第一章　整数的唯一分解定理

整数的唯一分解定理，又叫算术基本定理，它是初等数论中最基本的定理之一．本章将给出这个定理两种不同的证明，以及介绍与此有关的初等数论中最基本的概念和性质．

§1 整 除 性

两个整数的和、差、积仍然是整数，但是用一个不等于零的整数去除另一个整数所得的商却不一定是整数，因此，我们引进整除的概念．

定义　任给两个整数 a, b，其中 $b\neq 0$，如果存在一个整数 q 使得等式

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

成立，我们就说 b **整除** a，记作 $b\mid a$，此时我们把 b 叫做 a 的**因数**，把 a 叫做 b 的**倍数**．如果(1)里的整数 q 不存在，我们就说 b 不整除 a，记作 $b\nmid a$．

由整除的定义出发，下面一些性质是明显的．

1. 如果 $b\mid a, c\mid b$，则 $c\mid a$．
2. 如果 $b\mid a$，则 $cb\mid ca$．
3. 如果 $c\mid a, c\mid b$，则对任意的整数 m, n，有
$$c\mid ma+nb.$$
4. 如果 $b\mid a$ 且 $a\neq 0$，则 $|b|\leqslant|a|$．
5. 如果 $cb\mid ca$，则 $b\mid a$．
6. 如果 $b\mid a, a\neq 0$，则 $\dfrac{a}{b}\Big|a$．

一般地，有下面的定理.

定理 1 设 a, b 是两个整数，其中 $b>0$，则存在两个唯一的整数 q 及 r，使得

$$a=bq+r, \quad 0\leqslant r<b \tag{2}$$

成立.

证 作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots,$$

则 a 必在上述序列的某两项之间，即存在一个整数 q 使得

$$qb\leqslant a<(q+1)b$$

成立. 令 $a-qb=r$，则(2)成立.

设 q_1, r_1 是满足(2)的另一对整数，因为

$$bq_1+r_1=bq+r,$$

于是

$$b(q-q_1)=r_1-r,$$

故

$$b|q-q_1|=|r_1-r|.$$

由于 r 及 r_1 都是小于 b 的非负整数，所以上式右边是小于 b 的. 如果 $q\neq q_1$，则上式左边$\geqslant b$，这是不可能的. 因此，$q=q_1, r=r_1$.

证完

定义 我们把(2)中的 q 叫做 a 被 b 除得出的**不完全商**，r 叫做 a 被 b 除所得到的**余数**，也叫做**非负最小剩余**，常记作 $\langle a\rangle_b=r$. 以后，我们总假定除数 $b>0$ 以及因数为正.

在不致引起混淆的情况下，$\langle a\rangle_b$ 中的 b 常略去不写. 我们有

定理 2 对于整数 a_1, a_2, b，其中 $b>0$，常有

$$\langle a_1+a_2\rangle=\langle\langle a_1\rangle+\langle a_2\rangle\rangle, \tag{3}$$

$$\langle a_1-a_2\rangle=\langle\langle a_1\rangle-\langle a_2\rangle\rangle, \tag{4}$$

$$\langle a_1a_2\rangle=\langle\langle a_1\rangle\langle a_2\rangle\rangle. \tag{5}$$

证 设

$$a_1=bq_1+\langle a_1\rangle,\ a_2=bq_2+\langle a_2\rangle,$$
$$\langle a_1\rangle+\langle a_2\rangle=bq_3+\langle\langle a_1\rangle+\langle a_2\rangle\rangle,$$

故

$$\begin{aligned}a_1+a_2&=b(q_1+q_2)+\langle a_1\rangle+\langle a_2\rangle\\&=b(q_1+q_2+q_3)+\langle\langle a_1\rangle+\langle a_2\rangle\rangle.\end{aligned}\tag{6}$$

由定理 1，即得(3)式，类似地可证(4)和(5). 证完

§2 最大公因数与辗转相除法

利用上节的定理 1，我们来研究整数的最大公因数的存在问题和实际求法.

定义 设 $a_1, a_2, \cdots, a_n$ 是 n 个不全为零的整数. 若整数 d 是它们之中每一个的因数，那么 d 就叫做 $a_1, a_2, \cdots, a_n$ 的一个**公因数**. 这时，它们的公因数只有有限个. 整数 $a_1, a_2, \cdots, a_n$ 的公因数中最大的一个叫**最大公因数**，记作 $(a_1, \cdots, a_n)$，若 $(a_1, \cdots, a_n)=1$，我们说 $a_1, a_2, \cdots, a_n$ **互素**. 我们有下面的定理.

定理 1 设 a, b, c 是任意三个不全为零的整数，且

$$a=bq+c,$$

其中 q 是整数，则 $(a, b)=(b, c)$.

证 因为 $(a, b)\mid a$, $(a, b)\mid b$，所以有 $(a, b)\mid c$，因而 $(a, b)\leqslant(b, c)$. 同法可证 $(b, c)\leqslant(a, b)$，于是得到 $(a, b)=(b, c)$.

证完

因为，显然有 $(a_1, a_2, \cdots, a_n)=(|a_1|, |a_2|, \cdots, |a_n|)$，又因为，一组不全为零的整数的最大公因数，等于它们当中全体不为零的整数的最大公因数，所以，不妨设 $a_i>0\ (i=1, \cdots, n)$. 我们先讨论两个正整数的最大公因数的求法，即**辗转相除法**，并借此推出最大

公因数的若干性质.

任给整数 $a>0, b>0$, 由带余数的除法, 有下列等式:

$$\begin{aligned} a &= bq_1 + r_1, \quad 0<r_1<b, \\ b &= r_1 q_2 + r_2, \quad 0<r_2<r_1, \\ &\cdots \quad \cdots \quad \cdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad 0<r_n<r_{n-1}, \\ r_{n-1} &= r_n q_{n+1} + r_{n+1}, \quad r_{n+1} = 0, \end{aligned} \tag{1}$$

因为 $b>r_1>r_2>r_3>\cdots$, 故经有限次带余除法后, 总可以得到一个余数是零, 即(1)中 $r_{n+1}=0$.

现在我们证明

定理 2　若任给整数 $a>0, b>0$, 则 (a, b) 就是(1)中最后一个不等于零的余数, 即 $(a, b)=r_n$.

证　由定理 1 即得

$$r_n = (0, r_n) = (r_n, r_{n-1}) = \cdots = (r_2, r_1) = (r_1, b) = (a, b).$$

证完

从(1)中 $r_n = r_{n-2} - r_{n-1} q_n$, $r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$, 得

$$r_n = r_{n-2}(1 + q_n q_{n-1}) - r_{n-3} q_n,$$

再将 $r_{n-2} = r_{n-4} - r_{n-3} q_{n-2}$ 代入上式, 如此继续下去, 最后可得 $r_n = sa + tb$, 其中 s, t 是两个整数. 于是有

定理 3　若任给整数 $a>0, b>0$, 则存在两个整数 m, n 使得

$$(a, b) = ma + nb.$$

显然有

推论　a 和 b 的公因数是 (a, b) 的因数.

例　用辗转相除法求 $a=288, b=158$ 的最大公因数和 m, n, 使 $ma+nb=(a, b)$.

由

$$288 = 158 \cdot 1 + 130,$$

$$158=130\cdot1+28,$$

$$130=28\cdot4+18,$$

$$28=18\cdot1+10,$$

$$18=10\cdot1+8,$$

$$10=8\cdot1+2,$$

$$8=2\cdot4.$$

因此，$(288,158)=2$.

再由 $2=10-8\cdot1=10-(18-10)=10\cdot2-18$

$=(28-18\cdot1)2-18=28\cdot2-18\cdot3$

$=28\cdot2-(130-28\cdot4)3=-130\cdot3+28\cdot14$

$=-130\cdot3+(158-130\cdot1)14=14\cdot158-17\cdot130$

$=14\cdot158-17(288-158\cdot1)=31\cdot158-17\cdot288,$

故 $m=-17, n=31$.

对于§ 1的(2)中的余数，如果不要求它是正的，那么，对于整数 a 和 $b>0$，则存在整数 s, t，使 $a=bt+s$ 成立，其中 $|s|\leqslant\frac{b}{2}$. 这是因为，当§1,(2)中的 $r<\frac{b}{2}$ 时，取 $s=r$；当 $r>\frac{b}{2}$ 时，取 $s=r-b$；当 b 是偶数且 $r=\frac{b}{2}$ 时，则 s 可取 $\frac{b}{2}$ 和 $-\frac{b}{2}$ 两个数中的任意一个. 数 s 叫做 a 被 b 除所得到的**绝对最小剩余**. 如果我们在(1)的计算过程中，都取绝对最小剩余，并设最后一个不为零的余数为 s_m，则由定理1，仍然有 $|s_m|=(a,b)$. 仍用前例说明：

$$288=158\cdot2-28,$$

$$158=28\cdot6-10,$$

$$28=10\cdot3-2,$$

$$10=2\cdot5,$$

与一般的辗转相除法相比较计算步骤由 7 次减少为 4 次.

定理 4 若 $a|bc, (a,b)=1$, 则 $a|c$.

证 若 $c\neq 0$, 由 $(a,b)=1$ 知存在两个整数 m, n 使 $ma+nb=1$, 故 $mac+nbc=c$, 由 $a|bc$, 知 $a|c$; 若 $c=0$, 结论显然成立.

证完

现在来研究两个以上正整数的最大公因数. 设 $n>2$, $a_1>0$, $a_2>0, \cdots, a_n>0$, $(a_1,a_2)=d_2$, $(d_2,a_3)=d_3, \cdots, (d_{n-1},a_n)=d_n$, 那么有下面的定理.

定理 5 若 $a_1, \cdots, a_n$ $(n>2)$ 是 n 个正整数, 则

$$(a_1,a_2,\cdots,a_n)=d_n.$$

证 由 $d_n|a_n, d_n|d_{n-1}, d_{n-1}|a_{n-1}, d_{n-1}|d_{n-2}$, 可得

$$d_n|a_{n-1}, \quad d_n|d_{n-2}.$$

由此类推, 最后得到

$$d_n|a_n, \quad d_n|a_{n-1}, \cdots, d_n|a_1,$$

因此有 $d_n\leqslant(a_1,\cdots,a_n)$. 另一方面, 设 $(a_1,\cdots,a_n)=d$, 由定理 3 的推论可得

$$d|d_2, d|d_3, \cdots, d|d_n,$$

故

$$d\leqslant d_n.$$

于是得到 $(a_1,a_2,\cdots,a_n)=d_n$. 证完

由定理 5 可推出

定理 6 设 a_1, a_2, $\cdots$, a_n 均为正整数, $n>2$, 则存在整数 $x_1, \cdots, x_n$ 使得

$$a_1x_1+\cdots+a_nx_n=(a_1,\cdots,a_n)$$

成立.

§3 最小公倍数

定义 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数($n \geqslant 2$)，若 m 是这 n 个数中每一个数的倍数，则 m 就叫做这 n 个数的一个**公倍数**. 在 $a_1, a_2, \cdots, a_n$ 的一切公倍数中最小的正数叫做**最小公倍数**，记作 $[a_1, \cdots, a_n]$.

因为乘积 $|a_1||a_2|\cdots|a_n|$ 就是 $a_1, \cdots, a_n$ 的一个公倍数，故最小公倍数是存在的.

由于任何正整数都不是零的倍数，故讨论整数的最小公倍数时，总假定这些整数都不是零.

和最大公因数一样，显然有 $[a_1, \cdots, a_n]=[|a_1|, \cdots, |a_n|]$，所以只需对正整数讨论它们的最小公倍数.

我们先研究两个正整数的最小公倍数.

定理 1 设 a, b 是任给的两个正整数，则

① a, b 的所有公倍数就是 $[a, b]$ 的所有倍数.

② $[a, b]=\dfrac{ab}{(a, b)}$.

证 设 m 是 a, b 的任一公倍数，$m=ak=bk'$，令 $a=a_1(a, b)$，$b=b_1(a, b)$，代入 $ak=bk'$ 得 $a_1k=b_1k'$，因为 $(a_1, b_1)=1$，故 $b_1 | k$. 因此

$$m=ak=ab_1t=\frac{ab}{(a, b)}t, \tag{1}$$

其中 t 满足等式 $k=b_1t$. 反之，当 t 为任一整数时，$\dfrac{ab}{(a, b)}t$ 为 a，b 的一个公倍数，故(1)可以表示 a, b 的一切公倍数. 令 $t=1$，即得最小的正数，故 $[a, b]=\dfrac{ab}{(a, b)}$，这便证明了定理 1 中的②. 又由(1)式定理中的①也得证.

证完

现在讨论两个以上整数的最小公倍数. 设 $a_1, a_2, \cdots, a_n$ 是 n 个正整数，令

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

我们有

定理 2 若 $a_1, \cdots, a_n$ 是 n $(n>2)$ 个正整数，则

$$[a_1, a_2, \cdots, a_n] = m_n.$$

证 由(2)知 $m_i | m_{i+1}$, $i=2, 3, \cdots, n-1$, 且 $a_1 | m_2$, $a_i | m_i$, $i=2, \cdots, n$, 故 m_n 是 $a_1, \cdots, a_n$ 的一公倍数. 又设 m 是 $a_1, \cdots, a_n$ 的任一公倍数，则 $a_1 | m$, $a_2 | m$, 故由定理 1 知 $m_2 | m$, 又 $a_3 | m$, 同理可得 $m_3 | m$. 依此类推，最后得 $m_n | m$, 因此 $m_n \leqslant |m|$, 故

$$m_n = [a_1, \cdots, a_n].$$

证完

我们已经介绍了最大公因数的求法，上面两个定理又给出了最小公倍数的求法.

§4 整数的唯一分解定理

在正整数里，1 的因数就只有它本身. 任一个大于 1 的整数都至少有两个因数，即 1 和它本身.

定义 一个大于 1 的整数，如果它的正因数只有 1 和它本身，就叫做**素数**，否则就叫做**复合数**.

本节的主要目的就是要证明任何一个大于 1 的整数，如果不论次序，则能唯一地表成素数的乘积. 对于唯一性我们将给出两个不同的证明. 为此，先证明几个引理.

引理 1 设 a 是任一大于 1 的整数，则 a 的除 1 以外的最小正因数 q 是素数，并且当 a 是复合数时，

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

证 假定 q 不是素数，由定义，q 除 1 和它本身以外还有一正

因数 q_1，因而 $1<q_1<q$，但 $q_1 \mid a$，所以有 $q_1 \mid a$，这与 q 是最小正因数矛盾，故 q 是素数.

当 a 是复合数时，则 $a=a_1q$，且 $q \leqslant a_1$，故 $q \leqslant \sqrt{a}$. 证完

引理 2 若 p 是一素数，a 是任一整数，则有 $p \mid a$ 或 $(p, a)=1$.

证 因为 $(p, a) \mid p$，故 $(p, a)=1$ 或 $(p, a)=p$，后者即 $p \mid a$.

证完

引理 3 若 p 是素数，$p \mid ab$，则 $p \mid a$ 或 $p \mid b$.

证 若 $p \nmid a$，则由引理 2，$(p, a)=1$，再由 §2 的定理 4 知 $p \mid b$.

证完

定理(整数的唯一分解定理) 任一大于 1 的整数能表成素数的乘积，即对于任一整数 $a>1$，有

$$a=p_1p_2\cdots p_n,\ p_1 \leqslant p_2 \leqslant \cdots \leqslant p_n, \tag{1}$$

其中 $p_1, p_2\cdots, p_n$ 是素数. 并且若

$$a=q_1q_2\cdots q_m,\ q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m, \tag{2}$$

其中 $q_1, q_2, \cdots, q_m$ 是素数，则 $m=n$，$q_i=p_i\ (i=1, 2, \cdots, n)$.

定理的证明：首先我们用数学归纳法证明(1)式成立. 当 $a=2$ 时，(1)式显然成立. 假定对于一切小于 a 的正整数(1)式都成立. 此时，若 a 是素数，则(1)式对 a 成立；若 a 是复合数，则有两个正整数 b, c 满足条件

$$a=bc, 1<b \leqslant c<a,$$

由归纳法假设，b 和 c 分别能表成素数的乘积，故 a 能表成素数的乘积，即(1)式成立. 其次，证明唯一性. 若对 a 同时有(1)，(2)两式成立，则

$$p_1p_2\cdots p_n=q_1q_2\cdots q_m. \tag{3}$$

由引理 3 知有 p_k，q_j 使得 $p_1 \mid q_j$，$q_1 \mid p_k$，但 q_j，p_k 都是素数，所以 $p_1=q_j$，$q_1=p_k$. 又 $p_k \geqslant p_1$，$q_j \geqslant q_1$，故同时有 $q_1 \geqslant p_1$ 和 $p_1 \geqslant q_1$，因

而 $p_1=q_1$，由(3)式得 $p_2\cdots p_n=q_2\cdots q_m$. 同理可得 $p_2=q_2$，$p_3=q_3$，依此类推，最后得 $m=n$，$p_n=q_n$. 证完

在给出唯一性的第二个证明之前，再证一个引理.

引理 4　如果对于某一个确定的整数 $b>1$，分解是唯一的，且 p 是 b 的任一个素因子，则 p 必须出现在 b 分解为素数乘积的分解式中.

证　如果 $b=p$，则引理成立. 否则设 $b=pb_1$，$b_1>1$. 因为任一大于 1 的整数可表为素数的乘积，可设 $b_1=p_1\cdots p_k$，这里 $p_1,\cdots,p_k$ 是素数，则 $b=pp_1\cdots p_k$ 是 b 分解为素数乘积的分解式. 由假设，对 b 来说除了次序之外此分解式是唯一的，因此 p 出现在 b 分解为素数乘积的分解式中. 证完

定理中唯一性的第二个证明：如果分解不是唯一的，那么至少有一个整数 $a>1$，a 有两种不同的分解. 设 a 是具有这种性质的整数中最小的，它的两个不同的分解式为

$$a=p_1\cdots p_k,\quad p_1\leqslant p_2\leqslant\cdots\leqslant p_k,\ k\geqslant 2, \tag{4}$$

和

$$a=p'_1\cdots p'_j,\quad p'_1\leqslant p'_2\leqslant\cdots\leqslant p'_j,\ j\geqslant 2. \tag{5}$$

设集 $P=\{p_1,\cdots,p_k\}$，$P'=\{p'_1,\cdots,p'_j\}$，显然 $P\cap P'=$空集，否则，例如 $p_1=p'_1$，则 $\frac{a}{p_1}$ 满足 $1<\frac{a}{p_1}<a$，且有两种不同的分解，与所设 a 最小矛盾，根据引理 1，由(4)和(5)分别得 $a\geqslant p_1^2$，$a\geqslant p_1'^2$，因为 $p_1\neq p'_1$，故 $a>p_1p'_1$，设 $t=a-p_1p'_1$，因为 $p_1\mid a$，$p'_1\mid a$，故 $p_1\mid t$，$p'_1\mid t$，又因为 $1\leqslant t<a$，所以定理的唯一性对 t 成立，而且由引理 4 知

$$t=p_1p'_1t_1,$$

其中 $t_1>0$，故

$$a=p_1p'_1(t_1+1)=p_1p'_1q_1\cdots q_n, \tag{6}$$

$q_i(i=1,\cdots,n)$ 是素数，由(4)和(6)得

$$p_1'q_1\cdots q_n=\frac{a}{p_1}=p_2\cdots p_k. \tag{7}$$

因为 p_1' 不可能出现在(7)的右端，故(7)给出$\frac{a}{p_1}$两种不同的分解，与所设 a 最小矛盾. 证完

算术基本定理告诉我们，任一大于 1 的整数能够唯一地写成

$$a=p_1^{\alpha_1}\cdots p_k^{\alpha_k},\quad \alpha_i>0(i=1,\cdots,k), \tag{8}$$

其中 $p_i<p_j(i<j)$是素数.

(8)叫做 a 的**标准分解式**.

如果 $d|a, d>0$，则由(8)和引理 3，d 可表成

$$d=p_1^{\beta_1}\cdots p_k^{\beta_k},\quad \alpha_i\geqslant\beta_i\geqslant 0(i=1,\cdots,k) \tag{9}$$

的形式. 反之，如 d 可表成(9)的形式，则必有 $d|a, d>0$.

作为唯一分解定理一个简单而直接的应用，我们有：设 $a>0, b>0$，且

$$a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}, \alpha_i\geqslant 0(i=1,\cdots,k),$$
$$b=p_1^{\beta_1}\cdots p_k^{\beta_k}, \beta_i\geqslant 0(i=1,\cdots,k),$$

则

$$(a,b)=p_1^{r_1}\cdots p_k^{r_k}, r_i=\min(\alpha_i,\beta_i)\ (i=1,\cdots,k),$$
$$[a,b]=p_1^{\delta_1}\cdots p_k^{\delta_k}, \delta_i=\max(\alpha_i,\beta_i)\ (i=1,\cdots,k),$$

符号 $\min(\alpha_i,\beta_i)$表示 α_i,β_i 中较小的数，$\max(\alpha_i,\beta_i)$表示 α_i，β_i 中较大的数.

对于任意实数 x, y，显然有

$$x+y=\max(x,y)+\min(x,y),$$

由此，又得到在 §3 中已经证明过的结果：

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

上面从理论上证明了任意一个大于 1 的整数，可以写成它的标准分解式，而且这样一个分解式可以通过有限步的计算求出. 但

是，在实际计算时，特别当 a 很大时，仍然由于计算量太大，常常难以办到. 因此，用正整数的标准分解式来求最大公因数并不简单，而用辗转相除法来求的优点在于不必把正整数分解成标准分解式. 至于大整数的分解仍然是近代数论研究的重要课题之一，它不仅具有理论价值，而且有实际应用，我们将在第三章中介绍.

顺便指出，在自然数的子集

$$S=\{3k+1 \mid k=0,1,2,\cdots\}$$

中，如果定义其"素数"是恰有两个因子在 S 中，例如 4, 7, 10, 13, 19, 22, 25, 31, …都是 S 中的"素数"，那么 S 中的数 100 就有两种分解形式：

$$100=4\cdot 25, 100=10\cdot 10.$$

这说明当素数的定义改变后，整数的唯一分解定理就不成立了. 因此，这个定理反映了整数的本质.

数论中许多结果都依赖于唯一分解定理的成立，在本章后面的某些节中，将看到这样的例子.

§5 素数，厄拉多塞筛法

大约在公元前 250 年，古希腊数学家厄拉多塞 (Eratosthenes) 提出一个造出不超过 N 的素数表的方法，后来人们把它称为**厄拉多塞筛法**. 它基于这样一个简单的性质：如果 $n\leqslant N$，而 n 是复合数，则 n 必为一不大于 $\sqrt{N}$ 的素数所整除. 这个性质由 §4 的引理 1 即可推出. 厄拉多塞筛法的具体方法如下：先列出不超过 $\sqrt{N}$ 的全体素数，设为 $2=p_1<p_2<\cdots<p_k\leqslant\sqrt{N}$，然后依此排列 $2, 3, \cdots, N$，在其中留下 $p_1=2$，而把 p_1 的倍数全部划掉，再留下 p_2，而把 p_2 的倍数划掉，继续这一手续，直到最后留下 p_k 而划去 p_k 的全部倍数，根据前面提到的性质，留下的就是不超过 N 的全体素数. 近代素数表都是由此法略加变化造出的. 例如，1914

年莱梅(D. N. Lehmer)发表了 1 到 10006721 的素数表，1951 年，库利克(Kulik)等又把它增加到 10999997.

当然厄拉多塞筛法不可能造出全部素数，因为，素数是无穷的. 我们有

定理 1 素数的个数是无穷的.

证 如果素数的个数是有限的，那么设 $p_1=2, p_2=3, \cdots, p_k$ 是全体素数. 再设 $P=p_1p_2\cdots p_k+1$，q 是 p 的素因数，则有 $q\neq p_j(j=1,\cdots,k)$，因为否则至少有一个 $p_i, 1\leqslant i\leqslant k$，满足 $q=p_i$，从而 $q\mid 1$，与 q 是素数矛盾. 于是与 $p_1,\cdots,p_k$ 是全体素数矛盾. 证完

定理 2 存在无穷多个形如 $4n-1$ 的素数.

证 假如这样的素数是有限的，设 p 是它们当中最大的一个，考虑整数

$$N=2^2\cdot 3\cdot 5\cdots p-1,$$

其中 $3\cdot 5\cdots p$ 表示所有$\leqslant p$ 的奇素数的乘积. 因为 N 是 $4n-1$ 形的，而且 $N>p$，由 p 的假设知，N 不是素数. 显然，N 的所有素因数必须大于 p. 由于 N 的因数只能是 $4n+1$ 或 $4n-1$ 形的，而两个 $4n+1$ 形的数相乘仍然是 $4n+1$ 形的，因此 N 至少有一个 $4n-1$ 形的素因数，设为 q，而 $q>p$，与 p 最大矛盾.

证完

一般地，设 $k>0, l>0, (k,l)=1$，那么形如 $kn+l$ 的素数有无穷多个，这个定理叫狄利克雷 (Dirichlet)定理，由于它的证明需要较多的准备知识，本书就不准备证明了. 但是，在第七章中，我们将证明 $l=1$ 的情形.

对于素数的研究，曾经有一个时期，人们希望找到一个表示素数的方便公式，例如，是否存在一个不是常数的整系数多项式 $f(x)$，当整数 $x\geqslant x_0$ 时，$f(x)$ 都表示素数？回答是否定的.

定理 3　对于任意给定的整数 x_0，不存在整系数多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0(a_n\neq 0, n>0)$，使得 x 取所有 $\geqslant x_0$ 的整数时，$f(x)$ 都表示素数.

证　设 $f(x_0)=p$ 是一个素数，对于整数 y，有

$$f(x_0+py)-f(x_0)=pM,$$

即

$$f(x_0+py)=p(M+1),$$

其中 M 是一个整数. 由于最多有 $3n$ 个 y 使得

$$f(x_0+py)=0, \pm p,$$

因此对于充分大的 y，$f(x_0+py)$ 不是一个素数.　　证完

素数的性质是数论最早的研究课题之一，这方面有许多艰深的难题和猜想，迄今仍是一个活跃的领域，许多近代深入的结果，组成了解析数论的重要内容.

§6　麦什涅数，费马数

定义　设 p 是一个素数，形如 2^p-1 的数叫做**麦什涅数**，记作 $M_p=2^p-1$.

十七世纪，麦什涅(Mersenne)证明了当 $p=2, 3, 5, 7, 13, 17, 19, 31$ 时，M_p 是素数. 到目前为止，只知道 28 个麦什涅数是素数，除已提到的 8 个以外，另外 20 个是：$p=61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243$. 并且知道 M_{44497} 是第 27 个麦什涅素数，但不知道 M_{86243} 是否是第 28 个麦什涅素数.

现在我们来证明关于麦什涅数的一个结果.

定理 1　设 p 是一个奇素数，q 是 M_p 的一个素因数，则 q 形如 $q=2kp+1$.

证明这个定理之前，先证一个简单的引理.

引理 设 $a>0, b>0, s>1$，则

$$(s^a-1, s^b-1)=s^{(a,b)}-1.$$

证 不妨设 $a>b$，由辗转相除法得

$$a=bq_1+r_1, 0<r_1<b,$$

$$b=r_1q_2+r_2, 0<r_2<r_1,$$

$$\cdots\cdots$$

$$r_{n-2}=r_{n-1}q_n+r_n, 0<r_n<r_{n-1},$$

$$r_{n-1}=r_nq_{n+1},$$

其中 $r_n=(a,b)$. 因此

$$s^a-1=s^{r_1}\cdot\frac{s^{bq_1}-1}{s^b-1}(s^b-1)+s^{r_1}-1,$$

$$s^b-1=s^{r_2}\cdot\frac{s^{r_2q_2}-1}{s^{r_1}-1}(s^{r_1}-1)+s^{r_2}-1,$$

$$\cdots\cdots$$

$$s^{r_{n-2}}-1=s^{r_n}\cdot\frac{s^{r_{n-1}q_n}-1}{s^{r_{n-1}}-1}(s^{r_{n-1}}-1)+s^{r_n}-1,$$

$$s^{r_{n-1}}-1=\frac{s^{r_nq_{n+1}}-1}{s^{r_n}-1}(s^{r_n}-1).$$

由此即得 $(s^a-1, s^b-1)=s^{(a,b)}-1$. 证完

定理 1 的证明:

首先，我们证明对于任意一个素数 r，有

$$r\mid 2^r-2, \tag{1}$$

因为 $2^r-2=(1+1)^r-2=1+\binom{r}{1}+\binom{r}{2}+\cdots+\binom{r}{r-1}+1-2=\sum_{i=1}^{r-1}\binom{r}{i}$，其中 $\binom{r}{i}$ 表示组合数，r 是素数时，$r\left|\binom{r}{i}\right.$ $(1\leqslant i\leqslant r-1)$，故(1)式成立.

因 q 是奇素数，故由(1)得 $q\mid 2^{q-1}-1$. 又因为 $q\mid 2^p-1$，于是

由引理得

$$q\mid(2^p-1,2^{q-1}-1)=2^{(p,q-1)}-1. \tag{2}$$

因为 $q>1$，故(2)给出$(p,q-1)>1$，即得 $p\mid q-1$. 因为 p 是奇数，$q-1$ 是偶数，故 q 具有形状 $q=2kp+1$. 证完

寻找素数 p，使得麦什涅数 M_p 是素数，仍是近代数论研究的课题之一，通常是利用某些判别法则在计算机上进行运算. 在下一节，我们将看到，求偶完全数等价于求麦什涅数中的素数. 是否有无穷多个 p 使 M_p 为素数，是数论中尚未解决的难题. 还有一个未曾解决的猜想是：不存在素数 q，使 $q^2\mid M_p$. 1967 年，沃伦(Warren)证明了若素数 q 满足 $q^2\mid M_p$，则 $2^{q-1}\equiv 1(\mathrm{mod}q^2)$. 顺便指出，1981 年，莱梅(Lehmer, D. H.)证明了当 $q<6\cdot 10^9$，除素数 $q=1093$ 和 $q=3511$ 外，同余式 $2^{q-1}\equiv 1(\mathrm{mod}q^2)$ 没有其他的解.

