - 9\cdot 2 \equiv 32 \pmod{45},$$

$$x_5 \equiv 10\cdot 8 - 9\cdot 1 \equiv 26 \pmod{45},$$

$$x_6 \equiv 10\cdot 8 - 9\cdot 2 \equiv 17 \pmod{45}。$$

**例 2** 解同余方程

$$2x^2 + 13x - 34 \equiv 0 \pmod{5^3}。 \tag{11}$$

**解** 容易验证，同余方程

$$2x^2 + 13x - 34 \equiv 0 \pmod{5} \tag{12}$$

有两个解 $x \equiv -1$，2 (mod 5)。

令

$$x = -1 + 5t, \tag{13}$$

代入同余方程

$$2x^2 + 13 - 34 \equiv 0 \pmod{5^2}, \tag{14}$$

得到

$$2(-1 + 5t)^2 + 13(-1 + 5t) - 34 \equiv 0 \pmod{25},$$

$$-45 + 45t \equiv 0 \pmod{25},$$

$$9t \equiv 9 \pmod{5}，\ t \equiv 1 \pmod{5}。 \tag{15}$$

于是，将式(15)与式(13)联合，得到方程(14)的解

$$x = -1 + 5(1 + 5t_1) = 4 + 25t_1，\ t_1 \in \mathbf{Z}。 \tag{16}$$

将式(16)中的 $x$ 代入同余方程(11)，得到

$$2(4 + 25t_1)^2 + 13(4 + 25t_1) - 34 \equiv 0 \pmod{5^3},$$

$$50 + 725t_1 \equiv 0 \pmod{5^3},$$

$$2 + 29t_1 \equiv 0 \pmod{5},$$

$$t_1 \equiv 2 \pmod{5}。$$

将上式与(16)联合，得到同余方程(11)的一个解

$$x = 4 + 25t_1 = 4 + 25(2 + 5t_2) \equiv 54 \pmod{5^3}。$$

(ⅱ) 从同余方程(12)的另一个解 $x \equiv 2 \pmod{5}$出发利用上述方法，可以求出同余方程(11)的另一个解。（略，请读者补足）。

**例 3** 解同余方程

$$x^2 \equiv 1 \pmod{2^k},\ k\in\mathbf{N}。 \tag{17}$$

**解**　若 $k=1$，则方程(17)的解是 $x\equiv 1 \pmod 2$。

若 $k=2$，则方程(17)的解是 $x\equiv 1，-1 \pmod 4$。

若 $k\geq 3$，则同余方程(17)，即

$$x^2-1=(x+1)(x-1)\equiv 0 \pmod{2^k},$$

的解必是奇数，设 $x=2y+1$，则同余方程(1)成为

$$(2y+2)2y\equiv 0 \pmod{2^k},$$

$$y(y+1)\equiv 0 \pmod{2^{k-2}}。 \tag{18}$$

同余方程(18)的解是 $y_1\equiv 0$，$y_2\equiv -1 \pmod{2^{k-2}}$，即

$$y_1=2^{k-2}u,\quad y_2=-1+2^{k-2}v,\ u,v\in\mathbf{Z},$$

所以，方程(17)的解是

$$x_1=2^{k-1}u+1,\ x_2=2^{k-1}v-1,\quad u,v\in\mathbf{Z},$$

即

$$x\equiv 1，1+2^{k-1}，-1，-1+2^{k-1} \pmod{2^k}。$$

**例 4**　解同余方程 $x^2\equiv 2 \pmod{7^3}$。

**解**　设 $x$ 是这个同余方程的解，则它可以表示成

$$x=x_0+7x_1+7^2x_2,\ 0\leq x_i\leq 6,\ 0\leq i\leq 2,$$

代入原方程，得到

$$(x_0+7x_1+7^2x_2)^2\equiv 2 \pmod{7^3}, \tag{19}$$

因此

$$(x_0+7x_1+7^2x_2)^2\equiv 2 \pmod 7,$$

$$x_0^2\equiv 2 \pmod 7,$$

所以 $x_0\equiv 3$ 或 4 (mod 7)。于是 $x_0=3$ 或 4。

(ⅰ)　若 $x_0=3$，由式(19)，有

$$(3+7x_1+7^2x_2)^2\equiv 2 \pmod{7^2},$$

$$9+42x_1\equiv 2 \pmod{7^2},$$

$$6x_1\equiv -1 \pmod 7,$$

$$x_1\equiv 1 \pmod 7,\ x_1=1。$$

再由式(19)，有

$$(3+7\cdot 1+7^2x_2)^2\equiv 2 \pmod{7^3},$$

$$(10+49x_2)^2\equiv 2 \pmod{7^3},$$

$$3x_2\equiv -1 \pmod 7,\ x_2\equiv 2 \pmod 7,\ x_2=2。$$

这样，求得原同余方程的一个解是



$$x\equiv 3+7\cdot 1+7^2\cdot 2=108 \pmod{7^3}。$$

(ⅱ)　若 $x_0=4$，用同样的方法求出另一个解。(略)。

**注**：例 4 中的方法是利用数的 $b$ 进制表示，这一方法可以处理模 $b^k$ 的同余方程，而不必要求 $b$ 是素数。

## 习 题 三

**1.**　证明定理的推论。

**2.**　将例 2 中略去的部分补足。

**3.**　将例 4 中略去的部分补足。

**4.**　解同余方程 $x^2\equiv -1 \pmod{54}$。

**5.**　解同余方程 $f(x)=3x^2+4x-15\equiv 0 \pmod{75}$。

**6.**　证明：对于任意给定的正整数 $n$，必存在 $m$，使得同余方程 $x^2\equiv 1 \pmod m$的解数 $T>n$。

# 第四节　素数模的同余方程

在上节中，我们证明了，对于素数 $p$，模 $p^\alpha$的同余方程的求解可以转化为模 $p$ 的同余方程的求解。本节要对素数模的同余方程做些初步研究。

以下，设 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是整系数多项式，$p$ 是素数，$p\nmid a_n$。

**定理 1**　设 $k\leq n$，若同余方程

$$f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0 \pmod p \tag{1}$$

有 $k$ 个不同的解 $x_1,x_1,\cdots,x_k$，则对于任意的整数 $x$，有

$$f(x)\equiv (x-x_1)(x-x_2)\cdots(x-x_k)f_k(x) \pmod p,$$

其中 $f_k(x)$是一个次数为 $n-k$ 的整系数多项式，并且它的 $x^{n-k}$ 项的系数是 $a_n$。

**证明**　由多项式除法，有

$$f(x)=(x-x_1)f_1(x)+r_1, \tag{2}$$

其中 $f_1(x)$是首项系数为 $a_n$ 的 $n-1$ 次整系数多项式，$r_1$ 是常数。在式(2)

两边令 $x = x_1$，则由假设条件可知 $f(x_1) = r_1 \equiv 0 \pmod p$，因此，式(2)成为

$$f(x) \equiv (x - x_1)f_1(x) \pmod p。 \tag{3}$$

因此，当 $k = 1$ 时，定理成立。如果 $k > 1$，在上式中，令 $x = x_i$（$i = 2, 3, \cdots, k$），则有

$$0 \equiv f(x_i) \equiv (x_i - x_1)f_1(x_i) \pmod p。 \tag{4}$$

由于 $x_2, \cdots, x_k$ 对于模 $p$ 是两两不同余的，所以，上式给出

$$f_1(x_i) \equiv 0 \pmod p，\ i = 2, \cdots, k。 \tag{5}$$

由此及归纳法，即可证明定理。证毕。

**推论**　若 $p$ 是素数，则对于任何整数 $x$，有

$$x^{p-1} - 1 \equiv (x - 1)(x - 2)\cdots(x - p + 1) \pmod p。$$

**证明**　由 Fermat 定理（第二章第四节定理 2），数 1, 2, ⋯, $p - 1$ 是同余方程

$$x^{p-1} \equiv 1 \pmod p$$

的解，因此，利用定理 1 即可得证。

**定理 2**　同余方程(1)的解数$\le n$。

**证明**　假设同余方程(1)有 $n + 1$ 个不同的解

$$x \equiv x_i \pmod p，\ 1 \le i \le n + 1。$$

由定理 1，有 $f(x) \equiv a_n(x - x_1)\cdots(x - x_n) \pmod p$，因此

$$0 \equiv f(x_{n+1}) \equiv a_n(x_{n+1} - x_1)\cdots(x_{n+1} - x_n) \pmod p。 \tag{6}$$

由于 $p \nmid a_n$，$x_{n+1} \not\equiv x_i \pmod p$，$1 \le i \le n$，所以式(6)不能成立。这个矛盾说明同余方程(1)不能有 $n + 1$ 个解。证毕。

**推论**　若同余方程 $b_n x^n + \cdots + b_0 \equiv 0 \pmod p$的解数大于 $n$，则

$$p \mid b_i，\ 0 \le i \le n。 \tag{7}$$

**证明**　若式(7)不成立，设 $p \nmid b_d$，$d \le n$，$p \mid b_i$，　$d < j \le n$。则

$$b_n x^n + \cdots + b_0 \equiv b_d x^d + \cdots + b_0 \equiv 0 \pmod p。 \tag{8}$$

由定理 2，同余方程(8)的解数不大于 $d$，因而不大于 $n$，这与假设矛盾。因此，式(7)必成立。证毕。

**定理 3**　同余方程(1)或者有 $p$ 个解，或者存在次数不超过 $p - 1$ 的整系数多项式 $r(x)$，使得同余方程(1)与 $r(x) \equiv 0 \pmod p$等价。

**证明**　由多项式除法可知，存在整系数多项式 $g(x)$与 $r(x)$，使得

$$f(x) = g(x)(x^p - x) + r(x)。 \tag{9}$$



由 Fermat 定理，对于任意的整数 $x$，有 $x^p \equiv x \pmod p$，因此，如果 $r(x)$的系数都是 $p$ 的倍数，则对于任意的整数 $x$，$f(x) \equiv 0 \pmod p$，即同余方程(1)有 $p$ 个解。如果 $r(x)$的系数不都是 $p$ 的倍数，则 $r(x)$的次数不超过 $p - 1$。由式(9)看出，对于任意的整数 $x$，$f(x) \equiv r(x) \pmod p$，即同余方程(1)与 $r(x) \equiv 0 \pmod p$等价。证毕。

**定理 4**　设 $n \le p$，则同余方程

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod p \tag{10}$$

有 $n$ 个解的充要条件是存在整数多项式 $q(x)$和 $r(x)$，$r(x)$的次数$< n$，使得

$$x^p - x = f(x)q(x) + p \cdot r(x)。 \tag{11}$$

**证明**　必要性　由多项式除法，存在整系数多项式 $q(x)$与 $r_1(x)$，$r_1(x)$的次数$< n$，使得

$$x^p - x = f(x)q(x) + r_1(x)。 \tag{12}$$

若同余方程(10)有 $n$ 个解 $x \equiv x_i \pmod p$（$1 \le i \le n$），则由式(12)和 Fermat 定理，得到

$$r_1(x_i) \equiv 0 \pmod p，\ 1 \le i \le n。$$

由此及定理 2 推论，可知 $r_1(x)$的系数都能被 $p$ 整除，即

$$r_1(x) = p \cdot r(x)，$$

其中 $r(x)$是整系数多项式。这证明了式(11)。

充分性　若式(11)成立，由 Fermat 定理，对于任何整数 $x$，有

$$0 \equiv x^p - x \equiv f(x)q(x) \pmod p， \tag{13}$$

即同余方程

$$f(x)q(x) \equiv 0 \pmod p$$

有 $p$ 个解，但是，$q(x)$是 $p - n$ 次多项式，所以由定理 2，方程 $q(x) \equiv 0 \pmod p$的解数 $\le p - n$。以$\lambda$表示同余方程(10)的解数，则由第一节定理 1，有

$$\lambda + p - n \ge p，\ \lambda \ge n，$$

再利用定理 2，得到$\lambda = n$。　证毕。

**注：**若 $p \nmid a_n$，由辗转相除法可求出 $a_n'$，$p \nmid a_n'$使得 $a_n a_n' \equiv 1 \pmod p$，于是，同余方程(1)与同余方程

$$a_n' f(x) = x^n + a_n' a_{n-1} x^{n-1} + \cdots + a_n' a_1 x + a_n' a_0 \pmod p$$

等价。因此，定理 4 是有普遍性的。

**定理 5**　若 $p$ 是素数，$n \mid p - 1$，$p \nmid a$ 则

$$x^n \equiv a \pmod{p} \tag{14}$$

有解的充要条件是

$$a^{\frac{p-1}{n}} \equiv 1 \pmod{p}。 \tag{15}$$

若有解，则解数为 $n$。

**证明**　必要性　若方程(14)有解 $x_0$，则 $p \nmid x_0$，由 Fermat 定理，得到

$$a^{\frac{p-1}{n}} \equiv (x_0^n)^{\frac{p-1}{n}} = x_0^{p-1} \equiv 1 \pmod{p}。$$

充分性　若式(15)成立，则

$$x^{p-1} - x = x((x^n)^{\frac{p-1}{n}} - a^{\frac{p-1}{n}} + a^{\frac{p-1}{n}} - 1)$$

$$= (x^n - a)P(x) + x(a^{\frac{p-1}{n}} - 1),$$

其中 $P(x)$是关于 $x$ 的整系数多项式。由定理 4 可知同余方程(14)有 $n$ 个解。证毕。

**例 1**　判定同余方程 $2x^3 + 3x + 1 \equiv 0 \pmod 7$是否有三个解。

**解**　因为 $2 \cdot 4 \equiv 1 \pmod 7$，所以，原方程与

$$4 \cdot 2x^3 + 4 \cdot 3x + 4 \equiv 0 \pmod 7$$

即

$$x^3 - 2x - 3 \equiv 0 \pmod 7$$

等价。由于

$$x^7 - x = (x^3 - 2x - 3)(x^4 + 2x^2 + 3x + 4) + 12x^2 + 16x + 12,$$

所以，由定理 4 可知，原方程的解数小于 3。

**例 2**　解同余方程

$$3x^{14} + 4x^{10} + 6x - 18 \equiv 0 \pmod 5。$$

**解**　由 Fermat 定理，$x^5 \equiv x \pmod 5$，因此，原同余方程等价于

$$2x^2 + x - 3 \equiv 0 \pmod 5。 \tag{16}$$

将 $x \equiv 0, \pm 1, \pm 2 \pmod 5$分别代入方程(16)进行验证，可知这个同余方程解是 $x \equiv 1 \pmod 5$。



## 习 题 四

**1.**　解同余方程：

(ⅰ)　$3x^{11} + 2x^8 + 5x^4 - 1 \equiv 0 \pmod 7$；

(ⅱ)　$4x^{20} + 3x^{12} + 2x^7 + 3x - 2 \equiv 0 \pmod 5$。

**2.**　判定

(ⅰ)　$2x^3 - x^2 + 3x - 1 \equiv 0 \pmod 5$是否有三个解；

(ⅱ)　$x^6 + 2x^5 - 4x^2 + 3 \equiv 0 \pmod 5$是否有六个解？

**3.**　设$(a, m) = 1$，$k$ 与 $m$ 是正整数，又设 $x_0^k \equiv a \pmod m$，证明同余方程

$$x^k \equiv a \pmod m$$

的一切解 $x$ 都可以表示成 $x \equiv yx_0 \pmod m$，其中 $y$ 满足同余方程 $y^k \equiv 1 \pmod m$。

**4.**　设 $n$ 是正整数，$p$ 是素数，$(n, p-1) = k$，证明同余方程 $x^n \equiv 1 \pmod p$有 $k$ 个解。

**5.**　设 $p$ 是素数，证明：

(ⅰ)　对于一切整数 $x$，$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \pmod p$；

(ⅱ)　$(p-1)! \equiv -1 \pmod p$。

**6.**　设 $p \geq 3$ 是素数，证明：$(x-1)(x-2)\cdots(x-p+1)$的展开式中除首项及常数项外，所有的系数都是 $p$ 的倍数。

# 第五节　素数模的二次同余方程

设 $p$ 是素数，我们来研究素数模 $p$ 的二次同余方程

$$ax^2 + bx + c \equiv 0 \pmod p。 \tag{1}$$

如果 $p = 2$，则可以直接验证 $x \equiv 0$ 或 1 (mod 2)是否方程(1)的解。

如果$(a, p) = p$，则方程(1)成为一元一次同余方程。因此，只需考察 $p > 2$，$(a, p) = 1$ 的情形。此时，因为$(4a, p) = 1$，所以，方程(1)等价于方程

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod p,$$

即

$$(2ax+b)^2 \equiv b^2 - 4ac \pmod{p}。$$

这样，研究方程(1)归结为对方程

$$x^2 \equiv n \pmod{p} \tag{2}$$

的研究。

**定义 1**　给定整数 $p$，对于任意的整数 $n$，$(n, p) = 1$，若方程(2)有解，则称 $n$ 是模 $p$ 的二次剩余，记为 $n \in QR(p)$；否则，称 $n$ 是模 $p$ 的二次非剩余，记为 $n \in QNR(p)$。

显然，若 $n_1 \equiv n_2 \pmod{p}$，则它们同是模 $p$ 的二次剩余（或二次非剩余），因此，在谈到模 $p$ 的二次剩余（或二次非剩余）时，把 $n_1$ 和 $n_2$ 看作是同一个。

以下，在本节中，总假定 $p$ 是奇素数。

**定理 1**　若 $(n, p) = 1$，则

(ⅰ)　$n$ 是模 $p$ 的二次剩余的充要条件是

$$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}; \tag{3}$$

(ⅱ)　若 $n$ 是模 $p$ 的二次剩余，则方程(2)有两个解；

(iii)　$n$ 是模 $p$ 的二次非剩余的充要条件是

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}。 \tag{4}$$

**证明**　结论(ⅰ)与(ⅱ)由第四节定理 5 直接推出。

(iii)　若 $(n, p) = 1$，由第二章第四节定理 1，有

$$n^{p-1} \equiv 1 \pmod{p},$$

$$(n^{\frac{p-1}{2}} + 1)(n^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p}。 \tag{5}$$

因为 $p$ 是奇素数，所以式(3)式与式(4)必有且仅有一个成立，利用结论(ⅰ)，可得到结论(iii)。证毕。

**定理 2**　模 $p$ 的简化系中，二次剩余与二次非剩余的个数都是 $\frac{p-1}{2}$，而且，模 $p$ 的每个二次剩余与且仅与数列

$$1^2,\ 2^2,\ \cdots,\ (\frac{p-1}{2})^2 \tag{6}$$

中的一个数同余。

**证明**　显然，数列(6)包含了模 $p$ 的全部二次剩余。为了证明定理，



只需证明式(6)中的任何两个数对模 $p$ 不同余。

对任意的整数 $k$，$s$，$1 \le k < s \le \frac{p-1}{2}$，若

$$k^2 \equiv s^2 \pmod{p}, \tag{7}$$

则 $p \mid k+s$ 或 $p \mid k-s$。这都是不可能的，所以式(7)不能成立。证毕。

**定义 2**　给定奇素数 $p$，对于整数 $n$，定义 Legendre 符号为

$$(\frac{n}{p}) = \begin{cases} 0, & \text{当}(n, p) \ne 1; \\ 1, & \text{当} n \in QR(p); \\ -1, & \text{当} n \in QNR(p)。 \end{cases}$$

例如，由定理 1，1 与 4 是模 5 的二次剩余，2 与 3 是模 5 的二次非剩余，于是

$$(\frac{1}{5}) = 1,\ (\frac{2}{5}) = -1,\ (\frac{3}{5}) = -1,\ (\frac{4}{5}) = 1,$$

**定理 3**　设 $p$ 是奇素数，$n$ 是整数，则

(ⅰ)　$(\frac{n}{p}) \equiv n^{\frac{p-1}{2}} \pmod{p}$；

(ⅱ)　若 $n \equiv n_1 \pmod{p}$，则 $(\frac{n}{p}) = (\frac{n_1}{p})$；

(iii)　$(\frac{1}{p}) = 1,\ (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$；

(iv)　对任意的整数 $n_i$，$1 \le i \le k$，有

$$(\frac{a_1 a_2 \cdots a_k}{p}) = (\frac{a_1}{p})(\frac{a_2}{p}) \cdots (\frac{a_k}{p})。$$

**证明**　结论(ⅰ)与(ⅱ)容易由定义 2 及定理 1 得到。

为了证明结论(iii)，只需证明其中的第二个等式。由结论(ⅰ)，有

$$(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

其中同余式两端都只能取值 +1 或 −1，因此，结论(iii)的第二个等式成立。

最后，由结论(ⅰ)，有

$$\left(\frac{a_1a_2\cdots a_k}{p}\right)\equiv(a_1a_2\cdots a_k)^{\frac{p-1}{2}}\equiv a_1^{\frac{p-1}{2}}a_2^{\frac{p-1}{2}}\cdots a_k^{\frac{p-1}{2}}$$

$$\equiv\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_k}{p}\right)(\mathrm{mod}\ p)。$$

由于上式首端与末端都是只取值 $-1$，0 或 1 的整数，所以它们必相等。结论(iv)得证。证毕。

**推论** 设 $p$ 是奇素数，则 $-1\in QR(p)$的充要条件是 $p\equiv 1(\mathrm{mod}\ 4)$；$-1\in QNR(p)$的充要条件是 $p\equiv 3(\mathrm{mod}\ 4)$。

**例 1** 判断方程 $x^2\equiv 5\ (\mathrm{mod}\ 11)$有没有解。

**解** 由定理 2，因为

$$\left(\frac{5}{11}\right)\equiv 5^{\frac{11-1}{2}}=5^5\equiv 5\cdot 5^4\equiv 5\cdot 3^2\equiv 1\ \ (\mathrm{mod}\ 11),$$

方程有解。

**例 2** 设 $p$ 是奇素数，$p\equiv 1\ (\mathrm{mod}\ 4)$，则

$$\left(\pm\left(\frac{p-1}{2}\right)!\right)^2\equiv -1\ (\mathrm{mod}\ p)$$

**解** 由 Wilson 定理（第二章第二节例 3），有

$$-1\equiv(p-1)!=(-1)^{\frac{p-1}{2}}(p-1)!$$

$$=(-1)^{\frac{p-1}{2}}1\cdot 2\cdots\frac{p-1}{2}\frac{p+1}{2}\cdots(p-1)$$

$$\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2(\mathrm{mod}\ p)。$$

定理 2 和例 2 说明，当素数 $p\equiv 1(\mathrm{mod}\ 4)$时，模 $p$ 的所有二次剩余之积对模 $p$ 同余于 $-1$。此外，我们还得到了方程 $x^2\equiv -1\ (\mathrm{mod}\ p)$ 的解。