值得注意的是麦什涅素数在一些应用学科(如代数编码)中得到应用.

定义　我们把 $F_n=2^{2^n}-1, n\geqslant 0$，叫做**费马数**.

前五个费马数是 $F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537$，它们都是素数. 据此，1640 年，法国数学家费马(Fermat)猜想 F_n 均为素数. 1732 年，欧拉(Euler)发现 $F_5=641\cdot 6700417$，故费马猜想不真. 到目前为止，我们只知道以上五个数是素数. 此外，还证明了 48 个费马数是复合数. 这些复合数可以分成三类：①当 $n=5,6,7$ 时，得到了 F_n 的标准分解式；②当 $n=8,9,10,11,12,13,15,16,18,19,21,23,25,26,27,30,32,36,38,39,42,52,55,58,63,73,77,81,117,125,144,150,207,226,228,250,267,268,284,316,452,556,744,1945$ 时，只知道 F_n 的部分因数；③当 $n=14$ 时，只知道 F_{14} 是复合数，但它的任何真因数都不知道.

和麦什涅数类似，在费马数中，是否有无穷多个素数，是一个

尚未解决的难题. 另一个未能证明的猜想是: 不存在素数 q, 使 $q^2|F_n$. 1967 年,沃伦证明了: 如果素数 q 满足 $q^2|F_n$, 则 $2^{q-1}\equiv 1(\mathrm{mod}q^2)$.

费马数的有些简单性质是容易证明的. 如

定理 2 任给两个费马数 $F_m, F_n, m\neq n$, 则

$$(F_m, F_n)=1.$$

证 不失一般, 可设 $m>n\geqslant 0$, $m=n+k$, $k>0$, 而 $l|F_n$, $l|F_{n+k}$. 如果令 $x=2^{2^n}$, 我们有

$$\frac{F_{n+k}-2}{F_n}=\frac{2^{2^{n+k}}-1}{2^{2^n}+1}=\frac{x^{2^k}-1}{x+1}=x^{2^k-1}-x^{2^k-2}+\cdots-1,$$

故 $F_n|F_{n+k}-2$. 且因 $l|F_{n+k}, l|F_{n+k}-2$, 推出 $l|2$, 因为 F_t 是奇数, 故 $l=1$. 证完

1801 年, 高斯(Gauss)证明了当且仅当 $h=F_{n_1}F_{n_2}\cdots F_{n_s}(0\leqslant n_1<\cdots<n_s, s\geqslant 1)$, $F_{n_t}(t=1,\cdots,s)$ 都是素数时, 正 h 边形可用圆规和直尺来作图. 这说明费马数与平面几何的一些问题有联系. 费马数还和某些实际问题有联系, 例如在数字的信号和处理中, 用费马数给出的数论变换, 可用来计算整数序列的卷积.

§7 完 全 数

定义 设 n 是一个正整数, 如果 n 的全部因数的和等于 $2n$, n 就叫做**一个完全数**.

例如, 6 的因数的和是 $1+2+3+6=12$, 28 的因数的和是 $1+2+4+7+14+28=56$, 故 6 和 28 都是完全数. 先证一个有关 n 的诸因数和的结果.

定理 1 设 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 n 的标准分解式, $\sigma(n)=\sum_{d|n}d$ 表示 n 的诸因数的和, 则

$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}.$$

证　在§4中，我们已经知道，由整数的唯一分解定理，n 的全部因数可表成

$$p_1^{x_1}\cdots p_k^{x_k},\ 0\leqslant x_1\leqslant\alpha_1,\ \cdots,\ 0\leqslant x_k\leqslant\alpha_k,$$

故
$$\sigma(n)=\sum_{d\mid n}d=\sum_{x_1=0}^{\alpha_1}\cdots\sum_{x_k=0}^{\alpha_k}p_1^{x_1}\cdots p_k^{x_k}=\left(\sum_{x_1=0}^{\alpha_1}p^{x_1}\right)\cdots\left(\sum_{x_k=0}^{\alpha_k}p_k^{x_k}\right)$$
$$=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}.$$

证完

定理2　n 是一个偶完全数的充分必要条件是 n 具有形状 $2^{p-1}(2^p-1)$，其中 p 和 2^p-1 均为素数.

证　设 p 和 2^p-1 均为素数，$n=2^{p-1}(2^p-1)$，则 n 的诸因数和为

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

故 n 是一个完全数.

反之，设 $n=2^eq$ 是一个完全数，这里 q 是一个奇数，$e>0$. 于是由定理1，n 的诸因数和为

$$(2^{e+1}-1)\sigma(q)=2^{e+1}q,$$

其中 $\sigma(q)$ 表示 q 的诸因数之和，因此

$$\sigma(q)=q+d,$$

这里 $d=\frac{q}{2^{e+1}-1}$ 是一个整数，因此 d 是 q 的一个因数，q 和 d 是 q 的仅有的因数. 由整数的唯一分解定理即知 q 是素数，$q=2^{e+1}-1$. 因为 q 是素数，则 $e+1$ 必须是素数，令 $e+1=p$，这就证明了 $n=2^{p-1}(2^p-1)$.　　证完

证完

从定理 2 的证明，可以看出整数的唯一分解定理的重要性.

定理 2 告诉我们，有一个麦什涅素数存在，就对应着一个偶完全数，反过来也对.

完全数中另一个著名难题是：是否存在奇完全数？几百年来，尽管有许多数学家进行了大量的工作，这个问题仍未解决.

我们来证明关于奇完全数两个较易证明的结果.

定理 3 如果 n 是一个奇完全数，则 n 具有分解式

$$n=p^{\alpha}q_1^{2\beta_1}\cdots q_t^{2\beta_t}, \tag{1}$$

其中，$p, q_1, \cdots, q_t$ 是不同的素数，α 和 p 都是 $4h+1$ 形的数.

证 设 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 n 的标准分解式，$p_i(i=1, \cdots, k)$ 是奇素数，n 是完全数，由定理 1 可得

$$\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}=2p_1^{\alpha_1}\cdots p_k^{\alpha_k}.$$

不妨设

$$1+p_1+\cdots+p_1^{\alpha_1}=4f+2, \tag{2}$$

以及

$$1+p_j+\cdots+p_j^{\alpha_j}=2l_j+1,\ j=2, \cdots, k, \tag{3}$$

其中 f, l_j 为整数. 由(2)知 p_1 为 $4h+1$ 形，再由(2)知 α_1 也为 $4h+1$ 形，故可令 $\alpha_1=\alpha, p_1=p$. 由(3)知 α_j 是偶数，$j=2, \cdots, k$，可令 $2\beta_{j-1}=\alpha_j, q_{j-1}=p_j, j=2, \cdots, t+1, t+1=k$，便证明(1)式.

证完

定理 4 如果 n 是一个奇完全数，则(1)中 $t\geqslant 2$.

证 若 $t<2$，则由(1)给出

$$\frac{p^{\alpha+1}-1}{p-1}\,\frac{q_1^{2\beta_1+1}-1}{q_1-1}\cdots\frac{q_t^{2\beta_t+1}-1}{q_t-1}=2p^{\alpha}q_1^{2\beta_1}\cdots q_t^{2\beta_t},$$

因此，

$$2=\frac{1-\frac{1}{p^{\alpha+1}}}{1-\frac{1}{p}}\cdot\frac{1-\frac{1}{q_1^{2\beta_1+1}}}{1-\frac{1}{q_1}}\cdots\frac{1-\frac{1}{q_t^{2\beta_t+1}}}{1-\frac{1}{q_t}}<$$

$$\frac{p}{p-1}\cdot\frac{q_1}{q_1-1}\cdots\frac{q_t}{q_t-1}\leqslant\frac{p}{p-1}\cdot\frac{q_1}{q_1-1}\leqslant\frac{5}{4}\cdot\frac{3}{2},$$

这是一个矛盾结果，故 $t\geqslant 2$. 证完

定理 4 指出，如果奇完全数存在，则至少含 3 个不同的奇素因子. 这个值曾不断予以改进，目前，最好的结果是哈奇斯(Hagis)在 1980 年证明的，他证明了(1)中 $t\geqslant 7$，即奇完全数如果存在，则至少含 8 个不同的奇素因子. 哈奇斯还曾证明：如果 n 是奇完全数，则 $n>10^{50}$. 奇完全数的问题，是数论中最困难的问题之一.

§8 一次不定方程

二元一次不定方程是指

$$a_1x+a_2y=n, \tag{1}$$

其中 a_1, a_2, n 是给定的整数，$a_1a_2\neq 0$.

我们有

定理 1 方程(1)有整数解 x, y 的充分必要条件是

$$(a_1, a_2)\mid n. \tag{2}$$

证 如果(1)有解，显然(2)成立.

反之，不失一般，可设 $(a_1, a_2)=1$，以及 $a_1>0$，$a_2>0$. 由 §2 的定理 3 知，存在整数 u, v 使 $a_1u+a_2v=1$，于是 $x=nu, y=nv$，就是(1)的一组解. 证完

方程(1)的全部解，可由以下定理给出.

定理 2 设 $(a_1, a_2)=1$，则(1)的全部解可表为

$$x=x_0+a_2t, y=y_0-a_1t, \tag{3}$$

其中 x_0, y_0 为(1)的一组解，t 为任意整数.

证 设 t 为任意整数，把(3)代入(1)得

$$a_1(x_0+a_2t)+a_2(y_0-a_1t)=a_1x_0+a_2y_0=n,$$

故 t 为任意整数时，(3)均为(1)的解.

反之，设 x_1, y_1 为(1)的任意一组解，由

$$a_1x_1+a_2y_1=n,$$

和

$$a_1x_0+a_2y_0=n,$$

可得

$$a_1(x_1-x_0)+a_2(y_1-y_0)=0,$$

因 $(a_1, a_2)=1$，所以 $a_2 \mid x_1-x_0$，可设 $x_1-x_0=a_2t$，即 $x_1=x_0+a_2t$，故得 $y_1=y_0-a_1t$. 证完

类似定理 1 可证

定理 3 设 $s\geqslant 2$，s 元一次不定方程

$$a_1x_1+a_2x_2+\cdots+a_sx_s=n,\ a_1\cdots a_s\neq 0, \tag{4}$$

有整数解 $x_1, \cdots, x_s$ 的充分必要条件是

$$(a_1, \cdots, a_s) \mid n.$$

设 $s\geqslant 2$，考虑一次不定方程

$$a_1x_1+a_2x_2+\cdots+a_sx_s=n,\ a_i>0,\ (i=1, \cdots, s) \tag{5}$$

的正整数解 $x_i>0\ (i=1, \cdots, s)$ 的问题. 在 $s=2$ 时，十九世纪，西勒维斯特(Sylvester)证明了以下定理.

定理 4 在 $n>a_1a_2$ 时，(5)有正整数解 $x_1>0$，$x_2>0$，但在 $(a_1, a_2)=1, n=a_1a_2$ 时，(5)没有正整数解 $x_1>0, x_2>0$.

证 由定理 2 知

$$a_1x_1+a_2x_2=n,\ n>0,\ a_1>0,\ a_2>0 \tag{6}$$

的全部解可表为

$$x_1=x_1'-a_2t,\ x_2=x_2'-a_1t,$$

其中 x_1', x_2' 是(6)的一组解，t 为任意整数. 不难知道，可取 t_0 使

$$0<x_2-x_2'-a_1t_0\leqslant a_1,$$

又由 $n>a_1a_2$, 可得

$$(x_1'+a_2t_0)a_1=n-(x_2'-a_1t_0)a_2>a_1a_2-a_1a_2=0,$$

故对上述 t_0 来说,

$$x_1=x_1'+a_2t_0>0.$$

这就证明了 $n>a_1a_2$ 时,(6)有解 $x_1>0, x_2>0$.

如果在 $n=a_1a_2$, $(a_1, a_2)=1$ 时, (6)有解 $x_1>0$, $x_2>0$, 则由(6)可得

$$a_1a_2=a_1x_1+a_2x_2,$$

因 $(a_1, a_2)=1$, 故 $a_1|x_2, a_2|x_1$, $a_1\leqslant x_2$, $a_2\leqslant x_1$, 得 $a_1a_2=a_1x_1+a_2x_2\geqslant 2a_1a_2$, 此不可能. 证完

此定理也可叙述为: 设 $(a_1, a_2)=1$, $a_1>0$, $a_2>0$, 则凡大于 a_1a_2 的数必可表为 $a_1y_1+a_2y_2$ $(y_1>0, y_2>0)$ 之形状, 但 a_1a_2 不能表成此形状.

利用代换 $y_i=x_i+1(i=1, 2)$, 可得

推论 设 $(a_1, a_2)=1, a_1>0, a_2>0$, 则凡大于 $a_1a_2-a_1-a_2$ 的数必可表为 $a_1x_1+a_2x_2(x_1\geqslant 0, x_2\geqslant 0)$ 之形状, 但 $a_1a_2-a_1-a_2$ 不能表成此形状.

对于(5)的非负整数解问题, 我们有

定理 5 设 $d_i=(a_1, \cdots, a_i)$, $i=2, \cdots, s$, $s>1$, $d_1=a_1$, $d_s=1$, 则当 $n>N(a_1, \cdots, a_s)=\sum_{i=2}^{s}a_i\frac{d_{i-1}}{d_i}-\sum_{i=1}^{s}a_i$ 时, 方程(5) 有整数解 $x_i\geqslant 0$, $i=1, \cdots, s$.

证 我们对 s 施行归纳法. $s=2$ 时, $N(a_1, a_2)=a_1a_2-a_1-a_2$, 由定理 4 的推论知, 定理 5 成立. 设 $s-1(s\geqslant 3)$ 个元时定理成立, 我们来证明 s 元时的情形. 设 $(a_1, \cdots, a_{s-1})=d_{s-1}$, 由 $d_s=1$ 知, $(d_{s-1}, a_s)=1$. 再设 $a_i=d_{s-1}a_i'$, $i=1, \cdots, s-1$, $d_i'=(a_1', \cdots,$

$a_i'), i=2, \cdots, s-1, d_1'=a_1'$. 由 $(d_{s-1}, a_s)=1$ 可知，对任给的 n，存在 $0\leqslant b_s\leqslant d_{s-1}-1$，使得 $d_{s-1}\mid n-a_sb_s$，于是由(5)可得

$$a_1'x_1+\cdots+a_{s-1}'x_{s-1}=\frac{n-a_sb_s}{d_{s-1}}=n',\ (a_1', \cdots, a_{s-1}')=1, \tag{7}$$

因为 $n>N(a_1, \cdots, a_s)$，故

$$n'=\frac{n-a_sb_s}{d_{s-1}}\geqslant\frac{n-a_s(d_{s-1}-1)}{d_{s-1}}>\sum_{i=2}^{s-1}\frac{a_i}{d_{s-1}}\frac{d_{i-1}}{d_i}-\sum_{j=1}^{s-1}\frac{a_j}{d_{s-1}}$$

$$=\sum_{i=2}^{s-1}a_i'\frac{d_{s-1}d_{i-1}'}{d_{s-1}d_i'}-\sum_{j=1}^{s-1}a_j'=N(a_1', \cdots, a_{s-1}').$$

由归纳法假设，(7)有整数解 $x_1\geqslant 0, \cdots, x_{s-1}\geqslant 0$，即当 $n>N(a_1, \cdots, a_s)$ 时，(5)有整数解 $x_1\geqslant 0, \cdots, x_{s-1}\geqslant 0, x_s=b_s\geqslant 0$. 证完

定理 5 告诉我们，对 s 元 $(s\geqslant 2)$ 线性型 $a_1x_1+\cdots+a_sx_s$，$a_i>0(i=1, \cdots, s)$，$(a_1, \cdots, a_s)=1$，存在一个正整数 $F(a_1, \cdots, a_s)$，当 $n>F(a_1, \cdots, a_s)$ 时，n 可表为 $a_1x_1+\cdots+a_sx_s$ 之形状 $(x_j\geqslant 0, j=1, \cdots, s)$，但是 $F(a_1, \cdots, a_s)$ 却不能表为如上形状，$F(a_1, \cdots, a_s)$ 叫做线性型 $a_1x_1+\cdots+a_sx_s$ 的**最大不可表数**. 求出 $F(a_1, \cdots, a_s)$，就是著名的弗罗比尼乌斯 (Frobenius) 问题. 由定理 4 知 $F(a_1, a_2)=a_1a_2-a_1-a_2$. 对于 $s\geqslant 3$，特别是 $s=3$ 的情形，经过许多数学家的努力，已经找到了多种算法来计算 $F(a_1, a_2, a_3)$.

§9 抽屉原理

抽屉原理，又叫鸽舍原理. 为纪念十九世纪德国数学家狄利克雷，抽屉原理也叫狄利克雷原理. 这个原理最简单的表达方式是：假如有 $n+1$(或更多) 个物体装入 n 个盒子里，那么一定有某个盒子至少装有两个物体.

抽屉原理在数论和组合论中有着许多应用，下面给出几个应

用抽屉原理的定理.

定理 1　设 $1\leqslant a_1<a_2<\cdots<a_{n+1}\leqslant 2n$，则有 $1\leqslant i<j\leqslant n+1$，使得 $a_i\mid a_j$.

证　写 $a_i=2^{\lambda_i}b_i,\lambda_i\geqslant 0,2\nmid b_i(i=1,\cdots,n+1)$，其中 $b_i<2n$. 因为在 $1,2,\cdots,2n$ 中恰有 n 个不同的奇数，故在 $b_1,\cdots,b_{n+1}$ 中至少有两个相同，设 $b_i=b_j,1\leqslant i<j\leqslant n+1$，故 $a_i\mid a_j$.　　证完

定理 1 是 1935 年由安道什(Erdös)提出，并由莱梅证明的.

定理 2　假设 $a_1,\cdots,a_n$ 是数 $1,2,\cdots,n$ 的某种排列，$2\nmid n$，则乘积 $(a_1-1)(a_2-2)\cdots(a_n-n)$ 是偶数.

证　设 $n=2m+1$，则 $1,2,\cdots,n$ 中恰有 $m+1$ 个奇数，因此，乘积 $(a_1-1)(a_2-2)\cdots(a_n-n)$ 的各因子中被减数和减数各恰有 $m+1$ 个奇数，设 $a_{i_1},\cdots,a_{i_{m+1}}$ 是奇数，$1\leqslant i_1<i_2<\cdots<i_{m+1}\leqslant n$. 因为减数中恰有 m 个偶数，故 $i_1,\cdots,i_{m+1}$ 中至少有一个奇数，否则，有两个数相同，与假设不合. 不妨设 i_1 是奇数，则 $a_{i_1}-i_1$ 是偶数，故乘积 $(a_1-1)\cdots(a_n-n)$ 是偶数.　　证完

定理 3　设 $1\leqslant m<n$，联立方程组

$$\begin{aligned}
L_1&=a_{11}x_1+\cdots+a_{1n}x_n=0,\\
L_2&=a_{21}x_1+\cdots+a_{2n}x_n=0,\\
&\cdots\cdots\\
L_m&=a_{m1}x_1+\cdots+a_{mn}x_n=0,
\end{aligned}\tag{1}$$

其中 $a_{jk}(j=1,\cdots,m;k=1,\cdots,n)$ 为整数. 如果 $x_1,\cdots,x_n$ 是(1)的一组解，记为向量形式 $X=(x_1,\cdots,x_n)$，X 称为(1)的一个解向量. 则(1)存在解向量 $X=(x_1,\cdots,x_n)\neq 0$，且满足

$$|x_k|\leqslant(A_1\cdots A_m)^{\frac{1}{n-m}}\qquad(k=1,\cdots,n),\tag{2}$$

这里 $A_j=|a_{j1}|+|a_{j2}|+\cdots|a_{jn}|(j=1,\cdots,m)$.

证　设 $N=[(A_1\cdots A_m)^{\frac{1}{n-m}}]$，其中 $[x]$ 表示不大于 x 的最大整

数，B_j 表示 $a_{j1}, \cdots, a_{jn}$ 中正数的和，$-C_j$ 表示 $a_{j1}, \cdots, a_{jn}$ 中负数的和，故 $A_j = B_j + C_j (j = 1, \cdots, m)$. 当 y_k 取遍区间$[0, N]$中的整数值时$(k = 1, \cdots, n)$，可得出$(N+1)^n$ 个不同的向量的集 S:

$$S = \{(y_1, \cdots, y_n) \mid 0 \leqslant y_k \leqslant N, k = 1, \cdots, n\}.$$

对 S 中的每一个向量，有

$$-C_j N \leqslant L_j = a_{j1}y_1 + \cdots + a_{jn}y_n \leqslant B_j N,$$

故 L_j 可取 $(B_j + C_j)N + 1 = A_j N + 1 (j = 1, \cdots, m)$ 个不同的整数值，于是，当$(y_1, \cdots, y_n)$跑遍 S 中$(N+1)^n$ 个向量时，最多可得 $\prod_{j=1}^{m}(A_j N + 1)$ 个不同的向量 $(L_1, \cdots, L_m)$. 因为可设 $A_j \geqslant 1 (j = 1, \cdots, m)$，所以

$$\prod_{j=1}^{m}(A_j N + 1) \leqslant \prod_{j=1}^{m}(A_j N + A_j) = (N+1)^m \prod_{j=1}^{m} A_j,$$

而

$$\begin{aligned}(N+1)^n &= (N+1)^m (N+1)^{n-m} \\ &= (N+1)^m \left([(A_1 \cdots A_m)^{\frac{1}{n-m}}] + 1\right)^{n-m} \\ &> (N+1)^m \prod_{j=1}^{m} A_j \geqslant \prod_{j=1}^{m}(A_j N + 1),\end{aligned}$$

故至少有在 S 中两个不同的向量，设为$(y_1', \cdots, y_n')$，$(y_1'', \cdots, y_n'')$对应于同一个向量$(L_1, \cdots, L_m)$，令 $x_k = y_k' - y_k'' (k = 1, \cdots, n)$，$X = (x_1, \cdots, x_n) \neq 0$ 就是(1)的一个解向量，而且

$$|x_k| = |y_k' - y_k''| \leqslant N \leqslant (A_1 \cdots A_m)^{\frac{1}{n-m}}, k = 1, \cdots n,$$

故(2)成立.

证完

第一章 习 题

1. 证明 $6|n(n+1)(2n+1)$，其中 n 是任何整数.

2. 证明：任意 n 个连续整数中($n\geqslant 1$)，有一个且只有一个数被 n 除尽.

3. 证明：若 $m-p|(mn+qp)$，则 $m-p|(mq+np)$.

4. 证明：若 $p|(10a-b)$ 和 $p|(10c-d)$，则 $p|(ad-bc)$.

5. 证明：若 $(a,b)=1$，则 $(a+b,a-b)=1$ 或 2.

6. 证明：若 $(a,b)=1$，则 $(a+b,a^2-ab+b^2)=1$ 或 3.

7. 证明：若方程 $x^n+a_1x^{n-1}+\cdots+a_n=0$ ($n>0$, a_i 是整数，$i=1,\cdots,n$) 有有理数解，则此解必为整数.

8. 一个有理数 $\frac{a}{b}$，当 $(a,b)=1$ 时叫做既约分数. 证明：若两个既约分数 $\frac{a}{b}$, $\frac{c}{d}$ 的和是一个整数，则 $|b|=|d|$.

9. 如果一个整数不能被任一个素数的平方所整除则称为无平方因子. 证明：对每一个整数 $n\geqslant 1$，能唯一决定 $a>0, b>0$ 使得 $n=a^2b$，这里 b 无平方因子.

10. 证明：若 b^2 是 n 的最大平方因子，则由 $a^2|n$，可推出 $a|b$.

11. 给定 x 和 y，若 $m=ax+by$，$n=cx+dy$，这里 $ad-bc=\pm 1$，证明 $(m,n)=(x,y)$.

12. 证明：若 $n>0$, $a^n|b^n$，则 $a|b$.

13. 证明：若 $(a,b)=1$，且 $ab=c^n$，则 $a=x^n, b=y^n, c=xy$.

14. 证明：对于同样的整数 x 和 y，$17|2x+3y$ 的充分必要条件是 $17|9x+5y$.

15. 设 $5\nmid d$ $f(x)=ax^3+bx^2+cx+d$，$g(x)=dx^3+cx^2+bx+a$. 证明：若存在 m，使 $5|f(m)$，则存在 n，使 $5|g(n)$.

16. 证明：如果 a 和 b 是正整数，那么等差数列

$$a,\ 2a,\ 3a,\ \cdots,\ ba$$

中能被 b 整除的项的个数等于数 a 和 b 的最大公约数.

17. 假设 a,b,c,d 是整数，证明：若数 ac，$bc+ad$, bd 都能被某整数 u 整除，则 bc 和 ad 也都能被 u 整除.

18. 证明：若 a，b 是任意两个不全为零的整数，m 为任一正整数，则

$(am, bm) = (a, b)m$.

19. 证明 $(a_1, a_2, \cdots, a_n) = ((a_1, \cdots, a_s), (a_{s+1}, \cdots, a_n))$.

20. 证明 $[b_1, \cdots, b_n] = [[b_1, \cdots, b_s], [b_{s+1}, \cdots, b_n]]$.

21. 证明：若 $a>0, b>0, a'>0, b'>0, (a, b)=d, (a', b')=d'$，则 $(aa', ab', ba', bb') = dd'$.

22. 证明：若 $n>0, d \mid 2n^2$，则 n^2+d 不是完全平方.

23. 证明：对于给定的 $n>0$，数对 $\{u, v\}$ 适合 $[u, v]=n$ 的对数为 n^2 的因数的个数.

24. 证明：对于任何自然数 n，$\frac{21n+4}{14n+3}$ 是既约分数.

25. 证明：若 $m>0, n>0, (m, n)=1$，方程 $x^m=y^n$ 的全部整数解可以由 $x=t^n, y=t^m$ 给出，其中 t 取任意整数.

26. 证明：对于平面上任给的五个整点（即点的坐标都是整数的点）$A_i(x_i, y_i)\ (i=1, 2, \cdots, 5)$，必有其中两点的连线的中点也是整点.

27. 证明：若方程组

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1q}x_q &= 0, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2q}x_q &= 0, \\ \vdots \qquad\qquad & \quad \vdots \\ a_{p1}x_1 + a_{p2}x_2 + \cdots + a_{pq}x_q &= 0 \end{aligned}$$

中，未知数的个数 q 与方程的个数 p 间满足 $q=2p$，而且系数 a_{ij} 仅取 -1 或 0 或 $+1$. 则这个方程组必有满足下列条件的解 $(x_1, \cdots, x_q)$：

① 所有的 x_j 都是整数；

② 对于某些 $j\ (1 \leqslant j \leqslant q), x_j \neq 0$；

③ 对所有 $j\ (1 \leqslant j \leqslant q), |x_j| \leqslant q$.

28. 设 $n>2$，V_n 是一个形如 $1+kn$ 的数集（其中 $k=1, 2, \cdots$）. 一个数 $m \in V_n$，如果不存在 $p, q \in V_n$，使得 $pq=m$，则称 m 为 V_n 中的不可约数. 证明：存在着一个数 $r \in V_n$，这个数可以用不止一种方式分解成为数集 V_n 中若干不可约数的乘积.

29. 证明：$\dfrac{[a, b, c]^2}{[a, b][b, c][c, a]} = \dfrac{(a, b, c)^2}{(a, b)(b, c)(c, a)}$.

30. 证明：一正整数为其诸因数（除本身外）之积的充分必要条件是此

数为一素数的立方，或为两不同素数之积.

31. 证明 6 是仅有的无平方因子的完全数.

32. 证明 $2^{2^n}-1$ 至少有 n 个不同的素因数.

33. 证明 $\frac{1}{x}+\frac{1}{x+1}+\cdots+\frac{1}{x+n}(x>0)$ 不是整数.

34. 证明：若 p_n 表第 n 个素数，则 $p_n<2^{2^n}$.

35. 证明：若 $m>0, n>0$, m 是奇数，则 $(2^m-1, 2^n+1)=1$.

36. 证明：若 $(a,b)=1, m>0$，则数列

$$\{a+bk\},\quad k=0,1,\cdots$$

中存在无限多个数与 m 互素.

*37. 证明：若 $m>n\geqslant 1$，$a_1<a_2<\cdots<a_s$ 是不超过 m 且与 n 互素的全体正整数，则

$$\frac{1}{a_1}+\cdots+\frac{1}{a_s}$$

不是整数.

38. 证明：若 $(a,b)=1, a+b\neq 0$，且 p 是一个奇素数，则

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

*39. 设 $a>0, b>0$，且 $a>b$，用辗转相除法求 (a,b) 时所进行的除法次数为 k，b 在十进制表示中的位数是 l，证明 $k\leqslant 5l$.

*40. 证明：若 n 个整数 $1\leqslant a_1<a_2<\cdots<a_n\leqslant 2n$ 中任意两个整数 a_i, a_j 的最小公倍数 $[a_i, a_j]>2n$，则 $a_1>\left[\frac{2n}{3}\right]$.

*41. 证明：若 k 个整数 $1\leqslant a_1\leqslant\cdots\leqslant a_k\leqslant n$ 中，任意两个数 a_i，a_j 的最小公倍数 $[a_i, a_j]>n$，则 $\sum_{i=1}^{k}\frac{1}{a_i}<\frac{3}{2}$.

*42. 证明：若 n 个整数 $1<a_1<\cdots<a_n<2n$ 中没有一个数能被另一个数整除，则 $a_1\geqslant 2^k$，这里 k 满足 $3^k<2n<3^{k+1}$.

43. 证明：若 $2\nmid n, a_1, \cdots, a_n$ 是 n 个正整数 $b_1, \cdots, b_n$ 的某一个排列，则乘积 $(a_1-b_1)\cdots(a_n-b_n)$ 是偶数.

44. 设 $n>0$，求 $\binom{2n}{1}, \binom{2n}{3}, \cdots, \binom{2n}{2n-1}$ 的最大公因数.

45. 证明：若 $k>\left[\frac{n+1}{2}\right]$，则在 k 个整数 $1\leqslant a_1<a_2<\cdots<a_k\leqslant n$ 中存在 $a_i, a_j(1\leqslant i<j\leqslant k)$ 满足 $a_i+a_1=a_j$.

46. 设 $a_1, a_2, \cdots, a_{2n+1}$ 是 $2n+1$ 个有理数，它们具有以下性质：从中任取出 $2n$ 个，必能分成两组，每组含有 n 个数，且各组数之和相等，证明

$$a_1=a_2=\cdots=a_{2n+1}.$$

第二章　同　余　式

同余是数论中一个基本概念，它的引入简化了数论中许多问题．目前，同余理论已发展成为初等数论中内容丰富，应用广泛的一个分支．本章将着重介绍同余的基本性质和解某些同余式的一般方法．

§1　同余的定义和基本性质

定义　给定一个正整数 m，如果用 m 去除两个整数 a 和 b 所得的余数相同，我们就说 a, b 对模 m **同余**，记作 $a\equiv b(\mathrm{mod}m)$．如果余数不同，我们就说 a, b 对模 m 不同余，记作 $a\not\equiv b(\mathrm{mod}m)$．

由同余的定义出发，立即可得以下一些性质．

1. $a\equiv a(\mathrm{mod}m)$．(反身性)

2. 若 $a\equiv b(\mathrm{mod}m)$，则 $b\equiv a(\mathrm{mod}m)$．(对称性)

3. 若 $a\equiv b(\mathrm{mod}m), b\equiv c(\mathrm{mod}m)$，则 $a\equiv c(\mathrm{mod}m)$．(递推性)

我们有

定理 1　整数 a, b 对模 m 同余的充分必要条件是 $m\mid a-b$．

证　设 $a\equiv b(\mathrm{mod}m)$，则有 $a=mq_1+r, 0\leqslant r<m, b=mq_2+r, 0\leqslant r<m$，故 $a-b=m(q_1-q_2)$，$m\mid a-b$．反之，设 $a=mq_1+r_1, b=mq_2+r_2, 0\leqslant r_1<m, 0\leqslant r_2<m, m\mid a-b$，则有

$$m\mid a-b=m(q_1-q_2)+r_1-r_2,$$

故 $m\mid r_1-r_2$，又因 $|r_1-r_2|<m$，便得 $r_1=r_2$．　证完

定理 1 告诉我们同余又可定义如下：若 $m\mid a-b$，则称 a, b 对模 m 同余．

定理 2 如果 $a\equiv b(\mathrm{mod}m)$, $\alpha\equiv\beta(\mathrm{mod}m)$, 则有

① $ax-\alpha y\equiv bx+\beta y(\mathrm{mod}m)$, 其中 x, y 为任给的整数;

② $a\alpha\equiv b\beta(\mathrm{mod}m)$;

③ $a^n\equiv b^n(\mathrm{mod}m)$, 其中 $n>0$;

④ $f(a)\equiv f(b)(\mathrm{mod}m)$, 其中 $f(x)$ 为任意给定的一个整系数多项式.

证 ① 因为 $m|(a-b), m|(\alpha-\beta)$, 故有

$$m|x(a-b)+y(\alpha-\beta)=(ax+\alpha y)-(bx+\beta y).$$

② 由 $m|\alpha(a-b)+b(\alpha-\beta)=a\alpha-b\beta$ 便知.

③ 由②可证.

④ 由①和③可证. 证完

现在, 我们举几个例子来说明以上性质的应用.

例 1 一个整数 $n>0$ 被 9 整除的充分必要条件是 n 的各位数字(十进制)的和被 9 整除. 这是因为, 如果

$$n=a_0+10a_1+10^2a_2+\cdots+10^ka_k,$$

由 $10^i\equiv 1(\mathrm{mod}\ 9)\ (i=1,\cdots,k)$ 和定理 2 的④便得

$$n\equiv a_0+a_1+\cdots+a_k(\mathrm{mod}\ 9).$$

例 2 $641|F_5=2^{2^5}+1$. 我们有

$$2^8=256, 2^{16}=65536\equiv 154(\mathrm{mod}\ 641),$$

$$2^{32}\equiv(154)^2=23716\equiv 640\equiv -1(\mathrm{mod}\ 641).$$

例 3 当 n 是奇数时, $3|2^n+1$; 当 n 是偶数时, $3\nmid 2^n+1$. 这是因为 $2\equiv -1(\mathrm{mod}\ 3)$, 故 $2^n\equiv(-1)^n(\mathrm{mod}\ 3)$, $2^n+1\equiv(-1)^n+1(\mathrm{mod}\ 3)$, 即得 n 是奇数时, $2^n+1\equiv 0(\mathrm{mod}\ 3)$; n 是偶数时, $2^n+1\equiv 2(\mathrm{mod}\ 3)$.

定理 3 若 $ac\equiv bc(\mathrm{mod}\ m)$, 且若 $(m, c)=d$, 则

$$a\equiv b\left(\mathrm{mod}\frac{m}{d}\right).$$

证 因为 $m|c(a-b)$，故 $\frac{m}{d}\Big|\frac{c}{d}(a-b)$，又因 $\left(\frac{m}{d},\frac{c}{d}\right)=1$，便知 $\frac{m}{d}\Big|(a-b)$. 证完

定理 4 若 $a\equiv b(\mathrm{mod}\ m_i)$，$i=1,2,\cdots,n$，则

$$a\equiv b(\mathrm{mod}[m_1,\cdots,m_n]).$$

证 因为 $m_i|a-b$，$i=1,\cdots n$，把 $a-b$ 和 $m_i(i=1,\cdots,n)$ 都写成因子相同的标准分解式，即可知 $[m_1,\cdots,m_n]|a-b$. 所以

$$a\equiv b(\mathrm{mod}[m_1,\cdots,m_n]).$$ 证完

§2 剩余类和完全剩余系

在 §1 中指出同余关系满足反身性，对称性，递推性，这告诉我们，对于整数集来说，同余是一等价关系. 这样，对于给定的任一正整数 m，利用模 m 同余这个关系，就可以将全部整数分成若干类.

定义 设 m 是一个给定的正整数，$C_r(r=0,1,\cdots,m-1)$ 表示所有形如 $qm+r$ 的整数组成的集，其中 $q=0,\pm1,\pm2,\cdots$，则 $C_0,\cdots,C_{m-1}$ 叫做模 m 的**剩余类**.

我们有

定理 1 设 $m>0$，$C_0,C_1,\cdots,C_{m-1}$ 是模 m 剩余类，则有

① 每一个整数恰包含在某一个类 C_j 里，这里 $0\leqslant j\leqslant m-1$；

② 两个整数 x,y 属于同一类的充分必要条件是

$$x\equiv y(\mathrm{mod}m).$$

证 ① 设 a 是任一整数，则有

$$a=qm+r,\ 0\leqslant r<m,$$

故 a 恰包含在 C_r 中.

② 设 a,b 是两个整数，并且都在 C_r 内，则

$$a=q_1m+r,\ b=q_2m+r,$$

故 $m\mid a-b$. 反之，$m\mid a-b$，则由同余的定义即知 a 和 b 同在某一 C_r 类里，$0\leqslant r<m$. 证完

定义 在模 m 的剩余类 $C_0, C_1, \cdots, C_{m-1}$ 中各取一数 $a_j\in C_j$，$j=0, 1, \cdots, m-1$，此 m 个数 $a_0, a_1, \cdots, a_{m-1}$ 称为模 m 的一组**完全剩余系**.

由此定义立得

定理 2 m 个整数作成模 m 的一组完全剩余系的充分必要条件是两两对模 m 不同余.

最常用的完全剩余系 $0, 1, 2, \cdots, m-1$，它们称为模 m 的**非负最小完全剩余系**.

定理 3 设 $(k, m)=1$，而 $a_1, \cdots, a_m$ 是模 m 的一组完全剩余系，则 $ka_1, \cdots, ka_m$ 是模 m 的一组完全剩余系.

证 如果 $ka_i\equiv ka_j(\mathrm{mod}m)$，$1\leqslant i<j\leqslant m$，则 $m\mid k(a_i-a_j)$. 又因为 $(k, m)=1$，故 $m\mid a_i-a_j$，与所设矛盾. 这就是说 $ka_1, \cdots, ka_m$ 中没有两个数对模 m 同余，由定理 2 便知它们是模 m 的一组完全剩余系. 证完

定理 4 设 $m_1>0, m_2>0$，$(m_1, m_2)=1$，而 x_1, x_2 分别通过模 m_1, m_2 的完全剩余系，则 $m_2x_1+m_1x_2$ 通过模 m_1m_2 的完全剩余系.

证 由假设知道 x_1, x_2 分别通过 m_1, m_2 个整数，因此 $m_2x_1+m_1x_2$ 通过 m_1m_2 个整数. 由定理 2 只需证明这 m_1m_2 个整数对模 m_1m_2 两两不同余就够了. 假定

$$m_2x_1'+m_1x_2'\equiv m_2x_1''+m_1x_2''(\mathrm{mod}\ m_1m_2), \tag{1}$$

其中 x_1', x_1'' 是 x_1 所通过的完全剩余系中的整数，而 x_2', x_2'' 是 x_2 所通过的完全剩余系中的整数，则由(1)可得

$$m_2x_1'\equiv m_2x_1''(\mathrm{mod}\ m_1),\ m_1x_2'\equiv m_1x_2''(\mathrm{mod}\ m_2).$$

因为$(m_1, m_2)=1$，故得$x_1' \equiv x_1''(\bmod m_1)$，$x_2' \equiv x_2''(\bmod m_2)$，但$x_1'$，$x_1''$是取自模$m_1$的完全剩余系中的数，由此可得$x_1'=x_1''$，同理$x_2'=x_2''$．这表明若$\{x_1', x_2'\}$与$\{x_1'', x_2''\}$不同，则(1)式不能成立．证完

1948年，乔拉(Chowla)等证明了以下定理．

定理5　设$n>2$，并设$a_1, \cdots, a_n$和$b_1, \cdots, b_n$分别是模n的一组完全剩余系，则$a_1b_1, \cdots, a_nb_n$不是模n的一组完全剩余系．

证明这个定理之前，先证明一个定理．

定理6　设p是一个素数，则

$$(p-1)_1+1 \equiv 0(\bmod p). \tag{2}$$

证　$p=2, 3$时，(2)式显然成立．现设$p>3$是一个奇素数，$S=\{2, 3, \cdots, p-2\}$，$a \in S$．因为$(a, p)=1$，故有整数m, n使$am+pn=1$，即得$am \equiv 1(\bmod p)$．设$b=\langle m \rangle_p$，易知$b \neq 1$，$b \neq p-1$，故$b \in S$，且$ab \equiv 1(\bmod p)$．现在，我们来证明$a \neq b$，否则，由$a=b$推出

$$(b-1)(b+1) \equiv 0(\bmod p), \tag{3}$$

而$b \neq 1$，$b \neq p-1$，故(3)不能成立．现取$a' \in S$，$a' \neq a$，$a' \neq b$，则有$b' \in S$，使$a'b' \equiv 1(\bmod p)$，而且$b' \neq a'$，$b' \neq a$，$b' \neq b$．如此讨论下去，便知S中的数可分成$\frac{p-3}{2}$对，每一对数a，b，满足$ab \equiv 1(\bmod p)$，故得$2 \cdot 3 \cdots (p-2) \equiv 1(\bmod p)$，即得$(p-1)_1+1 \equiv 0(\bmod p)$　证完

定理6就是熟知的威尔逊(Wilson)定理．

定理5的证明：

设$4 \mid n$，如果$a_1b_1, \cdots, a_nb_n$是模n的一组完全剩余系，则其中有$\frac{n}{2}$个奇数和$\frac{n}{2}$个偶数．不失一般情况，假设$a_1b_1, \cdots, a_{n/2}b_{n/2}$是

$\frac{n}{2}$个奇数，则 $a_1, \cdots, a_{n/2}$ 和 $b_1, \cdots, b_{n/2}$ 分别是 $a_1, \cdots, a_n$ 和 $b_1, \cdots, b_n$ 中的$\frac{n}{2}$个奇数. 由完全剩余系定义知在 a_1b_1, $a_2b_2, \cdots, a_nb_n$ 中存在某个 j，使

$$a_jb_j \equiv 2 (\mathrm{mod}\ n),$$

故

$$a_jb_j \equiv 2 (\mathrm{mod}\ 4), \text{ 且 } \frac{n}{2}+1 \leqslant j \leqslant n, \tag{4}$$

但此时 $a_j \equiv b_j \equiv 0 (\mathrm{mod}\ 2)$，因此(4)式不可能.

当 $4 \nmid n$ 时，可设 $n = qm$，这里 $q = p$ 或 $q = 2p$，p 是一个奇素数，$2 \nmid m$. 由定理 6 知，在 $q \neq p$ 时，

$$\prod_{\substack{j=1 \\ (j,p)=1}}^{p} j = (p-1)! \equiv -1 (\mathrm{mod}\ p). \tag{5}$$

在 $q = 2p$ 时，

$$\prod_{\substack{j=1 \\ (j,2p)=1}}^{2p} j = 1 \cdot 3 \cdot 5 \cdots (p-2)(p+2)(p+4) \cdots (2p-1)$$

$$\equiv (p-1)! \equiv -1 (\mathrm{mod}\ p). \tag{6}$$

又

$$\prod_{\substack{j=1 \\ (j,2p)=1}}^{2p} j \equiv -1 (\mathrm{mod}\ 2). \tag{7}$$

由(6)和(7)及 §1 定理 4 得

$$\prod_{\substack{j=1 \\ (j,2p)=1}}^{2p} j \equiv -1 (\mathrm{mod} 2p). \tag{8}$$

由(5)和(8)可得

$$\prod_{\substack{j=1\\(j,q)=1}}^{n} j = \prod_{\substack{j=1\\(j,q)=1}}^{q-1} j \prod_{\substack{j=q+1\\(j,q)=1}}^{2q-1} j \cdots \prod_{\substack{j=(m-1)q+1\\(j,q)=1}}^{n} j \equiv (-1)^m = -1 \pmod{q}.$$

而

$$\prod_{\substack{j=1\\(a_j,q)=1}}^{n} a_j \equiv \prod_{\substack{j=1\\(b_j,q)=1}}^{n} b_j \equiv \prod_{\substack{j=1\\(j,q)=1}}^{n} j \pmod{q},$$

所以，如果 $n>2$，$a_1b_1, \cdots, a_nb_n$ 是模 n 的一组完全剩余系，则得

$$-1 \equiv \prod_{\substack{j=1\\(j,q)=1}}^{n} j \equiv \prod_{\substack{j=1\\(a_jb_j,q)=1}}^{n} a_jb_j$$

$$= \prod_{\substack{j=1\\(a_j,q)=1}}^{n} a_j \prod_{\substack{j=1\\(b_j,q)=1}}^{n} b_j \equiv 1 \pmod{q}. \tag{9}$$

而 $q>2$，所以(9)式不能成立. 这就证明了在 $n>2$ 时，$a_1b_1, \cdots, a_nb_n$ 不是模 n 的一组完全剩余系. 证完

顺便指出，模 m 的剩余类之间可以定义运算. 由 §1 的定理 1 知，在任给的两个模 m 的剩余类 C_i, C_j 中各取一代表 i, j，而令 $i+j$（或 $i\cdot j$）所在的剩余类为 $C_{<i+j>}$（或 $C_{<i\cdot j>}$），则 $C_{<i+j>}$（或 $C_{<i\cdot j>}$）仅与 C_i, C_j 有关，而与所选择之代表无关，故可定义 C_i, C_j 之间的加法⊕和乘法⊙为

$$C_i \oplus C_j = C_{<i+j>}, \quad C_i \odot C_j = C_{<i\cdot j>},$$

$C_0, C_1, \cdots, C_{m-1}$ 对上述加法和乘法成环，叫做模 m **剩余类环**，记为 Z_m，它为抽象代数提供了具体例子.

§3 缩 系

首先引进缩系的定义.

定义 如果一个模 m 的剩余类里面的数与 m 互素（显然，只需有一个与 m 互素，其余的均与 m 互素），就把它叫做一个**与模 m 互**

素的剩余类. 在与模m互素的全部剩余类中，各取一数所组成的集叫做模m的一组**缩系**.

在讨论缩系的过程中，需要引入一个常用的数论函数——欧拉函数$\varphi(n)$.

定义 **欧拉函数** $\varphi(n)$是一个定义在正整数上的函数，$\varphi(n)$的值等于序列$0, 1, 2, \cdots, n-1$中与n互素的数的个数.

由定义知$\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\cdots$. 当p是素数时，$\varphi(p)=p-1$.

定理 1 模m的一组缩系含有$\varphi(m)$个数.

定理 2 若$a_1, \cdots, a_{\varphi(m)}$是$\varphi(m)$个与$m$互素的整数，则$a_1, \cdots, a_{\varphi(m)}$是模$m$的一组缩系的充分必要条件是它们两两对模$m$不同余.

定理 1 和定理 2 都是显然的.

定理 3 若$(a, m)=1$，x通过模m的缩系，则ax也通过模m的缩系.

证 当x通过模m的缩系，则ax通过$\varphi(m)$个整数，由于$(a, m)=1$, $(x, m)=1$，故$(ax, m)=1$. 若$ax_1 \equiv ax_2 (\mathrm{mod}\, m)$，可得$x_1 \equiv x_2 (\mathrm{mod}\, m)$，与所设$x$通过模$m$的缩系矛盾，故$ax$通过模$m$的缩系. 证完

定理 4 设$m>1$, $(a, m)=1$，则

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

证 设$r_1, r_2, \cdots, r_{\varphi(m)}$是模$m$的一组缩系，则由定理 3，$ar_1$, $ar_2, \cdots, ar_{\varphi(m)}$也是模$m$的一组缩系，故

$$(ar_1)(ar_2)\cdots(ar_{\varphi(m)}) \equiv r_1 r_2 \cdots r_{\varphi(m)} (\mathrm{mod}\, m),$$

即

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} (\mathrm{mod}\, m). \tag{1}$$

由于

$$(r_i, m) = 1,\ i = 1, 2, \cdots, \varphi(m),$$

故

$$(r_1 r_2 \cdots r_{\varphi(m)}, m) = 1. \tag{2}$$

根据§1 定理 3，再由(2)和(1)得

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$ 证完

由定理 4 立刻推得定理 5，它通常叫做**费马小定理**.

定理5 若 p 是素数，则

$$a^p \equiv a (\mathrm{mod}\, p).$$

定理 6 设 $m_1 > 0, m_2 > 0, (m_1, m_2) = 1, x_1, x_2$ 分别通过模 m_1，m_2 的缩系，则 $m_2 x_1 + m_1 x_2$ 通过模 $m_1 m_2$ 的缩系.

证 首先证明 $(m_2 x_1 + m_1 x_2, m_1 m_2) = 1$. 否则，有素数 p，$p \mid m_2 x_1 + m_1 x_2, p \mid m_1 m_2$. 如 $p \mid m_1$，则 $p \mid m_2 x_1$，而 $p \nmid x_1$，故 $p \mid m_2$，此与 $(m_1, m_2) = 1$ 矛盾；如 $p \mid m_2$，可得出相同的矛盾. 这就证明当 x_1, x_2 分别过模 m_1 和 m_2 的缩系时，$\varphi(m_1) \cdot \varphi(m_2)$ 个数 $m_2 x_1 + m_1 x_2$ 均与 $m_1 m_2$ 互素.

反之，凡与 $m_1 m_2$ 互素之 a 有

$$a \equiv m_2 x_1 + m_1 x_2 (\mathrm{mod}\, m_1 m_2),\ (x_1, m_1) = (x_2, m_2) = 1. \tag{3}$$

这是因为，由§2 的定理 4 知有 x_1 和 x_2 使 $a \equiv m_2 x_1 + m_1 x_2 (\mathrm{mod}\, m_1, m_2)$，所以只需证明当 $(a, m_1 m_2) = 1$ 时，$(x_1, m_1) = (x_2, m_2) = 1$. 如果 $(x_1, m_1) > 1$，则有素数 q，$q \mid x_1$，$q \mid m_1$. 而 $a \equiv m_2 x_1 + m_1 x_2 (\mathrm{mod}\, m_1 m_2)$，由此推出 $q \mid a$，与 $(a, m_1 m_2) = 1$ 矛盾，故 $(x_1, m_1) = 1$. 同理可证 $(x_2, m_2) = 1$.

最后，再由§2 的定理 4 知 $m_2 x_1 + m_1 x_2$ 中任两个对模 $m_1 m_2$ 不同余. 证完

由定理 6，立得

推论 若 $(m_1, m_2) = 1$，则 $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.

定理 7 设 n 的标准分解 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，则

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

证 由定理 6 的推论得

$$\varphi(n)=\varphi(p_1^{a_1})\cdots\varphi(p_k^{a_k}).$$

今证明 $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$. 由 $\varphi(n)$的定义知,$\varphi(p^\alpha)$等于从 p^α 减去在 $1,\cdots,p^\alpha$ 中与 p 不互素的数的个数. 因为 p 是素数,故 $\varphi(p^\alpha)$等于从 p^α 减去在 $1,\cdots,p^\alpha$ 中被 p 整除的数的个数. 而在

$$1,\cdots,p,p+1,\cdots,2p,\cdots,p^{\alpha-1}\cdot p$$

中,易知 p 的倍数共有 $p^{\alpha-1}$ 个,即得 $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

证完

关于欧拉函数 $\varphi(n)$的一些性质,我们在下一章中再讨论.

§4 一次同余式

本节讨论一次同余式. 先给出同余式和同余式的解的概念.

定义 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$,其中 $n>0$, a_i $(i=0,1,\cdots,n)$是整数,又设 $m>0$,则

$$f(x)\equiv 0(\mathrm{mod}\,m) \tag{1}$$

叫做模 m 的**同余式**. 若 $a_n\not\equiv 0(\mathrm{mod}\,m)$, 则 n 叫做(1)的**次数**. 如果 x_0 满足 $f(x_0)\equiv 0(\mathrm{mod}\,m)$,则 $x\equiv x_0(\mathrm{mod}\,m)$ 叫做同余式(1)的**解**. 不同的解是指互不同余的解.

要求同余式(1)的解,只要逐个把 $0,1,\cdots,m-1$代入(1)中进行验算总可以决定. 但当 m 大时,计算量往往太大.

例 1 用验算的方法知同余式

$$x^5+2x^4+x^3+2x^2-2x+3\equiv 0(\mathrm{mod}7)$$

仅有解 $x\equiv 1,5,6(\mathrm{mod}7)$.

例 2 同余式

$$x^4-1\equiv 0(\mathrm{mod}16)$$

有 8 个解: $x\equiv 1,3,5,7,9,11,13,15 \pmod{16}$.

例 3 同余式

$$x^2+3\equiv 0 \pmod 5$$

没有解.

顺便指出, 设 $k\geqslant 2$, $F(x_1,\cdots,x_k)$是一个 k 个元的整系数多项式, 同余式

$$F(x,\cdots,x_k)\equiv 0 \pmod m \tag{2}$$

的解 $x_1\equiv a_1 \pmod m,\cdots,x_k\equiv a_k \pmod m$, 原则上也可以用验算的方法求出, 但更复杂. 这时, (2)的两个解$(a_1,\cdots,a_k)$, $(b_1,\cdots,b_k)$被叫做不同的解, 则至少有一 $j(1\leqslant j\leqslant k)$使 $a_j\not\equiv b_j \pmod m$.

例 4 同余式

$$y^2-x^3+1\equiv 0 \pmod p,\quad p \text{ 为素数}. \tag{3}$$

设 N_p 表示同余式(3)解的个数, 则有 $N_2=2, N_3=3, N_5=5, N_7=3$, 等等.

下面四个定理完全解决了一元一次同余式的解的问题.

定理 1 设$(a,m)=1, m>0$, 则同余式

$$ax\equiv b \pmod m \tag{4}$$

恰有一个解.

证 因为 $1,2,\cdots,m$ 组成一组模 m的完全剩余系, $(a,m)=1$, 故 $a,2a,\cdots,ma$ 也组成模 m 的一组完全剩余系, 故其中恰有一个数设为 aj, 适合 $aj\equiv b \pmod m$, $x\equiv j \pmod m$ 就是(4)的唯一解.

证完

定理 1 并没有告诉我们如何去决定这个解, 除非将 $1,2,\cdots,m$ 逐一代入验算. 下面这个定理, 直接给出了解.

定理 2 在定理 1 的条件下, $x\equiv ba^{\varphi(m)-1} \pmod m$是(4)的唯一解.

证 由 §3 的定理 4, 直接可得.

证完

定理 3 设$(a,m)=d, m>0$,同余式

$$ax\equiv b(\mathrm{mod}\, m) \tag{5}$$

有解的充分必要条件是$d|b$.

证 如果(5)有解,则由$d|a, d|m$, 推出$d|b$. 如果$d|b$, 则因$\left(\frac{a}{d},\frac{m}{d}\right)=1$,故同余式

$$\frac{a}{d}x\equiv\frac{b}{d}\left(\mathrm{mod}\frac{m}{d}\right)$$

有一组解,即(5)有一组解. 证完

定理 4 设$(a,m)=d, m>0, d|b$,则同余式

$$ax\equiv b(\mathrm{mod}\, m) \tag{6}$$

恰有d个解.

证 由$d|b$和定理 3 知(6)有解. 如有整数c适合(6),c也适合同余式

$$\frac{a}{d}x\equiv\frac{b}{d}\left(\mathrm{mod}\frac{m}{d}\right). \tag{7}$$

反之,如c适合同余式(7),c也适合同余式(6). 设t适合(7),则(7)有唯一解

$$x\equiv t\left(\mathrm{mod}\frac{m}{d}\right),$$

即全体整数

$$t+k\cdot\frac{m}{d}, k=0,\pm1,\pm2,\cdots.$$

对模m来说,恰可选出d个互不同余的整数

$$t, t+\frac{m}{d}, t+2\cdot\frac{m}{d}, \cdots, t+(d-1)\frac{m}{d}, \tag{8}$$

这是因为对于$t+k\frac{m}{d}$,设$k=qd+r$, $0\leqslant r<d$, 代入得$t+k\cdot\frac{m}{d}=t$

$+(qd+r)\frac{m}{d}=t+r\frac{m}{d}+qm\equiv t+r\frac{m}{d}(\mathrm{mod}\,m)$. 又若 $0\leqslant e<d$, $0\leqslant f<d$, $t+e\frac{m}{d}\equiv t+f\frac{m}{d}(\mathrm{mod}\,m)$, 则推出 $f=e$. 这就证明了(6)的任一解恰与(8)中的某一数模 m 同余, 而(8)中的 d 个数, 又模 m 两两互不同余, 即知(6)恰有 d 个解. 证完

一般地, 我们有

定理 5 设 $k\geqslant 1$, 同余式

$$a_1x_1+\cdots+a_kx_k+b\equiv 0(\mathrm{mod}\,m) \tag{9}$$

有解的充分和必要条件是

$$(a_1,\cdots,a_k,m)\mid b. \tag{10}$$

若条件(10)满足, 则(9)的解数为 $m^{k-1}(a_1,\cdots,a_k,m)$.

证 由定理 3 和定理 4 知此对 $k=1$ 为真. 现用归纳法来证明. 设 $(a_1,\cdots,a_k,m)=d$, $(a_1,\cdots,a_{k-1},m)=d_1$, 则 $(d_1,a_k)=d$.

由定理 4 知

$$a_kx_k+b\equiv 0(\mathrm{mod}\,d_1) \tag{11}$$

有 d 个解

$$x_k\equiv t(\mathrm{mod}\,d_1),\ x_k\equiv t+\frac{d_1}{d}(\mathrm{mod}\,d_1),\ \cdots,$$

$$x_k=t+\frac{d_1}{d}(d-1)(\mathrm{mod}\,d_1),$$

故对模 m 来说有 $d\cdot\frac{m}{d_1}$ 个解:

$$x_k\equiv t(\mathrm{mod}\,m),\ x_k\equiv t+d_1(\mathrm{mod}\,m),\ \cdots,\ x_k$$

$$\equiv t+d_1\left(\frac{m}{d_1}-1\right)(\mathrm{mod}\,m),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x_k\equiv t+\frac{d_1}{d}(d-1)(\mathrm{mod}\,m),\ \cdots,\ x_k\equiv t+\frac{d_1}{d}$$

$$(d-1)+d_1\left(\frac{m}{d_1}-1\right)(\mathrm{mod}\, m).$$

对(11)的一个解 x_k，设

$$\frac{a_n x_k-b}{d_1}=b_1,$$

由归纳法假定，

$$a_1x_1+\cdots+a_{k-1}x_{k-1}+b_1d_1\equiv 0(\mathrm{mod}\, m)$$

的解数为

$$m^{k-2}(a_1,\cdots,a_{k-1},m)=m^{k-2}d_1,$$

故(9)的解数为

$$m^{k-2}d_1\cdot d\cdot\frac{m}{d_1}=m^{k-1}d.$$

证完

§5 模是素数的同余式

前一节已经看到同余式解的个数是很不规则的，但是对素数为模的同余式，却有下面的拉格朗日(Lagrange)定理.

定理1 设 p 是一个素数，

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\ n>0,\ a_n\not\equiv 0(\mathrm{mod}\, p),$$

是一个整系数多项式. 则同余式

$$f(x)\equiv 0(\mathrm{mod}\, p) \tag{1}$$

最多有 n 个解.