**例 3** 设 $n$ 是整数，证明 $n^2+1$ 的任何奇因数都是 $4m+1$（$m\in\mathbf{Z}$）的形式。

**解** 由于任何奇数都可表成奇素数之积，而且任意多个形如 $4m+1$ 的整数之积也具有 $4m+1$ 的形式，我们只需证明：若素数 $p$ 是 $n^2+1$ 的因数，则 $p$ 具有 $4m+1$ 的形式。



事实上，若 $p\mid n^2+1$，则

$$n^2\equiv -1\ (\mathrm{mod}\ p),$$

即$-1\in QR(p)$。由定理 3 推论得出所需结论。

**例 4** 形如 $4m+1$（$k\in\mathbf{Z}$）的素数有无穷多个。

**解** 用反证法。假设只有有限多个形如 $4k+1$ 的素数 $p_1, p_2, \cdots, p_k$，记

$$N=4(p_1p_2\cdots p_k)^2+1。$$

由例 2，必有奇素数 $q$，$q\equiv 1\ (\mathrm{mod}\ 4)$，$q\mid N$，显然 $q\neq p_i\ (1\le i\le k)$，这与假设矛盾，所以形如 $4m+1$ 的素数有无穷多个。

**例 5** 若 $a\equiv 1\ (\mathrm{mod}\ 4)$，$2\mid b$，并且 $b$ 没有形如 $4k+3$（$k\in\mathbf{Z}$）的素因数，证明方程

$$y^2=x^3-a^3-b^2 \tag{8}$$

没有整数解。

**解** 用反证法。假设有整数 $x$，$y$ 满足方程(8)。

若 $2\mid x$，则由式(8)得则 $y^2\equiv -1(\mathrm{mod}\ 4)$这不可能。

若 $x\equiv 3\ (\mathrm{mod}\ 4)$，则由式(8)得到

$$y^2\equiv x^3-a^3-b^2\equiv 3^3-1^3-0\equiv 2\ (\mathrm{mod}\ 4),$$

这是不可能的。

若 $x\equiv 1\ (\mathrm{mod}\ 4)$，则

$$x^2+ax+a^2\equiv 1+a+a^2\equiv 3\ (\mathrm{mod}\ 4), \tag{9}$$

因此，必有素数 $p\equiv 3\ (\mathrm{mod}\ 4)$，使得

$$p\mid x^2+ax+a^2\ 。 \tag{10}$$

由式(8)与式(10)得到

$$y^2=x^3-a^3-b^2\equiv -b^2\ (\mathrm{mod}\ p), \tag{11}$$

即 $-b^2\in QR(p)$。但是，由假设，$p\nmid b^2$，所以有

$$\left(\frac{-b^2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right)=-1,$$

这与式(11)矛盾。

**例 6** 设 $p$ 是素数，证明：数例 1, 2, ⋯, $p-1$ 中的模 $p$ 的二次剩余之和是

$$S=\frac{p(p^2-1)}{24}-p\sum_{k=1}^{\frac{p-1}{2}}[\frac{k^2}{p}]。$$

**解**　对于整数 $k$，$1\le k\le\frac{p-1}{2}$，记

$$k^2=pq_k+r_k，\ q_k\in\mathbf{Z}，\ 1\le r_k\le p-1，$$

则 $q_k=[\frac{k^2}{p}]$，并且，由定理 2，有

$$S=\sum_{k=1}^{\frac{p-1}{2}}r_k=\sum_{k=1}^{\frac{p-1}{2}}k^2-p\sum_{k=1}^{\frac{p-1}{2}}[\frac{k^2}{p}]$$

$$=\frac{p(p^2-1)}{24}-p\sum_{k=1}^{\frac{p-1}{2}}[\frac{k^2}{p}]。$$

**例 7**　设 $p$ 是奇素数，证明：若同余方程

$$x^4+1\equiv 0\ (\mathrm{mod}\ p)\qquad(12)$$

有解，则 $p\equiv 1\ (\mathrm{mod}\ 8)$。

**解**　设 $x\equiv a\ (\mathrm{mod}\ p)$是方程(12)的解，则

$$a^4\equiv -1\ (\mathrm{mod}\ p)，\qquad(13)$$

$$a^8\equiv 1\ (\mathrm{mod}\ p)。\qquad(14)$$

以 $d_0$ 表示使

$$a^d\equiv 1\ (\mathrm{mod}\ p)\qquad(15)$$

成立的最小正整数 $d$，记 $8=qd_0+r$，$0\le r\le d_0-1$，则由式(14)与式(15)得到

$$1\equiv a^8=a^{qd_0+r}\equiv a^r\ (\mathrm{mod}\ p)，$$

因此，若 $r\ne 0$，则上式与 $d_0$ 的定义矛盾。所以 $r=0$，即 $d_0\mid 8$，这样，$d_0$ 的取值只可能是 1，2，4 或 8。由式(13)可知 $d_0=8$。

用同样方法以及 Fermat 定理可以证明 $8\mid p-1$ 即 $p\equiv 1\ (\mathrm{mod}\ 8)$。

## 习 题 五

**1.**　同余方程 $x^2\equiv 3\ (\mathrm{mod}\ 13)$有多少个解？



**2.**　求出模 23 的所有的二次剩余和二次非剩余。

**3.**　设 $p$ 是奇素数，证明：模 $p$ 的两个二次剩余的乘积是二次剩余；两个二次非剩余的乘积是二次剩余；一个二次剩余和一个二次非剩余的乘积是二次非剩余。

**4.**　设素数 $p\equiv 3\ (\mathrm{mod}\ 4)$，$(\frac{n}{p})=1$，证明 $x\equiv\pm n^{\frac{p+1}{4}}\ (\mathrm{mod}\ p)$是同余方程

$$x^2\equiv n\ (\mathrm{mod}\ p)$$

的解。

**5.**　设 $p$ 是奇素数，$(n,p)=1$，$\alpha$是正整数，证明同余方程

$$x^2\equiv n\ (\mathrm{mod}\ p^\alpha)$$

有解的充要条件是$(\frac{n}{p})=1$。

**6.**　设 $p$ 是奇素数，证明：模 $p$ 的所有二次剩余的乘积与 $(-1)^{\frac{p+1}{2}}$ 对模 $p$ 同余。

# 第六节　二次互反律

本节要对 Legendre 符号和二次剩余做进一步的研究。以下，总以 $p$ 表示奇素数。

**引理**　设$(n,p)=1$，对于整数 $k$（$1\le k\le\frac{p-1}{2}$），以 $r_k$ 表示 $nk$ 对模 $p$ 的最小非负剩余。设在 $r_1,r_2,\cdots,r_{\frac{p-1}{2}}$ 中大于 $\frac{p}{2}$ 的有 $m$ 个，则

$$(\frac{n}{p})=(-1)^m。$$

**证明**　在数列 $r_1,r_2,\cdots,r_{\frac{p-1}{2}}$ 中，假设大于 $\frac{p}{2}$ 的是 $a_1,a_2,\cdots,a_m$，小

于 $\frac{p}{2}$ 的是 $b_1, b_2, \cdots, b_t$，则

$$n^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!=\prod_{1\le k\le\frac{p-1}{2}}(nk)\equiv\prod_{i=1}^{m}a_i\prod_{i=1}^{t}b_i\ (\mathrm{mod}\ p)。\qquad(1)$$

因为 $\frac{p}{2}<a_i<p$，所以 $0<p-a_i<\frac{p}{2}$，而且对于任意的 $i$，$j$，$1\le i\le m$，$1\le j\le t$，有 $b_j\ne p-a_i$，否则，将有整数 $k_1$ 与 $k_2$，$1\le k_1,k_2\le\frac{p-1}{2}$，使得

$$nk_1+nk_2\equiv 0\ (\mathrm{mod}\ p),$$

即

$$p\mid n(k_1+k_2),$$

由于 $(n,p)=1$，于是 $p\mid k_1+k_2$，这是不可能的。这样，由式(1)推出

$$n^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv(-1)^m\prod_{i=1}^{m}(p-a_i)\prod_{i=1}^{t}b_i$$

$$\equiv(-1)^m\left(\frac{p-1}{2}\right)!(\mathrm{mod}\ p),$$

从而由第五节定理 3 推出引理结论。证毕。

**定理 1**　下面的结论成立：

(ⅰ)　$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$；　　(2)

(ⅱ)　若 $n$ 是奇数，$(n,p)=1$，则

$$\left(\frac{n}{p}\right)=(-1)^{\sum_{i=1}^{l}\left[\frac{ni}{p}\right]},\qquad(3)$$

其中 $l=\frac{p-1}{2}$。

**证明**　使用引理中的符号 $r_k$，$a_i$，$b_i$，$m$ 与 $t$，由

$$nk=p\left[\frac{nk}{p}\right]+r_k,\quad 1\le k\le\frac{p-1}{2},$$



及引理的证明过程，看到

$$\begin{aligned}n\frac{p^2-1}{2}&=\sum_{k=1}^{\frac{p-1}{2}}nk=p\sum_{k=1}^{l}\left[\frac{nk}{p}\right]+\sum_{k=1}^{l}r_k\\&=p\sum_{k=1}^{l}\left[\frac{nk}{p}\right]+\sum_{i=1}^{m}a_i+\sum_{i=1}^{t}b_i\\&=p\sum_{k=1}^{l}\left[\frac{nk}{p}\right]+\sum_{i=1}^{m}(p-a_i)+\sum_{i=1}^{t}b_i+2\sum_{i=1}^{m}a_i-mp\\&=p\sum_{k=1}^{l}\left[\frac{nk}{p}\right]+\sum_{i=1}^{l}i+2\sum_{i=1}^{m}a_i-mp\\&=p\sum_{k=1}^{l}\left[\frac{nk}{p}\right]+\frac{p^2-1}{2}+2\sum_{i=1}^{m}a_i-mp,\end{aligned}$$

因此

$$(n-1)\frac{p^2-1}{8}=p\sum_{k=1}^{l}\left[\frac{nk}{p}\right]+2\sum_{i=1}^{m}a_i-mp。\qquad(4)$$

若 $n=2$，则当 $1\le k\le l$ 时，$0<\frac{nk}{p}<1$，所以 $\left[\frac{nk}{p}\right]=0$，于是由式(4)得到

$$\frac{p^2-1}{8}\equiv m\ (\mathrm{mod}\ 2)。\qquad(5)$$

若 $2\nmid n$ 则由式(4)推出

$$\sum_{k=1}^{l}\left[\frac{nk}{p}\right]\equiv m\ (\mathrm{mod}\ 2)。\qquad(6)$$

由式(5)，式(6)及引理，证得定理。证毕。

**推论**　设 $p$ 是素数，则

$$\left(\frac{2}{p}\right)=\begin{cases}1, & \text{当}p\equiv\pm1(\mathrm{mod}\,8),\\-1, & \text{当}p\equiv\pm3(\mathrm{mod}\,8)。\end{cases}$$

**定理 2**(二次互反律)　设 $p$ 与 $q$ 是不相同的两个素数，则

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)。$$

**证明**　只需证明

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}。\tag{7}$$

记 $p_1=\dfrac{p-1}{2}$，$q_1=\dfrac{q-1}{2}$。由定理 1 ，有

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^r，\ r=\sum_{k=1}^{p_1}\left[\frac{kq}{p}\right]+\sum_{k=1}^{q_1}\left[\frac{kp}{q}\right]。\tag{8}$$

考察有序数对$(u, v)$所成的集合

$$S=\{(u,v)；\ u=py，\ v=qx，\ 1\le x\le p_1，\ 1\le y\le q_1\}$$

显然 $S$ 中有 $p_1q_1=\dfrac{p-1}{2}\cdot\dfrac{q-1}{2}$ 个元素。由于$(p, q)=1$，所以，对于任何$(u, v)\in S$，$u\ne v$ 记

$$S_1=\{(u,v)；\ (u,v)\in S，\ u>v\}$$
$$S_2=\{(u,v)；\ (u,v)\in S，\ v>u\}$$

则

$$S_1\cap S_2=\varnothing，\ S_1\cup S_2=S。\tag{9}$$

对于$(u, v)\in S_1$，有 $u>v$，即

$$py>xq，\ x<\frac{p}{q}y，\ 1\le y\le q_1，$$

因此 $S_1$ 中有 $\sum\limits_{y=1}^{q_1}\left[\dfrac{py}{q}\right]$ 个元素。同理，$S_2$ 中有 $\sum\limits_{x=1}^{p_1}\left[\dfrac{qx}{p}\right]$ 个元素，所以

$$\frac{p-1}{2}\cdot\frac{q-1}{2}=\sum_{k=1}^{p_1}\left[\frac{kq}{p}\right]+\sum_{k=1}^{q_1}\left[\frac{kp}{q}\right]。\tag{10}$$

联合式(7)，式(8), 和式(10)，证得定理。证毕。

利用第五节和本节中的定理，可以判定素数模的二次同余方程的可解性。一般地，若 $p$ 是素数，计算 Legendre 符号$\left(\dfrac{n}{p}\right)$可按以下步骤进行：

(ⅰ)　求出 $n_0\equiv n\pmod p$，$1\le n_0\le p$;

(ⅱ)　将 $n_0$ 写成 $n_0=Q^2q_1q_2\cdots q_k$ 的形式，其中 $Q\in\mathbf{Z}$，$q_1, q_2,\cdots, q_k$ 是互不相同的素数;



(iii)　若有某个 $q_i=2$，用定理 1 推论判定$\left(\dfrac{q_i}{p}\right)$之值;

(iv)　若 $q_i\ne 2$，利用定理 2 将$\left(\dfrac{q_i}{p}\right)$的计算转化为计算$\left(\dfrac{p}{q_i}\right)$;

(ⅴ)　重复以上步骤，直至求出每个$\left(\dfrac{q_i}{p}\right)$;

(vi)　计算$\left(\dfrac{q}{p}\right)=\prod\limits_{i=1}^{k}\left(\dfrac{q_i}{p}\right)$。

**例 1**　已知 563 是素数，判定方程 $x^2\equiv 429\pmod{563}$是否有解。

**解**　利用已有的定理，有

$$\left(\frac{429}{563}\right)=\left(\frac{3\cdot 11\cdot 13}{563}\right)=\left(\frac{3}{563}\right)\left(\frac{11}{563}\right)\left(\frac{13}{563}\right)$$
$$=(-1)^{\frac{3-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{3}\right)(-1)^{\frac{11-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{11}\right)(-1)^{\frac{13-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{13}\right)$$
$$=\left(\frac{2}{3}\right)\left(\frac{2}{11}\right)\left(\frac{4}{13}\right)=(-1)(-1)=1。$$

方程有解。

**例 2**　求所有的素数 $p$，使得 $-2\in QR(p)$，$3\in QR(p)$。

**解**　若 $-2\in QR(p)$，则$\left(\dfrac{-2}{p}\right)=1$，因此，

$$\begin{cases}\left(\dfrac{-1}{p}\right)=1\\ \left(\dfrac{2}{p}\right)=1\end{cases}\quad\text{或}\quad\begin{cases}\left(\dfrac{-1}{p}\right)=-1\\ \left(\dfrac{2}{p}\right)=-1\end{cases}，\tag{11}$$

所以，由定理 1 推论和第五节定理 3 推论，有

$$\begin{cases}p\equiv 1(\bmod 4)\\ p\equiv\pm 1(\bmod 8)\end{cases}\quad\text{或}\quad\begin{cases}p\equiv 3(\bmod 4)\\ p\equiv\pm 3(\bmod 8)\end{cases}，\tag{12}$$

由式(12)中的第一组同余式，得到

$$p \equiv 1 \pmod 8; \tag{13}$$

由式(12)中的第二组同余式，得到

$$p \equiv 3 \pmod 8。 \tag{14}$$

(ⅰ) 若式(13)成立，并且 $3 \in QR(p)$。由定理 2，有

$$1 = \left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right),$$

因此 $p \equiv 1 \pmod 3$。由此及式(13)，利用孙子定理得到

$$p \equiv 1 \pmod{24}。 \tag{15}$$

(ⅱ) 若式(14)成立，并且 $3 \in QR(p)$。由定理 2，有

$$1 = \left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right) = -\left(\frac{p}{3}\right),$$

因此 $p \equiv 2 \pmod 3$。由此及式(14)，利用孙子定理得到

$$p \equiv 11 \pmod{24}。 \tag{16}$$

由式(15)与(16)可知所求的素数具有形式

$$p = 24k + 1 \text{ 或 } p = 24k + 11，k \in \mathbf{Z}。$$

**例 3** 证明：形如 $8k + 7$（$k \in \mathbf{Z}$）的素数有无穷多个。

**解** 用反证法。假设只有有限个形如 $8k + 7$（$k \in \mathbf{Z}$）的素数 $p_1, p_2, \cdots, p_t$。记

$$N = (p_1 p_2 \cdots p_t)^2 - 2。$$

显然，$2 \nmid N$。设 $q$ 是 $N$ 的一个奇素因数，则

$$(p_1 p_2 \cdots p_t)^2 \equiv 2 \pmod q,$$

因此，由定理 1 推论，有 $q \equiv 1$ 或 $7 \pmod 8$。

若 $N$ 的所有奇素因数都具有 $8k + 1$ 的形式，则 $N$ 也是 $8k + 1$ 的形式，但是，由于任何奇数的平方对模 8 与 1 同余，所以应有

$$N \equiv 1 - 2 \equiv -1 \pmod 8。$$

这个矛盾说明，$N$ 至少有一个形如 $8k + 7$ 的奇素因数 $q$。显然，$q \neq p_i$（$1 \le i \le t$），这与个数有限的假设矛盾。这个矛盾说明，形如 $8k + 7$（$k \in \mathbf{Z}$）的素数有无穷多个。

**例 4** 证明：形如 $8k + 3$（$k \in \mathbf{Z}$）的素数无穷多个。

**解** 用反证法。假设只有有限个形如 $8k + 3$（$k \in \mathbf{Z}$）的素数 $p_1, p_2, \cdots, p_t$。记



$$N = (p_1 p_2 \cdots p_t)^2 + 2。$$

设 $q$ 是 $N$ 的一个素因数，显然 $q > 2$。由于 $-2 \in QR(q)$，所以

$$\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = 1。$$

考虑两种可能：

(ⅰ) $\left(\frac{-1}{q}\right) = 1$，$\left(\frac{2}{q}\right) = 1$，则

$$q \equiv 1 \pmod 4 \text{并且 } q \equiv 1 \text{ 或 } 7 \pmod 8,$$

这导出 $q \equiv 1 \pmod 8$。

(ⅱ) $\left(\frac{-1}{q}\right) = -1$，$\left(\frac{2}{q}\right) = -1$，则

$$q \equiv 3 \pmod 4 \text{ 并且 } q \equiv 3 \text{ 或 } 5 \pmod 8,$$

这导出 $q \equiv 3 \pmod 8$。

这样，$q$ 只能是 $8k + 1$ 或 $8k + 3$ 的形式。由于 $p_i \equiv 3 \pmod 3$，$p_i^2 \equiv 1 \pmod 8$（$1 \le i \le t$），所以，$N \equiv 3 \pmod 8$，因此，$N$ 的素因数不可能都是 $8k + 1$ 的形式，即至少有一个 $q$，$q \mid N$，$q$ 具有 $8k + 3$ 的形式。显然 $q \neq p_i$（$1 \le i \le t$）。这与个数有限的假设矛盾。因此，形如 $8k + 3$（$k \in \mathbf{Z}$）的素数无穷多个。

## 习 题 六

**1.** 已知 769 与 1013 是素数，判定方程

(ⅰ) $x^2 \equiv 1742 \pmod{769}$；

(ⅱ) $x^2 \equiv 1503 \pmod{1013}$。

是否有解。

**2.** 求所有的素数 $p$，使得下面的方程有解：

$$x^2 \equiv 11 \pmod p。$$

**3.** 求所有的素数 $p$，使得 $-2 \in QR(p)$，$-3 \in QR(p)$。

**4.** 设 $(x, y) = 1$，试求 $x^2 - 3y^2$ 的奇素数因数的一般形式。

**5.** 证明：形如 $8k + 5$（$k \in \mathbf{Z}$）的素数无穷多个。

**6.** 证明：对于任意的奇素数 $p$，总存在整数 $n$，使得

$$p \mid (n^2+1)(n^2+2)(n^2-2)。$$

## 第七节　Jacobi 符号

在上一节中我们看到，对于奇素数 $p$，利用计算 Legendre 符号可以判定方程

$$x^2 \equiv a \pmod{p} \tag{1}$$

是否有解。对于一般的正整数 $m$，如果它的标准分解式是

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

那么，由第二节定理 4 和第三节定理可知，判定方程

$$x^2 \equiv a \pmod{m} \tag{2}$$

是否有解，归结为对形如方程(1)（$p = p_i$，$1 \le i \le k$）的可解性判定。因此，在理论上，利用 Legendre 符号可以判定方程(2)是否有解。但是，写出正整数的标准分解式常会遇到实际困难，所以利用 Legendre 符号判定方程(2)的可解性并不常是容易实现的。为此，本节中要介绍一个更为切实可行的方法。

**定义 1**　给定正奇数 $m > 1$，$m = p_1 p_2 \cdots p_k$，其中 $p_i$（$1 \le i \le k$）是奇素数，对于任意的整数 $a$，定义

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right),$$

其中右端的 $\left(\frac{a}{p_i}\right)$（$1 \le i \le k$）是 Legendre 符号，称 $\left(\frac{a}{m}\right)$ 是 Jacobi 符号。

例如，取 $m = 45 = 3 \cdot 3 \cdot 5$，则

$$\left(\frac{2}{45}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1,$$

$$\left(\frac{28}{45}\right) = \left(\frac{28}{3}\right)\left(\frac{28}{3}\right)\left(\frac{28}{5}\right) = \left(\frac{3}{5}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1。$$

**注 1**：当 $m$ 是奇素数时，Jacobi 符号就是 Legendre 符号。前者是后者的推广。



**注 2**：如果 $m$ 是奇素数，当 $\left(\frac{a}{m}\right) = 1$ 时，方程(2)有解。当 $m$ 不是奇素数时，这个结论不一定成立。例如，方程 $x^2 \equiv 5 \pmod 9$无解，但是

$$\left(\frac{5}{9}\right) = \left(\frac{5}{3}\right)\left(\frac{5}{3}\right) = 1。$$

尽管如此，利用雅各比符号仍可对方程(2)的无解性给出判断。事实上，如果方程(2)有解，$m = p_1 p_2 \cdots p_k$，则对于每个 $p_i$（$1 \le i \le k$），当 $p = p_i$ 时方程(1)有解，因此，由雅各比符号的定义可知 $\left(\frac{a}{m}\right) = 1$。这样，若 $\left(\frac{a}{m}\right) = -1$，则方程(2)必无解。