证 我们对 $f(x)$ 的次数 n 进行归纳. 当 $n=1$ 时，设一次同余式为

$$a_1x+a_0\equiv 0(\mathrm{mod}\, p),\ p\nmid a_1.$$

因为 $p\nmid a_1$，故恰有一解. 现在，假设定理对次数为 $n-1(n\geqslant 2)$ 的同余式真，现在我们来证明(1)最多有 n 个解. 当 $n\geqslant p$ 时结论显然成立，故可设 $n\leqslant p-1$. 用反证法，假设同余式(1)有 $n+1$ 个解

$$x_0,x_1,\cdots,x_n,\quad x_i\not\equiv x_j(\mathrm{mod}\, p),\ 0\leqslant i<j\leqslant n,$$

我们将导致一个矛盾. 因为

$$f(x)-f(x_0)-\sum_{k=1}^{n}a_k(x^k-x_0^k)=(x-x_0)g(x),$$

这里 $g(x)$是首项系数为 a_n 的 $n-1$ 次整系数多项式,因此有

$$f(x_k)-f(x_0)=(x_k-x_0)g(x_k)\equiv 0(\bmod p),$$

但如 $k>0$, $x_k-x_0\not\equiv 0(\bmod p)$, 故 $n-1$ 次同余式 $g(x)\equiv 0(\bmod p)$ 有 n 个解,与归纳假设矛盾. 证完

应用拉格朗日定理可得下面的结果.

定理 2　设同余式

$$f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0(\bmod p)$$

的解的个数大于 n,这里 p 是素数, a_i 是整数 $(i=0,1,\cdots,n)$, 则 $p\mid a_i(i=0,1,\cdots,n)$.

证　如果有某些系数不被 p 整除, 设这些系数的足标最大的为 k,则 $k\leqslant n$. k 次同余式

$$a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0\equiv 0(\bmod p),\quad p\nmid a_k$$

的解的个数大于 k, 与定理 1 矛盾. 证完

定理 3　对于任给素数 p, 多项式

$$f(x)=(x-1)(x-2)\cdots(x-p+1)-x^{p-1}+1$$

的所有系数被 p 整除.

证　设 $g(x)=(x-1)(x-2)\cdots(x-p+1)$, 则 $1,\cdots,p-1$ 是同余式

$$g(x)\equiv 0(\bmod p)$$

的 $p-1$ 个解. 由费马小定理, $1,\cdots,p-1$ 也是同余式

$$h(x)=x^{p-1}-1\equiv 0(\bmod p)$$

的 $p-1$ 个解,故同余式

$$f(x)\equiv g(x)-h(x)\quad(\bmod p)$$

有 $p-1$ 个解,而 $f(x)$是 $p-2$ 次的多项式,由定理 2 知, 其所有系

数被 p 整除. 证完

注意到定理 3 中 $f(x)$的常数项是$(-1)^{p-1}(p-1)!+1$，因此这里又一次证明了威尔逊定理.

定理 4 设素数 $p>3$，则有

$$\sum_{k=1}^{p-1}\frac{(p-1)!}{k}\equiv 0(\bmod p^2).$$

证 设

$$\begin{aligned} g(x)&=(x-1)(x-2)\cdots(x-p+1)\\ &=x^{p-1}-s_1x^{p-2}+s_2x^{p-3}+\cdots-s_{p-2}x\\ &\quad+(p-1)!, \end{aligned} \tag{2}$$

其中 $s_j(j=1,\cdots,p-2)$是整数，且

$$s_{p-2}=\sum_{k=1}^{p-1}\frac{(p-1)!}{k}.$$

由定理 3 知，$p\mid s_j(j=1,\cdots,p-2)$，在(2)中令 $x=p$，由于 $g(p)=(p-1)!$，故(2)给出

$$p^{p-1}-s_1p^{p-2}+\cdots-ps_{p-2}=0. \tag{3}$$

因为 $p>3$，对(3)取模 p^3，得

$$ps_{p-2}\equiv 0(\bmod p^3),$$

故

$$s_{p-2}\equiv 0(\bmod p^2).$$

证完

§6 孙子定理及其应用举例

本节解一次同余式组

$$x\equiv b_1(\bmod m_1),\ x\equiv b_2(\bmod m_2),\ \cdots,\ x\equiv b_k(\bmod m_k). \tag{1}$$

在我国古代《孙子算经》里已经提出了这种形式的问题，并且很好地解决了它. 《孙子算经》里所提出的问题之一如下：

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩

二，问物几何？”这就是求一次同余式组：

$$x\equiv 2(\mathrm{mod}3),\ x\equiv 3(\mathrm{mod}5),\ x\equiv 2(\mathrm{mod}7)\text{的公解 }x.$$

把孙子所用算法推广就成为定理 1.

定理 1(孙子定理) 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，$m=m_1\cdots m_k$，$m=m_iM_i(i=1,\cdots,k)$，则同余式组(1)有唯一解

$$x\equiv M_1'M_1b_1+M_2'M_2b_2+\cdots+M_k'M_kb_k(\mathrm{mod}\,m), \tag{2}$$

其中

$$M_i'M_i\equiv 1(\mathrm{mod}\,m_i)\ (i=1,\cdots,k).$$

证 由于 $(m_i, m_j)=1$，$i\neq j$，即得 $(M_i, m_i)=1$. 由 §4 的定理 1 知对每一 M_i，有一 M_i' 存在使得 $M_i'M_i\equiv 1(\mathrm{mod}\,m_i)$. 另一方面，由 $m=m_iM_i$，因此 $m_j\mid M_i$，$i\neq j$，故

$$\sum_{j=1}^{k}M_j'M_jb_j\equiv M_i'M_ib_i\equiv b_i(\mathrm{mod}\,m_i),\quad i=1,\cdots,k,$$

即(2)为(1)的解.

若 x_1, x_2 是适合(1)式的任意两个整数，则

$$x_1\equiv x_2(\mathrm{mod}\,m_i)\ (i=1,\cdots,k).$$

因为 $(m_i, m_j)=1$，$i\neq j$，于是 $x_1\equiv x_2(\mathrm{mod}\,m)$，故(1)仅有解(2).

证完

定理 2 一次同余式组

$$x\equiv b_1(\mathrm{mod}\,m_1),\ x\equiv b_2(\mathrm{mod}\,m_2), \tag{3}$$

可解的充分必要条件是 $(m_1, m_2)\mid b_1-b_2$，且当(3)可解时对模 $[m_1, m_2]$ 有唯一解.

证 设(3)有公解 x_0，$(m_1, m_2)=d$，则有

$$x_0\equiv b_1(\mathrm{mod}\,d),\quad x_0\equiv b_2(\mathrm{mod}\,d),$$

两式相减即得 $d\mid b_1-b_2$.

反之，若 $(m_1, m_2)\mid b_1-b_2$，则因 $x\equiv b_1(\mathrm{mod}\,m_1)$ 的解可写为 $x=b_1+m_1y$，代入 $x\equiv b_2(\mathrm{mod}\,m_2)$ 得

$$m_1 y \equiv b_2 - b_1 (\mathrm{mod}\, m_2). \tag{4}$$

因为$(m_1, m_2) = d$, $d \mid b_2 - b_1$, 故(4)有解, 设为 y_0, 且对模$\frac{m_2}{d}$有唯一解$y \equiv y_0 \left(\mathrm{mod}\frac{m_2}{d}\right)$, 即

$$y = y_0 + \frac{m_2}{d} t \quad (t = 0, \pm 1, \pm 2, \cdots).$$

故(3)的全部解为

$$x = b_1 + m_1 y_0 + \frac{m_1 m_2}{d} t \quad (t = 0, \pm 1, \pm 2, \cdots).$$

这些解对模$[m_1, m_2]$来讲都是同余的, 故(3)的解对模$[m_1, m_2]$唯一. 证完

对于一次同余式组

$x \equiv b_1 (\mathrm{mod}\, m_1)$, $x \equiv b_2 (\mathrm{mod}\, m_2)$, $\cdots$, $x \equiv b_k (\mathrm{mod}\, m_k)$

$k \geqslant 3$ 的情形, 可先解前面两个得$x \equiv b_2' (\mathrm{mod}[m_1, m_2])$, 再与 $x \equiv b_3 (\mathrm{mod}\, m_3)$联立解出 $x \equiv b_3' (\mathrm{mod}[m_1, m_2, m_3])$. 如此继续下去, 最后可得唯一解 $x \equiv b_k' (\mathrm{mod}[m_1, \cdots, m_k])$. 如果中间有一步出现无解, 则同余式组无解.

孙子定理是初等数论中重要定理之一, 下面举一个孙子定理的简单应用的例子. 另一个应用孙子定理的例子在 §8 中介绍.

定理 3 若 m_1, m_2, $\cdots$, m_k 是 k 个两两互素的正整数, $m = m_1 \cdots m_k$, 则同余式

$$f(x) \equiv 0 (\mathrm{mod}\, m) \tag{5}$$

有解的充分必要条件是同余式

$$f(x) \equiv 0 (\mathrm{mod}\, m_i) \ (i = 1, \cdots, k) \tag{6}$$

的每一个有解. 并且, 若用 T_i 表示 $f(x) \equiv 0 (\mathrm{mod}\, m_i)$的解数, T 表示(5)的解数, 则 $T = T_1 T_2 \cdots T_k$.

证 设 x_0 是适合(5)的整数, 则由 $f(x_0) \equiv 0 (\mathrm{mod}\, m)$, 可得

$f(x_0)\equiv 0(\mathrm{mod}\ m_i)(i=1,\cdots,k)$. 反之，若 x_i 适合 $f(x_i)\equiv 0(\mathrm{mod}\ m_i)(i=1,\cdots,k)$，因为 $1\leqslant i<j\leqslant k$ 时，$(m_i,m_j)=1$，由孙子定理，有唯一的 x_0，$0\leqslant x_0<m$，适合 $x_0\equiv x_i(\mathrm{mod}\ m_i)(i=1,\cdots,k)$，且 $f(x_0)\equiv f(x_i)\equiv 0(\mathrm{mod}\ m_i)(i=1,\cdots,k)$，故 $f(x_0)\equiv 0(\mathrm{mod}\ m)$. 这就证明了同余式(5)有解的充分必要条件是同余式组(6)的每一个有解.

现设 $f(x)\equiv 0(\mathrm{mod}\ m_i)$ 的 T_i 个不同的解是

$$x\equiv u_{i,e_i}(\mathrm{mod}\ m_i),\ 0\leqslant u_{i,e_i}<m_i(e_i=1,2,\cdots,T_i;\ \ i=1,\cdots,k).$$

对其中任一组 $(u_{1,e_1}u_{2,e_2},\cdots,u_{k,e_k})$，由孙子定理可得唯一的 x，$0\leqslant x<m$，是(5)的解，且不同的组，得到的(5)的解 x 也不同，故有 $T_1T_2\cdots T_k\leqslant T$. 反之，设 $x_1,\cdots,x_T$，$0\leqslant x_i<m(i=1,\cdots,T)$，是(5)的 T 个解，则对某 $j(1\leqslant j\leqslant T)$，$(\langle x_j\rangle_{m_1},\cdots,\langle x_j\rangle_{m_k})$ 是某一组 $(u_{1,e_1},\cdots,u_{k,e_k})$，且 $(\langle x_i\rangle_{m_1},\cdots,\langle x_i\rangle_{m_k})$，$i=1,\cdots,T$，是不同的，故 $T\leqslant T_1\cdots T_k$，这就证明了 $T=T_1\cdots T_k$.

证完

例 解同余式 $6x^3+27x^2+17x+20\equiv 0(\mathrm{mod}30)$.

解 设 $f(x)=6x^3+27x^2+17x+20$，由定理 3 知解同余式 $f(x)\equiv 0(\mathrm{mod}30)$ 可先分别解以下两同余式：

$$f(x)\equiv 0(\mathrm{mod}5),\ f(x)\equiv 0(\mathrm{mod}6).$$

容易验证第一个同余式有解

$$x\equiv 0,1,2(\mathrm{mod}5),$$

第二个同余式有解

$$x\equiv 2,5(\mathrm{mod}\ 6).$$

由孙子定理，当 (b_1,b_2) 取 $(0,2)$，$(0,5)$，$(1,2)$，$(1,5)$，$(2,2)$，$(2,5)$ 时，得到 $f(x)\equiv 0(\mathrm{mod}30)$ 的 6 个解

$$x\equiv 6b_1+25b_2$$

$$\equiv 2, 5, 11, 17, 20, 26 \pmod{30}.$$

我们已经知道 $m>1$ 时，m 可写成标准分解式 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，由定理 3 知，欲解 $f(x)\equiv 0(\bmod m)$，只需解同余式组 $f(x)\equiv 0(\bmod p_i^{\alpha_i})(i=1, 2, \cdots, k)$. 下一节，就来讨论模为素数幂的同余式.

§7 模是素数幂的同余式

本节讨论模是素数幂的同余式

$$f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0(\bmod p^\alpha), \quad (1)$$

$$n>0, p^\alpha\nmid a_n,$$

其中 p 是素数，$\alpha\geqslant 1$.

显然，适合(1)的每一个整数都适合同余式

$$f(x)\equiv 0(\bmod p). \quad (2)$$

但反过来不一定成立，例如 2 是 $x^{10}-1\equiv 0(\bmod 11)$ 的解，但不是 $x^{10}-1\equiv 0(\bmod 11^2)$ 的解. 因此(1)的解可在(2)的解中去找. 如(2)无解，自然(1)也无解.

如何由(2)的解来找(1)的解呢？我们有

定理 设 $x\equiv x_1(\bmod p)$ 即

$$x=x_1+pt_1(t_1=0, \pm 1, \pm 2, \cdots) \quad (3)$$

是(2)的一个解，且 $p\nmid f'(x_1)$，这里 $f'(x)=\sum_{i=1}^{n}ia_ix^{i-1}$ 表示 $f(x)$ 的导函数，则(3)恰好给出(1)的一个解 $x\equiv x_\alpha(\bmod p^\alpha)$，即

$$x=x_\alpha+p^\alpha t_\alpha(t_\alpha=0, \pm 1, \pm 2, \cdots),$$

其中 $x_\alpha\equiv x_1(\bmod p)$.

证 我们用数学归纳法来证明. 当 $\alpha=1$ 时，定理显然成立. 现假定定理对 $\alpha-1(\alpha\geqslant 2)$ 成立，即(3)恰好给出

$$f(x)\equiv 0(\bmod p^{\alpha-1})$$

的一个解

$$x=x_{\alpha-1}+p^{\alpha-1}t_{\alpha-1}(t_{\alpha-1}=0,\pm1,\pm2,\cdots),$$

其中 $x_{\alpha-1}\equiv x_1(\mathrm{mod}\ p)$. 把 $x=x_{\alpha-1}+p^{\alpha-1}t_{\alpha-1}$ 代入(1)，由 $2\alpha-2\geqslant\alpha$, 可得

$$f(x_{\alpha-1})+p^{\alpha-1}t_{\alpha-1}f'(x_{\alpha-1})\equiv0(\mathrm{mod}\ p^{\alpha}),$$

但 $f(x_{\alpha-1})\equiv0(\mathrm{mod}\ p^{\alpha-1})$, 因此

$$t_{\alpha-1}f'(x_{\alpha-1})\equiv-\frac{f(x_{\alpha-1})}{p^{\alpha-1}}\ (\mathrm{mod}\ p).$$

由 $x_{\alpha-1}\equiv x_1(\mathrm{mod}\ p)$, 即得

$$t_{\alpha-1}f'(x_1)\equiv-\frac{f(x_{\alpha-1})}{p^{\alpha-1}}(\mathrm{mod}\ p).$$

由于 $(f'(x_1),p)=1$, 故上式恰有一解

$$t_{\alpha-1}=t'_{\alpha-1}+pt_{\alpha}(t_{\alpha}=0,\pm1,\cdots),$$

这就得到了(1)的解

$$\begin{aligned}x&=x_{\alpha-1}+p^{\alpha-1}(t'_{\alpha-1}+pt_{\alpha})\\&=x_{\alpha-1}+p^{\alpha-1}t'_{\alpha-1}+p^{\alpha}t_{\alpha}(t_{\alpha}=0,\pm1,\cdots).\end{aligned}$$

令 $x_{\alpha-1}+p^{\alpha-1}t'_{\alpha-1}=x_{\alpha}$, 即 $x\equiv x_{\alpha}(\mathrm{mod}\ p^{\alpha})$ 是(1)的一个解，且 $x_{\alpha}\equiv x_1$ $(\mathrm{mod}\ p)$. 证完

由这个定理可得以下推论.

推论 设 $f(x)\equiv0(\mathrm{mod}\ p)$ 和 $f'(x)\equiv0(\mathrm{mod}\ p)$ 无公解，则同余式 $f(x)\equiv0(\mathrm{mod}\ p^{\alpha})$ 和同余式 $f(x)\equiv0(\mathrm{mod}\ p)$ 的解数相同.

定理的证明是构造性的，它提供了一个由(2)的解求(1)的解的方法. 现举一例来说明.

例 求同余式 $f(x)=x^3-4x^2+5x-6\equiv0(\mathrm{mod}27)$.

解 $f(x)\equiv0(\mathrm{mod}3)$, $f'(x)\equiv0(\mathrm{mod}3)$ 无公解，$f(x)\equiv0(\mathrm{mod}3)$ 有唯一解 $x\equiv0(\mathrm{mod}3)$. 以 $x=3t_1$ 代入 $f(x)\equiv0(\mathrm{mod}9)$ 得

$$f(0)+3t_1f'(0)\equiv0(\mathrm{mod}9).$$

但 $f(0)\equiv 3(\mathrm{mod}9)$, $f'(0)\equiv 5(\mathrm{mod}9)$, 故

$$3+6t_1\equiv 0(\mathrm{mod}9),$$

$$1+2t_1\equiv 0(\mathrm{mod}3),$$

$$t_1\equiv 1(\mathrm{mod}3),$$

因此 $t_1=1+3t_2$, $x=3+9t_2$ 是 $f(x)\equiv 0(\mathrm{mod}9)$的唯一解. 将 $x=3+9t_2$ 代入 $f(x)\equiv 0(\mathrm{mod}27)$得

$$f(3)+9t_2f'(3)\equiv 0(\mathrm{mod}27).$$

但 $f(3)\equiv 0(\mathrm{mod}27)$, $f'(3)\equiv 8(\mathrm{mod}27)$, 故

$$8\cdot 9t_2\equiv 0(\mathrm{mod}27),$$

$$8t_2\equiv 0(\mathrm{mod}3),$$

$$t_2\equiv 0(\mathrm{mod}3),$$

设 $t_2=3t_3$, $x=3+27t_3$, $x\equiv 3(\mathrm{mod}27)$是 $f(x)\equiv 0(\mathrm{mod}27)$的唯一解.

§8 整数的剩余表示

同余理论在计算机技术中有用, 本节将要介绍整数的剩余表示, 就是应用之一.

定义 设$m_1>0,\cdots,m_k>0$, $(m_i,m_j)=1, 0<i<j\leqslant k$, 一个整数 x 对于模 m_1, …, m_k 的**剩余表示**是指序列$(\langle x\rangle_{m_1},\langle x\rangle_{m_2},\cdots,\langle x\rangle_{m_k})$, 记作 $x\longleftrightarrow(\langle x\rangle_{m_1},\langle x\rangle_{m_2},\cdots,\langle x\rangle_{m_k})$.

例 1 设 $m_1=2, m_2=3, m_3=5$, 则 22 的剩余表示为$(0,1,2)$.

显然, 一个数的剩余表示是唯一的. 但是, 反过来不真, 就是说可以有许多数具有同一个剩余表示.

例 2 设 $m_1=2, m_2=3, m_3=5$, 则所有形如 $30t+22$ 的整数, 其剩余表示均为$(0,1,2)$.

定理 1 设 $m_1>0,\cdots,m_k>0$, $(m_i,m_j)=1$, $0<i<j\leqslant k$, 两个整数 x, x' 对于模 $m_1,\cdots,m_k$ 的剩余表示相同的充分必要条件是 x

$\equiv x' \pmod{M}$，这里 $M=m_1\cdots m_k$.

证 设 x 和 x' 对于模 $m_1,\cdots,m_k$ 的剩余表示分别为

$$(\langle x\rangle_{m_1},\langle x\rangle_{m_2},\cdots,\langle x\rangle_{m_k})$$

和

$$(\langle x'\rangle_{m_1},\langle x'\rangle_{m_2},\cdots,\langle x'\rangle_{m_k}),$$

其中

$$\langle x\rangle_{m_i}=x-q_im_i,\ 0\leqslant\langle x\rangle_{m_i}<m_i;$$

$$\langle x'\rangle_{m_i}=x'-q_i'm_i,\ 0\leqslant\langle x'\rangle_{m_i}<m_i,$$

$$i=1,\cdots,k,$$

如果 $\langle x\rangle_{m_i}=\langle x'\rangle_{m_i}(i=1,\cdots,k)$，则

$$m_i\mid x-x',$$

故 $M\mid x-x'$.

反之，设 $M\mid x-x'$，因为 $x-x'=\langle x\rangle_{m_i}+q_im_i-q_i'm_i-\langle x'\rangle_{m_i}$ $(i=1,\cdots,k)$，故 $m_i\mid\langle x\rangle_{m_i}-\langle x'\rangle_{m_i}(i=1,\cdots,k)$，由此推出 $\langle x\rangle_{m_i}=\langle x'\rangle_{m_i}(i=1,\cdots,k)$. 证完

如果我们限定 $0\leqslant x<M=m_1\cdots m_k$，那么，不同的整数 x 对于模 $m_1,\cdots,m_k$ 的剩余表示，也是不同的.

例 3 取 $m_1=2,m_2=3,m_3=5$，则 0 到 29 的剩余表示为

$$0\longleftrightarrow(0,0,0),\qquad 1\longleftrightarrow(1,1,1),$$

$$2\longleftrightarrow(0,2,2),\qquad 3\longleftrightarrow(1,0,3),$$

$$4\longleftrightarrow(0,1,4),\qquad 5\longleftrightarrow(1,2,0),$$

$$6\longleftrightarrow(0,0,1),\qquad 7\longleftrightarrow(1,1,2),$$

$$8\longleftrightarrow(0,2,3),\qquad 9\longleftrightarrow(1,0,4),$$

$$10\longleftrightarrow(0,1,0),\qquad 11\longleftrightarrow(1,2,1),$$

$$12\longleftrightarrow(0,0,2),\qquad 13\longleftrightarrow(1,1,3),$$

$$14\longleftrightarrow(0,2,4),\qquad 15\longleftrightarrow(1,0,0),$$

$$16\longleftrightarrow(0,1,1),\qquad 17\longleftrightarrow(1,2,2),$$

$18\longleftrightarrow(0,0,3)$, $19\longleftrightarrow(1,1,4)$,

$20\longleftrightarrow(0,2,0)$, $21\longleftrightarrow(1,0,1)$,

$22\longleftrightarrow(0,1,2)$, $23\longleftrightarrow(1,2,3)$,

$24\longleftrightarrow(0,0,4)$, $25\longleftrightarrow(1,1,0)$,

$26\longleftrightarrow(0,2,1)$, $27\longleftrightarrow(1,0,2)$,

$28\longleftrightarrow(0,1,3)$, $29\longleftrightarrow(1,2,4)$,

我们有

定义 设 $m_1>0,\cdots,m_k>0$, $(m_i,m_j)=1,0<i<j\leqslant k$, $M=m_1\cdots m_k$, $0\leqslant x<M$, 此时整数 x 对于模 m_1, …, m_k 的剩余表示 $(\langle x\rangle_{m_1},\cdots,\langle x\rangle_{m_k})$ 也叫 x 的**模系数记数法**.

如果知道了整数 x 的模系数记数法 $(\langle x\rangle_{m_1},\cdots,\langle x\rangle_{m_k})$, 那么用孙子定理便知可唯一定出 x. 因此, 有

定理 2 设 Z 表整数集, $\mathbf{Z}_l=\{0,1,\cdots,l-1\}$ 表示 l 的最小非负剩余组成的集, 设 $m_1>0,\cdots,m_k>0$, $(m_i,m_j)=1,0<i<j\leqslant k$, $0\leqslant x<m_1\cdots m_k$, 则集

$$S=\{x\mid 0\leqslant x<m_1\cdots m_k\}$$

与集

$$S_1=\{(a_1,\cdots,a_k)\mid a_j\in\mathbf{Z}_{m_j},\ j=1,\cdots,k\}$$

之间存在一一对应.

关于整数的剩余表示, 还有以下两个重要性质.

定理 3 设 x 和 y 的剩余表示分别为 $(\langle x\rangle_{m_1},\cdots,\langle x\rangle_{m_k})$ 和 $(\langle y\rangle_{m_1},\cdots,\langle y\rangle_{m_k})$, 则有

① $\langle x\pm y\rangle_M$ 的剩余表示为 $(\langle\langle x\rangle_{m_1}\pm\langle y\rangle_{m_1}\rangle_{m_1},\cdots,\langle\langle x\rangle_{m_k}\pm\langle y\rangle_{m_k}\rangle_{m_k})$.

② $\langle x\cdot y\rangle_M$ 的剩余表示为 $(\langle\langle x\rangle_{m_1}\langle y\rangle_{m_1}\rangle_{m_1},\cdots,\langle\langle x\rangle_{m_k}\langle y\rangle_{m_k}\rangle_{m_k})$.

证 在第一章 §1 中, 我们证明了 $\langle x\pm y\rangle=\langle\langle x\rangle\pm\langle y\rangle\rangle$, $\langle xy\rangle$

$=\langle\langle x\rangle\langle y\rangle\rangle$，便知定理 3 成立.　　证完

显然有

推论　如果 $0\leqslant x<M$，$0\leqslant y<M$，$0\leqslant xy<M$，$0\leqslant x\pm y<M$，则在定理 3 中把整数的剩余表示换成整数的模系数记数法，则结论仍然成立.

例 4　对于模 4, 3, 5, 11,

$$x=102\longleftrightarrow(2,0,2,3),$$

$$y=211\longleftrightarrow(3,1,1,2),$$

则

$$\begin{array}{rr} 102 & (2,0,2,3) \\ +211 & (3,1,1,2) \\ \hline \langle 313\rangle_{660} & -313\longleftrightarrow(1,1,3,5) \end{array}$$

例 5　对于模 4, 3, 5, 11.

$$x=25\longleftrightarrow(1,1,0,3)$$

$$y=21\longleftrightarrow(1,0,1,10)$$

$$\begin{array}{rr} 25 & \\ \times 21 & \\ \hline 25 & (1,1,0,3) \\ 50 & (1,0,1,10) \\ \hline \langle 525\rangle_{660} & =525\longleftrightarrow(1,0,0,8) \end{array}$$

由定理 3 可知，这里乘法和加法无需进位，特别是乘法无需进位，这在计算机的制造和使用上，将带来很大的方便，特别是，用模系数记数法，Z_M 中的数对模 M 的运算，可以分别通过 Z_{m_j} 中的数对模 $m_j(j=1,\cdots,k)$ 的运算来完成.

§9　逐步淘汰原则

在数论中，常常遇到一些计数的问题，这些计数问题归结到计算有限集 S 中不属于某些指定子集的元素的个数，例如求 1000 中不能被 4 也不能被 5 整除的整数的个数. 设 $S=\{1,2,\cdots,1000\}$，

$S_1=\left\{4k,1\leqslant k\leqslant\left[\frac{1000}{4}\right]\right\}$，$S_2=\left\{5k,1\leqslant k\leqslant\left[\frac{1000}{5}\right]\right\}$，$S_1\cap S_2=\left\{20k,1\leqslant k\leqslant\left[\frac{1000}{20}\right]\right\}$，则所求个数$=|S|-|S_1|-|S_2|+|S_1S_2|=1000-250-200+50=600$. 这里记号$|A|$表集$A$中元素的个数，$S_1\cap S_1$简记为$S_1S_2$.

一般地，设$S_1,\cdots,S_n$是S的n个子集，T是S的一个子集，$S\setminus T$表示S中不在T中元素的集，故$S\setminus\bigcup_{i=1}^{n}S_i$表示$S$中所有不属于$S_1,\cdots,S_n$中任一个的元素的集. 我们有

定理1（逐步淘汰原则） 设$S_1,\cdots,S_n$是有限集S的给定的n个子集，则有

$$\left|S\setminus\bigcup_{i=1}^{n}S_i\right|=|S|-\sum_{1\leqslant i\leqslant n}|S_i|+\sum_{1\leqslant i<j\leqslant n}|S_iS_j|-\sum_{1\leqslant i<j<k\leqslant n}|S_iS_jS_k|+\cdots+(-1)^n|S_1\cdots S_n|. \tag{1}$$

证 我们用归纳法来证明(1)式. (1)中$n=2$时，显然有$|S\setminus S_1\cup S_2|=|S|-|S_1|-|S_2|+|S_1S_2|$. 现设$n=r-1$时(1)成立，来证$n=r$时，(1)也成立.

由于

$$S\setminus\bigcup_{i=1}^{r-1}S_i=\left(S\setminus\bigcup_{i=1}^{r}S_i\right)\cup\left(S\setminus\bigcup_{i=1}^{r-1}S_i\right)S_r$$

$$=\left(S\setminus\bigcup_{i=1}^{r}S_i\right)\cup\left(S_r\setminus\bigcup_{i=1}^{r-1}S_iS_r\right),$$

以及集$S\setminus\bigcup_{i=1}^{r}S_i$和集$S_r\setminus\bigcup_{i=1}^{r-1}S_iS_r$没有公共元素，故得

$$\left| S\setminus\bigcup_{i=1}^{r-1}S_i\right| = \left| S\setminus\bigcup_{i=1}^{r}S_i\right| + \left|S_r\setminus\bigcup_{i=1}^{r-1}S_iS_r\right|,$$

即

$$\left| S\setminus\bigcup_{i=1}^{r}S_i\right| = \left| S\setminus\bigcup_{i=1}^{r-1}S_i\right| - \left|S_r\setminus\bigcup_{i=1}^{r-1}S_iS_r\right| .$$

由归纳假设,故

$$\left| S\setminus\bigcup_{i=1}^{r}S_i\right| = |S| - \sum_{1\leqslant i\leqslant r-1}|S_i| + \sum_{1\leqslant i<j\leqslant r-1}|S_iS_j|$$

$$-\cdots+(-1)^{r-1}|S_1\cdots S_{r-1}| - \left(|S_r| - \sum_{1\leqslant i\leqslant r-1}|S_iS_r| + \right.$$

$$\left. \sum_{1\leqslant i<j\leqslant r-1}|S_iS_jS_r| - \cdots + (-1)^{r-1}|S_1\cdots S_{r-1}S_r|\right)$$

$$= |S| - \sum_{1\leqslant i\leqslant r}|S_i| + \sum_{1\leqslant i<j\leqslant r}|S_iS_j| - \cdots + (-1)^r|S_1\cdots S_r|.$$

这就证明了(1)在 $n=r$ 时也成立. 证完

作为逐步淘汰原则应用的一个例子,我们再次给出 $\varphi(n)$ 的公式.

例 设 $n=p_1^{a_1}\cdots p_k^{a_k}$, $p_1,\cdots,p_k$ 是不同的素数,则

$$\varphi(n) = n\prod_{p\mid n}\left(1-\frac{1}{p}\right).$$

设 $S=\{1,\cdots,n\}$, $S_j=\left\{tp_j,\ 1\leqslant t\leqslant\frac{n}{p_j}\right\}$, $1\leqslant j\leqslant k$. 因为当 $d\mid n$ 时, S 中有 $\frac{n}{d}$ 个 d 的倍数,故

$$|S_j| = \frac{n}{p_j},\quad |S_iS_j| = \frac{n}{p_ip_j},\ \cdots,\ |S_1\cdots S_k| = \frac{n}{p_1\cdots p_k}.$$

由定理1可得

$$\varphi(n)=\left|S\setminus\bigcup_{i=1}^{k}S_i\right|=n-\sum_{i=1}^{k}\frac{n}{p_i}+\sum_{1\leqslant i<j\leqslant k}\frac{n}{p_ip_j}-$$

$$\cdots+(-1)^k\frac{n}{p_1\cdots p_k}=n\sum_{p\mid n}\left(1-\frac{1}{p}\right).$$

下面，应用定理1来计算模 n 的缩系中属于某个给定的模 d 的剩余类中的数的个数，这里 $d\mid n$. 我们有

定理2 给定整数 $n>1, d>0$ 和 r，这里 $d\mid n$，且 $(r,d)=1$，则集

$$S=\left\{r+td,\ t=1,\cdots,\frac{n}{d}\right\}$$

中与 n 互素的数的个数是 $\dfrac{\varphi(n)}{\varphi(d)}$.

证 因为 $(r,d)=1$，故素数 p 若适合 $p\mid n$，及对某个 $r+td\in S$ 有 $p\mid r+td$，则 $p\nmid d$. 因此，设 $p_1,\cdots,p_m$ 是满足上述条件的所有素数，则 $p_j\nmid d, j=1,\cdots,m$，且设 $n'=p_1\cdots p_m$. S 中与 n 互素的数是那些不为 $p_1,\cdots,p_m$ 中任一个所整除的数. 设

$$S_i=\{x:x\in S, p_i\mid x\},\ i=1,\cdots,m.$$

因为 $p_i\nmid d$，故恰有唯一的 $t(\mathrm{mod}\,p_i)$ 满足

$$r+td\equiv 0(\mathrm{mod}\,p_i),$$

故在以下每一个区间

$$[1,p_i],[p_i+1,2p_i],\cdots,[(q-1)p_i+1,qp_i]$$

内恰有一个 t 满足 $r+td\equiv 0(\mathrm{mod}\,p_i)$，这里 $qp_i=\dfrac{n}{d}$，于是有

$$|S_i|=\frac{n}{dp_i},\ i=1,\cdots,m,$$

$$|S_iS_j|=\frac{n}{dp_ip_j},\quad |S_1\cdots S_m|=\frac{n}{dp_1\cdots p_m},$$

故

$$\left|S\setminus\bigcup_{i=1}^{m}S_i\right|=\frac{n}{d}\prod_{p\mid n}\left(1-\frac{1}{p}\right)=\frac{n\prod\limits_{p\mid n}\left(1-\frac{1}{p}\right)}{d\prod\limits_{p\mid d}\left(1-\frac{1}{p}\right)}=\frac{\varphi(n)}{\varphi(d)}.$$

证完

*§10 覆盖同余式组

易知，每一个整数至少满足下面同余式组中的一个：

$$x\equiv 0(\mathrm{mod}2),\ x\equiv 0(\mathrm{mod}3),\ x\equiv 1(\mathrm{mod}4),\ x\equiv 5(\mathrm{mod}6),$$
$$x\equiv 7(\mathrm{mod}12). \tag{1}$$

同余式组(1)就叫一组覆盖同余式组. 一般地，我们有以下定义.

定义 如果每一个整数都至少满足同余式组

$$x\equiv a_1(\mathrm{mod}n_1),\ x\equiv a_2(\mathrm{mod}n_2),\cdots,x\equiv a_k(\mathrm{mod}n_k),$$
$$1<n_1<n_2<\cdots<n_k,\quad 0\leqslant a_i<n_i,\ i=1,\cdots,k \tag{2}$$

中的一个，那么(2)就叫做一组**覆盖同余式组**.

利用电子计算机，对于 $2\leqslant n_1\leqslant 20$，已经证明了均存覆盖同余式组. 有两个著名的猜想尚未证明：①对任给的 $n_1>1$，都存在覆盖同余式组；②设 $N=[n_1,\cdots,n_k]$，如果(2)是一组覆盖同余式组，则有 $2\mid N$.

安道什曾经猜想下面的定理成立.

定理 1 如果(2)是一组覆盖同余式组，则有

$$\sum_{j=1}^{k}\frac{1}{n_j}>1. \tag{3}$$

现在来证明这个猜想.

证 设 $N=n_1\cdots n_k$，如果(2)是一组覆盖同余式组，又设 $1,2,\cdots,N$ 中有 N_j 个数满足

$$x\equiv a_j(\mathrm{mod}n_j),$$

则

$$N_j-\left[\frac{N-a_j}{n_j}\right]+\delta_j, \tag{4}$$

其中[x]表示不超过实数x的最大整数，

$$\delta_j=\begin{cases}0, & a_j=0,\\ 1, & a_j\neq 0.\end{cases} \tag{5}$$

由(4)、(5)和$N=n_1\cdots n_k$知

$$N_j=\frac{N}{n_j}\qquad (j=1,2,\cdots,k). \tag{6}$$

由(2)是一组覆盖同余式组知

$$\sum_{j=1}^{k}\frac{N}{n_j}\geqslant N,$$

即

$$\sum_{j=1}^{k}\frac{1}{n_j}\geqslant 1. \tag{7}$$

如果(7)中等号成立，则推出$0,1,\cdots,N-1$中每一个整数满足(2)中一个且仅一个同余式. 此时，$t_jn_j+a_j$, $t_j=0,1,\cdots,N_j-1$, $j=1,\cdots,k$, 恰给出了$0,1,\cdots,N-1$诸数. 于是有

$$1+x+x^2+\cdots+x^{N-1}=\sum_{j=1}^{k}\sum_{t_j=0}^{N_j-1}x^{t_jn_j+a_j},$$

设x是一个复变量，上式给出

$$\frac{1-x^N}{1-x}=\sum_{j=1}^{k}x^{a_j}\frac{1-x^N}{1-x^{n_j}}, \tag{8}$$

在(8)式中令$x=re^{\frac{2\pi i}{n_k}}$, $r<1$, 得

$$\frac{1}{1-re^{\frac{2\pi i}{n_k}}}=\frac{r^{a_1}e^{\frac{2\pi a_1 i}{n_k}}}{1-r^{n_1}e^{\frac{2\pi n_1 i}{n_k}}}+\cdots+\frac{r^{a_k}e^{\frac{2\pi a_k i}{n_k}}}{1-r^{n_k}} \tag{9}$$

在(9)中令 $r\to 1$，(9)中右端最后一项的模是无界的，而左端以及右端的其余诸项的模是有界的，此不可能，故(7)中等式不可能，这就证明了(3)式成立. 证完

定义 设同余式组

$$x\equiv a_1 (\mathrm{mod} n_1), x\equiv a_2 (\mathrm{mod} n_2), \cdots, x\equiv a_k (\mathrm{mod} n_k),$$

$$1<n_1\leqslant n_2\leqslant\cdots\leqslant n_k,\ 0\leqslant a_i<n_i, i=1,\cdots,k, \tag{10}$$

如果每一个整数满足(10)中一个且仅一个同余式，那么(10)就叫做**一组不相交的覆盖同余式组**.

下列定理是容易证明的.

定理 2 如果(10)是一组不相交的覆盖同余式组，则有

① $\sum_{i=1}^{k}\frac{1}{n_i}=1$;

② $(n_i, n_j)\neq 1, 1\leqslant i<j\leqslant k$;

③ 不可能有 $1<n_1<n_2<\cdots<n_k$.

证 设 $n=n_1\cdots n_k$，N_j 表示 $1,\cdots,n$ 中适合同余式 $x\equiv a_j (\mathrm{mod} n_j)$ 的个数，$j=1,\cdots,k$. 则有

$$n=\sum_{j=1}^{k} N_j=\sum_{j=1}^{k}\frac{n}{n_j},$$

这就证明了①.

如果 $(n_i, n_j)=1$，则 $x\equiv a_i (\mathrm{mod} n_i), x\equiv a_j (\mathrm{mod} n_j)$ 有公解，与所设不合. 这就证明了②.

如果(10)中 $1<n_1<n_2<\cdots<n_k$，则由定理1，我们有 $\sum_{j=1}^{k}\frac{1}{n_j}>1$，

此与①矛盾，这就证明了③. 证完

1974年，考雷克(Korec)曾经证明了兹拉姆(Znám)的一个猜想：设 $N=[n_1,\cdots,n_k]$，$N=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ 是 N 的标准分解式，则 $k\geqslant 1$

$+\sum_{j=1}^{r}\alpha_j(p_j-1)$.

1974年，兹拉姆还证明了如下比定理 2 中③更强的结果：设(10)是一组不相交的覆盖同余式组，p 是 n_k 的最小素因子，则 n_1，…，n_k 中至少有 p 个相等.

1972 年，兹拉姆在研究覆盖同余式组的过程中，曾提出一个问题：是否对每一个整数 $n>1$，都存在整数 $x_i>1(i=1,\cdots,n)$，使得对每一个 i，x_i 是 $x_1\cdots x_{i-1}x_{i+1}\cdots x_n+1$ 的真因子？ 1982 年，孙琦解决了这一问题，证明了 $n\geqslant 5$ 时，兹拉姆问题均有解，同时还给出了一个构造性的证明.

第二章　习　题

1. 设 S 是 n 个整数组成的集，证明：存在某个 S 的非空子集，其诸元的和被 n 整除.

2. 把整数写成 10 的幂的和，求出能被 11 整除的数的判别法.

3. 证明：若 $n\equiv 0(\mathrm{mod}2)$，$a_1,\cdots,a_n$ 和 $b_1,\cdots,b_n$ 是模 n 的任意两组完全剩余系，则 $a_1+b_1,\cdots,a_n+b_n$ 不是模 n 的完全剩余系.

4. 证明：若 p 是素数，则对任意的整数 $h_1,\cdots,h_a$ 均有

$$(h_1+\cdots+h_a)^p\equiv h_1^p+\cdots+h_a^p(\mathrm{mod}p),$$

由此推出费马小定理，进而推出欧拉定理.

5. 证明：若 $m^p+n^p\equiv 0(\mathrm{mod}p)$，则 $m^p+n^p\equiv 0(\mathrm{mod}p^2)$，这里 p 是奇素数.

6. 证明：若 $m_i>0(i=1,\cdots,k)$，x_i 通过模 m_i 的任一完全剩余系，则

$$x_1+m_1x_2+m_1m_2x_3+\cdots+m_1m_2\cdots m_{k-1}x_k$$

过模 $m_1\cdots m_k$ 的一组完全剩余系.

7. 证明：若 $x_n,x_{n-1},\cdots,x_1,x_0$ 互相独立地通过 $-1,0,1$ 时，

$$3^nx_n+3^{n-1}x_{n-1}+\cdots+3x_1+x_0$$

表示所有下面的数

$$-H,\cdots,-1,0,1,\cdots,H,\qquad H=\frac{3^{n+1}-1}{3-1},$$

并且每一个数都有唯一的表示法. 由此说明应用 $n+1$ 个特制的砝码，在天平上可以量出 1 到 H 克的任何一个克数.

8. 证明：若 $m>2, a_1, \cdots, a_{\varphi(m)}$ 为模 m 的任一缩系，则

$$\sum_{i=1}^{\varphi(m)} a_i \equiv 0 \pmod{m}.$$

*9. 求出 $(n-1)!+1=n^k$ 的全部正整数解 n, k.

10. 证明：若 n 是任意整数，则 $n^9-n^5\equiv 0 \pmod{504}$.

11. 证明：如果有三个不同的整点 (x, y)，适合 $p \mid xy-t$（这里 p 是一个素数，$p \nmid t$），且在一条直线上，则在这三点中至少有两个点，其纵、横坐标的差，分别被 p 整除.

*12. 如果 $(x, y)=1$，则称平面上整点 (x, y) 为既约整点. 证明：任给 $n>0$，存在一整点，它与每一个既约整点的距离大于 n.

13. 证明：若 p 是奇素数，则

① $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

② $2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

*14. 证明：若 p 是一个素数，则

① $\binom{n}{p} \equiv \left[\frac{n}{p}\right] \pmod{p^2}$;

② 如果 $p^s \left| \left[\frac{n}{p}\right] \right.$，则 $p^s \left| \binom{n}{p} \right.$.

15. 证明：对任意整数 x，$\frac{1}{5}x^5+\frac{1}{3}x^3+\frac{7}{15}x$ 是一个整数.

16. 求出最小的正整数，它的 $\frac{1}{2}$ 是一个整数的平方，它的 $\frac{1}{3}$ 是一个整数的三次方，它的 $\frac{1}{5}$ 是一个整数的五次方.

17. 证明：若 $n>1, 2 \nmid n$，则对任意的 m，$n \nmid m^{n-1}+1$.

18. 证明：若 p_1, p_2 是两个奇素数，$p_1>p_2$，则对任意的 m，$p_1 p_2 \nmid m^{p_1-p_2}+1$.

19. 求出一组 $n_1=3$ 的覆盖同余式组.

20. 证明 $61!+1\equiv 0 \pmod{71}$.

21. 证明：若 $p>3$ 是一个素数，且设

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}+\frac{1}{p}=\frac{r}{ps},\ (r,s)=1,$$

则 $p^2 \mid r-s$.

22. 证明：若 $n>0$，满足 $24 \mid n+1$，则 $24 \mid \sigma(n)$.

*23. 证明：若 $m>0$，则同余式

$$6xy-2x-3y+1\equiv 0 \pmod{m}$$

有解.

24. 证明：对于任给的 $n>0$，存在 $m>0$，使同余式

$$x^2\equiv 1 \pmod{m}$$

解的个数大于 n.

25. 证明：当 $u=0,1,\cdots,\ p^{s-t}-1,\ v=0,1,\cdots,p^t-1,\ t\leqslant s$ 时，$x=u+p^{s-t}v$ 通过 p^s 的一个完全剩余系.

26. 求下列同余式的解：

① $111x\equiv 75 \pmod{321}$,

② $256x\equiv 179 \pmod{337}$,

③ $1215x\equiv 560 \pmod{2755}$.

27. 求联立同余式

$$x+4y-29\equiv 0 \pmod{143},\ 2x-9y+84=0 \pmod{143}$$

的解.

28. 解下列同余式组：

① $x\equiv 1 \pmod 7,\ x\equiv 3 \pmod 5,\ x\equiv 5 \pmod 9$;

② $3x\equiv 5 \pmod 4,\ 5x\equiv 2 \pmod 7$;

③ $4x\equiv 3 \pmod{25},\ 3x\equiv 8 \pmod{20}$;

④ $x\equiv 8 \pmod{15},\ x\equiv 5 \pmod 8,\ x\equiv 13 \pmod{25}$.

29. 解下列高次同余式：

① $7x^4+19x+25\equiv 0 \pmod{27}$,

② $x^3+2x+2\equiv 0 \pmod{125}$,

③ $6x^3+27x^2+17x+20\equiv 0 \pmod{32}$.

30. 证明：若 p 是素数，则 $x^{p^l-1}\equiv 1 \pmod{p^l}$ 有 $p-1$ 个解，这里 $l\geqslant 1$.

31. ① 求出所有满足 $n^{13}\equiv n \pmod{1365}$ 的整数 n.

② 求出所有满足 $n^{17}\equiv n \pmod{4080}$ 的整数 n.

32. 证明：若 p 是一个奇素数，$q=\frac{p-1}{2}$，则

$$(q_1)^2+(-1)^q\equiv 0 \pmod{p}.$$

33. 设 $p>3, S=\{1,2,\cdots,p-1\}$，对每一个 $k\in S$，存在唯一 $x_k\in S$，使得 $kx_k\equiv 1 \pmod{p}$，因此 $kx_k=1+n_kp, k=1,\cdots,p-1$. 证明

$$\sum_{k=1}^{p-1} kn_k\equiv\frac{1}{2}(p-1) \pmod{p}.$$

34. 设 $a,b,\cdots,k,l$ 为正整数，求 $1,2,\cdots,n$ 中与 $a,b,\cdots,l$ 都互素的整数的个数.

*35. 设 $f(n_i)$ 表示所有覆盖同余式组中 k 的最小值，

① 证明 $f(n_i)\geqslant n_i+1$.

② 求 $f(2)$.

第三章　数论函数

在数论中，经常出现各种数论函数，它们在数论的研究中，起着重要作用.

定义　一个定义在正整数集上的实或复值函数 $f(n)$ 称作一个**数论函数或算术函数**.

例如，数列 a_n, n_l, n^λ 等等都是数论函数. 本章将介绍数论函数的某些一般理论，以及讨论几种重要的数论函数.

§1　数论函数 $\mathrm{pot}_p n$

定义　对于一给定的素数 p，设 $p^m \| n$，即 $p^m | n$, $p^{m+1} \nmid n$，则记 $\mathrm{pot}_p n = m$.

对于有理数 $\frac{m}{n}$，我们定义

$$\mathrm{pot}_p\left(\frac{m}{n}\right) = \mathrm{pot}_p m - \mathrm{pot}_p n.$$

对于给定的素数 p，$\mathrm{pot}_p n$ 是一个数论函数.

由定义，显然有以下简单的性质：

1. $\mathrm{pot}_p(mn) = \mathrm{pot}_p m + \mathrm{pot}_p n$;

2. $\mathrm{pot}_p n^k = k\mathrm{pot}_p n$，这里 $k>0$.

因此，有 $\mathrm{pot}_3 54 = \mathrm{pot}_3 3^3 + \mathrm{pot}_3 2 = 3$, $\mathrm{pot}_2 54 = \mathrm{pot}_2 3^3 + \mathrm{pot}_2 2 = 1$，等等.

本节主要求出 $\mathrm{pot}_p n_l$ 的公式. 为此，先介绍一个重要函数.

定义　函数 $[x]$ 是对于一切实数都有定义的函数，函数 $[x]$ 的值等于不大于 x 的最大整数.

这个函数在第一章 §9 及第二章的 §10 中已经用到过了，它

在数论中非常有用，有时，也把$[x]$叫做数论函数．由$[x]$的定义立刻可得下列简单性质：

1. $[x]\leqslant x<[x]+1$;

2. $[x]+[y]\leqslant[x+y]$;

3. 当 n 是整数时，$[n+x]=n+[x]$;

4. $[-x]=\begin{cases}-[x]-1, & \text{当 } x \text{ 不是整数时,}\\ -[x], & \text{当 } x \text{ 是整数时;}\end{cases}$

5. 若 a,b 是任意两个正整数，则不大于 a 而为 b 的倍数的正整数的个数是$\left[\frac{a}{b}\right]$.

我们有

定理 1 设 $p^k\leqslant n<p^{k+1}$，则有

$$\mathrm{pot}_p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^k}\right]. \tag{1}$$

证 因为

$$\mathrm{pot}_p(n!)=\mathrm{pot}_p 1+\mathrm{pot}_p 2+\cdots+\mathrm{pot}_p n$$

$$=\mathrm{pot}_p p+\mathrm{pot}_p(2p)+\cdots+\mathrm{pot}_p\left(\left[\frac{n}{p}\right]p\right)$$

和

$$\mathrm{pot}_p(jp)=\mathrm{pot}_p p+\mathrm{pot}_p j=1+\mathrm{pot}_p j,$$

我们有

$$\mathrm{pot}_p(n!)=\left[\frac{n}{p}\right]+\mathrm{pot}_p\left(\left[\frac{n}{p}\right]!\right). \tag{2}$$

由性质 5 可知$\left[\frac{\left[\frac{n}{p}\right]}{p}\right]=\left[\frac{n}{p^2}\right]$，故

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

$$\vdots$$

$$\mathrm{pot}_p\left(\left[\frac{n}{p^{k-1}}\right]!\right)=\left[\frac{n}{p^k}\right]+\mathrm{pot}_p\left(\left[\frac{n}{p^k}\right]!\right)-\left[\frac{n}{p^k}\right].$$

代入(2)便得(1). 证完

定理 1 的结果，也可写成 $\mathrm{pot}_p(n!)=\sum_{t=1}^{\infty}\left[\frac{n}{p^t}\right]$. 它给出了

$$n!=\prod_{p\le n}p^{\sum_{t=1}^{\infty}\left[\frac{n}{p^t}\right]}.$$

定理 2 设 $0<r<n$，则

$$\binom{n}{r}=\frac{n!}{r!\,(n-r)!}$$

是一个整数.

证 因为 $n=(n-r)+r$，故从$[x]$的性质 2 推出

$$\left[\frac{n}{p^t}\right]\geqslant\left[\frac{n-r}{p^t}\right]+\left[\frac{r}{p^t}\right],$$

$$\sum_{t=1}^{\infty}\left[\frac{n}{p^t}\right]\geqslant\sum_{t=1}^{\infty}\left[\frac{n-r}{p^t}\right]+\sum_{t=1}^{\infty}\left[\frac{r}{p^t}\right],$$

利用上面给出的 $n!$ 的公式，就证明了$\binom{n}{r}$是整数. 证完

定理 3 对于给定的素数 p 和 $0<r<p^c$，$c>0$，有

$$\mathrm{pot}_p\binom{p^c}{r}=c-\mathrm{pot}_p r. \tag{3}$$

证 $r=1$ 时，(3)显然成立. 设 $r>1$，有

$$\binom{p^c}{r}=\frac{p^c}{r}\cdot\frac{p^c-1}{1}\cdot\frac{p^c-2}{2}\cdots\frac{p^c-(r-1)}{r-1},$$

因为 $0<r<p^c$，故

$$\mathrm{pot}_p(p^c-j)=\mathrm{pot}_p j,\ j=1,\cdots,r-1,$$

$$\mathrm{pot}_p\binom{p^c}{r}=\mathrm{pot}_p p^c+\sum_{j=1}^{r-1}\mathrm{pot}_p(p^c-j)-\sum_{j=1}^{r}\mathrm{pot}_p(j)$$

$$-c-\mathrm{pot}_p r.$$

这证明了(3). 证完

定理 4 设 $n=a_h p^h+a_{h-1}p^{h-1}+\cdots+a_1 p+a_0$,

这里，$1\leqslant a_h<p, 0\leqslant a_j<p, j=0,1,\cdots,h-1$，$A(n,p)=\sum_{k=0}^{h}a_k$，则有

$$\frac{n-A(n,p)}{p-1}=\sum_{k=1}^{h}\left[\frac{n}{p^k}\right]=\mathrm{pot}_p(n!). \tag{4}$$

证 因为

$$n-A(n,p)=\sum_{k=0}^{h}a_k(p^k-1)=\sum_{k=1}^{h}a_k(p^k-1),$$

故

$$\frac{n-A(n,p)}{p-1}=\sum_{k=1}^{h}a_k(p^{k-1}+p^{k-2}+\cdots+p+1)$$

$$=a_1+a_2p+\cdots+a_hp^{h-1}+a_2+a_3p+\cdots+a_hp^{h-2}+\cdots+a_h$$

$$=\sum_{k=1}^{h}(a_hp^{h-k}+\cdots+a_{k+1}p+a_k)$$

$$=\sum_{k=1}^{h}\left[\frac{n}{p^k}\right].$$

因为 $p^h\leqslant n<p^{h+1}$，故由定理 1 $\sum_{k=1}^{h}\left[\frac{n}{p^k}\right]=\mathrm{pot}_p(n!)$. 证完

现在，我们可以进一步求出 $\mathrm{pot}_p\binom{n}{r}$.

定理 5 设 $0<r<n$，则

$$\mathrm{pot}_p\binom{n}{r}=\frac{A(r,p)+A(n-r,p)-A(n,p)}{p-1}.$$

证 因为

$$\mathrm{pot}_p\binom{n}{r}=\mathrm{pot}_p(n!)-\mathrm{pot}_p(r!)-\mathrm{pot}_p((n-r)!),$$

由(4)，故

$$\mathrm{pot}_p\binom{n}{r}=\frac{n-A(n,p)}{p-1}-\left(\frac{r-A(r,p)+n-r-A(n-r,p)}{p-1}\right)$$

$$=\frac{A(r,p)+A(n-r,p)-A(n,p)}{p-1}.$$ 证完

§2 麦比乌斯函数 $\mu(n)$

定义 **麦比乌斯 (Möbius)函数** $\mu(n)$，当 $n=1$ 时 $\mu(1)=1$；当 $n>1$ 时，设 $n=p_1^{l_1}\cdots p_s^{l_s}$ 为 n 的标准分解式，则 $\mu(n)$ 定义为

$$\mu(n)=\begin{cases}(-1)^s, & l_1=\cdots=l_s=1\text{ 时},\\ 0, & \text{有某个 } l_j>1\ (1\leqslant j\leqslant s)\text{ 时},\end{cases}$$

我们有

定理 1 如果 $n\geqslant 1$，则有

$$\sum_{d\mid n}\mu(d)=\left[\frac{1}{n}\right]. \tag{1}$$

证 $n=1$ 时，(1)显然成立. 现设 $n>1$，n 的标准分解式为 $n=p_1^{l_1}\cdots p_s^{l_s}$，则

$$\sum_{d\mid n}\mu(d)=\mu(1)+\mu(p_1)+\cdots+\mu(p_s)+\mu(p_1p_2)$$

$$+\cdots+\mu(p_{s-1}p_s)+\cdots+\mu(p_1\cdots p_s)$$

$$=1+\binom{s}{1}(-1)+\binom{s}{2}(-1)^2+\cdots+\binom{s}{s}(-1)^s$$

$$=(1-1)^s=0.$$ 证完

函数 $\mu(n)$ 在数论中经常出现，例如在第二章中我们已经证明了，欧拉函数

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right), \tag{2}$$

其中 $n=p_1^{l_1}\cdots p_s^{l_s}$ 是 n 的标准分解式，利用 $\mu(n)$，可将(2)改写为

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

定理 2 设 $n>1$，d 通过 n 的不含有多于 m 个素因数的因数时，则

$$\sum\mu(d)\begin{cases}\geqslant 0, & \text{当 } m \text{ 为偶数时},\\ \leqslant 0, & \text{当 } m \text{ 为奇数时}.\end{cases} \tag{3}$$

证 设 $n=p_1^{l_1}\cdots p_s^{l_s}$ 是 n 的标准分解式，则在 $m=s$ 时，由定理 1，(3)式成立. 现设 $m<s$. 因为 d 含有平方因子时，$\mu(d)=0$，故只须讨论 d 不含平方因子的情形，而 n 中不含平方因子的，含有 j 个素因数的因数 d 的个数是 $\binom{s}{j}$，而对于这些 d，$\mu(d)=(-1)^j$，故

$$\sum_{\substack{d\mid n\\ d=p_{i_1}\cdots p_{i_j}\\ j\leqslant m,\ 1\leqslant i_1<\cdots<i_j\leqslant s}}\mu(d)=\sum_{j=0}^{m}\binom{s}{j}(-1)^j.$$

但是

$$0=(1-1)^s=\binom{s}{0}-\binom{s}{1}+\cdots+(-1)^m\binom{s}{m}$$

$$+(-1)^{m+1}\binom{s}{m+1}+\cdots+(-1)^s,$$

于是

$$\sum_{j=0}^{m}\binom{s}{j}(-1)^j=(-1)^m\binom{s}{m+1}+(-1)^{m+1}\binom{s}{m+2}+\cdots+(-1)^{s+1}$$

$$=(-1)^m\left(\binom{s}{m-1}-\binom{s}{m+2}+\cdots+(-1)^{s-m+1}\right).$$

设 m 为偶数，当 $m=s-1$ 时，显然有 $\sum_{j=0}^{s-1}\binom{s}{j}(-1)^j=1$；而 $m\leqslant s-2$，且当 $2\leqslant t\leqslant m\leqslant\frac{s}{2}$ 时，则由 $\binom{s}{t}>\binom{s}{t-1}$，得

$$\sum_{j=0}^{m}\binom{s}{j}(-1)^j=\binom{s}{0}+\binom{s}{2}-\binom{s}{1}+\cdots+\binom{s}{m}-\binom{s}{m-1}$$

$$\geqslant 0.$$

当 $s-2\geqslant t\geqslant m>\frac{s}{2}$ 时，则由 $\binom{s}{t+1}>\binom{s}{t+2}$，知

$$\binom{s}{m+1}-\binom{s}{m+2}+\cdots+(-1)^{s-m+1}\geqslant 0.$$

m 为奇数时，类似可证. 证完

下面我们将看到，$\mu(n)$ 在反演公式中起重要作用.

§3 欧拉函数 $\varphi(n)$

对于欧拉函数 $\varphi(n)$ 的定义和公式，在第二章 §3 中已经给出. 本节将进一步给出欧拉函数 $\varphi(n)$ 的一些性质.