下面，我们研究雅各比符号的计算方法。

**定理 1**　使用定义 1 中的符号，下面的结论成立：

(ⅰ)　若 $a \equiv a_1 \pmod m$，则

$$\left(\frac{a}{m}\right) = \left(\frac{a_1}{m}\right); \tag{3}$$

(ⅱ)　$\left(\frac{1}{m}\right) = 1$；

(ⅲ)　对于任意的整数 $a_1, a_2, \cdots, a_t$，有

$$\left(\frac{a_1 a_2 \cdots a_t}{m}\right) = \left(\frac{a_1}{m}\right)\left(\frac{a_2}{m}\right)\cdots\left(\frac{a_t}{m}\right); \tag{4}$$

(ⅳ)　对于任意的整数 $a$，$b$，$(a, m) = 1$，有

$$\left(\frac{a^2 b}{m}\right) = \left(\frac{b}{m}\right)。 \tag{5}$$

**证明**　(ⅰ)　由 $a \equiv a_1 \pmod m$，可知

$$a \equiv a_1 \pmod{p_i},\ 1 \le i \le k,$$

因此

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

$$= \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\cdots\left(\frac{a_1}{p_k}\right) = \left(\frac{a_1}{m}\right),$$

结论(ⅱ)，(iii)，(iv)的证明留作习题。

**引理** 设 $a_i \equiv 1 \pmod m$，$1 \le i \le k$，$a = a_1 a_2 \cdots a_k$，则

$$\frac{a-1}{m} \equiv \frac{a_1 - 1}{m} + \cdots + \frac{a_k - 1}{m} \pmod m。 \tag{6}$$

**证明** 由假设条件，存在整数 $b_i \in \mathbf{N}$， 使得 $a_i = 1 + b_i m$（$1 \le i \le k$），因此

$$\begin{aligned} a - 1 &= a_1 a_2 \cdots a_k - 1 \\ &= (1 + b_1 m)(1 + b_2 m) \cdots (1 + b_k m) - 1 \\ &= m(b_1 + b_2 + \cdots + b_k) + m^2 A, \end{aligned}$$

其中 $A$ 是某个整数。于是

$$\begin{aligned} \frac{a-1}{m} &\equiv b_1 + b_2 \cdots + b_k \\ &= \frac{a_1 - 1}{m} + \frac{a_2 - 1}{m} + \cdots + \frac{a_k - 1}{m} \pmod m。 \end{aligned}$$

证毕。

**定理 2** 设 $m = p_1 p_2 \cdots p_k$ 是奇数，其中 $p_1, p_2, \cdots p_k$ 是素数，则下面的结论成立：

(ⅰ) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$；

(ⅱ) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$。

**证明** 由定义 1 及第五节定理 3，有

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_1-1}{2} + \frac{p_2-1}{2} + \cdots + \frac{p_k-1}{2}},$$

由此及式(6)推出结论(ⅰ)。

由定义 1 及第六节定理 1，有

$$\left(\frac{2}{m}\right) = \prod_{i=1}^{k} \left(\frac{2}{p_i}\right) = (-1)^{\frac{p_1^2-1}{8} + \frac{p_2^2-1}{8} + \cdots + \frac{p_k^2-1}{8}},$$

由此及式(6)推出结论(ⅱ)。证毕。

**定理 3** 设 $m$，$n$ 是大于 1 的奇整数，则

$$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \left(\frac{m}{n}\right)。 \tag{7}$$

**证明** 若$(m, n) > 1$，则由定义 1 可知式(7)成立。

若$(m, n) = 1$，设

$$m = p_1 p_2 \cdots p_k，\ n = q_1 q_2 \cdots p_l，$$

其中 $p_i$，$q_j$（$1 \le i \le k$，$1 \le j \le l$）都是素数，$(p_i, q_j) = 1$（$1 \le i \le k$，$1 \le j \le l$），则由定义 1 及第六节定理 2，有

$$\begin{aligned} \left(\frac{n}{m}\right) &= \prod_{i=1}^{k} \left(\frac{n}{p_i}\right) = \prod_{i=1}^{k} \prod_{j=1}^{l} \left(\frac{q_j}{p_i}\right) \\ &= \prod_{i=1}^{k} \prod_{j=1}^{l} (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} \left(\frac{p_i}{q_j}\right) \\ &= \prod_{i=1}^{k} \prod_{j=1}^{l} (-1)^{\frac{p_i-1}{2} \frac{q_j-1}{2}} \prod_{i=1}^{k} \prod_{j=1}^{l} \left(\frac{p_i}{q_j}\right) \\ &= (-1)^{\delta} \prod_{i=1}^{k} \left(\frac{p_i}{n}\right) = (-1)^{\delta} \left(\frac{m}{n}\right)， \end{aligned} \tag{8}$$

其中

$$\delta = \sum_{i=1}^{k} \sum_{j=1}^{l} \frac{p_i - 1}{2} \frac{q_j - 1}{2}。$$

由引理，因为 $2 \nmid n$， $2 \nmid m$，我们见到

$$\delta = \sum_{i=1}^{k} \frac{p_i - 1}{2} \sum_{j=1}^{l} \frac{q_j - 1}{2} \equiv \sum_{i=1}^{k} \frac{p_i - 1}{2} \cdot \frac{n-1}{2} \equiv \frac{m-1}{2} \cdot \frac{n-1}{2} \pmod 2。$$

将此式代入式(8)，得到式(7)。证毕。

利用以上定理，我们可以很容易地计算 Jacobi 符号，特别是 Legendre 符号的数值。但是，必须注意，如同在定义 1 的注 2 中指出的，在判断方程(2)的可解性时，Legendre 符号和 Jacobi 的作用是不一样的。对于一般的正奇数 $m$ 来说，$\left(\frac{a}{m}\right) = 1$ 并不能保证方程(2)有解。

**例 1** 设 $a$ 与 $b$ 是正奇数，求 $\left(\frac{2a}{4a+b}\right)$与$\left(\frac{b}{a}\right)$ 的关系。

**解** 我们有

$$\left(\frac{2a}{4a+b}\right)=\left(\frac{2}{4a+b}\right)\left(\frac{a}{4a+b}\right)=(-1)^{\frac{(4a+b)^2-1}{8}}\left(\frac{a}{4a+b}\right)$$

$$=(-1)^{ab+\frac{b^2-1}{8}}(-1)^{\frac{a-1}{2}\cdot\frac{4a+b-1}{2}}\left(\frac{4a+b}{a}\right)$$

$$=(-1)^{1+\frac{b^2-1}{8}+\frac{a-1}{2}\cdot\frac{b-1}{2}}\left(\frac{b}{a}\right)。$$

**例 2** 已知 3371 是素数，判断方程

$$x^2\equiv 12345 \pmod{3371} \tag{9}$$

是否有解。

**解** 利用 Jacobi 符号的性质，有

$$\left(\frac{12345}{3371}\right)=\left(\frac{2232}{3371}\right)=\left(\frac{2}{3371}\right)\left(\frac{4}{3371}\right)\left(\frac{279}{3371}\right)$$

$$=(-1)^{\frac{3371^2-1}{8}}(-1)^{\frac{3371-1}{2}\cdot\frac{279-1}{2}}\left(\frac{23}{279}\right)$$

$$=\left(\frac{23}{279}\right)=(-1)^{\frac{279-1}{2}\cdot\frac{23-1}{2}}\left(\frac{279}{23}\right)$$

$$=-\left(\frac{3}{23}\right)=-(-1)^{\frac{23-1}{2}\cdot\frac{3-1}{2}}\left(\frac{23}{3}\right)=-1。$$

因此，方程(9)无解。

**注：**在上面例题中，如果用计算 Legendre 符号的数值来判定方程的可解性，将比这里的方法繁复许多。

## 习 题 七

**1.** 证明定理的结论(ⅱ)，(iii)，(ⅳ)。

**2.** 已知 3019 是素数，判定方程 $x^2\equiv 374 \pmod{3019}$是否有解。

**3.** 设奇素数为 $p=4n+1$ 型，且 $d\mid n$，证明：$\left(\frac{d}{p}\right)=1$。



**4.** 设 $p,q$ 是两个不同的奇素数，且 $p=q+4a$，证明：$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$。

**5.** 设 $a>0$，$b>0$，$b$ 为奇数，证明：

$$\left(\frac{a}{2a+b}\right)=\begin{cases}\left(\frac{a}{b}\right) & 当a\equiv 0,1 \pmod 4\\ -\left(\frac{a}{b}\right) & 当a\equiv 2,3 \pmod 4。\end{cases}$$

**6.** 设 $a,b,c$ 是正整数，$(a,b)=1,2\nmid b,b<4ac$，求$\left(\frac{a}{4ac-b}\right)$与$\left(\frac{a}{b}\right)$的关系。

# 第六章　平方和

本章中要研究整数用整数的平方数之和表示的可能性，即对于给定的整数 $n$，是否存在整数 $x_1$，$x_2$，$x_3$，$x_4$，使得

$$n=x_1^2+x_2^2,\quad n=x_1^2+x_2^2+x_3^2,\quad n=x_1^2+x_2^2+x_3^2+x_4^2$$

成立？以下，“平方和”或“平方数之和”是指“整数的平方数之和”。

## 第一节　二平方之和

**定理 1**　若正整数 $n$ 可以表示成两个整数的平方之和，则在它的标准分解式

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

中，形如 $4k+3$ 的素因数的指数是偶数。

**证明**　设 $n=x^2+y^2$，$p_i$ 是 $n$ 的形如 $4k+3$ 的素因数。记 $p^{\alpha}=p_i^{a_i}$，则

$$p^{\alpha}\mid n,\quad p^{\alpha+1}\nmid n,\quad x^2+y^2\equiv 0\ (\mathrm{mod}\ p^{\alpha})。\tag{1}$$

（ⅰ）　若 $p\nmid y$，则存在整数 $y'$，使得 $yy'\equiv 1\ (\mathrm{mod}\ p)$，于是由式(1)得到

$$(xy')^2+1\equiv 0\ (\mathrm{mod}\ p),$$

即 $-1\in QR(p)$。因此由第五章第五节定理 3 推论，有

$$p=2\ 或\ p\equiv 1(\mathrm{mod}\ 4),$$

这是不可能的。

（ⅱ）　若 $p\mid y$，则由式(1)可知 $p\mid x$，以及

$$\left(\frac{x}{p}\right)^2+\left(\frac{y}{p}\right)^2\equiv 0\ (\mathrm{mod}\ p^{\alpha-2})。\tag{2}$$

下面说明，$\alpha$必是偶数，否则，将导致矛盾。

若$\alpha=2m+1$，则类似于上面的推导，依次得到



$$\left(\frac{x}{p^2}\right)^2+\left(\frac{y}{p^2}\right)^2\equiv 0\ (\mathrm{mod}\ p^{\alpha-4})。$$

$$\left(\frac{x}{p^3}\right)^2+\left(\frac{y}{p^3}\right)^2\equiv 0\ (\mathrm{mod}\ p^{\alpha-6})。$$

$$\cdots\cdots$$

$$\left(\frac{x}{p^m}\right)^2+\left(\frac{y}{p^m}\right)^2\equiv 0\ (\mathrm{mod}\ p)。\tag{3}$$

若 $p\nmid \dfrac{y}{p^m}$，则由结论(ⅰ)可知 $p\equiv 1\ (\mathrm{mod}\ 4)$，这不可能，所以 $p^{m+1}\mid y$，从而 $p^{m+1}\mid x$，于是 $p^{\alpha+1}=p^{2(m+1)}\mid n$，这与式(1)矛盾。证毕。

**引理**　设 $n$，$m$，$x$，$y$，和 $k$ 都是整数，$p$ 是素数，

$$x^2+y^2=p,\quad n^2+m^2=pk,\tag{4}$$

则 $k$ 可以表示成二平方之和。

**证明**　由式(4)，有

$$n^2\equiv -m^2\ (\mathrm{mod}\ p),\quad x^2\equiv -y^2\ (\mathrm{mod}\ p),\tag{5}$$

$$n^2x^2\equiv m^2y^2\ (\mathrm{mod}\ p),$$

$$(nx-my)(nx+my)\equiv 0\ (\mathrm{mod}\ p),$$

因此，必有

$$nx\equiv my\ \ 或\ \ nx\equiv -my\ (\mathrm{mod}\ p)。$$

若 $nx\equiv my\ (\mathrm{mod}\ p)$，则由式(4)得

$$(nx-my)^2+(ny+mx)^2=(x^2+y^2)(n^2+m^2)=p^2k,$$

于是 $p\mid ny+mx$，因此

$$\left(\frac{nx-my}{p}\right)^2+\left(\frac{ny+mx}{p}\right)^2=k。$$

若 $nx\equiv -my\ (\mathrm{mod}\ p)$，类似地可以证明 $k$ 能表示成二平方数之和。证毕。

**定理 2**　对于任意的自然数 $n$，$n^2+1$ 的素因数都可以表示成二平方数之和。

**证明**　用归纳法。

当 $n=1$ 时，结论显然成立。

假设当 $n<m$（$m>1$）时，$n^2+1$ 的每一个素因数都可以表示成二

平方数之和。

设

$$m^2+1=p_1p_2\cdots p_k\ , \tag{6}$$

其中 $p_i$（$1\le i\le k$）是素数，$p_1\le p_2\le\cdots\le p_k$ 。

（ⅰ） 如果 $p_k<m$，那么对于任何 $i$，$1\le i\le k$，都有 $p_i<m$，因此 $m-p_i<m$，并且 $p_i\mid(m-p_i)^2+1$，所以，由归纳假设，$p_i$ 可以表示成二平方数之和。

（ⅱ） 如果 $p_k\ge m$，则由式(6)可知 $p_k\ge m+1$，于是

$$p_i<m\ （1\le i\le k-1），$$

所以，由结论（ⅰ），$p_1,p_2,\cdots,p_{k-1}$ 都可以表示成二平方数之和。因此，依次利用引理，可知

$$\frac{m^2+1}{p_1},\quad \frac{m^2+1}{p_2p_1},\quad \cdots,\quad \frac{m^2+1}{p_{k-2}p_{k-3}\cdots p_1},\quad \frac{m^2+1}{p_{k-1}p_{k-2}\cdots p_1}$$

都可以表示成二平方数之和。最终一个数就是 $p_k$ 。这证明了定理对于 $n=m$ 成立。

由归纳法证得定理。证毕。

**定理 3** 正整数 $n$ 能表示成二平方数之和的充要条件，是在它的标准分解式中，形如 $4k+3$ 的素因数的指数是偶数。

**证明** 由定理 1，只需证明充分性。设

$$n=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}q_1^{2\beta_1}\cdots q_s^{2\beta_s}\ ,$$

其中 $p_i$（$1\le i\le r$）是形如 $4k+1$ 的素数，$q_i$（$1\le i\le s$）是形如 $4k+3$ 的素数。对于每个 $p_i$，由第五章第五节定理 3，有 $-1\in QR(p_i)$，即存在整数 $n_i$ 使得

$$n_i^2\equiv -1\ (\mathrm{mod}\ p_i)，\ p_i\mid n_i^2+1。$$

由此及定理 2，$p_i$（$1\le i\le r$）可以表示成二平方数之和。显然

$$2=1^2+1^2，\ \ q_i^{2\beta_i}=(q_i^{\beta_i})^2+0^2\ （1\le i\le s）$$

都是二平方数之和，因此，$n$ 是若干个二平方和的乘积。利用恒等式

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$$

可知 $n$ 是二平方数之和。证毕。

**例 1** 正整数 $n$ 能表示成不同的两个平方数之差的充要条件是

$$n\not\equiv 2\ (\mathrm{mod}\ 4)。 \tag{7}$$



**解** 必要性 对任意的整数 $x$，$x^2\equiv 0$ 或 $1(\mathrm{mod}\ 4)$，因此，对于任意的整数 $x$，$y$，有

$$x^2-y^2\equiv 0，\ 1，\ 3\ (\mathrm{mod}\ 4)。 \tag{8}$$

必要性得证。

充分性 若 $n\equiv 1$ 或 $3\ (\mathrm{mod}\ 4)$，则 $n+1$ 与 $n-1$ 都是偶数，于是

$$n=\left(\frac{n+1}{2}\right)^2-\left(\frac{n-1}{2}\right)^2。$$

若 $n\equiv 0\ (\mathrm{mod}\ 4)$，则

$$n=\left(\frac{n}{4}+1\right)^2-\left(\frac{n}{4}-1\right)^2。$$

**例 2** 设 $p$ 是素数，$a\ge b>0$，$x\ge y>0$，$(a,b)=(x,y)=1$，且

$$p=a^2+b^2=x^2+y^2, \tag{9}$$

则 $a=x$，$b=y$。

**解** 由定理 1，$p=2$ 或 $p\equiv 1\ (\mathrm{mod}\ 4)$。

若 $p=2$，结论显然成立。

若 $p\equiv 1\ (\mathrm{mod}\ 4)$，由第五章第五节定理 3 推论，存在整数 $c$，使得

$$c^2\equiv -1\ (\mathrm{mod}\ p)，\ c\ne 0。 \tag{10}$$

由式(9)及式(10)，有

$$a^2+b^2\equiv 0\ (\mathrm{mod}\ p)，$$
$$a^2\equiv -b^2\ (\mathrm{mod}\ p)，$$
$$a^2\equiv c^2b^2\ (\mathrm{mod}\ p)，$$

即

$$a^2-c^2b^2\equiv 0\ (\mathrm{mod}\ p)，$$

所以

$$a\equiv cb\ 或\ a\equiv -cb\ (\mathrm{mod}\ p)。 \tag{11}$$

同理，有

$$x\equiv cy\ 或\ x\equiv -cy\ (\mathrm{mod}\ p)。 \tag{12}$$

由式(11)与式(12)，可知下面四种情形可能发生：

（ⅰ） $a\equiv cb\ (\mathrm{mod}\ p)$，$x\equiv cy\ (\mathrm{mod}\ p)$；

（ⅱ） $a\equiv -cb\ (\mathrm{mod}\ p)$，$x\equiv cy\ (\mathrm{mod}\ p)$；

（ⅲ） $a\equiv cb\ (\mathrm{mod}\ p)$，$x\equiv -cy\ (\mathrm{mod}\ p)$；

（ⅳ） $a\equiv -cb\ (\mathrm{mod}\ p)$，$x\equiv -cy\ (\mathrm{mod}\ p)$。

假设情形（ⅰ）发生，则

$$ay \equiv cby \pmod p,\quad bx \equiv cby \pmod p,$$
$$ay \equiv bx \pmod p。 \tag{13}$$

利用式(9)，有

$$p^2 = (ax + by)^2 + (ay - bx)^2, \tag{14}$$
$$(ay - bx)^2 < p^2。$$

因此，由上式及式(13)得到 $ay = bx$。由于$(a, b) = (x, y) = 1$，所以由式(14)可得到 $a = x$，$b = y$。

在情形(ⅱ)，(ⅲ)，(ⅳ)发生时，可用同样方法进行证明。

## 习 题 一

**1.** 设 $n$ 是正整数，证明：不定方程 $x^2 + y^2 = z^n$ 总有正整数解 $x$，$y$，$z$。

**2.** 设 $p$ 是奇素数，$(k, p) = 1$，则

$$\sum_{i=0}^{p-1}\left(\frac{i(i+k)}{p}\right) = -1,$$

此处$\left(\frac{a}{p}\right)$是 Legender 符号。

**3.** 设素数 $p \equiv 1 \pmod 4$，$(k, p) = 1$，记

$$S(k) = \sum_{i=0}^{p-1}\left(\frac{i(i^2+k)}{p}\right),$$

则 $2 \mid S(k)$，并且，对于任何整数 $t$，有

$$S(kt^2) = \left(\frac{t}{p}\right)S(k),$$

此处$\left(\frac{a}{p}\right)$是 Legender 符号。

**4.** 设 $p$ 是奇素数，$\left(\frac{m}{p}\right) = 1$，$\left(\frac{n}{p}\right) = -1$，则

$$m\cdot 1^2,\ m\cdot 2^2,\cdots,\ m\cdot\left(\frac{p-1}{2}\right)^2,\ n\cdot 1^2,\ n\cdot 2^2,\cdots,\ n\cdot\left(\frac{p-1}{2}\right)^2$$



构成模 $p$ 的一个简化剩余系。

**5.** 在第 3 题的条件下，并沿用第 2 题的记号，有

$$p = \left(\frac{1}{2}S(m)\right)^2 + \left(\frac{1}{2}S(n)\right)^2。$$

即上式给出了形如 $4k + 1$ 的素数的二平方和表示的具体方法。

**6.** 利用题 5 的结论，试将 $p = 13$ 写成二平方和。

## 第二节　四平方之和

本节要证明：任何正整数都可以表示成四平方数之和，并且指出，就平方数的个数而言，这是最佳结果。

**引理 1**　设素数 $p > 2$，则存在整数 $x_0$，$y_0$ 与 $m_0$，$1 \le m_0 < p$，使得

$$x_0^2 + y_0^2 + 1 = m_0 p。$$

**证明**　集合

$$A = \{\, 0^2, 1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2 \,\}$$

与

$$B = \{\, -1 - 0^2, -1 - 1^2, -1 - 2^2, \cdots, -1 - \left(\frac{p-1}{2}\right)^2 \,\}$$

都含有 $\frac{p+1}{2}$ 个元素，因此，在并集 $A \cup B$ 中必有两个数对模 $p$ 同余。

容易证明这两个数不可能同属于 $A$ 或 $B$，因此必有整数 $x_0, y_0$ 及 $m_0 \ge 1$，使得

$$x_0^2 + y_0^2 + 1 = m_0 p,\ \ 0 \le x_0, y_0 \le \frac{p-1}{2}。 \tag{1}$$

由于 $p > 2$，我们有

$$x_0^2 + y_0^2 + 1 \le 2\left(\frac{p-1}{2}\right)^2 + 1 = \frac{p^2}{2} - p + \frac{3}{2} < \frac{p^2}{2},$$

所以，$1 \le m_0 < p$。证毕。

**引理 2**　若 $a$ 与 $b$ 都可以表示成四平方数之和，则 $ab$ 也可表成四平方之和。

**证明** 设 $a=x_1^2+x_2^2+x_3^2+x_4^2$，$b=y_1^2+y_2^2+y_3^2+y_4^2$，由

$$\begin{aligned}&(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)\\&=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\&\quad+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2\end{aligned}$$

即可证明引理。证毕。

**定理 1** 每个素数 $p$ 都可以表示成四个平方数之和。

**证明** 不妨设 $p>2$。

由引理 1 可知，存在整数 $x_1$，$x_2$，$x_3$，$x_4$，$m_0$，$1\le m_0<p$ 使得

$$x_1^2+x_2^2+x_3^2+x_4^2=m_0p\ 。\tag{2}$$

不妨假设 $m_0$ 就是使式(2)成立的最小的正整数。

下面要证明 $m_0=1$。

(ⅰ) 首先，证明 $x_1$，$x_2$，$x_3$，$x_4$ 是互素的。记 $d=(x_1,x_2,x_3,x_4)$。若 $d>1$，则存在素数 $q\mid d$。由式(2)可知

$$q^2\mid m_0p\ 。\tag{3}$$

因为$(m,p)=1$，所以 $q^2\mid m_0$ 或 $q^2\mid p$。由 $m_0$ 的最小性，可知 $q^2\nmid m_0$。但是，因为 $p$ 是素数，所以 $q^2\mid p$ 也是不可能的。因此，必是 $d=1$。

(ⅱ) 其次，证明 $2\nmid m_0$。否则，若 $2\mid m_0$，则 $x_1$，$x_2$，$x_3$，$x_4$ 中奇数的个数必是偶数，所以不妨设 $2\mid x_1+x_2$，$2\mid x_3+x_4$，由此及式(2)得到

$$\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2=\frac{m_0}{2}p\ ,$$

这与 $m_0$ 的最小性矛盾。

(iii) 用反证法证明 $m_0=1$。若 $m_0>1$，则 $m_0\ge 3$，因此，存在整数 $y_1$，$y_2$，$y_3$，$y_4$，使得

$$y_i\equiv x_i\ (\mathrm{mod}\ m_0),\ |y_i|<\frac{m_0}{2}\ ,\ i=1,2,3,4。\tag{4}$$

如果 $y_1=y_2=y_3=y_4=0$，则 $x_1\equiv x_2\equiv x_3\equiv x_4\equiv 0\ (\mathrm{mod}\ m_0)$，由此及式(2)得到 $m_0\mid p$，$m_0=p$，这不可能，因此，整数 $y_1$，$y_2$，$y_3$，$y_4$ 不全为零。由式(2)，有

$$y_1^2+y_2^2+y_3^2+y_4^2\equiv x_1^2+x_2^2+x_3^2+x_4^2\equiv 0\ (\mathrm{mod}\ m_0)。$$

由此及



$$0<y_1^2+y_2^2+y_3^2+y_4^2<4\cdot\left(\frac{m_0}{2}\right)^2=m_0^2$$

可知存在整数 $m_1$，使得

$$y_1^2+y_2^2+y_3^2+y_4^2=m_0m_1，\ 0<m_1<m_0。\tag{5}$$

由引理 2 及式(2)可知，有

$$z_1^2+z_2^2+z_3^2+z_4^2=m_0^2m_1p，\tag{6}$$

其中

$$\begin{aligned}z_1&=x_1y_1+x_2y_2+x_3y_3+x_4y_4\equiv x_1^2+x_2^2+x_3^2+x_4^2\equiv 0\ (\mathrm{mod}\ m_0)，\\z_2&=x_1y_2-x_2y_1+x_3y_4-x_4y_3\equiv 0\ (\mathrm{mod}\ m_0)，\\z_3&=x_1y_3-x_3y_1+x_4y_2-x_2y_4\equiv 0\ (\mathrm{mod}\ m_0)，\\z_4&=x_1y_4-x_4y_1+x_2y_3-x_3y_2\equiv 0\ (\mathrm{mod}\ m_0)。\end{aligned}$$

因此，存在整数 $t_i$（$i=1$，2，3，4），使得

$$z_i=m_0t_i\ ，\ i=1，2，3，4。$$

代入式(6)，得到

$$t_1^2+t_2^2+t_3^2+t_4^2=m_1p，\ 0<m_1<m_0。$$

这与 $m_0$ 的最小性矛盾。这个矛盾说明 $m_0=1$，即素数 $p$ 可以表示成 $x_1^2+x_2^2+x_3^2+x_4^2$。证毕。

**定理 2** 每个正整数都可以表示成四平方之和。

**证明** 由定理 1 和引理 2，再利用算术基本定理，即可得证。证毕。

下面的定理说明，若将定理中的四平方和改为三平方和，则定理 2 不成立。

**定理 3** 若 $n$ 是形如 $4^m(8k+7)$（$m\ge 0$，$k\ge 0$）的整数，则 $n$ 不能表成三平方之和。

**证明** 使用归纳法。对任意的整数 $x$，有

$$x^2\equiv 0，1\text{ 或 }4\ (\mathrm{mod}\ 8)，\tag{7}$$

因此，对任意的整数 $x_1$，$x_2$，$x_3$，有

$$x_1^2+x_2^2+x_3^2\not\equiv 7\ (\mathrm{mod}\ 8)，$$

即形如 $8k+7$（$k\ge 0$）的整数不能表成三平方数之和，定理结论对于 $m=0$，$k\ge 0$ 成立。

假设定理结论对于 $r<m$（$m\ge 1$）成立，即形如 $4^r(8k+7)$（$0\le r<m$，$k\ge 0$）的整数不能表成三平方之和。那么，形如 $4^m(8k+7)$（$k\ge 0$）的整数必不能表成三平方之和。事实上，若有整数 $x_1$，$x_2$，$x_3$，使得

$$x_1^2 + x_2^2 + x_3^2 = n = 4^m(8k+7), \tag{8}$$

则由式(7)容易看出 $2 \mid x_1$，$2 \mid x_2$，$2 \mid x_3$，于是由式(8)得到

$$\left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2 = 4^{m-1}(8k+7),$$

这与归纳假设矛盾。所以式(8)不能成立，即定理当 $r = m$ 时成立。定理由归纳法得证。证毕。

**例 1**　每个正整数 $n$ 可以写成 $n = x^2 + y^2 - z^2$ 的形式，其中 $x$，$y$，$z$ 是整数。

**解**　当 $2 \mid n$ 时，

$$n = 1^2 + \left(\frac{n}{2}\right)^2 - \left(\frac{n}{2} - 1\right)^2;$$

当 $2 \nmid n$ 时，

$$n = 0^2 + \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2。$$

**例 2**　若 $n = 2 \cdot 4^m$（$m \in \mathbf{N}$），则 $n$ 不能表示成四个正整数的平方之和。

**解**　当 $m = 0$ 时，结论显然成立。

设结论对于 $k < m$（$m \geq 1$）成立，即形如 $n = 2 \cdot 4^k$（$k < m$，$k \in \mathbf{N}$）的整数不能表示成四个正整数平方之和。

若有正整数 $a$，$b$，$c$，$d$，使得

$$a^2 + b^2 + c^2 + d^2 = 2 \cdot 4^m, \tag{9}$$

那么，因为任何奇数的平方被 8 除的余数是 1，所以，由式(9)可知，$2 \mid (a, b, c, d)$，于是有

$$\left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2 + \left(\frac{d}{2}\right)^2 = 2 \cdot 4^{m-1}。$$

但是，由归纳假设，上式不可能成立，所以式(9)不能成立， 即结论当 $k = m$ 时也成立，由归纳法得证。证毕。

## 习 题 二

**1.** 若 $(x, y, z) = 1$，则不存在整数 $n$，使得

$$x^2 + y^2 + z^2 = 4n^2。$$



**2.** 设 $k$ 是非负整数，证明 $2^k$ 不能表示三个正整数平方之和。

**3.** 证明：每一个正整数 $n$ 必可以表示为 5 个立方数的代数和。

**4.** 证明：$16k + 15$ 型的整数至少需要 15 个四次方数的和表之。

**5.** 证明：$16^k \cdot 31$ 不能表示为 15 个四次方数的和。

# 第七章　原 根

原根是数论的理论和应用中一个很重要的概念。本章要介绍原根以及与它有关的基本知识。

## 第一节　指数及其基本性质

**定义 1**　设 $m>1$，$(a, m)=1$，则使

$$a^r \equiv 1 \pmod m \tag{1}$$

成立的最小的正整数 $r$，称为 $a$ 对模 $m$ 的指数，记为 $\delta_m(a)$，在不致误会的情况下，简记为 $\delta(a)$。

由 Euler 定理，当 $r=\varphi(m)$ 时式(1)成立，因此，恒有 $\delta_m(a) \le \varphi(m)$。

若 $a \equiv b \pmod m$，$(a, m)=1$，则显然有 $\delta_m(a)=\delta_m(b)$。

**定义 2**　若 $\delta_m(a)=\varphi(m)$，则称 $a$ 是模 $m$ 的原根。

例如，当 $m=7$ 时，因为

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1 \pmod 7,$$

所以 $\delta_7(2)=3$。又因为

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \pmod 7,$$

所以 $\delta_7(3)=6=\varphi(7)$，3 是模 7 的原根。

以后，在谈到 $a$ 对模 $m$ 的指数时，总假定 $m>1$，$(a, m)=1$。

**定理 1**　记 $\delta=\delta_m(a)$，则

$$a^0, a^1, \cdots, a^{\delta-1}$$

对模 $m$ 两两不同余。

**证明**　用反证法。若有 $0 \le i<j \le \delta-1$，使得

$$a^i \equiv a^j \pmod m,$$

则由 $(a, m)=1$ 得到

$$a^{j-i} \equiv 1 \pmod m,$$

这与 $\delta=\delta_m(a)$ 的定义矛盾，所以定理成立。证毕。



定理 1 说明，若 $g$ 是模 $m$ 的原根，则

$$g^0, g^1, \cdots, g^{\varphi(m)-1}$$

构成模 $m$ 的简化剩余系。

**定理 2**　设 $\delta=\delta_m(a)$，$r$ 与 $r'$ 是正整数，则

$$a^r \equiv a^{r'} \pmod m \tag{2}$$

的充要条件是

$$r \equiv r' \pmod \delta。 \tag{3}$$

特别地，$a^r \equiv 1 \pmod m$ 的充要条件是 $\delta \mid r$。

**证明**　不妨设 $r>r'$。因为 $(a, m)=1$，所以式(2)等价于

$$a^{r-r'} \equiv 1 \pmod m。 \tag{4}$$

若式(4)成立，记 $r-r'=q\delta+t$，$q \in \mathbf{N}$，$0 \le t<\delta$，则由定义 1，有

$$a^t \equiv a^{q\delta+t}=a^{r-r'} \equiv 1 \pmod m。$$

由 $\delta_m(a)$ 的定义可知 $t=0$，即 $\delta \mid r-r'$，也即式(3)成立。必要性得证。

若式(3)成立，则存在 $q \in \mathbf{N}$，使得 $r-r'=q\delta$，则由定义 1，有

$$a^{r-r'}=a^{q\delta} \equiv 1 \pmod m,$$

即式(4)成立，从而式(2)成立，充分性得证。

取 $r'=0$，得到定理的第二个结论。证毕。

**推论**　$\delta_m(a) \mid \varphi(m)$。

**证明**　由 Euler 定理及定理 2 得证。

**定理 3**　设 $k$ 是非负整数，则

$$\delta_m(a^k)=\frac{\delta_m(a)}{(\delta_m(a), k)}。$$

**证明**　记 $\delta=\delta_m(a)$，$\delta'=\delta_m(a^k)$，$\delta''=\dfrac{\delta}{(\delta, k)}$，则由定理 2 及

$$a^{k\delta''} \equiv 1 \pmod m$$

可知

$$\delta' \mid \delta''。 \tag{5}$$

由定理 2 及 $a^{k\delta'}=(a^k)^{\delta'} \equiv 1 \pmod m$ 可知 $\delta \mid k\delta'$，因此

$$\delta''=\frac{\delta}{(\delta, k)} \mid \frac{k\delta'}{(\delta, k)}。 \tag{6}$$

由于 $\left(\dfrac{\delta}{(\delta,k)}, \dfrac{k}{(\delta,k)}\right)=1$，所以由式(6)可以推出 $\delta'' \mid \delta'$。由此及式(5)得

到$\delta'' = \delta'$。证毕。

**推论** 若$\delta_m(a) = kl$，$k > 0$，$l > 0$，则$\delta_m(a^k) = l$。

**定理 4** 等式

$$\delta_m(ab) = \delta_m(a)\delta_m(b) \tag{7}$$

与

$$(\delta_m(a), \delta_m(b)) = 1 \tag{8}$$

是等价的。

**证明** 记$\delta_1 = \delta_m(a)$，$\delta_2 = \delta_m(b)$，$\delta_3 = \delta_m(ab)$，$\lambda = [\delta_1, \delta_2]$。

若式(7)成立，则$\lambda \mid \delta_1\delta_2 = \delta_3$。由$\lambda$的定义和定理 2，以及

$$(ab)^{\lambda} = a^{\lambda}b^{\lambda} \equiv 1 \pmod m$$

又得到$\delta_3 \mid \lambda$。因此$\delta_3 = \lambda$，即$\delta_1\delta_2 = [\delta_1, \delta_2]$，所以$(\delta_1, \delta_2) = 1$，即式(8)成立。

若式(8)成立，则由定理 2 及

$$1 \equiv [(ab)^{\delta_3}]^{\delta_2} \equiv (ab)^{\delta_3\delta_2} \equiv a^{\delta_3\delta_2} \pmod m$$

得到$\delta_1 \mid \delta_2\delta_3$。由式(8)推出$\delta_1 \mid \delta_3$。同理可推出$\delta_2 \mid \delta_3$。所以

$$\lambda = [\delta_1, \delta_2] \mid \delta_3。$$

但是，由式(8)可知$[\delta_1, \delta_2] = \delta_1\delta_2$，所以

$$\delta_1\delta_2 \mid \delta_3。$$

另一方面，由定理 2 及

$$(ab)^{\delta_1\delta_2} \equiv 1 \pmod m$$

得到$\delta_3 \mid \delta_1\delta_2$。所以$\delta_3 = \delta_1\delta_2$，即式(7)成立。证毕。

**例 1** 求 1，2，3，4，5，6 对模 7 的指数。

根据定义 1 直接计算，得到

$$\delta_7(1) = 1，\ \delta_7(2) = 3，\ \delta_7(3) = 6，$$
$$\delta_7(4) = 3，\ \delta_7(5) = 6，\ \delta_7(6) = 2。$$

例 1 中的结果可列表如下：

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\delta_7(a)$ | 1 | 3 | 6 | 3 | 6 | 2 |

这样的表称为指数表。这个表就是模 7 的指数表。

下面是模 10 的指数表：



| $a$ | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| $\delta_{10}(a)$ | 1 | 4 | 4 | 2 |

**例 2** 若$(a, m) = 1$，$aa' \equiv 1 \pmod m$，则

$$\delta_m(a) = \delta_m(a')。$$

**解** 显然$(a', m) = 1$。要证明的结论由

$$a^d \equiv 1 \pmod m \Longleftrightarrow (a')^d \equiv 1 \pmod m$$

即可得出。

**例 3** 若$n \mid m$，则$\delta_n(a) \mid \delta_m(a)$。

**解** 由$n \mid m$及定理 2 有

$$a^{\delta_m(a)} \equiv 1 \pmod m \Longrightarrow a^{\delta_m(a)} \equiv 1 \pmod n \Longrightarrow \delta_n(a) \mid \delta_m(a)。$$

**例 4** 若$(m, n) = 1$，$(a, mn) = 1$，则

$$\delta_{mn}(a) = [\delta_m(a), \delta_n(a)]。 \tag{9}$$

**解** 记$\delta = \delta_{mn}(a)$，$\delta' = [\delta_m(a), \delta_n(a)]$，由例 3 有

$$\delta_m(a) \mid \delta，\ \delta_n(a) \mid \delta \Longrightarrow \delta' \mid \delta。 \tag{10}$$

又由

$$a^{\delta'} \equiv 1 \pmod m，\ a^{\delta'} \equiv 1 \pmod n$$

得到

$$a^{\delta'} \equiv 1 \pmod{mn}。$$

因此，由定理 2，有$\delta \mid \delta'$。由此及式(10)推出式(9)。

**例 5** 若$(m, n) = 1$，$a_1$，$a_2$是任意整数，$(a_1, m) = (a_2, n) = 1$，则存在整数$a$，$(a, mn) = 1$，使得

$$\delta_{mn}(a) = [\delta_m(a_1), \delta_n(a_2)]。$$

**解** 设方程组

$$\begin{cases} x \equiv a_1 \pmod m \\ x \equiv a_2 \pmod n \end{cases}$$

的解是$x \equiv a \pmod{mn}$，则$(a, mn) = 1$，并且由例 4 可知

$$\delta_{mn}(a) = [\delta_m(a), \delta_n(a)] = [\delta_m(a_1), \delta_n(a_2)]。$$

## 习 题 一

**1.** 写出模 11 的指数表。

**2.** 求模 14 的全部原根。

**3.** 设 $m>1$，模 $m$ 有原根，$d$ 是$\varphi(m)$的任一个正因数，证明：在模 $m$ 的简化剩余系中，恰有$\varphi(d)$个指数为 $d$ 的整数，并由此推出模 $m$ 的简化剩余系中恰有$\varphi(\varphi(m))$个原根。

**4.** 设 $m\geq 3$，$g$ 是模 $m$ 的原根，$x_1, x_2, \cdots, x_{\varphi(m)}$是模 $m$ 的简化剩余系，证明：

(ⅰ) $g^{\frac{\varphi(m)}{2}} \equiv -1 \pmod{m}$;

(ⅱ) $x_1x_2\cdots x_{\varphi(m)} \equiv -1 \pmod{m}$。

**5.** 设 $p=2^n+1$ 是一个奇素数，证明：模 $p$ 的全部二次非剩余就是模 $p$ 的全部原根。

**6.** 证明：

(ⅰ) 设 $p$ 奇素数，则 $M_p=2^p-1$ 的素因数必为 $2pk+1$ 型；

(ⅱ) 设 $n\geq 0$，则 $F_n=2^{2^n}+1$ 的素因数必为 $2^{n+1}k+1$ 型。

## 第二节　原 根

对于什么样的正整数 $m$，模 $m$ 的原根是存在的？这是本节要研究的问题。

为了叙述方便，对于正整数 $n$，设它的标准分解式是

$$n=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},$$

其中 $p_i$（$1\leq i\leq k$）是奇素数，记

$$\lambda(n)=[\varphi(2^{\alpha}),\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\cdots,\varphi(p_k^{\alpha_k})]。$$

**定理 1**　模 $m$ 有原根的必要条件是 $m=1$，2，4，$p^{\alpha}$或 $2p^{\alpha}$，其中 $p$ 是奇素数，$\alpha\geq 1$。

**证明**　若 $m$ 不具备定理中所述形式，则必是

$$m=2^{\alpha}\ (\alpha\geq 3), \tag{1}$$

$$m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\ (\alpha\geq 2,\ k\geq 1), \tag{2}$$

或

$$m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\ (\alpha\geq 0,\ k\geq 2), \tag{3}$$



其中 $p_i$（$1\leq i\leq k$）是奇素数，$\alpha_i$（$1\leq i\leq k$）是正整数。

如果 $m$ 是形如式(2)的数，那么对于任意的 $a$，$(a,m)=1$，有

$$a^{\varphi(2^{\alpha})}\equiv 1(\bmod 2^{\alpha}),$$

$$a^{\varphi(p_i^{\alpha_i})}\equiv 1(\bmod p_i^{\alpha_i}),\quad 1\leq i\leq k,$$

$$a^{\lambda(m)}\equiv 1(\bmod 2^{\alpha}),$$

$$a^{\lambda(m)}\equiv 1(\bmod p_i^{\alpha_i}),\quad 1\leq i\leq k,$$

$$a^{\lambda(m)}\equiv 1 \pmod{m}。 \tag{4}$$

容易验证

$$\lambda(m)<\varphi(m)。$$

因此，由式(4)可知，任何与 $m$ 互素的数 $a$ 不是模 $m$ 的原根。

同样方法可以证明，若 $m$ 是形如式(1)或式(3)中的数，模 $m$ 也没有原根。证毕。

下面我们要证明，定理 1 中的条件也是充分条件。为此，先要证明几个引理。

**引理 1**　设 $m$ 是正整数。对任意的整数 $a$，$b$，一定存在整数 $c$，使得

$$\delta_m(c)=[\delta_m(a),\delta_m(b)]。$$

**证明**　由第一章第六节习题 6，存在正整数$\lambda_1$，$\lambda_2$，$\mu_1$，$\mu_2$，使得

$$\delta_m(a)=\lambda_1\lambda_2,\quad \delta_m(b)=\mu_1\mu_2,\quad (\lambda_2,\mu_2)=1,$$

$$[\delta_m(a),\delta_m(b)]=\lambda_2\mu_2\ 。 \tag{5}$$

由第一节定理 3，有

$$\delta_m(a^{\lambda_1})=\lambda_2,\quad \delta_m(b^{\mu_1})=\mu_2\ ,$$

因此，由第一节定理 4 得到

$$\delta_m(a^{\lambda_1}b^{\mu_1})=\delta_m(a^{\lambda_1})\delta_m(b^{\mu_1})=\lambda_2\mu_2=[\delta_m(a),\delta_m(b)]。$$

取 $c=a^{\lambda_1}b^{\mu_1}$ 即可得证。证毕。

**引理 2**　若 $p$ 是奇素数，则模 $p$ 有原根。

**证明**　由引理 1 及归纳法容易证明，存在整数 $g$，$(g,p)=1$，使得

$$\delta=\delta_p(g)=[\delta_p(1),\delta_p(2),\cdots,\delta_p(p-1)]。$$

显然

$$\delta\mid p-1,\quad \delta_p(j)\mid\delta,\quad 1\leq j\leq p-1。 \tag{6}$$

另一方面，由式（6）可知同余方程

$$x^{\delta}-1\equiv 0 \pmod p$$

有解 $x\equiv i \pmod p$，$1\le i\le p-1$。所以，由第五章第四节定理 2，可知，$p-1\le\delta$。由此及式(6)，得到 $p-1=\delta$，即 $g$ 是模 $p$ 的原根。证毕。

**引理 3** 设 $p$ 是奇素数，$\alpha$是正整数，则模 $p^{\alpha}$有原根。

**证明** 不妨设$\alpha>1$。设 $g$ 是模 $p$ 的原根，则$(g,p)=1$。因此，存在整数 $x_0$，使得

$$g^{p-1}=1+px_0\ ,$$

因此，对于任意的整数 $t$，有

$$(g+pt)^{p-1}=g^{p-1}+p(p-1)tg^{p-2}+\cdots=1+p(x_0-g^{p-2}t)+p^2Q_2,$$

其中 $Q_2\in\mathbf{Z}$，即

$$(g+pt)^{p-1}\equiv 1+p(x_0-g^{p-2}t) \pmod{p^2}。\tag{7}$$

取

$$t_0=0,\quad 当\ p\nmid x_0;$$
$$t_0=1,\quad 当\ p\mid x_0,$$

则 $p\nmid x_0-g^{p-2}t_0=y_0$，于是

$$(g+pt_0)^{p-1}=1+py_0\not\equiv 1 \pmod{p^2},\ p\nmid y_0。\tag{8}$$

由式(8)，有

$$(g+pt_0)^{p(p-1)}=(1+py_0)^p=1+p^2y_1,$$

其中

$$y_1=y_0+\mathrm{C}_p^2y_0^2+\cdots+p^{p-2}y_0^p\equiv y_0 \pmod p。\tag{9}$$

因此，$p\nmid y_1$。类似地，由式(9)可以依次得到

$$\begin{aligned}&(g+pt_0)^{p^2(p-1)}=(1+p^2y_1)^p=1+p^3y_2\ ,\\&(g+pt_0)^{p^3(p-1)}=(1+p^3y_1)^p=1+p^4y_3\ ,\\&\quad\cdots\cdots\\&(g+pt_0)^{p^{\alpha-1}(p-1)}=(1+p^{\alpha-1}y_1)^p=1+p^{\alpha}y_{\alpha-1}\ ,\end{aligned}\tag{10}$$