定理 1 设 $n\geqslant 1$，则有

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

证 考虑有理数集

$$S=\left\{\frac{r}{n},\ r=1,2,3,\cdots,n\right\},$$

把S中的每一个分数化为既约分数得S^*,S^*中没有两个分数的值是相同的. 对于任一个给定的$r\leqslant n$, $\frac{r}{n}=\frac{h}{k}$是既约分数,则

$$(h,k)=1,\ h\leqslant k,\ k\mid n. \tag{1}$$

反之,对于给定的n,任一个满足(1)中三个条件的分数$\frac{h}{k}$在S^*中,这是因为,由$k\mid n$,可设$n=kg$,$r=hg$,故$\frac{h}{k}=\frac{hg}{kg}=\frac{r}{n}$,$r\leqslant n$. 满足(1)中三个条件的分数$\frac{h}{k}$的全体为$\sum\limits_{d\mid n}\varphi(d)$个,而$S^*$中有$n$个分数,故

$$\sum_{d\mid n}\varphi(d)=n. \qquad \text{证完}$$

利用缩系,在第二章的§3中我们证明了当$(m,n)=1$时,$\varphi(mn)=\varphi(n)\varphi(m)$,这里我们将用不同的方法再予证明. 证明这个结论之前,先证明一个引理.

引理 设$(m,n)=1$,如果t_1跑过m的全部因子,t_2跑过n的全部因子,则$t=t_1t_2$跑过mn的全部因子.

证 因为$t_1\mid m$,$t_2\mid n$,故$t_1t_2\mid mn$,且当$t_1'\mid m$,$t_2'\mid n$,$\{t_1,t_2\}\neq\{t_1',t_2'\}$时,由$(m,n)=1$得$t_1t_2\neq t_1't_2'$. 反之,任给$t\mid mn$,由于$(m,n)=1$,设$(t,m)=t_1$,$(t,n)=t_2$,显然$t=t_1t_2$,$t_1\mid m$,$t_2\mid n$.

证完

定理2 设$(m,n)=1$,则$\varphi(mn)=\varphi(m)\varphi(n)$.

证 设$h=mn$,我们对h施行归纳法. $h=1$时,定理显然成立. 现设$h=1,2,\cdots,nm-1$时,定理2成立. 设$t\mid mn$,$t=t_1t_2$,$t_1\mid m$,$t_2\mid n$,由归纳假设,除开$t_1=m$,$t_2=n$外,均有$\varphi(t_1t_2)=$

$\varphi(t_1)\varphi(t_2)$，因此，由引理，有

$$\sum_{t_1\mid m}\varphi(t_1)\sum_{t_2\mid n}\varphi(t_2)=\Big(\sum_{t\mid mn}\varphi(t)-\varphi(mn)\Big)+\varphi(m)\varphi(n).$$

由定理 1，上式给出 $mn=(mn-\varphi(mn))+\varphi(m)\varphi(n)$，即 $\varphi(mn)=\varphi(m)\varphi(n)$. 证完

定理 3 ① 设 $(m,n)=d$，则有

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

② 若 $a\mid b$，则有 $\varphi(a)\mid\varphi(b)$.

证 ① 由

$$\frac{\varphi(mn)}{mn}=\prod_{p\mid mn}\Big(1-\frac{1}{p}\Big)=\frac{\prod\limits_{p\mid m}\Big(1-\frac{1}{p}\Big)\prod\limits_{p\mid n}\Big(1-\frac{1}{p}\Big)}{\prod\limits_{p\mid(m,n)}\Big(1-\frac{1}{p}\Big)}$$

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

故得 $\varphi(mn)=\varphi(m)\varphi(n)\dfrac{d}{\varphi(d)}$.

② 设 $b=ac$，由①我们有

$$\varphi(b)=\varphi(ac)=\varphi(a)\varphi(c)\frac{d}{\varphi(d)}=d\varphi(a)\frac{\varphi(c)}{\varphi(d)},\qquad(2)$$

其中 $(a,c)=d$.

由于 $d\mid c$，因而 $\dfrac{d\varphi(c)}{\varphi(d)}=\dfrac{c\prod\limits_{p\mid c}\Big(1-\frac{1}{p}\Big)}{\prod\limits_{p\mid d}\Big(1-\frac{1}{p}\Big)}$ 是整数，故(2)式给出 $\varphi(a)\mid\varphi(b)$. 证完

1932 年，莱梅 (Lehmer, D. H.) 提出了一个与 $\varphi(n)$ 有关的猜

想.

猜想:不存在复合数 n 使得 $\varphi(n)|n-1$.

1962 年,我们曾经证明这样的复合数如果存在,至少是 12 个不同的奇素数的乘积. 1980 年,柯恩(Cohen)和哈奇斯利用计算机进一步证明了它至少是 14 个不同的奇素数的乘积.

这些结果的证明,依赖以下定理.

定理 4 设 $k\geqslant 2$,

$$k\varphi(n)=n-1, \tag{3}$$

则有

① $n=p_1\cdots p_s$,其中 $p_1,\cdots,p_s$ 是不同的奇素数.

② 若奇素数 $p|n$,则 n 不含有 $pt+1$ 形的素因子.

③ 若 $k\not\equiv 1(\mathrm{mod}3)$,则 $n\not\equiv 0(\mathrm{mod}3)$.

证 因为 $k\geqslant 2$,故由(3)知 $n>2$,且因 $2|\varphi(n)$,故 $2\nmid n$. 如果素数 $p|n$,n 含有 $pt-1$ 形的素因子或 $p^2|n$,则 $p|\varphi(n)$,由(3)推出 $p|n-1$,这是不可能的,这就证明了①和②.

对于③,当 $k\equiv 0(\mathrm{mod}3)$时,结论显然成立. 当 $k\equiv 2(\mathrm{mod}3)$,如果 $n\equiv 0(\mathrm{mod}3)$,由①,不妨设 $n=p_1\cdots p_s$,$p_1=3$,$p_2,\cdots,p_s$ 是不同的奇素数. 由(3)得

$$2k\prod_{j=2}^{s}(p_j-1)=3\prod_{j=2}^{s}p_j-1, \tag{4}$$

由②知 $p_j\equiv -1(\mathrm{mod}6)$,(4)的两端取模 3,得

$$2\equiv 0(\mathrm{mod}3),$$

此不可能. 证完

看来,完全解决莱梅猜想是非常困难的,就是证明 $2\varphi(n)=n-1$ 无解也不容易.

§4 数论函数的狄利克雷乘积

我们知道

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

其右端的和的形状，在数论中经常出现．我们有

定义 设 $f(n)$，$g(n)$是两个数论函数，它们的**狄利克雷乘积** $h(n)$也是一个数论函数，由下式给出

$$h(n)=\sum_{d\mid n}f(d)g\left(\frac{n}{d}\right),$$

简记为 $h(n)=f(n)*g(n)$.

定理 1 任给数论函数 $f(n),g(n),k(n)$，则有

$$f(n)*g(n)=g(n)*f(n), \tag{1}$$

和

$$(f(n)*g(n))*k(n)=f(n)*(g(n)*k(n)). \tag{2}$$

证 由于

$$f(n)*g(n)=\sum_{d\mid n}f(d)g\left(\frac{n}{d}\right)=\sum_{d\mid n}f\left(\frac{n}{d}\right)g(d)$$

$$=\sum_{d\mid n}g(d)f\left(\frac{n}{d}\right)=g(n)*f(n),$$

故(1)成立.

设 $A(n)=g(n)*k(n)$, $B(n)=f(n)*g(n)$, 则

$$f(n)*A(n)=\sum_{ad=n}f(a)A(d)=\sum_{ad=n}f(a)\sum_{bc=d}g(b)k(c)$$

$$=\sum_{abc=n}f(a)g(b)k(c).$$

$$B(n)*k(n)=\sum_{ad=n}B(d)k(a)=\sum_{ad=n}\sum_{bc=d}f(b)g(c)k(a)$$

$$=\sum_{abc=n}f(b)g(c)k(a).$$

故(2)成立. 证完

设

$$I(n)=\left[\frac{1}{n}\right]=\begin{cases}1, & \text{若 } n=1,\\ 0, & \text{若 } n>1.\end{cases}$$

我们有

定理 2 对于所有的数论函数 $f(n)$,均有

$$f(n)*I(n)=I(n)*f(n)=f(n).$$

证 由于

$$f(n)*I(n)=\sum_{d|n}f(d)I\left(\frac{n}{d}\right)=\sum_{d|n}f(d)\left[\frac{d}{n}\right]=f(n).$$

故定理成立. 证完

定义 对于狄利克雷乘积,$I(n)$起单位元的作用,简称 $I(n)$ **为单位数论函数.**

定理 3 设数论函数 $f(n)$,满足 $f(1)\neq 0$,则存在唯一的数论函数 $f^{-1}(n)$,称为 $f(n)$的**狄利克雷逆函数**,使得

$$f(n)*f^{-1}(n)=f^{-1}(n)*f(n)=I(n).$$

且 $f^{-1}(n)$由下面的递推公式给出

$$f^{-1}(1)=\frac{1}{f(1)},$$

$$f^{-1}(n)=\frac{-1}{f(1)}\sum_{\substack{d|n\\ d<n}}f\left(\frac{n}{d}\right)f^{-1}(d)\quad (n>1).$$

证 我们用归纳法来证明函数值 $f^{-1}(1), f^{-1}(2), \cdots, f^{-1}(n), \cdots$可唯一决定. 对于 $n=1$,由

$$f(1)*f^{-1}(1)=I(1),$$

推出

$$f(1)f^{-1}(1)=1,$$

故 $f^{-1}(1)=\frac{1}{f(1)}$唯一决定. 现在假设对于所有的 $k<n(n\geqslant 2)$, 函数值 $f^{-1}(k)$已经唯一决定, 由

$$\sum_{d|n}f\left(\frac{n}{d}\right)f^{-1}(d)=0,\quad n>1,$$

可得

$$f(1)f^{-1}(n)+\sum_{\substack{d|n\\ d<n}}f\left(\frac{n}{d}\right)f^{-1}(d)=0.$$

因为由归纳法假设, $f^{-1}(d)$对于所有小于 n 的因子 d 已经唯一决定, 故可唯一决定

$$f^{-1}(n)=\frac{-1}{f(1)}\sum_{\substack{d|n\\ d<n}}f\left(\frac{n}{d}\right)f^{-1}(d).$$

这个归纳定义的唯一确定的函数 $f^{-1}(n)$就是 $f(n)$的狄利克雷逆.

证完

由于 $f(1)*g(1)=f(1)g(1)$, 故当 $f(1)\neq 0, g(1)\neq 0$ 时, $f(1)*g(1)\neq 0$, 这样, 由以上三个定理可知: 对于狄利克雷乘积*, 全体 $f(1)\neq 0$ 的数论函数 $f(n)$组成一个阿贝尔(Abel)群, 记为 D.

§5 麦比乌斯反演公式

我们知道

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

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

一般地，我们有

定义 若数论函数 $f(n)$ 和 $g(n)$ 适合

$$f(n)=\sum_{d\mid n}g(d)=\sum_{d\mid n}g\left(\frac{n}{d}\right),$$

称 $f(n)$ 为 $g(n)$ 的**麦比乌斯变换**，而 $g(n)$ 为 $f(n)$ 的**麦比乌斯逆变换**.

由定义知，n 是 $\varphi(n)$ 的麦比乌斯变换，$\varphi(n)$ 是 n 的麦比乌斯逆变换.

定理 若任意两个数论函数 $f(n)$ 和 $g(n)$ 满足等式

$$f(n)=\sum_{d\mid n}g(d), \tag{1}$$

则有

$$g(n)=\sum_{d\mid n}\mu(d)f\left(\frac{n}{d}\right), \tag{2}$$

反过来，若满足(2)，则(1)也成立.

证 若 $f(n)$ 和 $g(n)$ 满足(1)，则

$$\sum_{d\mid n}\mu(d)f\left(\frac{n}{d}\right)=\sum_{d\mid n}\mu(d)\sum_{d'\mid\frac{n}{d}}g(d')=\sum_{dd'\mid n}\mu(d)g(d')$$

$$=\sum_{d'\mid n}\sum_{d\mid\frac{n}{d'}}\mu(d)g(d')=\sum_{d'\mid n}g(d')\sum_{d\mid\frac{n}{d'}}\mu(d)=g(n),$$

上面最后一个等式用到 §2 定理 1，故(2)成立.

反过来，设 $f(n)$ 和 $g(n)$ 满足(2)，则同法可证

$$\sum_{d\mid n}g(d)=\sum_{d\mid n}g\left(\frac{n}{d}\right)=\sum_{d\mid n}\sum_{d'\mid\frac{n}{d}}\mu\left(\frac{n}{dd'}\right)f(d')$$

$$=\sum_{dd'\mid n}\mu\left(\frac{n}{dd'}\right)f(d')=\sum_{d'\mid n}f(d')\sum_{d\mid\frac{n}{d'}}\mu\left(\frac{n}{dd'}\right)=f(n).$$

证完

实际上，用上一节有关狄利克雷乘积的结果，证明是明显的.

定理的另一个证明：

设对任意的正整数 n，数论函数 $e(n)=1$.

等式(1)可表为 $f(n)=g(n)*e(n)$，则有 $f(n)*\mu(n)=(g(n)*e(n))*\mu(n)=g(n)*(e(n)*\mu(n))=g(n)*I(n)=g(n)$，即(2)成立. 反过来，若(2)成立，(2)可写成 $f(n)*\mu(n)=g(n)$，则有 $g(n)*e(n)=(f(n)*\mu(n))*e(n)=f(n)*(\mu(n)*e(n))=f(n)*I(n)=f(n)$，即(1)成立. 证完

下面举几个例子.

例 1 由 §2 的定理 1 知 $I(n)$ 是 $\mu(n)$ 的麦比乌斯变换.

例 2 冯·曼哥特(Von Mangoldt)函数 $\Lambda(n)$ 是指：

$$\Lambda(n)=\begin{cases}\log p, \text{若 } n=p^m, m\geqslant 1, p \text{ 是素数;}\\ 0, n \text{ 是其他情形.}\end{cases}$$

设 $n=p_1^{l_1}\cdots p_k^{l_k}$ 是 n 的标准分解式，则有

$$\sum_{d\mid n}\Lambda(d)=\sum_{s_1=0}^{l_1}\cdots\sum_{s_k=0}^{l_k}\Lambda(p_1^{s_1}\cdots p_k^{s_k})$$

$$=\sum_{s_1=1}^{l_1}\Lambda(p_1^{s_1})+\cdots+\sum_{s_k=1}^{l_k}\Lambda(p_k^{s_k})$$

$$=\sum_{s_1=1}^{l_1}\log p_1+\cdots+\sum_{s_k=1}^{l_k}\log p_k$$

$$=l_1\log p_1+\cdots+l_k\log p_k=\log n.$$

故 $\log n$ 是 $\Lambda(n)$ 的麦比乌斯变换.

例 3 因为 $\Lambda(n)$ 是 $\log n$ 的麦比乌斯逆变换，故

$$\Lambda(n)=\sum_{d\mid n}\mu(d)\log\frac{n}{d}$$

$$=\log n\sum_{d\mid n}\mu(d)-\sum_{d\mid n}\mu(d)\log d-I(n)\log n$$

$$-\sum_{d\mid n}\mu(d)\log d=\sum_{d\mid n}-\mu(d)\log d.$$

故 $\Lambda(n)$ 是 $-\mu(n)\log n$ 的麦比乌斯变换.

§6 积性函数

实际上,积性函数的概念,我们在上一章已经遇见过了. 在第二章 §3 中,我们证明了 $(m,n)=1,\varphi(mn)=\varphi(m)\varphi(n)$,这就是一个积性函数. 一般地,我们有

定义 如果数论函数 $f(n)$ 不恒等于 0, 且当 $(m,n)=1$ 时, $f(mn)=f(m)f(n)$, 则 $f(n)$ 叫做**积性函数**. 如果一个积性函数,对所有的 m,n 均有 $f(mn)=f(m)f(n)$,则称**完全积性函数**.

例 1 $\varphi(n)$ 是积性函数,但不是完全积性函数.

例 2 $f_\alpha(n)=n^\alpha$,这里 α 为任一实数,是一个完全积性函数.

例 3 $I(n)=\left[\frac{1}{n}\right]$ 是一个完全积性函数.

例 4 麦比乌斯函数 $\mu(n)$ 是一个积性函数,但不是完全积性函数.

例 5 设

$$\sigma_\alpha(n)=\sum_{d\mid n}f_\alpha(d),$$

则 $\sigma_\alpha(n)$ 是一个积性函数 (用下面的定理 2 很容易证明), 但不是完全积性函数.

下面,我们将证明积性函数的几个基本的性质.

定理 1 如果 $f(n)$ 是一个积性函数,则 $f(1)=1$.

证 因为, 对所有的正整数 n, 有 $(n,1)=1$, 故 $f(n)=f(n)\cdot$

$f(1)$，又因为 $f(n)$不恒为 0，故

$$f(1)=1.$$ 证完

定理 2 如果 $f(n)$ 和 $g(n)$ 是积性的，那么 $f(n)*g(n)$ 也是积性的.

证 设 $h(n)=f(n)*g(n)$，$(m,n)=1$，则

$$h(mn)=\sum_{t\mid mn}f(t)g\left(\frac{mn}{t}\right).$$

令 $t=t_1t_2$，$t_1\mid m$，$t_2\mid n$. 根据本章 §3 中证明过的引理：设 $(m,n)=1$，如果 t_1 跑过 m 的全部因子，t_2 跑过 n 的全部因子，则 $t=t_1t_2$ 跑过 mn 的全部因子，因此，

$$\begin{aligned}h(mn)&=\sum_{t\mid mn}f(t)g\left(\frac{mn}{t}\right)=\sum_{t_1\mid m}\sum_{t_2\mid n}f(t_1t_2)g\left(\frac{m}{t_1}\frac{n}{t_2}\right)\\&=\sum_{t_1\mid m}\sum_{t_2\mid n}f(t_1)f(t_2)g\left(\frac{m}{t_1}\right)g\left(\frac{n}{t_2}\right)\\&=\sum_{t_1\mid m}f(t_1)g\left(\frac{m}{t_1}\right)\cdot\sum_{t_2\mid n}f(t_2)g\left(\frac{n}{t_2}\right)\\&=h(m)h(n).\end{aligned}$$ 证完

取 $f(n)=f_\alpha(n)$，$g(n)=e(n)$，由定理 2 知

$$f_\alpha(n)*e(n)=\sum_{d\mid n}f_\alpha(d)=\sigma_\alpha(n)$$

是积性函数. 这里 $\sigma_0(n)=\sum_{d\mid n}1=d(n)$，$d(n)$ 表示 n 的因数的个数. $\sigma_1(n)$ 即通常的 n 的全部因子的和 $\sigma(n)$. 于是，设 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 n 的标准分解式，就有

$$\sigma_\alpha(n)=\sigma_\alpha(p_1^{\alpha_1})\cdots\sigma_\alpha(p_k^{\alpha_k}),$$

而 $$\sigma_\alpha(p_j^{\alpha_j})=1+p_j^{\alpha}+p_j^{2\alpha}+\cdots+p_j^{\alpha_j\alpha}$$

$$=\begin{cases}\dfrac{p_j^{\alpha(\alpha_j+1)}-1}{p_j^{\alpha}-1}, & \alpha\neq 0,\\ \alpha_j+1, & \alpha=0,\end{cases}$$

故

$$\sigma_\alpha(n)=\begin{cases}\displaystyle\prod_{j=1}^{k}\frac{p_j^{\alpha(\alpha_j+1)}-1}{p_j^{\alpha}-1}, & \alpha\neq 0,\\ \displaystyle\prod_{j=1}^{k}(\alpha_j+1). & \alpha=0.\end{cases}$$

定理 3 如果 $g(n)$ 和 $h(n)=f(n)*g(n)$ 都是积性函数，则 $f(n)$ 也是积性函数.

证 如果 $f(n)$ 不是积性函数，则存在一对正整数 m, n, $(m,n)=1$，使得

$$f(mn)\neq f(m)f(n),$$

于是我们可以选择这样一对 m, n，使得 mn 最小.

如果 $mn=1$，则 $f(1)\neq f(1)f(1)$，故 $f(1)\neq 1$. 因为 $h(1)=f(1)g(1)=f(1)\neq 1$，这将得出 $h(n)$ 不是积性函数，与所设矛盾.

如果 $mn>1$，则对所有正整数对 a, b, $(a,b)-1$，$ab<mn$，有 $f(ab)=f(a)f(b)$. 于是有

$$h(mn)=\sum_{a\mid m}\sum_{b\mid n}f(ab)g\left(\frac{mn}{ab}\right)$$

$$=\sum_{\substack{a\mid m,\,b\mid n\\ ab<mn}}f(ab)g\left(\frac{m}{a}\,\frac{n}{b}\right)+f(mn)g(1)$$

$$=\sum_{\substack{a\mid m,\,b\mid n\\ ab<mn}}f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)+f(mn)$$

$$=\sum_{a\mid m}f(a)g\left(\frac{m}{a}\right)\cdot\sum_{b\mid n}f(b)g\left(\frac{n}{b}\right)$$

$$-f(m)f(n)+f(mn)$$
$$=h(m)h(n)-f(m)f(n)+f(mn).$$

因为 $f(mn)\neq f(m)f(n)$，故 $h(mn)\neq h(m)h(n)$，此与 $h(n)$ 是积性函数矛盾. 证完

定理 4 如 $g(n)$是一个积性函数，则 $g(n)$的狄利克雷逆函数也是一个积性函数.

证 因为 $g(n)$和 $g(n)*g^{-1}(n)=I(n)$ 都是积性函数，故由定理 3 知，$g^{-1}(n)$也是积性函数. 证完

定理 2 和定理 4 指出全体积性函数组成阿贝尔群 D 的一个子群. (阿贝尔群 D 的定义见本章 § 4)

完全积性函数的狄利克雷逆是容易决定的. 我们有

定理 5 设 $f(n)$是一个积性函数，则 $f(n)$ 是一个完全积性函数的充分必要条件是

$$f^{-1}(n)=\mu(n)f(n),$$

证 设 $g(n)=\mu(n)f(n)$，如果 $f(n)$是一个完全积性函数，则有

$$g(n)*f(n)=\sum_{d|n}\mu(d)f(d)f\left(\frac{n}{d}\right)=f(n)\sum_{d|n}\mu(d)$$
$$=f(n)I(n)=I(n),$$

故 $f^{-1}(n)=g(n)$.

反之，假设 $f^{-1}(n)=\mu(u)f(n)$，为了证明 $f(n)$是完全积性函数，只需证明对于素数的方幂 p^α，有 $f(p^\alpha)=f(p)^\alpha$. 对于 $n>1$，我们有

$$\sum_{d|n}\mu(d)f(d)f\left(\frac{n}{d}\right)=0,$$

因此，取 $n=p^\alpha,\alpha>0$，我们有

$$\mu(1)f(1)f(p^\alpha)+\mu(p)f(p)f(p^{\alpha-1})=0$$

即

$$f(p^{\alpha})=f(p)f(p^{\alpha-1}).$$

由此可推出 $f(p^{\alpha})=f^{\alpha}(p)$，故 $f(n)$ 是完全积性函数. 证完

§7 数论函数 $\pi(n)$

我们用数论函数 $\pi(n)$ 表示不大于 n 的素数的个数. 在第一章中，已经证明了素数的个数是无穷的，即 $\pi(n)\to\infty$. 本节将用初等方法，进一步证明以下定理.

定理 1 设 $n\geqslant 2$，则有

$$\frac{1}{8}\frac{n}{\log n}\leqslant\pi(n)\leqslant 12\frac{n}{\log n}. \tag{1}$$

证 对于每一个素数 p，$p\leqslant 2n$，存在唯一的整数 r_p，使得 $p^{r_p}\leqslant 2n<p^{r_p+1}$. 我们首先证明

$$\prod_{n<p\leqslant 2n}p\mid\frac{(2n)!}{n!\,n!} \tag{2}$$

和

$$\frac{(2n)!}{n!\,n!}\mid\prod_{p\leqslant 2n}p^{r_p}. \tag{3}$$

因为当素数 p 满足 $n<p\leqslant 2n$ 时，$p\mid(2n)!$，但 $p\nmid n!$，故(2)式成立. 由本章 §1 定理 1 知

$$\mathrm{pot}_p(2n)!=\sum_{i=1}^{r_p}\left[\frac{2n}{p^i}\right],\qquad \mathrm{pot}_p n!=\sum_{i=1}^{r_p}\left[\frac{n}{p^i}\right].$$

又因为 $[x]-2\left[\frac{x}{2}\right]=0$ 或 1，故

$$\mathrm{pot}_p\binom{2n}{n}=\sum_{m=1}^{r_p}\left\{\left[\frac{2n}{p^m}\right]-2\left[\frac{n}{p^m}\right]\right\}\leqslant\sum_{m=1}^{r_p}1=r_p.$$

这就证明了(3). 由(2)和(3)，我们得到

$$n^{\pi(2n)-\pi(n)}<\prod_{n<p\leqslant 2n}p\leqslant\binom{2n}{n}\leqslant\prod_{p\leqslant 2n}p^{r_i}\leqslant(2n)^{\pi(2n)},\ n\geqslant 1.\quad(4)$$

又因

$$\binom{2n}{n}=\frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1}=\prod_{i=1}^{n}\frac{n+i}{i}\geqslant\prod_{i=1}^{n}2=2^n$$

和

$$\binom{2n}{n}\leqslant(1+1)^{2n}=2^{2n},$$

故由(4)得

$$n^{\pi(2n)-\pi(n)}<2^{2n},\ 2^n\leqslant(2n)^{\pi(2n)},\ n\geqslant 1.\quad(5)$$

令 $n=2^h, h=0,1,2,\cdots$, 可得

$$2^{h(\pi(2^{h+1})-\pi(2^h))}<2^{2^{h+1}},\quad 2^{2^h}\leqslant 2^{(h+1)\pi(2^{h+1})},\ h\geqslant 0,$$

即得

$$h(\pi(2^{h+1})-\pi(2^h))<2^{h+1},\ 2^h\leqslant(h+1)\pi(2^{h+1}).\quad(6)$$

显然, $h\geqslant 0$ 时, 有 $\pi(2^{h+1})\leqslant 2^h$, 故由(6)得

$$(h+1)\pi(2^{h+1})-h\pi(2^h)<2^{h+1}+\pi(2^{h+1})\leqslant 3\cdot 2^h,\ h\geqslant 0,$$

令上式中 h 过 $0,1,\cdots,k$, 而将所得诸式相加, 得

$$(k+1)\pi(2^{k+1})<3(1+2+\cdots+2^k)<3\cdot 2^{k+1},\ k\geqslant 0,\quad(7)$$

由(6)和(7)可知

$$\frac{1}{2}\frac{2^{k+1}}{k+1}\leqslant\pi(2^{k+1})<3\cdot\frac{2^{k+1}}{k+1},\ k\geqslant 0,\quad(8)$$

设 $n\geqslant 2$, 取 k 使

$$2^{k+1}\leqslant n<2^{k+2},\quad k\geqslant 0.\quad(9)$$

因为当 $l>0$ 时,

$$\sum_{t=2}^{2^l}\frac{1}{t}=\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\cdots+$$

$$+\left(\frac{1}{2^{l-1}+1}+\cdots+\frac{1}{2^l}\right)$$

$$\geqslant\frac{1}{2}+\left(\frac{1}{4}+\frac{1}{4}\right)+\left(\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}\right)+\cdots$$

$$+\left(\frac{1}{2^l}+\cdots+\frac{1}{2^l}\right)$$

$$=\frac{l}{2},$$

以及

$$\sum_{t=2}^{2^l}\frac{1}{t}=\left(\frac{1}{2}+\frac{1}{3}\right)+\left(\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}\right)+\cdots+\frac{1}{2^l}$$

$$\leqslant\left(\frac{1}{2}+\frac{1}{2}\right)+\cdots+\left(\frac{1}{2^{l-1}}+\cdots\right.$$

$$\left.+\frac{1}{2^{l-1}}\right)+\frac{1}{2^l}\leqslant l,$$

故由(8)和(9)得

$$\pi(n)\leqslant\pi(2^{k-2})<3\cdot\frac{2^{k+2}}{k+2}\leqslant 6\frac{2^{k+1}}{\sum_{t=2}^{2^{k+2}}\frac{1}{t}}\leqslant 6\frac{n}{\sum_{t=2}^{2^{k+2}}\frac{1}{t}}$$

$$\leqslant\frac{6n}{\sum_{t=2}^{n}\frac{1}{t}} \tag{10}$$

和

$$\pi(n)\geqslant\pi(2^{k+1})\geqslant\frac{1}{2}\frac{2^{k+1}}{k+1}$$

$$=\frac{1}{8}\frac{2^{k+2}}{\frac{k+1}{2}}\geqslant\frac{1}{8}\frac{2^{k+2}}{\sum_{t=2}^{2^{k+1}}\frac{1}{t}}\geqslant\frac{1}{8}\frac{n}{\sum_{t=2}^{n}\frac{1}{t}}. \tag{11}$$

又当 $n\geqslant 2$ 时,

$$\log\frac{n}{2}=\int_2^n\frac{dt}{t}<\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}<\int_1^n\frac{dt}{t}=\log n,$$

$n\geqslant 4$ 时，

$$\log\frac{n}{2}\geqslant\frac{1}{2}\log n.$$

我们另有 $\frac{1}{2}\log 3\leqslant\frac{1}{2}+\frac{1}{3}$，$\frac{1}{2}\log 2\leqslant\frac{1}{2}$，故由(10)和(11)得

$$\frac{1}{8}\frac{n}{\log n}\leqslant\pi(n)\leqslant\frac{12n}{\log n}.$$ 证完

下面，我们将给出 $\pi(n)$ 一个更好的下界，所用方法也更简短一些.