其中 $y_{\alpha-1}\equiv y_{\alpha-2}\equiv\cdots\equiv y_0 \pmod p$。因此

$$p\nmid y_i,\ 0\le i\le\alpha-1。\tag{11}$$

由于 $g$ 是模 $p$ 的原根，所以 $g+pt_0$ 也是模 $p$ 的原根，设 $g+pt_0$ 对模 $p^{\alpha}$的指数是$\delta$，则有

$$(g+pt_0)^{\delta}\equiv 1 \pmod{p^{\alpha}},$$



$$(g+pt_0)^{\delta}\equiv 1 \pmod p,$$

因此，由指数的性质可知$\delta_p(g+pt_0)\mid\delta$，即 $p-1\mid\delta$。另一方面，由$\delta$的定义及第一节定理 2 的推论，有$\delta\mid\varphi(p^{\alpha})=p^{\alpha-1}(p-1)$，所以

$$\delta=p^{r-1}(p-1),\ 1\le r\le\alpha,$$

即

$$(g+pt)^{p^{r-1}(p-1)}\equiv 1 \pmod{p^{\alpha}}。\tag{12}$$

由式(10)，有

$$(g+pt)^{p^{r-1}(p-1)}=1+p^ry_{r-1}\ ,$$

所以，由上式及式(12)推出

$$1+p^ry_{r-1}\equiv 1 \pmod{p^{\alpha}},$$
$$p^ry_{r-1}\equiv 0 \pmod{p^{\alpha}}。$$

由此及式(11)得到 $r\ge\alpha$。所以 $r=\alpha$，即 $g+pt_0$ 是模 $p^{\alpha}$的原根。证毕。

**引理 4** 设 $p$ 是奇素数，$\alpha\ge 1$，则模 $2p^{\alpha}$有原根。

**证明** 设 $g$ 是模 $p^{\alpha}$的原根，则 $g+p^{\alpha}$也是模 $p^{\alpha}$的原根，以 $g_1$ 表示 $g$ 与 $g+p^{\alpha}$中的奇数，则

$$g_1^{\varphi(p^{\alpha})}\equiv 1 \pmod{p^{\alpha}},\ g_1\equiv 1 \pmod 2,$$

因为$(2,p)=1$，$\varphi(p^{\alpha})=\varphi(2p^{\alpha})$，所以

$$g_1^{\varphi(2p^{\alpha})}\equiv 1 \pmod{2p^{\alpha}}。\tag{13}$$

我们指出，不存在正整数 $r<\varphi(2p^{\alpha})$，使得

$$g_1^{\,r}\equiv 1 \pmod{2p^{\alpha}}。$$

否则，由上式得到

$$(g_1,p^{\alpha})=1,\ g_1^{\,r}\equiv 1 \pmod{p^{\alpha}},$$

从而 $g_1$ 不能是模 $p^{\alpha}$的原根。

以上证明了 $\delta_{2p^{\alpha}}(g_1)=\varphi(2p^{\alpha})$，即 $g_1$ 是模 $2p^{\alpha}$的原根。证毕。

**定理 2** 设 $p$ 是奇素数，$m=2$，4，$p^{\alpha}$，$2p^{\alpha}$，则模 $m$ 有原根。

**证明** 由引理 3 和引理 4，只需证明模 2 与模 4 有原根，这容易验证：1 是模 2 的原根，3 是模 4 的原根。证毕。

**定理 3** 设 $m>1$，$\varphi(m)$的所有不同的素因数是 $p_1,p_2,\cdots,p_k$，$(g,m)=1$，则 $g$ 是模 $m$ 的原根的充要条件是

$$g^{\frac{\varphi(m)}{p_i}}\not\equiv 1 \pmod m,\ 1\le i\le k。\tag{14}$$

**证明** （ⅰ） 必要性是显然的。

（ⅱ） 设式(14)成立。记$\delta=\delta_m(g)$，由第一节定理 2 推论，有$\delta\mid\varphi(m)$。若$\delta<\varphi(m)$，则$\dfrac{\varphi(m)}{\delta}>1$，所以，必有某个$p_i$（$1\le i\le k$），使得$p_i\mid\dfrac{\varphi(m)}{\delta}$，因此

$$\delta\mid\frac{\varphi(m)}{p_i},\quad g^{\frac{\varphi(m)}{p_i}}\equiv 1\ (\mathrm{mod}\ m),$$

这与式(14)矛盾。因此$\delta=\varphi(m)$，即 $g$ 是模 $m$ 的原根。证毕。

**例 1** 求模 7 的原根。

**解** 由第一节例题 1 可知模 7 有两个原根 3 和 5。

**例 2** 已知 5 是模 23 的原根，解同余方程

$$x^8\equiv 18\ (\mathrm{mod}\ 23)。\tag{15}$$

**解** 由第一节定理 1，$5^i\ (\mathrm{mod}\ 23)$（$i=0, 1, 2, \cdots, 21$）构成模 23 的简化系，列表为

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $5^i\ (\mathrm{mod}\ 23)$ | 1 | 5 | 2 | 10 | 4 | 20 | 8 | 17 | 16 | 11 | 9 |
| $i$ | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| $5^i\ (\mathrm{mod}\ 23)$ | 22 | 18 | 21 | 13 | 19 | 3 | 15 | 6 | 7 | 12 | 14 |

由上表可知$5^{12}\equiv 18\ (\mathrm{mod}\ 23)$。

设$x\equiv 5^y\ (\mathrm{mod}\ 23)$，$0\le y\le 22$，则由第一节定理 2，方程(15)等价于

$$8y\equiv 12\ (\mathrm{mod}\ 22)。\tag{16}$$

因为$(8, 22)=2\mid 12$，所以方程(16)有两个解：

$$y_1\equiv 7，\ y_2\equiv 18\ (\mathrm{mod}\ 22)。$$

因此，方程(15)有两个解

$$x_1\equiv 5^7\equiv 17，\quad x_2\equiv 5^{18}\equiv 6\ (\mathrm{mod}\ 23)。$$

**注**：若模 $m$ 有原根 $g$，则模 $m$ 的简化剩余系$A=\{a_1, a_2, \cdots, a_{\varphi(m)}\}$与集合$B=\{g^i;\ 1\le i\le\varphi(m)\}$有一个一一对应关系，即，对于任意的$a_0\in A$，存在唯一的$g^{i_0}\in B$，使得$a_0\equiv g^{i_0}\ (\mathrm{mod}\ m)$。此时，称 $i_0$ 是 $a_0$ 对模 $m$ 的以 $g$ 为底的指标，记为$i_0=\mathrm{ind}_g a_0$。从例 2 看出，利用指标的概念，我们可以将求解指数同余方程$x^n\equiv a\ (\mathrm{mod}\ m)$的问题转化为求解线性同余方程$n\mathrm{ind}_g x\equiv\mathrm{ind}_g a\ (\mathrm{mod}\ \varphi(m))$。



## 习 题 二

**1.** 求模 29 的最小正原根。

**2.** 分别求模$29^3$和模$2\cdot 29^3$的原根。

**3.** 解同余方程：$x^{12}\equiv 16\ (\mathrm{mod}\ 17)$。

**4.** 设 $p$ 和 $q=4p+1$ 都是素数，证明：2 是模 $q$ 的一个原根。

**5.** 设 $m\ge 3$，$g_1$ 和 $g_2$ 都是模 $m$ 的原根，则 $g=g_1g_2$ 不是模 $m$ 的原根。

**6.** 设 $p$ 是奇素数，证明：当且仅当 $p-1\nmid n$ 时，有

$$1^n+2^n+\cdots+(p-1)^n\equiv 0\ (\mathrm{mod}\ p)。$$

# 第八章　代数数与超越数

我们对于全体复数有不同的分类方法。例如，可以将它们分为整数和非整数，有理数和非有理数（无理数），实数和非实数，等等。本章要介绍一种对复数的分类方法：代数数与超越数，并且介绍这两类数的一些简单知识。

以下，若无特殊声明，“数”都是指一般意义下的复数。

## 第一节　代数数

**定义 1**　若$\alpha$满足有理系数代数方程

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0, \tag{1}$$

即$\alpha$是有理系数多项式$f(x)$的零点，则称$\alpha$是代数数；若 $a_{n-1},\ldots,a_0$ 都是整数，则称$\alpha$是代数整数。

例如，$\frac{i}{2}$，$a+b^{\frac{1}{n}}$（$a$，$b$，$n$ 是正整数）是代数数；$\sqrt{2}$，$\sqrt[3]{5}$ 是代数整数。

容易看出，定义 1 等价于下面的定义 1’。

**定义 1’**　设$\alpha$满足整系数代数方程

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0, \tag{2}$$

则称$\alpha$是代数数；若 $a_n=1$，　则称$\alpha$是代数整数。

**定义 2**　一个有理系数多项式若不能等于两个非常数的有理系数多项式的乘积，则称为不可约多项式。在定义 1’ 中，若 f(x)是不可约多项式，并且$(a_0,\cdots,a_n)=1$，则称$\alpha$是 n 次代数数，记为 $d(\alpha)=n$, 并称$h=h(\alpha)=\max(|a_0|,\cdots,|a_n|)$是它的高。

**定理 1**　两个代数数的和、差、积、商（分母不为零）是代数数。



**证明**　设 α 和 β 是代数数，它们分别是有理系数多项式

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

和

$$g(x)=x^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$$

的零点。设 f(x)和 g(x)的全部零点分别是 $\alpha_1,\cdots,\alpha_n$ 和 $\beta_1,\cdots,\beta_m$，则 $\alpha+\beta$ 是多项式

$$h(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-(\alpha_i+\beta_j))$$

的零点。显然，多项式 h(x) 的系数是 $\alpha_1,\cdots,\alpha_n$ 与 $\beta_1,\cdots,\beta_m$ 的对称多项式。因此，由对称多项式的性质，h(x)是有理系数多项式，即 $\alpha+\beta$ 是代数数。同样地可以证明 $\alpha-\beta$，$\alpha\beta$，以及 $\frac{\alpha}{\beta}(\beta\neq0)$ 是代数数（留作习题）。证毕。

**定理 2**　若$\alpha$是代数数，则存在正整数 m, 使得 $m\alpha$ 是代数整数。

**证明**　（留作习题）。

**定理 3**　设$\alpha\neq0$ 是代数数, 满足方程（2），则

$$\frac{1}{h+1}<|\alpha|<h+1, \tag{3}$$

其中 $h=\max(|a_0|,\cdots,|a_n|)$。

**证明**　若$\alpha\neq0$ 满足方程（2），则 $\frac{1}{\alpha}$ 满足方程

$$a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0,$$

因此，我们只需证明式(3)的右半部分。

如果$|\alpha|<h+1$ 不成立，则

$$|\alpha|\geq h+1。 \tag{4}$$

下面要说明，由此会推出一个矛盾。

事实上，由

$$a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0$$

我们得到

$$\alpha=-\frac{a_{n-1}}{a_n}-\frac{a_{n-2}}{a_n}\cdot\frac{1}{\alpha}-\cdots-\frac{a_1}{a_n}\left(\frac{1}{\alpha}\right)^{n-2}-\frac{a_0}{a_n}\left(\frac{1}{\alpha}\right)^{n-1}。$$

由此，利用式(4)及

$$1 \leqslant |a_i| \le h,\ 0 \le i \le \mathrm{n}, \tag{5}$$

我们得到

$$\begin{aligned} |\alpha| &\le h + \cdots + h\left|\frac{1}{\alpha}\right|^{n-1} \\ &\le h\left(1 + \frac{1}{h+1} + \cdots + \left(\frac{1}{h+1}\right)^{n-1}\right) \\ &< h\frac{1}{1-\frac{1}{h+1}} = h+1。 \end{aligned}$$

这与式(4)矛盾。这个矛盾说明式(4)不可能成立。证毕。

**例 1**　设$\alpha$是代数数，满足整系数代数方程

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0,$$

则对于任何正整数 $n$，有等式

$$(a_d\alpha)^n = A_{d-1}^{(n)}\alpha^{d-1} + A_{d-2}^{(n)}\alpha^{d-2} + \cdots + A_0^{(n)},$$

其中 $A_i^{(n)}$（$0 \le i \le d-1$）是绝对值不超过$(2\max(|a_0|, \cdots, |a_n|))^n$的整数。

**证明**　用归纳法。记 $h = \max(|a_0|, \cdots, |a_n|)$。

当 $n \le d-1$ 时，结论显然正确。

假设结论当 $n = k$（$k \ge d-1$）时成立，则存在整数 $A_i^{(k)}$（$0 \le i \le d-1$），使得

$$(a_d\alpha)^k = A_{d-1}^{(k)}\alpha^{d-1} + A_{d-2}^{(k)}\alpha^{d-2} + \cdots + A_0^{(k)},\ \ |A_i^{(k)}| \le (2h)^k。 \tag{6}$$

于是

$$\begin{aligned} (a_d\alpha)^{k+1} &= a_d\alpha(A_{d-1}^{(k)}\alpha^{d-1} + \cdots + A_0^{(k)}) \\ &= a_d A_{d-1}^{(k)}\alpha^d + \cdots + a_d A_0^{(k)}\alpha \\ &= A_{d-1}^{(k)}(-a_{d-1}\alpha^{d-1} - \cdots - a_0) + a_d A_{d-2}^{(k)}\alpha^{d-1} + \cdots + a_d A_0^{(k)}\alpha。 \end{aligned}$$

记

$$\begin{aligned} A_0^{(k+1)} &= -a_0 A_{d-1}^{(k)}, \\ A_i^{(k+1)} &= a_d A_{i-1}^{(k)} - a_i A_{d-1}^{(k)},\ \ 1 \le i \le d-1, \end{aligned}$$



则

$$(a_d\alpha)^{k+1} = A_{d-1}^{(k+1)}\alpha^{d-1} + A_{d-2}^{(k+1)}\alpha^{d-2} + \cdots + A_0^{(k+1)},$$

因此，由式(6)得到

$$|A_i^{(k+1)}| \le 2h(2h)^k = (2h)^{k+1},$$

即当 $n = k+1$ 时结论成立。由归纳法证得例 1 中的结论。

**例 2**　设数$\alpha \ne 0$，并且满足方程

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0,$$

(7)

其中 $a_1, a_2, \cdots, a_n$ 是任意的实数，并且

$$|a_i| \le i,\ 1 \le i \le n, \tag{8}$$

则

$$|\alpha| \le \frac{3+\sqrt{5}}{2}。$$

**解**　不妨设$|\alpha| > 1$。设$\lambda > 1$ 是任意固定的常数。如果

$$|\alpha| > \lambda, \tag{9}$$

那么，由式(7)，(8)及(9)，得到

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$$

以及

$$\begin{aligned} |\alpha^n| &\le |a_1||\alpha^{n-1}| + \cdots + |a_{n-1}||\alpha| + |a_n|, \\ |\alpha| &\le |a_1| + |a_2||\alpha|^{-1} + \cdots + |a_{n-1}||\alpha|^{-n+2} + |a_n||\alpha|^{-n+1} \\ &\le 1 + 2|\alpha|^{-1} + \cdots + (n-1)|\alpha|^{-n+2} + n|\alpha|^{-n+1} \\ &< \frac{1}{\left(1-\left|\frac{1}{\alpha}\right|\right)^2} = \frac{|\alpha|^2}{(|\alpha|-1)^2} \le \frac{\lambda^2}{(\lambda-1)^2}。 \end{aligned} \tag{10}$$

这样，若取$\lambda$使得

$$\lambda = \frac{\lambda^2}{(\lambda-1)^2}, \tag{11}$$

那么，式(10)就与式(9)矛盾，因此，式(9)不能成立，所以$|\alpha| \le \lambda$。从式(11)容易求出$\lambda = \frac{3+\sqrt{5}}{2}$，这就是要证的结论。

**注**：从这个例子中，可以看出式(3)中的 $h+1$ 是如何确定出来的。

## 习 题 一

**1.** 补足定理 1 的证明。
**2.** 证明定理 2。
**3.** 证明：有理数为代数整数的充要条件是这个有理数为整数。

# 第二节　超越数

除了代数数还有一类数，即超越数。本节将对代数数的有理逼近性质做一简单介绍，并构造一类超越数。

**定义 1**　不是代数数的数，称为超越数。

**定理 1**　超越数是存在的。

**证明**　用 $E_{n,h}$ 表示所有的次数为 $n$、系数绝对值不超过 $h$ 的整系数多项式的零点的集合，用 $A$ 表示所有代数数的集合，则

$$A=\bigcup_{n=1}^{\infty}\bigcup_{h=1}^{\infty}E_{n,h}\ 。$$

由于每个 $E_{n,h}$ 是有限集合，所以 $A$ 是一个可数集合。但是，全体复数的集合是不可数集合，因此，超越数是存在的。证毕。

这个定理肯定了超越数的存在性，但并未确切地举出超越数的例子。为了能构造一些具体的超越数，我们来证明一个定理。

**定理 1**(Liouville)　设$\alpha$是次数为 $d$ 的实代数无理数，则存在只与$\alpha$有关的正常数 $c=c(\alpha)$，使得对于任何整数 $p$，$q$，$(p,q)=1$，有

$$\left|\alpha-\frac{p}{q}\right|\geq\frac{c}{q^{d}}\ 。\tag{1}$$

**证明**　不妨设

$$\left|\alpha-\frac{p}{q}\right|\leq 1\ 。\tag{2}$$

设$\alpha$的最小多项式是 $f(x)$，则 $f(\alpha)=0$，于是，由微分学中值定理可知

$$-f\left(\frac{p}{q}\right)=f(\alpha)-f\left(\frac{p}{q}\right)=\left(\alpha-\frac{p}{q}\right)f'(\xi)\ ,\tag{3}$$



其中$\xi$是介于$\alpha$与 $\frac{p}{q}$ 之间的某个数，因此，由式(2)，有

$$|\xi-\alpha|\leq 1\ 。$$

以 $M$ 表示 $f'(x)$在区间$[-|\alpha|-1,|\alpha|+1]$中的最大值，则由式(3)得到

$$\left|\alpha-\frac{p}{q}\right|\geq\frac{1}{M}\left|f\left(\frac{p}{q}\right)\right|\ ,\tag{4}$$

因为 $f(x)$是不可约多项式，并且$\alpha$是无理数，所以 $d\geq 2$，因此 $f\left(\frac{p}{q}\right)\neq 0$，从而

$$\left|f\left(\frac{p}{q}\right)\right|\geq\frac{1}{q^{d}}\ ,$$

由此及式(4)得到式(1)，证毕。

**推论**　设$\alpha$是实无理数，若存在常数 $M$，有理数列 $\left\{\frac{p_n}{q_n}\right\}$，以及递增的实数列$\{s_n\}$，$s_n\to\infty$，使得

$$\left|\alpha-\frac{p_n}{q_n}\right|\leq\frac{M}{q_n^{s_n}}\tag{5}$$

对于 $n\geq 1$ 成立，则$\alpha$是超越数。

**证明**　若$\alpha$是代数数，设它的次数是 $d$，由定理 1，存在常数 $c$，使得

$$\left|\alpha-\frac{p_n}{q_n}\right|>\frac{c}{q_n^{d}}$$

对于所有的 $n\geq 1$ 成立，但是，由于 $s_n\to\infty$，当 $n$ 充分大时，这与式(5)矛盾，所以$\alpha$不能是代数数。证毕。

关于定理 1，有两点说明：

(ⅰ)　定理 1 表明，若$\alpha$是实的代数无理数，那么，它与有理数的差不能太小。

(ⅱ)　可以证明，式(1)右端的因数 $q^{-d}$ 能改进为 $q^{-(2+\varepsilon)}$，其中$\varepsilon>0$ 是任意常数，但是，不能改进为 $q^{-2}$。事实上，在第三章第三节中我们知道：对于任何无理数$\alpha$，都有无穷多个有理数 $\frac{p}{q}$，使得

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2},\ q>0,\ (p,q)=1。$$

现在，我们来构造具体的超越数。

设

$$r_1, r_2,\cdots, r_n, \cdots 与\ s_0, s_1,\cdots, s_n, \cdots$$

是严格增加的正整数列，满足条件

$$0=s_0\le r_1<s_1\le r_2<\cdots,\ \lim_{n\to\infty}\frac{s_n}{r_n}=\infty。\tag{6}$$

又设整数列 $a_1, a_2,\cdots, a_n, \cdots$ 满足条件

$$a_k=0\ (r_n<k<s_n,\ n=1,2,3,\cdots),\tag{7}$$

$$a_{r_n}\ne 0,\ a_{s_n}\ne 0,\ n=1,2,3,\cdots,\tag{8}$$

并且 $f(x)=\sum_{k=0}^{\infty}a_k x^k$ 的收敛半经是 1。

**定理 2**　设 $\frac{p}{q}$ 是区间(0, 1)中的有理数 $\frac{p}{q}$。若 $f\left(\frac{p}{q}\right)$ 不是有理数，则必是超越数。

**证明**　若 $\frac{p}{q}\in(0,1)$，则必存在 $x\in(0,1)$，使得 $\frac{p}{q}<x$。由于

$$f(x)=\sum_{k=0}^{\infty}a_k x^k$$

收敛，所以，存在常数 $M$，使得

$$|a_k x^k|\le M,\ k=0,1,2,\cdots。\tag{9}$$

由式(7)，对于任何正整数 $n$，有

$$f\left(\frac{p}{q}\right)-\sum_{k=0}^{r_n}a_k\left(\frac{p}{q}\right)^k=\sum_{k=s_n}^{\infty}a_k\left(\frac{p}{q}\right)^k=\sum_{k=s_n}^{\infty}a_k x^k\left(\frac{p}{qx}\right)^k。$$

记 $y=\frac{p}{qx}<1$，则由上式及式(9)得到

$$f\left(\frac{p}{q}\right)-\sum_{k=0}^{r_n}a_k\left(\frac{p}{q}\right)^k\le M\sum_{k=s_n}^{\infty}y^k=My^{s_n}\frac{1}{1-y}\le M' y^{s_n},\tag{10}$$

其中 $M'$是常数。由式(6)，我们有



$$M' y^{s_n}=M' q^{s_n\frac{\log y}{\log q}}=M' q^{-r_n\lambda_n},$$

其中

$$\lambda_n=-\frac{\log y}{\log q}\cdot\frac{s_n}{r_n}\to\infty,\quad n\to\infty\ 。$$

在式(10)中，$\sum_{k=0}^{r_n}a_k\left(\frac{p}{q}\right)^k$ 是一个分母 $\le q^{r_n}$ 的有理分数，因此，利用定理 1 的推论可知，若 $f(\alpha)$不是有理数，则它必是超越数。证毕。

**推论**　设正整数数列$\{r_n\}$满足条件

$$r_1<r_2<\cdots<r_n<r_{n+1}<\cdots,\ \frac{r_{n+1}}{r_n}\to\infty,\ n\to\infty,$$

则对于任何整数 $a\ge 2$，$\alpha=\sum_{n=1}^{\infty}a^{-r_n}$ 是超越数。

**证明**　由定理 2，只需证明$\alpha$不是有理数。设$\alpha$是有理数，$\alpha=\frac{p}{q}$，$p$ 与 $q$ 是互素的整数，记

$$\sum_{k=1}^{n}a^{-r_k}=\frac{p_n}{q_n},$$

则 $q_n\le a^{r_n}$，并且

$$0\ne\left|\alpha-\frac{p_n}{q_n}\right|=\left|\frac{p}{q}-\frac{p_n}{q_n}\right|\ge\frac{1}{qq_n}\ge\frac{1}{q}a^{-r_n}。\tag{11}$$

另一方面，由假设条件，存在 $N$，当 $k>N$ 时，有 $r_k\ge 2$，$r_{k+1}\ge 2r_k$，因此

$$r_{k+1}-r_k\ge r_k\ge 2,$$

于是，当 $n>N$ 时，有

$$r_{n+2}-r_{n+1}\ge 2,$$
$$r_{n+3}-r_{n+1}\ge 4,$$
$$r_{n+i}-r_{n+1}\ge 2(i-1),$$
$$\cdots\cdots$$

从而

$$\alpha-\frac{q_n}{p_n}=\sum_{k=n+1}^{\infty}a^{-r_k}=a^{-r_{n+1}}\sum_{k=n+1}^{\infty}a^{r_{n+1}-r_k}$$

$$\le a^{-r_{n+1}}(1-\sum_{i=2}^{\infty}a^{-2(i-1)})$$

$$=a^{-r_{n+1}}\left(1-\frac{1}{a^2-1}\right)=\frac{a^2-2}{a^2-1}a^{-r_{n+1}}\text{。}\qquad(12)$$

当 $n$ 充分大时，式(11)与式(12)矛盾，所以$\alpha$不是有理数。证毕。

**例** 下面的两个数是超越数：

(ⅰ) $\frac{1}{2}+\frac{1}{2^{2!}}+\frac{1}{2^{3!}}+\cdots+\frac{1}{2^{n!}}+\cdots$；

(ⅱ) $\frac{1}{2}+\frac{1}{2^{2^2}}+\frac{1}{2^{3^3}}+\cdots+\frac{1}{2^{n^n}}+\cdots$。

**解** 留作习题。

做为本节的结束语，我们指出，利用 Liouville 定理及定理 2 可以具体构造一些超越数。但是，能用它们来判定的超越数只是超越数集合中的很小一部分。对于给定的数的超越性的判定，常常是非常困难的。

## 习 题 二

**1.** 证明例中的结论。

**2.** 证明连分数

$$\frac{1}{10}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\cdots+\frac{1}{10^{n!}}+\cdots$$

是超越数。

**3.** 设$\xi$是一个超越数，$\alpha$是一个非零的代数数，证明：$\xi+\alpha$，$\xi\alpha$，$\frac{\xi}{\alpha}$都是超越数。



# 第三节 数 *e* 的超越性

本节要证明数 $e$ 是超越数。为此，首先证明一个定理。

**定理 1** 设 $f(x)$是实系数多项式，次数为 $m$，记

$$I(t)=\int_0^t e^{t-u}f(u)du\text{，}\qquad(1)$$

其中 $t$ 是任意实数，则

$$I(t)=e^t\sum_{i=0}^{m}f^{(i)}(0)-\sum_{i=0}^{m}f^{(i)}(t)\text{。}$$

**证明** 对于任意的正整数 $k$，$k\le m$，由分部积分得到

$$\int_0^t e^{-u}u^k du=-\int_0^t u^k de^{-u}=-t^k e^{-t}+k\int_0^t u^{k-1}e^{-u}du$$

$$=-t^k e^{-t}-k\int_0^t u^{k-1}de^{-u}$$

$$=-e^{-t}(t^k+kt^{k-1})+k(k-1)\int_0^t u^{k-2}e^{-u}du$$

$$=\cdots=-e^{-t}(t^k+kt^{k-1}+\cdots+k!)+k!$$

$$=-e^{-t}\sum_{i=0}^{k}\frac{d^i}{dx^i}(x^k)\Big|_{x=t}+\sum_{i=0}^{k}\frac{d^i}{dx^i}(x^k)\Big|_{x=0}\text{。}\qquad(2)$$

由于 $k\le m$，所以式(2)就是

$$\int_0^t e^{t-u}u^k du=-\sum_{i=0}^{m}\frac{d^i}{dx^i}(x^k)\Big|_{x=t}+e^t\sum_{i=0}^{m}\frac{d^i}{dx^i}(x^k)\Big|_{x=0}\text{。}\qquad(3)$$

设

$$f(x)=\sum_{i=0}^{m}a_k x^k\text{，}$$

则由式(3)得到

$$I(t)=\int_0^t e^{t-u}f(u)du=\int_0^t e^{t-u}\sum_{k=0}^{m}a_k u^k du$$

$$=\sum_{i=0}^{m}a_k\int_0^t e^{t-u}u^k du$$

$$=-\sum_{k=0}^{m}a_k\sum_{i=0}^{m}\frac{d^i}{dx^i}(x^k)\big|_{x=t}+e^t\sum_{k=0}^{m}a_k\sum_{i=0}^{m}\frac{d^i}{dx^i}(x^k)\big|_{x=0}$$

$$=-\sum_{i=0}^{m}\frac{d^i}{dx^i}(f(x))\big|_{x=t}+e^t\sum_{i=0}^{m}\frac{d^i}{dx^i}(f(x))\big|_{x=0}。$$

证毕。

为了证明数 $e$ 的超越性，我们要引进多项式

$$f(x)=\frac{1}{(p-1)!}x^{p-1}(x-1)^p\cdots(x-d)^p，\tag{4}$$

其中 $p$ 是素数，$d$ 是正整数。

**引理 1**　$f(x)$具有以下性质：

(ⅰ)　对于 $i=0, 1, \cdots, p-1$，有

$$f^{(i)}(x)=0，\ x=1, 2, \cdots, d;$$

(ⅱ)　对于 $i=p, p+1, \cdots, (d+1)p-1$，多项式 $f^{(i)}(x)$的系数都是整数且能被 $p$ 整除；

(ⅲ)　$f^{(p-1)}(0)=(-1)^{dp}(d!)^p$。

**证明**　留作习题。

**定理 2**　数 $e$ 是超越数。

**证明**　设 $e$ 是代数数，满足整系数代数方程

$$a_d x^d+a_{d-1}x^{d-1}+\cdots+a_0=0,\tag{5}$$

其中 $a_0\neq 0$。我们要由此导出一个矛盾。

记

$$F(x)=f(x)+f'(x)+\cdots+f^{(n)}(x),\tag{6}$$

其中 $f(x)$由式(4)定义，$n=(d+1)p-1$。

因为数 $e$ 满足方程(5)，由定理 1 得到

$$\sum_{k=0}^{d}a_k\int_0^k e^{k-u}f(u)du=F(0)\sum_{k=0}^{d}a_k e^k-\sum_{k=0}^{d}a_k F(k)$$



$$=-\sum_{k=0}^{d}a_k F(k)。\tag{7}$$

由引理 1 可知，

$$p\mid F(k)，\ k=1, 2, 3, \cdots, d,$$

并且在表示式

$$F(0)=f(0)+f'(0)+\cdots+f^{(p-1)}(0)+f^{(p)}(0)+\cdots+f^{((d+1)p-1)}(0)\tag{8}$$

中，有

$$f(0)=f'(0)=\cdots=f^{(p-2)}(0)=0,\tag{9}$$

$$p\mid(f^{(p)}(0)+\cdots+f^{((d+1)p-1)}(0))。\tag{10}$$

由引理 1 的结论(ⅲ)，有

$$f^{(p-1)}(0)=(-1)^{dp}(d!)^p,$$

将这个等式与式(8)，式(9)和式(10)联合，得到

$$F(0)\equiv(-1)^{dp}(d!)^p a_0\ (\mathrm{mod}\ p)$$

以及

$$\sum_{k=0}^{d}a_k F(k)\equiv(-1)^{dp}(d!)^p a_0\ (\mathrm{mod}\ p)。\tag{11}$$

另一方面，对于 $x\in[0, d]$，有

$$|f(x)|\leq\frac{1}{(p-1)!}d^{(d+1)p-1}\leq\frac{1}{(p-1)!}{M_1}^p，\tag{12}$$

其中 $M_1=d^{d+1}$。于是

$$\Big|\sum_{k=0}^{d}a_k\int_0^k e^{k-u}f(u)du\Big|\leq\frac{1}{(p-1)!}M_1^p\sum_{k=0}^{d}k\,|a_k|=\frac{1}{(p-1)!}M_1^p M_2，\tag{13}$$

其中 $M_2$ 是与 $p$ 无关的常数。

由式(7)与式(13)，得到

$$\Big|\sum_{k=0}^{d}a_k F(k)\Big|\leq\frac{1}{(p-1)!}M_1^p M_2。$$

因此，存在常数 $M_3$，使得当 $p>M_3$ 时，有

$$\Big|\sum_{k=0}^{d}a_k F(k)\Big|<1。\tag{14}$$

但是，当 $p>\max\{d, a_0\}$时，$p\nmid(d!)^p a_0$，因此，由式(11)可知，整数

$$\sum_{k=0}^{d} a_k F(k) \neq 0。 \tag{15}$$

这样，如果取 $p$ 充分大，使得 $p > \max\{d, a_0, M_3\}$，则式(14)与式(15)矛盾，这个矛盾说明，数 $e$ 不可能满足使任何形如(5)的代数方程。$e$ 是超越数。证毕。

在定理 2 的证明中，定理 1 的作用是很重要的，它把数 $e$ 的代数性质与函数的解析性质联系了起来。下面的关于数$\pi$的无理性的定理的证明，有类似的思路。

**引理 2** 设 $f(x)$是 $2n$ 次多项式，则对任意的实数 $t$，有

$$\int_0^t f(u)\sin u du = (F'(u)\sin u - F(u)\cos u)\Big|_0^t, \tag{16}$$

其中

$$F(x) = f(x) - f''(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x)。$$

**证明** 使用分部积分法即可。证毕。

**定理 3** $\pi$是无理数。

**证明** 设$\pi = \frac{a}{b}$，$a$ 与 $b$ 是正整数，$(a, b)=1$。我们将由此导出矛盾。

事实上，在式(16)中取 $t = \pi = \frac{a}{b}$，$f(x) = \frac{1}{n!}x^n(a - bx)^n$，则

$$\frac{1}{n!}\int_0^\pi u^n(a-bu)^n \sin u du = F(\pi) + F(0) = F\left(\frac{a}{b}\right) + F(0),$$

其中 $F(x)$见于引理 2。

但是，当 $0<x<\pi$ 且 $n$ 充分大时，有

$$0 < f(x)\sin x < \frac{\pi^n a^n}{n!} < \frac{1}{\pi},$$

$$0 < \frac{1}{n!}\int_0^\pi u^n(a-bu)^n \sin u du < 1。$$

因此，如果 $F\left(\frac{a}{b}\right) + F(0)$是整数，就得到一个矛盾，从而证得定理。

可以证明，$F\left(\frac{a}{b}\right) + F(0)$是非零整数（留作习题）。证毕。



## 习 题 三

**1.** 证明引理 1。

**2.** 证明定理 3 中的 $F\left(\frac{a}{b}\right) + F(0)$是整数。

# 第九章　数论的应用

在一个很长的时期里，数论被认为是很难有应用价值的。但是，二十世纪中后期，数论的应用，特别是在密码学等学科中的应用，改变了人们的看法，数论的研究也增加了新的内容。在这一章中我们要介绍数论的几个应用。

## 第一节　计算星期几

要知道几十天以后的某一天是星期几，这是不难的，因为只要计算一下被 7 除的余数就可以了。但是，如果要知道几十年以后的某一天是星期几，那就比较困难了，因为在这段时间里有闰年，而且，每个月所含的天数也不一样。在这一节，我们要给出一个公式，可以方便地解决这个问题。

按现行的公历历法，每年有 365 天，若这一年是闰年，则有 366 天，二月有二十九天。闰年是这样确定的：公元年份数不被 100 整除但被 4 整除，或者年份数被 400 整除。

如果某一年是闰年，这一年的二月比正常年份的二月多一天，这样，从这一年的三月一日开始，星期数都受到这闰月的影响，同时，这一年的一月和二月里的星期数却不受影响。这样，就使得同一年里的计算有些不方便。所以，为了计算方便，我们把三月一日作为计算星期数的基点。

1600 年以来，全世界大部分地区使用现行的公历历法。因此，我们考虑一个从 1600 年起使用的计算星期几的公式。

以下，我们使用记号：

$N=100c+y$ 表示年份，其中 $0\le y\le 99$；

$m$ 表示月份，$m=1$ 表示三月，$m=2$ 表示四月，……，$m=12$ 表示二月；



$d_N(m)$表示第 $N$ 年 $m$ 月 1 日的星期数。

假设 $d_{1600}(1)$是已知的，我们首先计算 $d_N(1)$，即第 $N$ 年 3 月 1 日的星期数。我们知道：如果没有闰月，一年有 365 天，因为

$$365\equiv 1\ (\mathrm{mod}\ 7),$$

所以，每过一个正常年，星期数就增加 1；每过一个闰年，星期数就增加 2。

以 $r$ 表示从 1600 年到 $N$ 年的闰年数，我们得到

$$d_N(1)\equiv \mathrm{d}_{1600}(1)+N-1600+r\ (\mathrm{mod}\ 7)。\tag{1}$$

由闰年的确定方法，我们有

$$\begin{aligned} r&=\Big[\frac{100c+y-1600}{4}\Big]-\Big[\frac{100c+y-1600}{100}\Big]+\Big[\frac{100c+y-1600}{400}\Big]\\ &=25c+\Big[\frac{y}{4}\Big]-400-c-\Big[\frac{y}{100}\Big]+16+\Big[\frac{100c+y}{400}\Big]-4\\ &=\Big[\frac{y}{4}\Big]+24c-\Big[\frac{y}{100}\Big]+\Big[\frac{100c+y}{400}\Big]-388。\end{aligned}\tag{2}$$

设 $c=4q+s$，$0\le s\le 3$，那么，由于 $0\le y\le 99$，$100s+y<400$，所以

$$\Big[\frac{y}{100}\Big]=0，\ \Big[\frac{100s+y}{400}\Big]=0，$$

因此，由式(2)得到

$$\begin{aligned} r&=\Big[\frac{y}{4}\Big]+24c+\Big[\frac{400q+100s+y}{400}\Big]-388\\ &=\Big[\frac{y}{4}\Big]+24c+q-388\\ &=\Big[\frac{y}{4}\Big]+24c+[\frac{c}{4}]-388，\end{aligned}\tag{3}$$

$$\begin{aligned} d_N(1)&\equiv d_{1600}(1)+N-1600+r\\ &\equiv d_{1600}(1)+100c+y-1600+\Big[\frac{y}{4}\Big]+24c+\Big[\frac{c}{4}\Big]-388\end{aligned}$$

$$\equiv d_{1600}(1)-2c+y+\left[\frac{y}{4}\right]+\left[\frac{c}{4}\right]\ (\mathrm{mod}\,7)。\qquad (4)$$

为了确定 $d_{1600}(1)$的数值，我们把一个已知的数据代入式(4)，例如，我们知道 1998 年 3 月 1 日是星期日，即 $d_{1998}(1)\equiv 0\ (\mathrm{mod}\ 7)$，代入式(4)，得到

$$0\equiv d_{1600}(1)-2\cdot 19+98+\left[\frac{98}{4}\right]+\left[\frac{19}{4}\right]\equiv d_{1600}(1)+4\ (\mathrm{mod}\ 7)，$$

所以 $d_{1600}(1)=3$，即 1600 年的 3 月 1 日是星期三。将这个数值代入式(4)，得到

$$d_N(1)\equiv 3-2c+y+\left[\frac{y}{4}\right]+\left[\frac{c}{4}\right](\mathrm{mod}\ 7)。\qquad (5)$$

现在，我们已经能够计算 $N$ 年的 3 月 1 日是星期几。剩下的问题是如何计算这一年的 $m$ 月 $k$ 日是星期几。

我们先计算 $d_N(m)$，即 $N$ 年 $m$ 月 1 日的星期数。容易知道：

3 月是 31 天，所以 $d_N(2)\equiv d_N(1)+3\ (\mathrm{mod}\ 7)$，
4 月是 30 天，所以 $d_N(3)\equiv d_N(1)+5\ (\mathrm{mod}\ 7)$，
5 月是 31 天，所以 $d_N(4)\equiv d_N(1)+8\ (\mathrm{mod}\ 7)$，
6 月是 30 天，所以 $d_N(5)\equiv d_N(1)+10\ (\mathrm{mod}\ 7)$，
7 月是 31 天，所以 $d_N(6)\equiv d_N(1)+13\ (\mathrm{mod}\ 7)$，
8 月是 31 天，所以 $d_N(7)\equiv d_N(1)+16\ (\mathrm{mod}\ 7)$，
9 月是 30 天，所以 $d_N(8)\equiv d_N(1)+18\ (\mathrm{mod}\ 7)$，
10 月是 31 天，所以 $d_N(9)\equiv d_N(1)+21\ (\mathrm{mod}\ 7)$，
11 月是 30 天，所以 $d_N(10)\equiv d_N(1)+23\ (\mathrm{mod}\ 7)$，
12 月是 31 天，所以 $d_N(11)\equiv d_N(1)+26\ (\mathrm{mod}\ 7)$，
1 月是 31 天，所以 $d_N(12)\equiv d_N(1)+29\ (\mathrm{mod}\ 7)$。

现在，计算 $N$ 年 $m$ 月 $k$ 日的星期数已经是很容易的事了。但是，我们希望找一个更简单的公式。从上面的数字可以看出，从 3 月 1 日到 2 月 1 日的 11 个月中，星期数“增加”了 29 天，平均每月“增加”2.6 天，因此，我们来找一个形如$[2.6m-a]$的公式，其中 $m$ 是月份，$a$ 是某个适当的数。经过验证，发现函数 $f(m)=[2.6m-0.2]-2$ 满足这些条件：

$f(1)=0$，$f(2)=3$，$f(3)=5$，$f(4)=8$，…，$f(12)=29$。



利用这个函数，我们得到 $N$ 年 $m$ 月 1 日的星期数是

$$d_N(m)\equiv d_N(1)+[2.6m-0.2]-2\ (\mathrm{mod}\ 7)。$$

因此，$N$ 年 $m$ 月 $k$ 日的星期数 $W(N, m, k)$是

$$W(N, m, k)=d_N(m)+k-1\equiv d_N(1)+[2.6m-0.2]+k-3\ (\mathrm{mod}\ 7)，$$

由式(5)，得到

$$W(N, m, k)\equiv k-2c+y+\left[\frac{y}{4}\right]+\left[\frac{c}{4}\right]+[2.6m-0.2]\ (\mathrm{mod}\ 7)。\qquad (6)$$

利用上式我们就能较容易地计算出任意给定的 $N$ 年 $m$ 月 $k$ 日的星期数的星期数 $W(N, m, k)$了。

**例 1**　问：1976 年 8 月 6 日是星期几？

**解**　将 $N=1976$，$c=19$，$y=76$，$m=6$，$k=6$ 代入式(6)，得到

$$W(1976, 6, 6)\equiv 6-38+76+\left[\frac{76}{4}\right]+\left[\frac{19}{4}\right]+[2.6\cdot 6-0.2]\equiv 5\ (\mathrm{mod}\ 7)，$$

即 1976 年 8 月 6 日是星期五。

**例 2**　问：1978 年 2 月 24 日是星期几？

**解**　将 $N=1977$，$c=19$，$y=77$，$m=12$，$k=24$ 代入式(6)，得到

$$W(1977,12,24)\equiv 24-38+77+\left[\frac{77}{4}\right]+\left[\frac{19}{4}\right]+[2.6\cdot 12-0.2]\equiv 5\ (\mathrm{mod}\ 7)，$$

即 1978 年 2 月 24 日是星期五。

注意，由例 2 我们看到，一月和二月分别是作为上一年的十一月和十二月。

## 习 题 一

**1.** 问：1948 年 2 月 14 日是星期几？
**2.** 问：1999 年 10 月 1 日是星期几？

# 第二节　循环比赛

有 $N$ 个球队要进行循环赛。我们希望知道：最少需要按排几轮比

赛，才能完成循环赛？

我们先来做一些分析。首先，由于是进行循环赛，每个队要和另外的队都比赛过，所以至少要进行 $N-1$ 轮比赛。其次，用 $r$ 表示在每一轮比赛中所进行的比赛场数，则

$$r=\begin{cases}\dfrac{N}{2}, & \text{当}N\text{是偶数；}\\ \dfrac{N-1}{2}, & \text{当}N\text{是奇数。}\end{cases}$$

如果 $N$ 是奇数，那么，在每一轮比赛中总有一个队不参加比赛。这时，我们把一个“假想的”球队 $A$ 加到这 $N$ 个球队中，就有了 $N+1$ 个球队。现在，在每一轮比赛中对这 $N+1$ 个球队进行按排，并且规定：凡是被按排和 $A$ 队比赛的球队，就是没有比赛的球队。这样，$N$ 是奇数的情形就可以化为 $N$ 是偶数的情形，因此，下面我们总假定 $N$ 是偶数。

为了叙述方便，我们用 $1,2,\cdots,N$ 表示这 $N$ 个球队，用 $x_i$（$1\le x_i\le N$）表示在第 $i$ 轮比赛中与 $x$ 队进行比赛的球队。

下面，我们给出一个按排比赛的方法，它说明，用 $N-1$ 轮比赛就可以完成循环赛。

按排方法：在第 $i$（$1\le i\le N-1$）轮比赛中，对于每个球队 $x$ 我们这样确定与它比赛的球队 $x_i$：

（ⅰ） 当 $x=N$ 时，取

$$N_i=\begin{cases}\dfrac{i}{2}, & \text{当}i\text{是偶数；}\\ \dfrac{i+N-1}{2}, & \text{当}i\text{是奇数。}\end{cases}\tag{1}$$

显然 $N\ne N_i$。

（ⅱ） 当 $x\ne N$ 且

$$x\ne\begin{cases}\dfrac{i}{2}, & \text{当}i\text{是偶数；}\\ \dfrac{i+N-1}{2}, & \text{当}i\text{是奇数}\end{cases}\tag{2}$$