定理 2 对于 $n\geqslant 4$，

$$\pi(n)\geqslant\log 2\frac{n}{\log n}.$$

证 对于 $1\leqslant m\leqslant n$，考虑积分

$$I(m,n)=\int_0^1 x^{m-1}(1-x)^{n-m}dx=\sum_{r=0}^{n-m}(-1)^r\binom{n-m}{r}\frac{1}{m+r}.$$

(12)

设 $d_n=[1,2,\cdots,n]$，显然，$d_nI(m,n)$ 是一个整数. 另一方面，容易计算，$I(m,n)=\dfrac{1}{m\binom{n}{m}}$，故对每一个 m，$1\leqslant m\leqslant n$，均有 $m\binom{n}{m}\mid d_n$，特别地，因为 $n\binom{2n}{n}\mid d_{2n}$，$(2n+1)\binom{2n}{n}=(n+1)\binom{2n+1}{n+1}$，$d_{2n}\mid d_{2n+1}$，故 $n\binom{2n}{n}$ 和 $(2n+1)\binom{2n}{n}$ 均整除 d_{2n+1}. 又因 $(n,2n+1)=1$，故

$$n(2n+1)\binom{2n}{n}\mid d_{2n+1}.$$ (13)

又因

$$(1+1)^{2n}\leqslant(2n+1)\binom{2n}{n}, \tag{14}$$

于是,(13)和(14)给出

$$e_{2n+1}\geqslant n(2n+1)\binom{2n}{n}\geqslant n\cdot 4^n.$$

故当 $n\geqslant 4$ 时,

$$d_{2n+2}\geqslant d_{2n+1}\geqslant n\cdot 4^n\geqslant 4^{n+1}=2^{2n+2},$$

也即 $N\geqslant 9$ 时,

$$d_N\geqslant 2^N. \tag{15}$$

设 $p^a\| d_N$,则必有某个 m, $1\leqslant m\leqslant N$,使得 $p^a\mid m$,故 $p^a\leqslant N$,因此

$$d_N=\prod_{p^a\leqslant N}p^a\leqslant\prod_{p\leqslant N}p^{\frac{\log N}{\log p}}. \tag{16}$$

由(15)和(16)得

$$N\log 2\leqslant\log d_N\leqslant\sum_{p\leqslant N}\log N=\log N\cdot\pi(N),$$

故得 $N\geqslant 9$ 时,

$$\pi(N)\geqslant\log 2\cdot\frac{N}{\log N}.$$

对于 $4\leqslant N\leqslant 8$ 时,以上不等式可直接证明. 证完

定理 1 就是著名的切比雪夫 (Чебышев)定理. 尽管(1)中的系数还可以改进,但无法由此得到素数定理: $\lim\limits_{x\to\infty}\dfrac{\pi(x)}{\dfrac{x}{\log x}}=1$. 关于素数定理本书不准备证明了.

§8 卢卡斯序列

十九世纪,卢卡斯(Lucas)研究了整数序列

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta},\qquad n=0,1,\cdots \tag{1}$$

和

$$v_n=\alpha^n+\beta^n,\quad n=0,1,\cdots, \tag{2}$$

其中 α,β 为以下整系数二次方程的两个根:

$$x^2-Px+Q=0,\quad (P,Q)=1. \tag{3}$$

我们把(1)和(2)都叫做**卢卡斯序列**. 这类序列在大整数的分解,不定方程等方面都有用.

显然有

定理 1 序列(1)和(2)分别为以下整数序列

$$u_{n+2}=Pu_{n+1}-Qu_n, u_0=0,\quad u_1=1, \tag{4}$$

和

$$v_{n+2}=Pv_{n+1}-Qv_n,\quad v_0=2,\quad v_1=P. \tag{5}$$

证 只需把(1),(2)分别代入(4)和(5)的右端,并利用(3)便知. 证完

(4)和(5)这样的序列,叫做**循环序列**.

定理 2 序列 u_n 和 v_n 满足以下诸关系式

$$u_{2n}=u_nv_n, \tag{6}$$

$$v_n^2-(\alpha-\beta)^2u_n^2=4Q^n, \tag{7}$$

$$2u_{m+n}=u_mv_n+u_nv_m, \tag{8}$$

$$2v_{m-n}=Du_mu_n+v_mv_n,\quad D=P^2-4Q, \tag{9}$$

$$u_n^2-u_{n-1}u_{n+1}=Q^{n-1}. \tag{10}$$

证 (6)是明显的. 因为

$$(v_n-(\alpha-\beta)u_n)(v_n+(\alpha-\beta)u_n)=(\alpha^n+\beta^n-(\alpha^n-\beta^n))$$
$$(\alpha^n+\beta^n+\alpha^n-\beta^n)=4(\alpha\beta)^n=4Q^n,$$

这就证明了(7).

将(1)和(2)代入(8)的右端便知(8)成立.

由于 $P^2-4Q=(\alpha-\beta)^2$，再用证(8)的方法可证得(9)。

由

$$u_n^2-u_{n-1}u_{n+1}=\left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)^2-\frac{(\alpha^{n-1}-\beta^{n-1})(\alpha^{n+1}-\beta^{n+1})}{(\alpha-\beta)^2}$$

$$=\frac{1}{(\alpha-\beta)^2}(\alpha^{2n}+\beta^{2n}-2(\alpha\beta)^n-(\alpha^{2n}-\alpha^2(\alpha\beta)^{n-1}$$

$$-\beta^2(\alpha\beta)^{n-1}+\beta^{2n}))$$

$$=\frac{(\alpha\beta)^{n-1}(\alpha^2+\beta^2-2\alpha\beta)}{(\alpha-\beta)^2}=Q^{n-1},$$

可知(10)成立。 证完

定理 3 设 p 是一个素数，$p\nmid 2Q$，设 u_l 是序列 u_1，u_2，…中被 p 整除的脚标最小的数，则 $p\mid u_n$ 的充分必要条件是 $l\mid n$。

证 设 $l\mid n$，则有 $n=lm$，$m\geqslant 1$，

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}=\frac{\alpha^{lm}-\beta^{lm}}{\alpha-\beta}=\frac{\alpha^l-\beta^l}{\alpha-\beta}f(\alpha,\beta),$$

因为 α^l，β^l 是二次方程 $x^2-v_lx+Q^l=0$ 的两个根，因此，类似(4)，可证

$$f(\alpha,\beta)=\frac{(\alpha^l)^m-(\beta^l)^m}{\alpha^l-\beta^l}$$

是一个整数，故 $u_l\mid u_n$。由 $p\mid u_l$，即得 $p\mid u_n$。

反之，设 $p\mid u_n$，$n=ql+r$，$0\leqslant r<l$，由(8)式得

$$2u_{ql+r}=u_{ql}v_r+u_rv_{ql}.$$

因为 $p\mid u_{ql+r}$，$p\mid u_{ql}$，故 $p\mid u_rv_{ql}$。由 $p\nmid 2Q$ 和(7)知 $p\nmid v_{ql}$，故 $p\mid u_r$。因为 $0\leqslant r<l$，故 $r=0$，即知

$$l\mid n.$$ 证完

如果设 $P=1$，$Q=-1$，(1) 就给出了著名的斐波那契 (Fibonacci)数列

$$F_{n+2}=F_{n+1}+F_n,\quad n\geqslant 0,\ F_0=F_1=1.$$

下一章，当我们引入了二次剩余的概念后，我们将介绍卢卡斯序列在整数分解上的应用.

*§9 陷门单向函数与公开密钥码

传统的保密系统，收发双方有相同的加密密钥和相同的解密密钥，而且加密密钥和解密密钥也是相同的，其密钥需要严格保密不能丢失. 这样，整个系统的密钥数量往往很大，难以分配和管理. 另一方面，收方可以修改内容，发方也可以否认所发的内容，双方可能因此发生争执. 公开密钥码最重要之处有两点：一是将加密密钥和解密密钥分开，加密密钥可以公开，而解密密钥则是严格保密的；二是，这一体制可以发送签了名的消息. 因此，公开密钥体制的提出，解除了上述传统的保密系统所产生的困难，这是密码学中的重大突破.

公开密钥码体制是基于 1976 年，迪费 (Diffie) 和海尔曼 (Hellman) 提出的陷门单向函数，这样的函数满足以下三个条件 (一般可设为某一区间上的数论函数).

定义 把数论函数 $f(n)$ 叫做**陷门单向函数**，如果它满足：

① 对 $f(n)$ 的定义域中的每一个 n，均存在函数 $f^{-1}(l)$，使 $f^{-1}(f(n))=f(f^{-1}(n))=n$.

② $f(n)$ 与 $f^{-1}(l)$ 都容易计算.

③ 仅根据已知的计算 $f(n)$ 的算法，去找出计算 $f^{-1}(l)$ 的容易算法是非常困难的.

利用陷门单向函数，就可以构成如下的公开密钥码体制. 有一个部门，下设 $A,B,C,\cdots$ 若干机构，各机构均有自己的陷门单向函数，分别设为 $f_A(n)$，$f_B(n)$，$f_C(n)$，$\cdots$，各函数的算法分别作为各部门的编码 (加密) 方法而予公开，而诸 $f_A^{-1}(l)$，$f_B^{-1}(l)$，$f_C^{-1}(l)$，$\cdots$ 的容易算法，作为解密密钥则是保密的. 这样，部门中

的任一机构(包括部门外的机构)，都可给其中的一个机构发保密信. 例如，B 向 A 发保密信，方法是，设 B 向 A 所发的明文为 n，代入 A 所公开的陷门单向函数 $f_A(n)$，得 $f_A(n)=m$，m 即为密文，由于只有 A 知道 $f_A^{-1}(m)$ 的容易算法，因此，A 可由 $f_A^{-1}(m)=f_A^{-1}(f_A(n))=n$ 脱密.

另外，部门内的各成员可以彼此发签名信. 例如，B 给 A 发签名信，方法是，设明文为 n，先用 $f_B^{-1}(l)$ 对 n 加密得 $f_B^{-1}(n)=m$，再用 $f_A(n)$ 对 m 加密得 $f_A(m)=t$. A 收到 t 后，由 $f_A^{-1}(t)=m$ 得 $f_B(m)=f_B(f_B^{-1}(n))=n$，即可读到 B 发出的原信了. 因为只有 B 才能发这样的双重加密信，所以，B 的签名是无法伪造的.

1977 年，里凡斯特(Rivest)等，首先找到一类便于应用的陷门单向函数，通常称 RSA 体制. 我们有以下定理.

定理 设 $m=pq$，适当选择两个给定的奇素数 p、q，以及正整数 s 满足 $(s,p-1)=(s,q-1)=1$，则可使

$$f(n)=\langle n^s\rangle_m \tag{1}$$

是区间 $[1,m-1]$ 上的一个陷门单向函数.

证 由于 $(s,(p-1)(q-1))=1$，故存在整数 h 满足

$$sh\equiv 1(\mathrm{mod}\varphi(m)),\ 0<h<\varphi(m). \tag{2}$$

设 $f(n)=\langle n^s\rangle_m=l$，$n\in[1,m-1]$，定义

$$F(l)=\langle l^h\rangle_m. \tag{3}$$

我们来证明 $F(l)=f^{-1}(l)$. 设 $n\in[1,m-1]$，由(1)和(2)，有

$$F(f(n))=\langle f(n)^h\rangle_m\equiv f(n)^h\equiv n^{sh}(\mathrm{mod}m), \tag{4}$$

如果 $(n,\ m)=1$，利用第二章 §3 定理 4，再由(2)，(4)式给出 $F(f(n))\equiv n(\mathrm{mod}m)$，即得

$$F(f(n))=n.$$

如果 $(n,m)>1$，则 $p\mid n$ 或 $q\mid n$，由(4)分别取模 p 或模 q，仍然给出 $F(f(n))=n$. 同样的方法，可以证明 $f(F(n))=n$. 这就证明了

$f^{-1}(l)=F(l)$.

(1)式和(2)式均为整数的乘幂然后求模 m 的最小非负剩余，这一运算在计算机上是容易计算的. 然而，适当选择大素数 p,q，要想通过 m 和 s 来求出 p 和 q（或 t），这是非常困难的. 因为 m 适当大，求出其标准分解式，要花费惊人的时间，几乎是不可能的. 因此，适当选择两个给定的奇素数 p,q，可使(1)给出区间$[1,m-1]$上的一个陷门单向函数. 证完

公开密钥体制的提出，是数论在密码学中的重要应用，同时，也促进了数论学科本身的发展. 例如，采用 RSA 体制，首先需要寻求一些大素数，目前，关于判定大数是否素数方面，有许多重要的工作. 其次，需要寻找分解整数 m 的有效方法，这方面，目前还没有找到有效的方法. 因此，采用 RSA体制的公开密钥码还很难破. 里凡斯特等人给出的一个具体例子是定理中的 p 是一个 64 位的素数，q 是一个 65 位的素数，$m=pq$ 是一个 130 位的数，$s=9007$. 编码方法是把需要加密的拼音文字首先译成一个数 n(例如，26 个英文字母，可设 $A=01, B=02,\cdots, Z=26$，并用 00 表示词与词的间隔)，如果 $n\geqslant m$，可将 n 分段处理，使每段的数值小于 m. 不失一般，可设 $0<n<m$，用电子计算机，计算$\langle n^{9007}\rangle_m$只需几秒时间，但是分解这个 130 位的数却需要花费多得惊人的时间，可以说是无法实现的. 这就是一个具体的陷门单向函数给出的一个公开密钥码.

第三章　习　题

1. 证明：若 n 为正整数，α 为实数，则

① $\left[\frac{[n\alpha]}{n}\right]=[\alpha]$.

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

2. 证明不等式

$$[2\alpha]+[2\beta]\geqslant[\alpha]+[\alpha+\beta]+[\beta].$$

3. 证明：若 $a>0, b>0, n>0$，满足 $n\mid a^n-b^n$，则

$$n\left|\frac{a^n-b^n}{a-b}\right..$$

*4. 证明：若 $n>0, m>1$，则

$$n_!\left|\prod_{i=1}^{n-1}(m^n-m^i)\right..$$

5. 证明：若 $n\geqslant 5, 2\leqslant b\leqslant n$，则

$$b-1\left|\left[\frac{(n-1)_!}{b}\right]\right..$$

6. 证明：对于任意正整数 n，

$$\frac{(2n)_!}{n_!(n+1)_!}$$

是一个整数.

7. 证明：设 $n=\sum_{j=1}^{k}n_j$，则

① $\dfrac{n_!}{n_1!n_2!\cdots n_k!}$是一个整数.

② 如 n 是一个素数，而 $\max(n_1,\cdots,n_k)<n$，则

$$n\left|\frac{n_!}{n_1!\cdots n_k!}\right..$$

8. 证明：如果在自然数列

$$1\leqslant a_1<a_2<\cdots<a_k\leqslant n$$

中，任意两个数 a_i, a_j 的最小公倍数 $[a_i, a_j]>n$，则 $k\leqslant\left[\dfrac{n+1}{2}\right]$.

9. 证明：若 $k>0$，则

$$\sum_{\varphi(d)=k}\mu(d)=0.$$

10. 证明

$$\sum_{d^2\mid n}\mu(d)=\mu^2(n).$$

11. 证明对于任一个素数 p，

$$\sum_{d\mid n}\mu(d)\mu((p,d))=\begin{cases}1,\text{若 } n=1,\\2,\text{若 } n=p^{\alpha},\alpha\geqslant 1,\\0,\text{若 } n \text{ 是其余情形.}\end{cases}$$

12. 证明

$$\frac{n}{\varphi(n)}=\sum_{d\mid n}\frac{\mu^2(d)}{\varphi(d)}.$$

13. 证明：$\sum_{d\mid n}\mu(d)\varphi(d)=0$ 的充分必要条件是 $n\equiv 0\pmod 2$.

14. 证明

$$\sum_{d=1}^{n}\varphi(d)\left[\frac{n}{d}\right]=\frac{n(n+1)}{2}(n>0).$$

15. 计算

$$S(n)=\sum_{d\mid n}\mu(d)\,\mu\left(\frac{n}{d}\right).$$

16. 证明：n 是素数的充分必要条件是 $\sigma(n)+\varphi(n)=nd(n)$.

17. 证明：如果有正整数 n 满足

$$\varphi(n+3)=\varphi(n)+2,$$

则 $n=2p^{\alpha}$ 或 $n+3=2p^{\alpha}$，其中 $\alpha\geqslant 1$，$p\equiv 3\pmod 4$，p 是素数.

*18. 求出满足

$$d(n)=\varphi(n)$$

的全部正整数 n.

19. 证明

$$\varphi(n)\geqslant\frac{n}{d(n)}.$$

20. 求出满足

$$\varphi(mn)=\varphi(m)+\varphi(n)$$

的全部正整数对 (m,n).

21. 证明：若 $n>0$，满足 $24\mid n+1$，则

$$24\mid\sigma(n).$$

22. 证明：若 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，$k\leqslant 8$，则

$$\varphi(n)>\frac{n}{6}.$$

23. 设 $\omega(1)=0, n>1, \omega(n)$ 是 n 的不同的素因子的个数，证明：

$$f(n)=\omega(n)*\mu(n)=0 \text{ 或 } 1.$$

24. 设 $f(x)$ 的定义域是 $[0,1]$ 中的有理数，

$$F(n)=\sum_{k=1}^{n} f\left(\frac{k}{n}\right), \qquad F^*(n)=\sum_{\substack{k=1\\(k,n)=1}}^{n} f\left(\frac{k}{n}\right),$$

证明：$F^*(n)=\mu(n)*F(n)$.

25. 证明：若 $f(n)$ 是完全积性函数，则对所有的数论函数 $g(n), h(n)$，有

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

*26. 证明 $g(n)$ 的麦比乌斯变换的麦比乌斯变换为

$$\sum_{d_1\mid n} g(d_1)d\left(\frac{n}{d_1}\right), \text{其中 } d(n)=\sum_{d\mid n}1.$$

27. 证明：若 $f(n)$ 和 $f_1(n)$ 各为 $g(n), g_1(n)$ 的麦比乌斯变换，则

$$\sum_{d\mid n} f(d)g_1\left(\frac{n}{d}\right)=\sum_{d\mid n} g(d)f_1\left(\frac{n}{d}\right).$$

*28. 设 $f(x)$ 是一个整系数多项式，$\psi(n)$ 代表

$$f(0), f(1), \cdots, f(n-1) \tag{1}$$

中与 n 互素的数的个数，证明：

① $\psi(n)$ 是积性数论函数.

② $\psi(p^\alpha)=p^{\alpha-1}(p-b_p)$，$b_p$ 代表(1)中被素数 p 整除的数的个数.

29. 证明 $\sum_{t\mid n}(d(t))^3=\left(\sum_{t\mid n} d(t)\right)^2$.

30. 找出所有的正整数 n 分别满足

① $\varphi(n)=\frac{n}{2}$；② $\varphi(n)=\varphi(2n)$；③ $\varphi(n)=12$.

31. 证明：若 $F(n), f(n)$ 是二个数论函数，则 $F(n)=\prod_{d\mid n} f(d)$ 的充分必要条件是 $f(n)=\prod_{d\mid n} F(d)^{\mu\left(\frac{n}{d}\right)}$.

*32. 证明：若 k 个整数

$$1<a_1<a_2<\cdots<a_k\leqslant n$$

中，没有一个数能整除其余各数的乘积，则

$$k\leqslant\pi(n).$$

33. 证明：设 p_n 表示第 n 个素数，则存在正常数 C_1, C_2，使

$$C_1 n\log n<p_n<C_2 n\log n.$$

34. 证明：设 $F_0=F_1=1$，$F_{n+1}=F_{n+1}+F_n(n\geqslant 0)$，则

$$(F_m, F_n)=F_{(m,n)}.$$

35. 证明：设 $f(n)$ 是一个积性函数，若对素数的方幂 $p^a(a\geqslant 1)$ 有

$$f(p^a)=f(p)^a,$$

则 $f(n)$ 是完全积性的.

第四章　二 次 剩 余

本章介绍二次剩余理论，其中二次互反定律是数论中重要的定理，在数论许多方面都很有用．本章还将介绍二次剩余理论的一些应用．

§1 二 次 剩 余

在一般的二次同余式中，最基本的是二次同余式

$$x^2\equiv n(\mathrm{mod}m),\ (n,m)=1. \tag{1}$$

我们有以下的定义．

定义　设 $m>1$，若(1)有解，则 n 叫做模 m 的**二次剩余**；若无解，则 n 叫做模 m 的**二次非剩余**．

在第二章中，我们已经知道，解同余式(1)归结到 m 为素数的情形．因为 $m=2$ 时，解同余式(1)变得极为容易，所以，我们着重讨论 $m=p$ 的情形，这里 p 是一个奇素数，即二次同余式

$$x^2\equiv n(\mathrm{mod}p),\ (p,n)=1. \tag{2}$$

定理 1　在模 p 的缩系 $1,2,\cdots,p-1$ 中，有 $\frac{1}{2}(p-1)$ 个模 p 的二次剩余和 $\frac{1}{2}(p-1)$ 个模 p 的二次非剩余，且

$$1,\langle 2^2\rangle_p,\cdots,\left\langle\left(\frac{p-1}{2}\right)^2\right\rangle_p \tag{3}$$

就是模 p 缩系中的全部二次剩余．

证　设 $1\leqslant n\leqslant p-1$ 是模 p 的一个二次剩余，则二次同余式(2)有解 x_1，显然 $p-x_1$ 也是(2)的解．由于 $x_1\not\equiv p-x_1(\mathrm{mod}p)$，再由第二章 §5 的定理 1 知(2)若有解，则恰有二解．于是，不失一

般，可设 $1\leqslant x_1\leqslant\frac{p-1}{2}$，故由 $1\leqslant n\leqslant p-1$，$\langle x_1^2\rangle_p\equiv x_1^2\equiv n(\mathrm{mod}p)$，可知 n 必与(3)中之一数相等. 反之，(3)中之每一个数，显然都是模 p 的缩系中的二次剩余，而且(3)中没有两个数是相等的. 因为，如果(3)中有两个数相等，设为 $1\leqslant j<i\leqslant\frac{p-1}{2}$，$\langle j^2\rangle_p=\langle i^2\rangle_p$，则有

$$j^2\equiv\langle j^2\rangle_p=\langle i^2\rangle_p\equiv i^2(\mathrm{mod}p),$$

即得

$$(j-i)(j+i)\equiv 0(\mathrm{mod}p).$$

因为 $1<j+i<p$，故 $p\nmid j-i$，与所设 $1\leqslant j<i\leqslant\frac{p-1}{2}$ 矛盾. 这就证明了(3)给出了模 p 的缩系 $1,2,\cdots,p-1$ 中全部的二次剩余. 因此，二次非剩余也有 $\frac{p-1}{2}$ 个. 证完

定理 2 如果 n 是模 p 的二次剩余，则

$$n^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}p),\tag{4}$$

而如果 n 是模 p 的二次非剩余，则

$$n^{\frac{p-1}{2}}\equiv -1(\mathrm{mod}p).\tag{5}$$

证 如果 n 是模 p 的二次剩余，则(2)有解 x_1，且 $(x_1,p)=1$，利用第二章 §3 定理 5，由(2)推出

$$1\equiv x_1^{p-1}\equiv n^{\frac{p-1}{2}}(\mathrm{mod}p),$$

即(4)成立. 再由 $n^{p-1}\equiv 1(\mathrm{mod}p)$，推出

$$(n^{\frac{p-1}{2}}-1)(n^{\frac{p-1}{2}}+1)\equiv 0(\mathrm{mod}p).$$

因为 p 是奇素数，所以(4)和(5)中有一个且只有一个成立. 我们已经证明了，如果 n 是模 p 的二次剩余则(4)成立，故(3)给出了 $x^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}p)$ 的 $\frac{p-1}{2}$ 个解，而由第二章 §5 的定理 2 知，(3)给出了

它的全部解，于是由定理1知模 p 的缩系中 $\frac{p-1}{2}$ 个二次非剩余给出了 $x^{\frac{p-1}{2}}\equiv -1(\mathrm{mod}p)$ 的全部解. 这就证明了若 n 是模 p 的二次非剩余，则(5)成立. 证完

显然有以下推论.

推论 n 是模 p 的二次剩余的充分必要条件是 $n^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}p)$；$n$ 是模 p 的二次非剩余的充分必要条件是 $n^{\frac{p-1}{2}}\equiv -1(\mathrm{mod}p)$.

§2 勒让德符号

上一节定理2给出的判别 n 是否模 p 的二次剩余的法则，在 p 大时，很难实际应用. 现在引入勒让德(Legendre)符号，以便给出一个易于实际计算的判别方法.

定义 设 p 为奇素数，$(p,n)=1$，令

$$\left(\frac{n}{p}\right)=\begin{cases}1, & \text{若 } n \text{ 是模 } p \text{ 的二次剩余;}\\ -1, & \text{若 } n \text{ 是模 } p \text{ 的二次非剩余.}\end{cases}$$

函数 $\left(\frac{n}{p}\right)$ 叫做**勒让德符号**.

由勒让德符号的定义，上一节的定理2可改写为：设 p 是一个奇素数，$p\nmid n$，则

$$\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}}(\mathrm{mod}p). \tag{1}$$

由(1)，显然有 $\left(\frac{1}{p}\right)=1$.

由于 $n\equiv n'(\mathrm{mod}p)$ 时，n 和 n' 同为模 p 的二次剩余或同为模 p 的二次非剩余，故有 $\left(\frac{n}{p}\right)=\left(\frac{n'}{p}\right)$.

当 $n\equiv 0(\mathrm{mod}p)$，如果我们定义$\left(\frac{n}{p}\right)=0$，则有下面的定理.

定理 1 对于给定的奇素数 p，勒让德符号$\left(\frac{n}{p}\right)$是一个完全积性函数.

证 如果 $p\mid mn$，则 $p\mid m$或 $p\mid n$，故$\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)=0$. 如果 $p\nmid mn$，则 $p\nmid m$，$p\nmid n$，故

$$\left(\frac{mn}{p}\right)\equiv(mn)^{\frac{p-1}{2}}=m^{\frac{p-1}{2}}\cdot n^{\frac{p-1}{2}}\equiv\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)(\mathrm{mod}p). \qquad (2)$$

因为$\left(\frac{mn}{p}\right)-\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)=\pm 2,0$，故(2)给出$\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$.

证完

于是，当 $n=\pm 2^m q_1^{l_1}\cdots q_s^{l_s}$，其中 $2<q_1<\cdots<q_s$，$q_i(i=1,\cdots,s)$是素数时，有

$$\left(\frac{n}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m\left(\frac{q_1}{p}\right)^{l_1}\cdots\left(\frac{q_s}{p}\right)^{l_s}.$$

因为$\left(\frac{1}{p}\right)=1$，所以任给一个整数 n，计算$\left(\frac{n}{p}\right)$时，只需算出下面的三种值：

$$\left(\frac{-1}{p}\right),\ \left(\frac{2}{p}\right),\ \left(\frac{q}{p}\right)(q\text{ 为奇素数}).$$

定理 2 对于每一个奇素数 p，我们有

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1,\text{如果 } p\equiv 1(\mathrm{mod}4).\\ -1,\text{如果 } p\equiv 3(\mathrm{mod}4),\end{cases}$$

证 因为

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}(\mathrm{mod}p),$$

故

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$ 证完

定理3 对于每一个奇素数 p，我们有

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, \text{如果 } p\equiv\pm1(\mathrm{mod}8),\\ -1, \text{如果 } p\equiv\pm3(\mathrm{mod}8).\end{cases}$$

证 考虑以下$\frac{p-1}{2}$个同余式

$$\begin{aligned}p-1&\equiv1(-1)(\mathrm{mod}p),\\ 2&\equiv2(-1)^2(\mathrm{mod}p),\\ p-3&\equiv3(-1)^3(\mathrm{mod}p),\\ 4&\equiv4(-1)^4(\mathrm{mod}p),\\ &\vdots\\ r&\equiv\frac{p-1}{2}(-1)^{\frac{p-1}{2}}(\mathrm{mod}p),\end{aligned}$$

其中

$$r=\begin{cases}p-\frac{p-1}{2}, \text{当 } p\equiv3(\mathrm{mod}4);\\ \frac{p-1}{2}, \text{当 } p\equiv1(\mathrm{mod}4).\end{cases}$$

将以上$\frac{p-1}{2}$个同余式相乘，注意左边都是偶数，得

$$2\cdot4\cdot6\cdots(p-3)(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}}(\mathrm{mod}p),$$

即 $$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}}(\mathrm{mod}p).$$

因为 $p\nmid\left(\frac{p-1}{2}\right)!$ 和 $2^{\frac{p-1}{2}}\equiv\left(\frac{2}{p}\right)(\mathrm{mod}p)$，故

$$\left(\frac{2}{p}\right)\equiv(-1)^{\frac{p^2-1}{8}}(\mathrm{mod}p),$$

又因为 p 是奇素数，即得

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$ 证完

§3 高斯引理

十九世纪初，高斯证明了以下结果，通常称高斯引理.