时，取 $x_i$ 满足

$$x+x_i\equiv i\ (\mathrm{mod}\ N-1),\quad 1\le x_i\le N-1。\tag{3}$$



下面，我们要证明，这样的按排满足要求。

首先，我们指出，在每一轮比赛中，不同球队的比赛对手是不同的，即，若 $x\ne x'$，则 $x_i\ne x_i'$（$1\le i\le N-1$）。

我们分三种情况进行讨论。

（ⅰ） 若 $x$ 与 $x'$ 都不等于 $N$，则 $1\le x,x'\le N-1$，于是

$$x-x'\not\equiv 0\ (\mathrm{mod}\ N-1),$$

由式(3)得到

$$x+x_i\equiv x'+x_i',\ \ 0\not\equiv x-x'\equiv x_i'-x_i\ (\mathrm{mod}\ N-1),\tag{4}$$

因此，$x_i\ne x'_i$。

（ⅱ） 若 $x=N$，$x'=N_i$，则 $x_i=N_i$，$x_i'=N$，显然 $x_i\ne x_i'$。

（ⅲ） 若 $x=N$，但 $x'$ 不满足式(2)，则 $x_i'$ 由式(3)定义，此时，如果 $x_i'=x_i=N_i$，那么，由式(3)和式(1)，当 $i$ 是偶数，我们有

$$x'+x_i'=x'+\frac{i}{2}\equiv i,\quad x'\equiv\frac{i}{2}\ (\mathrm{mod}\ N-1);\tag{5}$$

当 $i$ 是奇数，我们有

$$x'+x_i'=x'+\frac{i+N-1}{2}\equiv i,\quad x'\equiv\frac{i+N-1}{2}\ (\mathrm{mod}\ N-1)。\tag{6}$$

但是，由于对 $x'$ 的假定，式(5)或式(6)都不能成立。

其次，我们指出，每一个队 $x$ 在每一轮比赛中的对手不是它自己，即对于 $1\le i\le N-1$，必定 $x\ne x_i$。当 $x=N$ 时，由式(1)可知 $N\ne N_i$。当 $1\le x\le N-1$，且式(2)满足时，若 $x=x_i$，则式(3)给出

$$2x\equiv x+x_i\equiv i\ (\mathrm{mod}\ N-1),$$

由此推出 $x$ 不满足式(2)，这个矛盾说明 $x\ne x_i$。

最后，我们指出，对于每一个确定的队 $x$，它在每一轮比赛中的对手是不同的，即

$$x_{i_1}\ne x_{i_2},\ \ i_1\ne i_2,\ \ (1\le i_1,i_2\le N-1)。\tag{7}$$

（ⅰ） 先看球队 $N$。如果

$$N_{i_1}=N_{i_2}\ (1\le i_1,i_2\le N-1)。$$

由式(1)可知，

$$i_1\equiv 2N_{i_1}=2N_{i_2}\equiv i_2\ (\mathrm{mod}\ N-1),$$

因此 $i_1=i_2$。

（ⅱ） 再看球队 $x$，$x<N$。如果

$$x_{i_1} = x_{i_2} = N，\text{则} N_{i_1} = N_{i_2} \quad (1 \le i_1, i_2 \le N-1)，$$

因此，由上面在(ⅰ)中的讨论，可知 $i_1 = i_2$。如果 $x_{i_1} = x_{i_2} \ne N$，那么，由式(3)得到

$$i_1 \equiv x + x_{i_1} = x + x_{i_2} \equiv i_2 \pmod{N-1}，$$

因此 $i_1 = i_2$ 。

以上讨论说明，用上面的按排方法可以在 $N-1$ 轮比赛中完成 $N$ 个球队的循环赛。

下面，我们举了两个例子说明具体的按排方法。表格中，第 $k$ 行第 $m$ 列上的数字就是第 $k$ 轮中与球队 $m$ 进行比赛的球队所对应的数字。如果在这个位置上没有数字，就表示球队 $m$ 在第 $k$ 轮比赛中没有赛事。

**例 1**　五个球队进行循环赛的比赛程序：

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 5 | 4 | | 2 | 1 |
| 2 | | 5 | 4 | 3 | 2 |
| 3 | 2 | 1 | 5 | | 3 |
| 4 | 3 | | 1 | 5 | 4 |
| 5 | 4 | 3 | 2 | 1 | |

**例 2**　八个球队进行循环赛的比赛程序：

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 7 | 6 | 5 | 8 | 3 | 2 | 1 | 4 |
| 2 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 3 | 2 | 1 | 7 | 6 | 8 | 4 | 3 | 5 |
| 4 | 3 | 8 | 1 | 7 | 6 | 5 | 4 | 2 |
| 5 | 4 | 3 | 2 | 1 | 7 | 8 | 5 | 6 |
| 6 | 5 | 4 | 8 | 2 | 1 | 7 | 6 | 3 |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 8 | 7 |



## 习 题 二

**1.** 编一个有十个球队进行循环赛的程序表。

**2.** 编一个有九个球队进行循环赛的程序表。

# 第三节　仿射加密方法

在很长的一个历史时期内，数论被认为是一门没有应用价值的“纯”理论学科。事实并非如此。本章以下几节将要介绍数论在信息保密技术中的几个应用。

现实社会中，充满了各种各样的信息，例如，军事情报，商业秘密，金融消息，计算机文件，私人通信等等。在很多情况下，人们希望在秘密的情况下保存或传送信息，这就导致了对信息加密的研究。

对于那些一目了然的信息，我们称为“明文”。当我们要把某个信息传送给某些人（称之为“合法接收人”）时，是先把明文进行“加密”处理，这种经过加密处理的明文，我们称为“密文”。密文不是随便甚麼人都可以看懂的。只有合法接收人，他们掌握了一定的方法，才能把它“翻译”成加密处理之前的明文。总的来说，关于信息加密的研究主要是两个方面：第一，研究把明文翻译成密文的方法，这个方法要尽可能的简单易行；第二，研究这种加密方法的保密性（安全性），即，除合法接收人外，其他人从密文了解到明文内容（全部或部分）的可能性。

把明文翻译成密文的过程，称为加密过程，或加密；所用的方法（或公式），称为加密方法（或加密公式）。把密文翻译成明文的过程，称为解密过程，或解密；所用的方法（或公式），称为解密方法（或解密公式）。

为了能将数论用于明文的加密，首先需要建立明文与正整数的对应关系。一个文件总是由文字和其他符号（标点符号，数字，特殊记号，等等）组成的。如果用汉语拼音书写汉字，那么，文件就可以用26个拉丁字母和一些符号来表达。假设所使用的字母和符号共有 $N$ 个，如果把这些符号和 $N$ 个正整数 0，1，2，…，$N-1$ 建立一一对应的关系，那么，文字、符号、句子和文件就都和正整数建立了一一对应的

关系。例如，假设使 26 个拉丁字母 a，b，c，…，y，z 与数字 00，01，02，…，24，25 建立了下表所示的一一对应关系：

表　1

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

那么，与“woyaolai”（我要来）对应的数字就是 2214240014110008。

在实际应用中，一个文件所对应的整数是一个很大的数字，所以，人们往往要对大的正整数进行处理，使它们可以与较小的正整数列对应，从而容易进行加密运算。我们知道，对于给定的正整数 $k$，任何正整数 $P$ 都可以唯一地表示成

$$P = p_n k^n + p_{n-1}k^{n-1} + \cdots + p_1 k + p_0,\ 0 \le p_i \le k-1,\ 0 \le i \le n。$$

这样，任何整数 $P$ 就与整数列 $\{p_n, p_{n-1}, \cdots, p_0\}$ 建立了一一对应的关系，对大整数 $P$ 的加密就转化为对不超过 $k$ 的整数 $p_i$（$0 \le i \le n$）的加密。

以下几节中，我们总用 $P$ 表示明文，用 $E(P)$ 或 $E$ 表示与 $P$ 相应的密文。

在这一节，我们主要介绍历史较长久的一类加密方法，即仿射加密方法。用 $\Omega$ 表示需要加密的所有明文 $P$ 的集合，并且假定集合 $\Omega$ 的上界是 $A$。用仿射加密方法对明文 $P$ 加密的过程是这样的：

（ⅰ）　取大正整数 $M > A$，以及正整数 $a$，$b$，$a'$，使得

$$(a, M) = 1,\ aa' \equiv 1 \pmod{M}。 \tag{1}$$

（注意：因此，明文 $P$ 满足 $0 \le P < M$。）

（ⅱ）　加密：对于明文 $P$，计算

$$E \equiv aP + b \pmod{M},\ 0 \le E < M。 \tag{2}$$

$E$ 就是与 $P$ 对应的密文。

(ⅲ)　解密：对于密文 $E$，计算

$$P_0 \equiv a'(E - b) \pmod{M},\ 0 \le P_0 < M, \tag{3}$$

$P_0$ 就是与 $E$ 对应的明文 $P$。

现在，我们说明式(3)中确定的 $P_0$ 就是明文 $P$。事实上，由式(3)，式(2)和式(1)，我们得到



$$P_0 \equiv a'(E-b) \equiv a'((aP+b)-b) \equiv aa'P \equiv P \pmod{M},$$

由于 $0 \le P < M$，$0 \le P_0 < M$，所以，由上式得到 $P_0 = P$。

**例 1**　设符号 a，b，…，y，z 分别与整数 0，1，…，24，25 对应，使用仿射加密方法，取 $M = 26$，$a = 1$，$b = 3$，$a' = 1$，对明文 $P$ 中的每一个符号用这一方法加密：

$$E \equiv P + 3 \pmod{26}。$$

这就是所谓的“恺撒密码”。在古罗马时代，恺撒大帝在传送军事命令时，把每个英文字母用它后面的第三个字母代替，即按表 2 的替换方式：

表　2

| $P$ | a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $E$ | d | e | f | g | h | i | j | k | l | m | n | o | p |
| $P$ | n | o | p | q | r | s | t | u | v | w | x | y | z |
| $E$ | q | r | s | t | u | v | w | x | y | z | a | b | c |

例如，使用例 1 中的加密方法，明文“jiudianzhong”（九点钟）被加密成“mlxgldqckrqj”。

以下，为了叙述方便，我们用“$\longrightarrow$”表示数字与符号的对应关系，例如，“a $\longrightarrow$ 00”，“d $\longrightarrow$ 03”，等等。又用“$\Longrightarrow$”表示明文和密文的对应关系，例如，“s $\Longrightarrow$ a”“men $\Longrightarrow$ phq”，等等。

**例 2**　已知明文所使用的符号只是 26 个英文字母 a，b，…，y，z，它们分别与整数 00，01，…，24，25 对应，又知道使用公式

$$E \equiv P + b \pmod{26},\ 0 \le E < 26 \tag{4}$$

对每个符号加密。已经知道明文字母 e 与密文字母 u 对应，试求出解密方法。

**解**　将已知的 e $\Longrightarrow$ u 以及 e $\longrightarrow$ 04，u $\longrightarrow$ 20 代入式(4)，得到

$$20 \equiv 4 + b \pmod{26},$$

所以 $b \equiv 16 \pmod{26}$，再由式(4)得到

$$P \equiv E - 16 \equiv E + 10 \pmod{26},\ 0 \le P < 26,$$

这就是解密方法，也可以用下表说明：

表　3

| $E$ | a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $P$ | k | l | m | n | o | p | q | r | s | t | u | v | w |
| $E$ | n | o | p | q | r | s | t | u | v | w | x | y | z |
| $P$ | x | y | z | a | b | c | d | e | f | g | h | i | j |

一般地，对于由式(2)定义的仿射加密方法，只要知道两对（不同的）相对应的明文和密文 $P_1$，$E_1$ 与 $P_2$，$E_2$，就可以求出解密方法。事实上，由式(2)及已知的对应关系，得到

$$E_1 \equiv aP_1 + b \pmod{M},$$
$$E_2 \equiv aP_2 + b \pmod{M}, \qquad (4)$$

所以

$$E_2 - E_1 \equiv a(P_2 - P_1) \pmod{M}。$$

以

$$x \equiv a_i \pmod{M}，\ 0 \le a_i < M，\ 1 \le i \le r$$

表示同余方程

$$x(P_2 - P_1) \equiv E_2 - E_1 \pmod{M}$$

的全部解，并且记

$$b_i \equiv E_1 - a_iP_1 \pmod{M}，\ 0 \le b_i < M,$$

则 $a_i$ 与 $b_i$（$1 \le i \le r$）就可能是式(2)中所使用的 $a$ 和 $b$。

当$(P_2 - P_1, M) = 1$ 时，这样的 $a_i$ 与 $b_i$ 只有一组，当$(P_2 - P_1, M) > 1$ 时，为了确定出正确的 $a$ 与 $b$，首先，利用$(a, M) = 1$ 删去某些 $a_i$ 与 $b_i$，其次，用它们验证式（4）是否成立，并用它们试译部分密文，就可以确定正确的 $a$ 与 $b$。将确定的 $a$，$b$ 代入式(3)，就得到解密公式。

在现实生活中，无论使用什么语言符号传送信息，各个符号的出现频率总是有差别的。例如，有统计数字表明，在报刊文章中，英语的 26 个字母中，出现频率较高的，依次是 e，t，a，o 等；较低的，依次是 z，q，j，x 等。这样，在对密文中的每个字母的出现频率进行统计之后，可以对于明文字母和密文字母之间的对应关系作出猜测，然后试行解密。

**例 3**　已知明文由 26 个英文字母 a，b，…，y，z（分别与 00，01，…，24，25 对应）及符号“!”和“？”（分别与 26 和 27 对应）组成，用这 28 个符号写成的正常英文中，出现频率最高的依次是!，e 与 t。在对一组密文做了统计分析之后，发现密文中出现频率最高的三个符



号依次是 b，?与 i，试求解密公式。

**解**　设解密公式为

$$P \equiv a'E + b' \pmod{28}，\ 0 \le P < 28，$$

则由已知的符号与数字的对应关系，比较出现频率的高低，可以假定“!”与“e”分别对应着“b”与“?”，于是

$$26 \equiv a' \cdot 1 + b' \pmod{28},$$
$$4 \equiv a' \cdot 27 + b' \pmod{28},$$

将两式相减，得到

$$26a' \equiv -22 \pmod{28}。$$

这个同余方程有两个解：$a_1' \equiv 11 \pmod{28}$，$a_2' \equiv 25 \pmod{28}$，相应的，$b_1' \equiv 15 \pmod{28}$，$b_2' \equiv 1 \pmod{28}$。

这样，得到了两个可能的解密方法：

(ⅰ)　$P \equiv 11E + 15 \pmod{28}$，$0 \le P < 28$，

(ⅱ)　$P \equiv 25E + 1 \pmod{28}$，$0 \le P < 28$。

再通过比较出现频率，又可假定 i 与 t 对应（它们对应的数字分别是 8 与 19），将这两个数字分别代入(ⅰ)与(ⅱ)进行验证，可知解密方法(ⅰ)是正确的。

## 习 题 三

**1.**　利用例 1 中的加密方法，将“ICOMETODAY”加密。

**2.**　已知字母 a，b，…，y，z，它们分别与整数 00，01，…，24，25 对应，又已知明文 h 与 p 分别与密文 e 与 g 对应，试求出密解公式：

$$P \equiv a'E + b' \pmod{26},$$

并破译下面的密文：“IRQXREFRXLGXEPQVEP”。

# 第四节　RSA 加密方法

对信息进行加密的目的，当然是希望这个信息的内容不被某一部分人（以后，我们称他们为“敌方”）了解；同时，这个信息的内容应该能够被另一部分人（以后，我们称他们为“友方”）很容易地了解。

上一节所介绍的仿射加密方法具有计算方便的优点，其中，参数 $a$ 和 $b$ 是两个关键的数据。我们已经看到，利用统计的方法，能够很容易地确定这两个数据，此外，为了提高保密性，即增加敌方从密文得到密文的困难程度，需要经常更换 $a$ 和 $b$ 的数值，于是，就要随时把这些数值及时通知友方，这就增加了敌方获取 $a$ 和 $b$ 的数值的可能性。因此，仿射加密方法的保密性（安全性）是不好的。在这一节，我们介绍一种加密方法，在很大程度上克服了上述缺点。

从实用的观点来看，保密是有时间性的。如果加密后的文件在一个足够长的时间内不被敌方了解，就可以认为这个加密是安全的。当我们谈论“把某一份文件加密，使它不被敌方了解”的时候，其实是包含着一个时间界限的。就是说，这里指的是，在某一个时期内，加密后的文件不被敌方了解。例如，一个发动某次战役的具体时间，在战役开始之前是绝对要保密的，但是，战役结束之后，就不存在保密的必要了。

用 $P$ 和 $E$ 分别表示明文和密文，从数学的观点来看文件加密的问题，加密方法和解密方法其实就是两个满足下述条件的函数 $f(P)$和 g($E$)：

(ⅰ) 对于某个整数集合中的数 $P$，有确定的函数值 $E=f(P)$与之对应，同时，计算 $f(P)$是容易的；

(ⅱ) 对于某个整数集合中的数 $E$，有确定的函数值 $P=g(E)$与之对应，同时，计算 $g(E)$是困难的；

(iii) 如果掌握了关于函数 $g(E)$的某种条件（信息），计算 $g(E)$是容易的。

在这一节，我们要介绍满足上述三个条件的一个加密方法，它以下面的命题为基础。

**命题** 已知两个素数，计算它们的的乘积是容易的；但是，已知两个大素数的乘积，求这两个素数却是非常困难的。

从这一个命题出发，R. L. Rivest 与 A. Shamir，L. M. Adleman 提出了下面的加密方法。

**RSA 加密方法**

Ⅰ 参数的选取

随机地选取大素数 $p$，$q$，计算

$$n=pq,\quad \varphi(n)=(p-1)(q-1),$$



再随机地取正整数 $e$，$(e, \varphi(n))=1$，并计算 $d$，使得

$$ed\equiv 1 \pmod{\varphi(n)}。\tag{1}$$

公开 $n$，$e$，供加密使用（称它们为 RSA 加密钥）；将 $p$，$q$，$\varphi(n)$和 $d$ 保密（称它们为保密钥）。

Ⅱ 加密

设明文是 $P$，$0\le P<n$，则与之相应的密文是

$$E\equiv P^{e} \pmod{n},\quad 0\le E<n。\tag{2}$$

Ⅲ 解密

已知密文 $E$ 时，明文 $P$ 由下式确定：

$$P\equiv E^{d} \pmod{n},\quad 0\le P<n。\tag{3}$$

我们将以上设计的 RSA 加密方法简记为 RSA($n$, e)。

下面的定理给出了解密方法的依据。

**定理 1** 设 $n=p_1p_2\cdots p_k$ 是 $k$ 个不同的素数之积，$e$ 与 $d$ 是正整数，$(e, \varphi(n))=1$，并且式(1)成立，则对于任意的 $a\in\mathbf{N}$，有

$$a^{ed}\equiv a \pmod{n}。$$

**证明** 对于任意的 $p_i$（$1\le i\le k$），若$(a, p_i)=1$，则由 Euler 定理可知

$$a^{p_i-1}\equiv 1 \pmod{p_i}。$$

由式(1)，$ed=r\varphi(n)+1=r(p_1-1)\cdots(p_k-1)+1$，其中 $r$ 是非负整数，所以，

$$a^{ed}\equiv a \pmod{p_i},\quad i=1, 2, \cdots, k。\tag{4}$$

当$(a, p_i)>1$ 时，这个同余式当然也成立。由于 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，由式(4)及同余式的性质即可证得定理。证毕。

一般来说，从密文求明文，有许多可能的方法，例如：

(ⅰ) 将 $n$ 分解因数，求出 $p$ 和 $q$，使得 $n=pq$，然后计算$\varphi(n)=(p-1)(q-1)$，利用辗转相除法求出 $d$，使得式(1)成立。再利用式(3)从密文 $E$ 计算明文 $P$。容易看出，用这种方法从密文求出明文的难度，就是将大整数分解因数的难度。

(ⅱ) 如果能用某种方法（不是先将 $n$ 分解因数）求出$\varphi(n)$，则也可以从密文 $E$ 求出明文 $P$。因为，利用辗转相除法，由 $e$ 可以求出 $d$ 使得式(1)成立，于是，由式(3)可以从密文 $E$ 计算明文 $P$。但是，如果$\varphi(n)=(p-1)(q-1)$是已知的，那么，有 $pq=n$ 以及

$$p+q=pq-\varphi(n)+1=n-\varphi(n)+1。$$

由此，可以利用一元二次方程的求解公式求出 $p$ 和 $q$。这说明，这种方法的难度不会低于将大整数分解因数的难度。

除此之外，还有一些别的方法。对于这些方法的分析，有兴趣的读者可以查阅关于密码学的文献。总的来说，RSA 加密方法被认为有较好的安全性。

RSA 加密方法的特点，在于加密方法是公开的，而且加密时所使用的参数也是公开的。这是它与仿射加密方法的重要区别。 通常，称具有这种特点的加密方法为公钥加密方法。公钥加密方法使得信息的加密传送更为方便。例如，每个单位或个人可以像公布电话号码一样公布自己的 RSA 加密钥。于是，凡是要向它或他发送加密信息的单位或个人都可以使用这些参数发送加密信息。此外，RSA 加密方法还有更广泛的用途。下面介绍的数字签名的方法就是一个例子。

**数字签名**

在社会生活中，在处理具体事件时，常需要当事人进行签证（签名），以保证他做出的许诺或送出的信息的可靠性与合法性。例如，在签署文件时，由当事人签名，盖章，签署日期以及重要的特殊记号，常是不可少的环节。这样的签证，应该满足一定的要求。

假设 $A$ 签证一个文件给 $B$，那么，

(ⅰ) $B$ 应该能够确定这是否 $A$ 的签证；

(ⅱ) 任何其他人，无法伪造 $A$ 的签证，即 $A$ 有其独特的签证方式；

(iii) 有一个仲裁签证是否由 $A$ 发出的方法，例如，当 $A$ 否认这个签证时，这样的方法可以鉴定签证的真伪。

下面我们说明，RSA 加密方法可以用来进行签证，不需要当事人到场，只需传送必要的信息。

假设要签证的信息是 $M$（例如，它是签证人的姓名，签证日期，特定的标志，等等），并且，已经根据信息 $M$ 所使用的符号将它与一个正整数对应。为方便计，我们就同时用 $M$ 表示签证以及它所对应的正整数。

设 $A$ 要将签证信息 $M$ 传送给 $B$。又设向 $A$ 和 $B$ 传送信息时使用的 RSA 加密方法分别是 RSA($n_A$, $e_A$)和 RSA($n_B$, $e_B$)，设 $A$ 和 $B$ 的保密钥分别是 $d_A$，$p_A$，$q_A$，和 $d_B$，$p_B$，$q_B$ 。



在第一节中我们已经谈到，不妨假定 $M<n_A$ 。

$A$ 要将签证信息 $M$ 传送给 $B$ 时，首先计算

$$E_1\equiv M^{d_A}\ (\mathrm{mod}\ n_A)，\ 0\le E_1<n_A 。 \tag{5}$$

同样地，不妨假定 $E_1<n_B$ 。再计算

$$E\equiv E_1^{e_B}\ (\mathrm{mod}\ n_B)，\ 0\le E<n_B 。 \tag{6}$$

然后，$A$ 将 $E$ 传送给 $B$。$n_B$ 和 $e_B$ 是公开的，而 $d_A$ 却只有 $A$ 知道，所以，其他人是无法依照上述步骤进行伪造的。

$B$ 收到信息 $E$ 后，计算

$$M_1\equiv E^{d_B}\ (\mathrm{mod}\ n_B)，\ 0\le M_1<n_B ， \tag{7}$$

$$M_0\equiv M_1^{e_A}\ (\mathrm{mod}\ n_A)，\ 0\le M_0<n_A ， \tag{8}$$

并且进行验证是否 $M_0=M$。事实上，由定理 1 以及式(5)，式(6)，式(7)和式(8)，应该有

$$M_1\equiv E^{d_B}\equiv E_1^{e_Bd_B}\equiv E_1\ (\mathrm{mod}\ n_B)，\qquad M_1=E_1，$$

$$M_0\equiv M_1^{e_A}\equiv E_1^{e_A}\equiv M^{e_Ad_A}\equiv M\ (\mathrm{mod}\ n_A)，\ M_0=M。$$

对 $B$ 来说，上述验证过程是容易的，因为他知道 $d_B$ 。

显然，任何第三者都可以按照式(7)和式(8)鉴定收到的信息是否 $A$ 的签证。这样，此处所提供的数字签名方法是满足上面的三个要求的。

做为本节的结尾，我们指出，RSA 加密方法的基础是命题“将大整数分解成素因数乘积在计算上是困难的”。此处所谓“计算上困难”与素因数的大小以及人们的计算能力是有关的。如果限定素因数的大小，那么，当人们的计算能力达到一定水平的时候，这个命题就不成立了，那时，RSA 加密方法也就不再是安全的了。

## 习 题 四

**1.** 设一 RSA 的公开加密钥为 $n=943$，$e=9$，试将明文 $P=100$ 加密成密文 $E$。

**2.** 设 RSA($n_A$, $e_A$) = RSA(33, 3)，RSA($n_B$, $e_B$) = RSA(35, 5)，$A$ 的签证信息为 $M=3$，试说明 $A$ 向 $B$ 发送签证 $M$ 的传送和认证过程。

# 第五节　孙子定理的应用

本节要介绍孙子定理在信息加密中的两个应用。

## 一、文件集合的加密

假设 $A$ 是由 $n$ 个文件 $F_1, F_2, \cdots, F_n$ 组成的集合，它们分别属于 $n$ 个单位（例如，$n$ 个个人，公司，工厂，等等）。又设按某种方法使这 $n$ 个文件与 $n$ 个整数对应。为简便计，我们仍用 $F_1, F_2, \cdots, F_n$ 表示每个文件所对应的整数。

下面叙述一种对集合 $A$ 的加密方法，满足这样的要求：每个单位可以很方便地查阅集合 $A$ 中属于自己的文件，却很难查阅集合 $A$ 中不属于自己的文件。

设正整数 $m_1, m_2, \cdots, m_n$ 满足条件

$$m_i > F_i \ (1 \le i \le n),\ (m_i, m_j) = 1 \ (i \ne j,\ 1 \le i,\ j \le n),$$

记

$$M = m_1 m_2 \cdots m_n,\ M_i = \frac{M}{m_i} \ (1 \le i \le n)。 \tag{1}$$

又设 $M_i'$（$1 \le i \le n$）由下面的同余式确定：

$$M_i M_i' \equiv 1 \pmod{m_i},\ 1 \le M_i' \le m\ 。 \tag{2}$$

$e_i \equiv M_i M_i' \pmod{M}$，$0 \le e_i \le M\text{-}1$。

将集合 $A$ 按下面的方式进行加密：

$$E = E(A) \equiv \sum_{i=1}^{n} e_i F_i \pmod{M},\ 1 \le E \le M。 \tag{3}$$

若要从密文 $E$ 求出 $F_i$，可利用同余式

$$F_i \equiv E \equiv \sum_{i=1}^{n} e_i F_i \pmod{m_i},\ 0 \le F_i < m_i。 \tag{4}$$

在上面所用的加密方法中，数据 $m_i$，$M_i$ 以及 $M_i'$（$1 \le i \le n$）都是保密的。显然，

(ⅰ) 只有掌握 $m_i$，才能利用式(4)由 $E$ 得到 $F_i$；

(ⅱ) 在掌握 $m_i$ 的情况下，可以求出 $F_i$，也可以对它进行修改。



例如，修改成 $F_i'$，并且，在修改之后，还可以重新对由 $F_1, \cdots, F_{i-1}, F_i', F_{i+1}, \cdots, F_n$ 组成的新集合 $A'$进行加密；

(ⅲ) 无论求出 $F_i$ 或者对 $F_i$ 进行修改，都对其他文件 $F_j$（$j \ne i$）没有影响。

**例 1**　设某数据库含四段文字：$F_1 = 7$，$F_2 = 9$，$F_3 = 12$，$F_4 = 15$，取

$$m_1 = 11，\ m_2 = 13，\ m_3 = 17，\ m_4 = 19，$$

则

$$M = 11 \cdot 13 \cdot 17 \cdot 19 = 46189，$$

$$M_1 = 13 \cdot 17 \cdot 19 = 4199，\ M_2 = 11 \cdot 17 \cdot 19 = 3553，$$

$$M_3 = 11 \cdot 13 \cdot 19 = 2717，\ M_4 = 11 \cdot 13 \cdot 17 = 2431，$$

$$M_1' = 7，\ M_2' = 10，\ M_3' = 11，\ M_4' = 18,$$

$$e_1 = 4199 \cdot 7,\ e_2 = 3553 \cdot 10,\ e_3 = 2717 \cdot 11,\ e_4 = 2431 \cdot 18。$$

对集合{7, 9, 12, 15}加密，得到

$$\begin{aligned} E = E(A) &\equiv \sum_{i=1}^{n} e_i F_i \\ &= 4199 \cdot 7 \cdot 7 + 3553 \cdot 10 \cdot 9 + 2717 \cdot 11 \cdot 12 + 2431 \cdot 18 \cdot 15 \\ &\equiv 16298 \pmod{46189}, \end{aligned}$$

即 $E = 16298$。

若要求出 $F_2$，则由

$$F_2 \equiv 16298 \equiv 9 \pmod{13}$$

得到 $F_2 = 9$。若要将 $F_2$ 改变成 10，并且将新的数据库加密，则使用上面的方法，对{7, 10, 12, 15}加密，得到

$$\begin{aligned} E' &\equiv 4199 \cdot 7 \cdot 7 + 3553 \cdot 10 \cdot 10 + 2717 \cdot 11 \cdot 12 + 2431 \cdot 18 \cdot 15 \\ &\equiv 5639 \pmod{46189} \end{aligned}$$

即 $E' = 5639$。

## 二、秘密共享

假定有一个文件 $M$ 与 $r$ 个人有关。为了共同的利益，他们约定，只有当他们中的至少 $s$（$s \le r$）个人同意时，才可以把 $M$ 公开。这样，就需要一种满足下述条件的加密方法：

(ⅰ) $r$ 个人各掌握一个与这个加密方法有关的数据；

(ⅱ) 利用 $s$ 个不同的数据可以很容易地求出 $M$；

(iii) 如果知道的数据少于 $s$ 个，那么求出 $M$ 是很难的。

现在，我们来提出一个满足这些条件的加密方法。

选取素数 $p > M$，又选取两两互素的正整数 $m_1, m_2, \cdots, m_r$，使得

$$m_1 < m_2 < \cdots < m_r \ ,\ p \nmid m_1 m_2 \cdots m_r \ ,$$

$$m_1 m_2 \cdots m_s \geq p m_r m_{r-1} \cdots m_{r-s+2} 。 \tag{5}$$

又随机地选取正整数 $t$，使得

$$t \leq \frac{m_1 m_2 \cdots m_s}{p} - 1 。 \tag{6}$$

我们这样来计算第 $i$（$i = 1, 2, \cdots, r$）个人所要掌握的数据：

$$E_i \equiv M + tp \pmod{m_i}，\ 0 \leqslant E_i < m_i，\quad i = 1, 2, \cdots, r 。$$

下面，我们说明 $E_1, E_2, \cdots, E_r$ 是满足上述要求(ⅰ)，(ⅱ)，(iii)的数据。显然，只需证明条件(ⅱ)和(iii)是满足的。

条件(ⅱ)：由 $s$ 个不同的数据可以容易地求出 $M$。

设这 $s$ 个数据 $E_{i_1}, E_{i_2}, \cdots, E_{i_s}$。由孙子定理我们知道，存在唯一的 $x_0$，$0 \leq x_0 < m_{i_1} m_{i_2} \cdots m_{i_s}$，满足方程组

$$x \equiv E_{i_k} \pmod{m_{i_k}} \ ,\ 1 \leq k \leq s \ 。 \tag{7}$$

显然 $M + tp$ 满足方程组(7)，而且，由于 $p > M$ 以及式(6)，有

$$M + tp < (t+1)p \leq m_1 m_2 \cdots m_s \leq m_{i_1} m_{i_2} \cdots m_{i_l} \ , \tag{8}$$

因此，必是 $x_0 = M + tp$，即 $M = x_0 - tp$。

条件(iii)：如果仅仅知道 $E_{i_1}, E_{i_2}, \cdots, E_{i_l}$，$l \leq s - 1$，则确定 $M$ 是很困难的。

事实上，由孙子定理，方程组

$$x \equiv E_{i_k} \pmod{m_{i_k}} \ ,\ 1 \leq k \leq l \tag{9}$$

对模 $m_{i_1} m_{i_2} \cdots m_{i_l}$ 有唯一解 $x_0$，$0 \leq x_0 < m_{i_1} m_{i_2} \cdots m_{i_l}$。因为 $m_{i_1}, m_{i_2}, \cdots, m_{i_l}$ 是两两互素的，由 $E_i$ 的定义，显然

$$x_0 \equiv M + tp \pmod{m_{i_1} m_{i_2} \cdots m_{i_l}} 。 \tag{10}$$

即

$$M + tp - x_0 = \lambda m_{i_1} m_{i_2} \cdots m_{i_l} \ , \tag{11}$$

其中 $\lambda$ 是整数。要确定 $M$ 的值，必须确定 $\lambda$ 的数值。我们要说明，确定



$\lambda$ 的数值是困难的。事实上，由式(11)，得到

$$0 \leq \lambda \leq \frac{M + tp - x_0}{m_{i_1} m_{i_2} \cdots m_{i_l}} 。 \tag{12}$$

另一方面，由式(5)式(6)和 $l \leq s - 1$，以及

$$0 \leq x_0 < m_{i_1} m_{i_2} \cdots m_{i_l} < m_r m_{r-1} \cdots m_{r-s+2}$$

得到

$$\frac{M + tp - x_0}{m_{i_1} m_{i_2} \cdots m_{i_l}} > \frac{M + tp}{m_r m_{r-1} \cdots m_{r-s+2}} - 1 。$$

由式(8)我们见到，$M + tp$ 的取值范围是从 1 到 $m_1 m_2 \cdots m_s$，因此，利用式(5)可知，$\dfrac{M + tp - x_0}{m_{i_1} m_{i_2} \cdots m_{i_l}}$ 的取值范围是从 1 到 $p - 1$，于是，由式(12)，$\lambda$ 的取值范围是从 0 到 $p - 1$，当 $p$ 很大的时候，确定 $\lambda$ 的数值显然是困难的，

**例 2** 设由三方共同管理的一份文件是 $M = 5$。取 $p = 7$，$m_1 = 11$，$m_2 = 12$，$m_3 = 17$，则 $11 \cdot 12 > 7 \cdot 17$。

取 $t = 14 < \dfrac{1}{p} m_1 m_2 - 1 = \dfrac{1}{7} \cdot 11 \cdot 12 - 1$，分配给三方的数据分别是

$$E_1 \equiv 5 + 14 \cdot 7 \equiv 4 \pmod{11}，\ E_1 = 4；$$

$$E_2 \equiv 5 + 14 \cdot 7 \equiv 7 \pmod{12}，\ E_2 = 7；$$

$$E_3 \equiv 5 + 14 \cdot 7 \equiv 1 \pmod{17}，\ E_3 = 1。$$

由 $E_1$，$E_2$ 与 $E_3$ 中的任意两个都可以确定出 $M$。例如，假设已知 $E_1 = 4$ 和 $E_2 = 7$，则利用孙子定理，得到方程组

$$x \equiv 4 \pmod{11}，\ x \equiv 7 \pmod{12}$$

的解 $x_0 \equiv 103 \pmod{11 \cdot 13}$，于是

$$M = x_0 - tp = 103 - 14 \cdot 7 = 5 \ 。$$

## 习 题 五

**1.** 设某数据库由四个文件组成：$F_1 = 4$，$F_2 = 6$，$F_3 = 10$，$F_4 = 13$。试设计一个对该数据库加密的方法，但要能取出个别的 $F_i$（$1 \leq i \leq 4$），

同时不影响其他文件的保密。

**2.** 利用本节中的秘密共享方案，设计一个由三方共管文件 $M=3$ 的方法，要求：只要有两方提供他们所掌握的数据，就可以求出文件 $M$，但是，仅由任何一方的数据，不能求出文件 $M$。（提示：取 $p=5$，$m_1=8$，$m_2=9$，$m_3=11$）

# 第六节　背包型加密方法

假设 $a_1, a_2, \cdots, a_n$ 是正整数，对于给定的整数 $b$，方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \tag{1}$$

是否有 0–1 解，即解$(x_1, x_2, \cdots, x_n)$，$x_i=0$ 或 1（$1 \le i \le n$）？这就是“背包问题”。一般地，求解背包问题是计算上困难的。但是，对于某些特殊的 $a_1, a_2, \cdots, a_n$，背包问题是容易解决的。例如，若 $a_1, a_2, \cdots, a_n$ 满足条件

$$a_i > a_1 + a_2 + \cdots + a_{i-1}\ ,\ 2 \le i \le n\ , \tag{2}$$

则解方程(1)可以按以下步骤进行：

(ⅰ) 比较 $b$ 与 $a_n$，若 $a_n > b$，则 $x_n=0$；否则，$x_n=1$；

(ⅱ) 若 $x_n, x_{n-1}, \cdots, x_{k+1}$ 已经确定，则由方程

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = b - (a_nx_n + \cdots + a_{k+1}x_{k+1})$$

及步骤(ⅰ)确定 $x_k$。

(iii) 重复步骤(ⅰ)与(ⅱ)，直到求出所有的 $x_i$（$1 \le i \le n$）：或者，断定方程(1)没有 0–1 解。

**定义 1**　若 $a_1, a_2, \cdots, a_n$ 都是正整数，则称向量$(a_1, a_2, \cdots, a_n)$是背包向量。称满足条件(2)的背包向量为超增背包向量，或超增向量。

如上所述，一般地，求解背包问题是计算上困难的。但是，对于某些特殊的背包向量（例如，超增背包向量），求解背包问题并不困难。求解一般的背包问题与特殊的背包问题在计算困难程度上的差别，是设计背包型加密方法的基础。1978 年，R. C. Merkel 与 M. E. Hellman 提出了一个加密方法，是以求解背包问题的计算困难性为基础的，这个方法，称为 MH 加密方法。

**MH 加密方法的设计**



Ⅰ　参数的选取

随机地选取正整数 $M$，$k$，$(M, k)=1$，以及超增背包向量$(a_1, a_2, \cdots, a_n)$，使得

$$a_1 + a_2 + \cdots + a_n < M; \tag{3}$$

计算

$$b_i \equiv ka_i \pmod{M},\ 1 \le b_i < M,\ 1 \le i \le n \tag{4}$$

以及正整数 $k^{-1}$，使得

$$kk^{-1} \equiv 1 \pmod{M}。 \tag{5}$$

将背包向量$(b_1, b_2, \cdots, b_n)$公开，称为加密钥。正整数 $M$，$k$，$k^{-1}$ 则保密。

Ⅱ　明文的加密

设明文的二进制表示是 $P=(p_1p_2\cdots p_n)_2$，则与 $P$ 对应的密文是

$$E = b_1p_1 + b_2p_2 + \cdots + b_np_n。 \tag{6}$$

Ⅲ　解密

(ⅰ) 计算

$$E_0 \equiv k^{-1}E \pmod{M},\ 0 \le E_0 < M。 \tag{7}$$

(ⅱ) 由

$$E_0 = a_1p_1 + a_2p_2 + \cdots + a_np_n \tag{8}$$

求出 $p_1, p_2, \cdots, p_n$。

**注 1**：一般地，用 MH$(b_1, b_2, \cdots, b_n)$表示上面所定义的加密方法。

**注 2**：我们来说明由式(8)所确定的$(p_1p_2\cdots p_n)_2$ 就是明文 $P$。事实上，由式(6)和式(5)，有

$$\begin{aligned} k^{-1}E &= k^{-1}(b_1p_1 + b_2p_2 + \cdots + b_np_n) \\ &\equiv kk^{-1}(a_1p_1 + a_2p_2 + \cdots + a_np_n) \\ &\equiv a_1p_1 + a_2p_2 + \cdots + a_np_n \pmod{M}。 \end{aligned}$$

由式(3)，得到

$$0 \le a_1p_1 + a_2p_2 + \cdots + a_np_n \le a_1 + a_2 + \cdots + a_n < M。$$

所以，由上式和式(7)，可知 $E_0 = a_1p_1 + a_2p_2 + \cdots + a_np_n$。因此，由式(8)得到的 $p_1, p_2, \cdots, p_n$ 就是明文 $P$ 的二进制表示的位数码。

**例 1**　利用超增背包向量(2, 3, 6, 12, 24, 48)设计一个背包型加密方法，将明文 $P=47$ 加密。

**解**　取 $M=99$，$k=5$，$k^{-1}=20$，计算

$$b_1 \equiv 5\cdot 2 = 10 \pmod{99},$$

取 $b_1 = 10$。同样的，计算

$$b_2 \equiv 5\cdot 3 = 15 \pmod{99}，取\ b_2 = 15，$$
$$b_3 \equiv 5\cdot 6 = 30 \pmod{99}，取\ b_3 = 30，$$
$$b_4 \equiv 5\cdot 12 = 60 \pmod{99}，取\ b_4 = 60，$$
$$b_5 \equiv 5\cdot 24 \equiv 21 \pmod{99}，取\ b_5 = 21，$$
$$b_6 \equiv 5\cdot 48 \equiv 42 \pmod{99}，取\ b_6 = 42。$$

对外公开的加密向量是(10, 15, 30, 60, 21, 42)。

由于 $P = 47 = (101111)_2$，所以与 $P$ 对应的密文是

$$E = 10\cdot 1 + 15\cdot 0 + 30\cdot 1 + 60\cdot 1 + 21\cdot 1 + 42\cdot 1 = 163。$$

若要从密文 163 得到明文 $P$，计算

$$k^{-1}E = 20\cdot 163 = 3260 \equiv 92 \pmod{99},$$

解方程

$$92 = 2p_1 + 3p_2 + 6p_3 + 12p_4 + 24p_5 + 48p_6,$$

其中 $p_i = 0$ 或 1，$i = 1, 2, 3, 4, 5, 6$，得到 $p_1 = 1$，$p_2 = 0$，$p_3 = 1$，$p_4 = 1$，$p_5 = 1$，$p_6 = 1$，即明文是 $P = (101111)_2 = 47$。

在加密一个文件时，自然希望有很好的保密性。于是，出现了这样一个问题：把加密过的密文再加密一次是否能会提高保密性？ 事实并非总是如此。为了说明这一点，我们来看一下用 MH 方法两次施行加密的情况。

迭代 *M*H 加密方法的设计

Ⅰ 参数的选取

随机地选取超增向量$(a_1, a_2, \cdots, a_n)$，正整数 $M_1$，$k_1$，$(M_1, k_1) = 1$，使得 $a_1 + a_2 + \cdots + a_n < M_1$，计算

$$c_i \equiv k_1 a_i \pmod{M_1}，\ 1 \le c_i < M_1，\ 1 \le i \le n;$$

再随机地选取正整数 $M_2$，$k_2$，$(M_2, k_2) = 1$，使得 $c_1 + c_2 + \cdots + c_n < M_2$，计算

$$b_i \equiv k_2 c_i \pmod{M_2}，\ 1 \le b_i < M_2，\ 1 \le i \le n。$$

将$(b_1, b_2, \cdots, b_n)$公开，作为加密钥。

将$(a_1, a_2, \cdots, a_n)$，$k_1$，$k_2$，$M_1$，$M_2$ 以及由下式确定的 $k_1^{-1}$ 与 $k_2^{-1}$ 保密：

$$k_i k_i^{-1} \equiv 1 \pmod{M_i}，\quad i = 1, 2。$$

Ⅱ 加密 仍使用式(6)。

Ⅲ 解密 由密文 $E$，首先计算



$$E_0' \equiv k_2^{-1}E \pmod{M_2}，\ 0 \le E_0' < M_2;$$

再计算

$$E_0 \equiv k_1^{-1}E_0' \pmod{M_2}，\ 0 \le E_0 < M_1，$$

再由式(8)求出明文 $P$。

粗看起来，迭代 MH 加密方法应该具有更好的保密性。其实不然。下面就是一个例子。

**例 2** 给定超增背包向量（5, 10, 20），以及 $M_1 = 47$，$k_1 = 17$，$M_2 = 89$，$k_2 = 3$，由

$$c_i \equiv 17a_i \pmod{47}，\ 1 \le i \le 3，\ 0 \le c_i \le 46$$

得到$(c_1, c_2, c_3) = (38, 29, 11)$，再由

$$b_i \equiv 3c_i \pmod{89}，\ 1 \le i \le 3，\ 0 \le b_i \le 88$$

得到$(b_1, b_2, b_3) = (25, 87, 33)$，这就是要公开的加密钥。这显然是一个超增背包向量，因此，用它所得到的密文很容易被解密。

## 习 题 六

**1.** 设明文 $P$ 的二进制表示是 $P = (p_1p_2p_3p_4p_5p_6p_7p_8)_2$，与 $P$ 对应的密文是 $E$ 是 $E = a_1p_1 + a_2p_2 + \cdots + a_8p_8$，如果这里的超增背包向量$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (5, 17, 43, 71, 144, 293, 626, 1280)$，并且已知密文 $E = 1999$，求明文 $P$。

**2.** 给定超增背包向量(2, 3, 7, 13, 29, 59)，试设计一个背包型加密方法，将明文 $P = 51$ 加密。（提示：取 $M = 118$，$k = 77$）。