定理1 设 p 是一个奇素数，$(p,n)=1$，且 $\frac{1}{2}(p-1)$ 个数

$$\langle n\rangle_p,\ \langle 2n\rangle_p,\ \cdots,\ \left\langle\frac{(p-1)n}{2}\right\rangle_p \tag{1}$$

中有 m 个大于 $\frac{1}{2}p$，则

$$\left(\frac{n}{p}\right)=(-1)^m.$$

证 以 $a_1,\cdots,a_l$ 表示(1)中所有小于 $\frac{1}{2}p$ 的数，$b_1,\cdots,b_m$ 表示(1)中所有大于 $\frac{1}{2}p$ 的数，显然，$l+m=\frac{1}{2}(p-1)$，且

$$\prod_{s=1}^{l}a_s\prod_{t=1}^{m}b_t\equiv\prod_{k=1}^{\frac{1}{2}(p-1)}kn=\left(\frac{p-1}{2}\right)!\,n^{\frac{p-1}{2}}\pmod p. \tag{2}$$

$p-b_t$ 也在1和 $\frac{1}{2}(p-1)$ 之间，故 $a_s,\ p-b_t(s=1,\cdots,l;\ t=1,\cdots,m)$ 是1和 $\frac{1}{2}(p-1)$ 之间的 $\frac{1}{2}(p-1)$ 个数. 现证这 $\frac{1}{2}(p-1)$ 个数各不相同，这只需证 $a_s\neq p-b_t$. 如果 $a_s=p-b_t$，则有

$$xn+yn\equiv 0\pmod p,\ \left(1\leqslant x\leqslant\frac{p-1}{2},\ 1\leqslant y\leqslant\frac{p-1}{2}\right),$$

即 $$x+y\equiv 0\pmod p.$$

此不可能，故

$$\prod_{s=1}^{l}a_s\prod_{t=1}^{m}(p-b_t)=\left(\frac{p-1}{2}\right)!.$$

由(2)

$$\left(\frac{p-1}{2}\right)!=\prod_{s=1}^{l}a_s\prod_{t=1}^{m}(p-b_t)$$

$$\equiv(-1)^m\prod_{s=1}^{l}a_s\prod_{t=1}^{m}b_t\equiv(-1)^m\left(\frac{p-1}{2}\right)!\,n^{\frac{p-1}{2}}$$

$$(\mathrm{mod}\,p).$$

故得

$$n^{\frac{p-1}{2}}\equiv(-1)^m(\mathrm{mod}\,p).$$

由于 $n^{\frac{p-1}{2}}\equiv\left(\frac{n}{p}\right)(\mathrm{mod}\,p)$，故

$$\left(\frac{n}{p}\right)\equiv(-1)^m(\mathrm{mod}\,p),$$

即得 $\left(\frac{n}{p}\right)=(-1)^m$. 证完

由高斯引理，可给 §2 中定理 3 另一个证明:

在定理 1 中取 $n=2$，则(1)给出

$$2,2\cdot2,3\cdot2,\cdots,\left(\frac{p-1}{2}\right)\cdot2.$$

现求出适合

$$\frac{p}{2}<2k<p\left(\text{即}\frac{p}{4}<k<\frac{p}{2}\right)$$

的 k 的个数，即得 $m=\left[\frac{p}{2}\right]-\left[\frac{p}{4}\right]$.

令 $p=8a+r$，$r=1,3,5,7$，则得

$$m=2a+\left[\frac{r}{2}\right]-\left[\frac{r}{4}\right]\equiv0,1,1,0(\mathrm{mod}2),$$

故

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

高斯引理可以作如下推广. 首先给出一个定义.

定义 设 p 是一个奇素数，如果$\frac{p-1}{2}$个数 $r_1,\cdots, r_{\frac{p-1}{2}}$ 使得 $p-1$ 个数 $\pm r_1, \pm r_2,\cdots, \pm r_{\frac{p-1}{2}}$组成模 p 的一组缩系，则称 $r_1,\cdots, r_{\frac{p-1}{2}}$是模 p 的一组**半系**.

我们有下面的定理.

定理 2 设 $p\nmid n, r_1,\cdots, r_{\frac{p-1}{2}}$是模 p 的一组半系，且

$$nr_i\equiv(-1)^{e_i}r_{i'}(\mathrm{mod}p),\ i=1,\cdots,\ \frac{p-1}{2};1\leqslant i'\leqslant\frac{p-1}{2},\quad(3)$$

则

$$\left(\frac{n}{p}\right)=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}e_i}.$$

证 由于 $r_1,\cdots,r_{\frac{p-1}{2}}$是模 p 的一组半系，所以(3) 中的 e_i (mod2)和 $r_{i'}$ 都是唯一决定的. 现在我们来证明如果 $i\neq j$，则 $i'\neq j'$. 否则，由

$$nr_i\equiv(-1)^{e_i}r_{i'}(\mathrm{mod}p)$$

和

$$nr_j\equiv(-1)^{e_j}r_{j'}(\mathrm{mod}p),$$

推出

$$nr_j\equiv\pm nr_i(\mathrm{mod}p),$$

即得

$$r_j\equiv\pm r_i(\mathrm{mod}p).$$

由于 $r_1,\cdots,r_{\frac{p-1}{2}}$是模 p 的一组半系，只能有 $i=j$，与所设矛盾. 这

就证明了 $r_1', \cdots, r_{(\frac{p-1}{2})}'$ 是 $r_1, \cdots, r_{\frac{p-1}{2}}$ 的某一个排列，故将(3)中的 $\frac{p-1}{2}$ 个同余式相乘，得

$$n^{\frac{p-1}{2}} r_1 \cdots r_{\frac{p-1}{2}} \equiv (-1)^{\sum_{j=1}^{\frac{p-1}{2}} e_j} r_1 \cdots r_{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

由于 $p \nmid r_1 \cdots r_{\frac{p-1}{2}}$，故

$$n^{\frac{p-1}{2}} \equiv (-1)^{\sum_{j=1}^{\frac{p-1}{2}} e_j} \quad (\mathrm{mod}\, p),$$

即得

$$\left(\frac{n}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} e_j}.$$

证完

推论　设 $p \nmid n$，

$$ni \equiv (-1)^{e_i} i' (\mathrm{mod}\, p), \qquad i = 1, \cdots, \frac{p-1}{2};\ 1 \leqslant i' \leqslant \frac{p-1}{2},$$

则

$$\left(\frac{n}{p}\right) = (-1)^t,$$

其中 t 表示 $e_1, \cdots, e_{\frac{p-1}{2}}$ 中奇数的个数.

证　因为 $\sum_{i=1}^{\frac{p-1}{2}} e_i \equiv t (\mathrm{mod}\, 2)$.　　证完

这个推论，实际上就是高斯引理，这是因为当 e_i 为偶数时 $\langle ni \rangle_p = i' < \frac{p}{2}$，$e_i$ 为奇数时 $\langle ni \rangle_p = p - i' > \frac{p}{2}$，故 t 就是(1)中大于 $\frac{p}{2}$ 的个数.

§4 二次互反定律

利用高斯引理，高斯证明了著名的二次互反定律.

定理(二次互反定律) 设 $p>2, q>2$ 是两个素数，$p\neq q$，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)}{4}\frac{(q-1)}{4}}$$

证 首先，我们利用高斯引理来计算$\left(\frac{q}{p}\right)$.

当$1\leqslant k\leqslant\frac{p-1}{2}$，有

$$kq=q_k p+r_k, q_k=\left[\frac{kq}{p}\right], 1\leqslant r_k\leqslant p-1.$$

令

$$a=\sum_{s=1}^{l}a_s, b=\sum_{t=1}^{m}b_t,$$

此处 a_s 和 b_t 的含意见 §3 中定理 1 (取 $n=q$)的证明，则得

$$a+b=\sum_{k=1}^{\frac{p-1}{2}}r_k. \tag{1}$$

由高斯引理的证明知，$a_s, p-b_t(s=1,2,\cdots,l, t=1,2,\cdots,m)$ 正好是 $1,2,\cdots,\frac{1}{2}(p-1)$ 各数，故有

$$\frac{p^2-1}{8}=1+2+\cdots+\frac{p-1}{2}=a+mp-b. \tag{2}$$

又

$$\frac{p^2-1}{8}q=\sum_{k=1}^{\frac{p-1}{2}}kq=p\sum_{k=1}^{\frac{p-1}{2}}q_k+\sum_{k=1}^{\frac{p-1}{2}}r_k=p\sum_{k=1}^{\frac{p-1}{2}}q_k+a+b. \tag{3}$$

(3)式减去(2)式得

$$\frac{p^2-1}{8}(q-1)=p\sum_{k=1}^{\frac{p-1}{2}}q_k-mp+2b,$$

故

$$m\equiv\sum_{k=1}^{\frac{p-1}{2}}q_k\pmod 2,$$

即得

$$\left(\frac{q}{p}\right)=(-1)^m=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}q_k}=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]}.$$

同理可证

$$\left(\frac{p}{q}\right)=(-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]}.$$

剩下来，只需证明

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}. \tag{4}$$

设

$$f(x,y)=qx-py,$$

当 $x=1,\ 2,\cdots,\ \frac{p-1}{2},\ y=1,2,\cdots,\frac{q-1}{2}$ 时，$f(x,y)$ 取

$$\frac{p-1}{2}\cdot\frac{q-1}{2}$$

个值，且没有两个值相等，否则

$$f(x,y)-f(x',y')=0,$$

即

$$(x-x')q=(y-y')p,$$

推出

$$p|x-x', q|y-y',$$

故 $x=x', y=y'$. 这就证明了对于不同的有序对(x, y), $f(x, y)$取不同的值. 下面来计算其中正值的个数和负值的个数. 对于每一个固定的 x, $f(x, y)>0$ 当且仅当 $y<\frac{qx}{p}$, 即 $y\leqslant\left[\frac{qx}{p}\right]$, 因此全部正值的个数是

$$\sum_{x=1}^{\frac{p-1}{2}}\left[\frac{qx}{p}\right].$$

类似可证全部负值的个数是

$$\sum_{y=1}^{\frac{q-1}{2}}\left[\frac{py}{q}\right].$$

这就证明了(4). 证完

二次互反定律可以用来决定对于给定的整数 n 和素数 p, n 是否是模 p 的二次剩余, 也可以用来决定对于给定的整数 n, 有哪些素数 p 使 n 是模 p 的二次剩余. 下面就来举两个例子.

例 1 设 $p=593, n=438$, 计算$\left(\frac{438}{593}\right)$.

因为 $438=2\cdot3\cdot73$, 故

$$\left(\frac{438}{593}\right)=\left(\frac{2}{593}\right)\left(\frac{3}{593}\right)\left(\frac{73}{593}\right).$$

因为 $593\equiv1\ (\mathrm{mod}8)$, 再利用二次互反定律和前面讲到的有关性质, 有

$$\left(\frac{438}{593}\right)=\left(\frac{593}{3}\right)\left(\frac{593}{73}\right)=\left(\frac{2}{3}\right)\left(\frac{9}{73}\right)=-1.$$

故 438 是模 593 的二次非剩余.

例 2 决定所有的奇素数 p, 使 3 为模 p 的二次剩余, 同时决定所有的奇素数 p, 使 3 为模 p 的二次非剩余.

首先$p\neq 3$，由二次互反定律，我们有

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

当 $p=12k+1$ 形的素数时，

$$\left(\frac{3}{p}\right)=\left(\frac{1}{3}\right)(-1)^{6k}=1.$$

当$p=12k+5$ 形的素数时，

$$\left(\frac{3}{p}\right)=\left(\frac{2}{3}\right)(-1)^{6k+2}=-1.$$

当 $p=12k+7$ 形的素数时，

$$\left(\frac{3}{p}\right)=\left(\frac{1}{3}\right)(-1)^{6k+3}=-1.$$

当 $p=12k+11$ 形的素数时，

$$\left(\frac{3}{p}\right)=\left(\frac{2}{3}\right)(-1)^{6k+5}=1.$$

故当 $p\equiv\pm 1\pmod{12}$ 时，3 为模 p 的二次剩余；当 $p\equiv\pm 5\pmod{12}$时，3 为模 p 的二次非剩余.

二次互反定律是数论中一个深刻的结果，除了能够方便地计算勒让德符号外，在数论许多方面都非常有用. 这个定理是由欧拉提出，高斯首先证明的. 到目前为止，已经有了一百五十多个不同的证明. 由二次互反定律引伸出来的工作，导致了代数数论的发展和类域论的形成.

§5 二次剩余理论应用举例

本节介绍二次剩余理论在整数循环序列，二元周期序列和不定方程等方面的一些应用.

定理 1 设 u_n是一个卢卡斯序列，即

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta},\ n=0,1,\cdots \tag{1}$$

其中 α、β 为以下整系数二次方程的两个根:

$$x^2-Px+Q=0,(P,Q)=1. \tag{2}$$

再设 q 是一个奇素数,$q\nmid Q$,$D=P^2-4Q$,则

$$q\mid u_{q-\left(\frac{D}{q}\right)}, \tag{3}$$

(3) 中$\left(\frac{D}{q}\right)$是勒让德符号.

证 由(2),可设

$$\alpha=\frac{P+\sqrt{D}}{2},\beta=\frac{P-\sqrt{D}}{2},$$

故

$$u_q=\frac{\alpha^q-\beta^q}{\alpha-\beta}=\frac{qP^{q-1}+\binom{q}{3}P^{q-3}D+\cdots+P^2\binom{q}{q-2}D^{\frac{q-3}{2}}+D^{\frac{q-1}{2}}}{2^{q-1}},$$

即得

$$2^{q-1}u_q=qP^{q-1}+\binom{q}{3}P^{q-3}D+\cdots+P^2\binom{q}{q-2}D^{\frac{q-3}{2}}+D^{\frac{q-1}{2}}.$$

如果 $q\mid D$,则有 $q\mid u_q$,定理成立. 如果 $q\nmid D$,因为 q 是奇素数,故有

$$u_q\equiv D^{\frac{q-1}{2}}\equiv\left(\frac{D}{q}\right)=\pm1(\mathrm{mod}q). \tag{4}$$

而

$$2^qu_{q+1}=(q+1)P^q+\binom{q+1}{3}P^{q-2}D+\cdots$$

$$+\binom{q+1}{q-2}P^3D^{\frac{q-3}{2}}+\binom{q+1}{q}PD^{\frac{q-1}{2}},$$

由于 $q\mid\binom{q+1}{t}(3\leqslant t\leqslant q-2)$,故

$$2u_{q+1}\equiv P\left(1+\left(\frac{D}{q}\right)\right)(\mathrm{mod}q). \tag{5}$$

如果$\left(\frac{D}{q}\right)=-1$，由(5)得 $q\mid u_{q+1}$；如果$\left(\frac{D}{q}\right)=1$，由(5)可得

$$u_{q+1}\equiv P(\mathrm{mod}q) \tag{6}$$

利用第三章 §8 的定理 1，

$$u_{q+1}=Pu_q-Qu_{q-1}, \tag{7}$$

由(4)、(6)、(7)可得

$$Qu_{q-1}\equiv 0(\mathrm{mod}q).$$

由于 $q\nmid Q$，故得 $q\mid u_{q-1}$. 总上所述，我们证明了(3)式. 证完

这个定理使我们得到某些大数的一个素因子.

取 $P=4, Q=1$，利用卢卡斯序列

$$v_0=2, v_1=4, v_{n+2}=4v_{n+1}-v_n,$$

1930 年，莱梅给出了判别麦什涅数 2^q-1 是否素数的一个有效方法：设 q 是一个奇素数，定义序列

$$L_0=4, L_{n-1}=\langle L_n^2-2\rangle_{2^q-1},$$

则 2^q-1 是素数当且仅当

$$L_{q-2}=0.$$

以后一些素数判别的重要结果，都是以莱梅法为基础的.

定理 2 不定方程

$$y^2=x^3+3b^2-a^3, \tag{8}$$

当 $a\equiv 1(\mathrm{mod}4), b\equiv\pm 2(\mathrm{mod}6)$，且 b 没有 $12k\pm 5$形的素因数时，无整数解.

证 当 $x\equiv 0(\mathrm{mod}2)$时，(8)式取模 4，得 $y^2\equiv 3(\mathrm{mod}4)$，这是不可能的. 当 $x\equiv 3(\mathrm{mod}4)$时，(8)式取模 4，得 $y^2\equiv 2(\mathrm{mod}4)$，仍不可能. 故可设 $x\equiv 1(\mathrm{mod}4)$，再对(8)取模 3 可得

$$x-a\equiv y^2(\mathrm{mod}3),$$

因此 $x\equiv a, a+1(\mathrm{mod}3)$. 当 $x\equiv a(\mathrm{mod}3)$ 时，有 $x^3\equiv a^3(\mathrm{mod}9)$，由(8)给出 $y^2\equiv 3(\mathrm{mod}9)$，这是不可能的. 当 $x\equiv a+1(\mathrm{mod}3)$时，有

$$x^2+ax+a^2\equiv 1(\mathrm{mod}3)$$

和

$$x^2+ax+a^2\equiv 3(\mathrm{mod}4).$$

故

$$x^2+ax+a^2\equiv 7(\mathrm{mod}12),$$

于是，x^2+ax+a^2 的素因子不能是 3，也不能都是 $12t\pm 1$ 形的数，故存在素数 $p|x^2+ax+a^2, p\equiv\pm 5(\mathrm{mod}12)$，由(8)得

$$y^2\equiv 3b^2(\mathrm{mod}p). \tag{9}$$

而 $p\nmid b$，$\left(\frac{3b^2}{p}\right)=\left(\frac{3}{p}\right)=-1$，与(9)式矛盾. 证完

最后，我们介绍二次剩余理论在二元周期序列中的一点应用. 在数字通信系统中，广泛采用取值为±1 的周期序列.

定义 二元序列

$$a_0, a_1, a_2, \cdots, a_h, \cdots, \quad a_h=1 \text{ 或 } -1 (h=0, 1, 2, \cdots) \tag{10}$$

叫做**周期的**，是指存在正整数 t，使

$$a_{n+t}=a_n, n=0, 1, 2, \cdots,$$

满足以上条件的最小正整数 t，叫做序列(6)的**周期**.

显然，如果有正整数 l，使 $a_{n+l}=a_n, n=0, 1, 2, \cdots$，则 $t|l$.

设序列(10)的周期为 t，

$$c(l)=\frac{1}{t}\sum_{k=0}^{t-1}a_k a_{k+l}, 0\leqslant l\leqslant t-1,$$

称 $c(0)=1$ 为序列(10)的**自相关主值**，$c(l)(1\leqslant l\leqslant t-1)$为序列(10)的**自相关非主值**.

定义 设

$$c=\max_{1\leqslant l\leqslant t-1}|c(l)|,$$

如果 c 很小，则称序列(10)是**自相关良好的序列.**

自相关良好的取值 ±1 的序列，在数字通信中有用.

定理 3 设 p 是奇素数，定义(10)中

$$a_n=\begin{cases}\left(\dfrac{n}{p}\right), & \text{当 } p\nmid n,\\ 1, & \text{当 } p\mid n.\end{cases}$$

则有

$$c\leqslant\frac{3}{p}.$$

证 因为 $a_{k+p}=a_k$, $k=0,1,\cdots$，故其周期为 p. 否则，周期 $t=1$，推出 $a_0=a_1=a_2=\cdots$，这是不可能的. 当 $1\leqslant l\leqslant p-1$ 时，

$$c(l)=\frac{1}{p}\sum_{k=0}^{p-1}a_k a_{k-l}=\frac{1}{p}\left(a_0a_l+a_{p-l}a_p+\sum_{\substack{k=1\\k\neq p-l}}^{p-1}a_k a_{k+l}\right)$$

$$=\frac{1}{p}\left(\left(\frac{l}{p}\right)+\left(\frac{-l}{p}\right)+\sum_{\substack{k=1\\k\neq p-l}}^{p-1}\left(\frac{k}{p}\right)\left(\frac{k+l}{p}\right)\right)$$

$$=\frac{1}{p}\left(\left(\frac{l}{p}\right)+\left(\frac{-l}{p}\right)+\sum_{k=1}^{p-1}\left(\frac{k(k+l)}{p}\right)\right).$$

因为 $(l,p)=1$ 时，$\sum_{k=1}^{p-1}\left(\dfrac{k(k+l)}{p}\right)=-1$(见本章习题)，故

$$c(l)=\frac{1}{p}\left(\left(\frac{l}{p}\right)+\left(\frac{-l}{p}\right)-1\right)$$

$$=\begin{cases}-\frac{1}{p}, \text{若 } p\equiv 3(\mathrm{mod}4)\\ \frac{1}{p}, \text{若 } p\equiv 1(\mathrm{mod}4),\left(\frac{l}{p}\right)=1.\\ \frac{-3}{p}, \text{若 } p\equiv 1(\mathrm{mod}4),\left(\frac{l}{p}\right)=-1,\end{cases}$$

$$c=\max_{1\leqslant l\leqslant p-1}|c(l)|\leqslant\frac{3}{p}\sqrt{p}.$$ 证完

定理 3 给出的序列也叫**二次剩余序列**，当 p 较大时，它自然是一个自相关良好的序列.

§6 二次同余式的解法和解数

对于二次同余式

$$x^2\equiv n(\mathrm{mod}p),\ p \text{ 是奇素数},\ p\nmid n, \tag{1}$$

如果勒让德符号$\left(\frac{n}{p}\right)=-1$，则无解；如果 $\left(\frac{n}{p}\right)=1$，则(1)有解. 当 p 不太大时，可将 $x=1,2,\cdots,\frac{p-1}{2}$直接代入(1) 中求解. 但是当 p 大时，求出(1)的解却不是一件容易的事.

我们有以下的定理.

定理1 设$\left(\frac{n}{p}\right)=1$，则有

① 当 $p\equiv 3(\mathrm{mod}\ 4)$时，$\pm n^{\frac{1}{4}(p+1)}$为(1)的解；

② 当 $p\equiv 5(\mathrm{mod}8)$，$n^{\frac{1}{4}(p-1)}\equiv 1(\mathrm{mod}p)$时，$\pm n^{\frac{1}{8}(p+3)}$为(1)的解；当 $p\equiv 5(\mathrm{mod}8)$，$n^{\frac{1}{4}(p-1)}\equiv -1(\mathrm{mod}p)$时，$\pm\left(\frac{p-1}{2}\right)!\cdot n^{\frac{1}{8}(p+3)}$为(1)的解.

证 ① 当 $p\equiv 3(\mathrm{mod}4)$时，因$\left(\frac{n}{p}\right)=1$，故

$$n^{\frac{1}{2}(p-1)}\equiv 1(\mathrm{mod}p),$$

即得

$$\left(n^{\frac{p+1}{4}}\right)^2\equiv n(\mathrm{mod}p).$$

② 当 $p\equiv 5(\mathrm{mod}8)$时，先求 $n=-1$ 的解. 由威尔逊定理，

$$-1\equiv(p-1)!=1\cdot 2\cdots\left(\frac{p-1}{2}\right)\cdot\left(p-\frac{p-1}{2}\right)\cdots(p-2)(p-1)$$

$$\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2(\mathrm{mod}p).$$

因为$\left(\frac{n}{p}\right)=1$，故

$$n^{\frac{1}{2}(p-1)}-1\equiv 0(\mathrm{mod}p).$$

n 适合

$$n^{\frac{1}{4}(p-1)}\equiv 1(\mathrm{mod}p),$$

或

$$n^{\frac{1}{4}(p-1)}\equiv -1(\mathrm{mod}p)$$

时，分别给出

$$\left(n^{\frac{p+3}{8}}\right)^2\equiv n(\mathrm{mod}p)$$

和

$$\left(\left(\frac{p-1}{2}\right)!\,n^{\frac{p+3}{8}}\right)^2\equiv n(\mathrm{mod}p).$$

证完

定理 2 设 $p\equiv 1(\mathrm{mod}8),\left(\frac{n}{p}\right)=1,\left(\frac{N}{p}\right)=-1$，则同余式(1)有解

$$\pm n^{\frac{A+1}{2}}N^{\frac{B}{2}},$$

其中 h 满足 $p=2^k h+1, 2\nmid h, s_k\geqslant 0$ 是某个整数.

证 由 $p\equiv 1(\mathrm{mod}8)$, 可设 $p=2^k h+1, k\geqslant 3, 2\nmid h$.

由$\left(\frac{n}{p}\right)=1, \left(\frac{N}{p}\right)=-1$, 我们得出

$$n^{2^{k-1}h}\equiv 1(\mathrm{mod}p),$$

$$N^{2^{k-1}h}\equiv -1(\mathrm{mod}p).$$

因此下面的两个同余式有且只有一个成立

$$n^{2^{k-2}h}\equiv 1(\mathrm{mod}p),$$

$$n^{2^{k-2}h}\equiv -1(\mathrm{mod}p).$$

故有非负整数 $s_2=hf(f=0$ 或 $1)$使

$$n^{2^{k-2}h}\cdot N^{2^{k-1}s_2}\equiv 1(\mathrm{mod}p)$$

成立.

于是下面两个同余式有且只有一个成立

$$n^{2^{k-3}h}N^{2^{k-2}s_2}\equiv 1(\mathrm{mod}p),$$

$$n^{2^{k-3}h}N^{2^{k-2}s_2}\equiv -1(\mathrm{mod}p),$$

故又有非负的 $s_3=s_2+2hf_1(f_1=0$ 或 $1)$满足下式

$$n^{2^{k-3}h}N^{2^{k-2}s_3}\equiv 1(\mathrm{mod}p).$$

因为 k 是有限整数, 故必有一非负的 s_k 使得

$$n^h\cdot N^{2s_k}\equiv 1(\mathrm{mod}p),$$

故

$$n^{h+1}N^{2s_k}\equiv n(\mathrm{mod}p),$$

即

$$\left(n^{\frac{h+1}{2}}N^{s_k}\right)^2\equiv n(\mathrm{mod}p).$$ 证完

对于二次同余式的解数, 我们有以下定理.

定理 3 设 p 是素数，$p\nmid n$，二次同余式

$$x^2\equiv n(\mathrm{mod}\,p^l)\quad l>0, \tag{2}$$

在 $p>2$ 时，有 $1+\left(\frac{n}{p}\right)$ 个解. 在 $p=2$ 时，有下面三种情形：

① $l=1$，则有一个解；

② $l=2$，当 $n\equiv 1(\mathrm{mod}4)$ 或 $n\equiv 3(\mathrm{mod}4)$，有二个解或无解；

③ $l>2$，当 $n\equiv 1(\mathrm{mod}8)$ 或 $\not\equiv 1(\mathrm{mod}8)$，有四个解或无解.

证 在 $p>2$，$p\nmid n$ 时，因为 $x^2\equiv n(\mathrm{mod}p)$ 与 $x\equiv 0(\mathrm{mod}p)$ 无公解，由第二章 §7 定理的推论，得此结论.

在 $p=2$ 时：

① $l=1$，显然只有一个解.

② $l=2$，$x^2\equiv 1(\mathrm{mod}4)$ 时有二个解 $x=\pm 1$；$x^2\equiv 3(\mathrm{mod}4)$ 时无解，故结论成立.

③ $l>2$ 时，若 $n\not\equiv 1(\mathrm{mod}8)$，则(2)无解，否则(2)的解 x 必为奇，由(2)给出 $n\equiv 1(\mathrm{mod}8)$，与所设矛盾. 若 $n\equiv 1(\mathrm{mod}8)$，在 $l=3$ 时，显然有四个解：1, 3, 5, 7. 当 $l>3$ 时，我们用归纳法来证明 $n\equiv 1(\mathrm{mod}8)$ 时(2)有解：设 a 满足 $a^2\equiv n(\mathrm{mod}2^{l-1})$，显然 $2\nmid a$，则

$$(a+2^{l-2}b)^2=a^2+ab2^{l-1}+2^{2(l-2)}b^2\equiv a^2+b2^{l-1}(\mathrm{mod}2^l),$$

取 $b=\frac{n-a^2}{2^{l-1}}$，由上式知 $a+2^{l-2}b$ 满足 $x^2\equiv n(\mathrm{mod}2^l)$. 现设 x_1 为 $x^2\equiv n(\mathrm{mod}2^l)$ 的一个解，则 $\pm x_1$，$\pm x_1+2^{l-1}$ 是它的四个解. 现设 x_2 是 $x^2\equiv n(\mathrm{mod}2^l)$ 的任一解，则

$$(x_2-x_1)(x_2+x_1)\equiv 0(\mathrm{mod}2^l),$$

因 x_2-x_1，x_2+x_1 皆为偶数，故上式给出

$$\frac{x_2-x_1}{2}\cdot\frac{x_2+x_1}{2}\equiv 0(\mathrm{mod}2^{l-2}). \tag{3}$$

又因 x_2 为奇，故 $\frac{x_2-x_1}{2}$，$\frac{x_2+x_1}{2}$ 一奇一偶，(3)式给出

$$\frac{x_2-x_1}{2}\equiv 0(\mathrm{mod}2^{l-2})$$

或

$$\frac{x_2+x_1}{2}\equiv 0(\mathrm{mod}2^{l-2}),$$

故 $x_2=x_1+k2^{l-1}$ 或 $x_2=-x_1+k2^{l-1}$. 无论哪一种情形，x_2 与 $\pm x_1$，$\pm x_1+2^{l-1}$ 之一模 2^l 同余. 这就证明了 $l\geqslant 3$ 时，$x^2\equiv n(\mathrm{mod}2^l)$ 有四个解. 证完

§7 雅可比符号

计算勒让德符号 $\left(\frac{n}{p}\right)$，需要把 n 分解成标准分解式，这常常是很麻烦的，这也是运用勒让德符号进行计算时的缺点，避开这个缺点的一个方法就是引进雅可比(Jacobi)符号.

定义 设 m 是一个正奇数，$m=p_1p_2\cdots p_t$，$p_i(i=1,\cdots,t)$ 是素数，$(m,n)=1$，则

$$\left(\frac{n}{m}\right)=\prod_{i=1}^{t}\left(\frac{n}{p_i}\right)$$

叫做**雅可比符号**.

例如，$\left(\frac{1}{m}\right)=1$；如 $(a,m)=1$，则 $\left(\frac{a^2}{m}\right)=1$.

它的计算法则，容易由勒让德符号的性质推出. 下面的定理1是显然的.

定理1 设 m,m_1 为正奇数.

① 若 $n\equiv n_1(\mathrm{mod}m)$ 和 $(n,m)=1$，则

$$\left(\frac{n}{m}\right)=\left(\frac{n_1}{m}\right);$$

② 若$(n, m)-(n, m_1)=1$，则

$$\left(\frac{n}{m}\right)\left(\frac{n}{m_1}\right)=\left(\frac{n}{mm_1}\right);$$

③ 若$(n, m)=(n_1, m)=1$，则

$$\left(\frac{n}{m}\right)\left(\frac{n_1}{m}\right)=\left(\frac{nn_1}{m}\right).$$

定理 2 $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$.

证 因为

$$m=\prod_{i=1}^{t}p_i=\prod_{i=1}^{t}(1+p_i-1)=1+\sum_{i=1}^{t}(p_i-1)+$$

$$+\sum_{1\leqslant i<j\leqslant t}(p_i-1)(p_j-1)+\cdots,$$

故由上式可得 $m\equiv 1+\sum_{i=1}^{t}(p_i-1)\pmod 4$，即

$$\frac{m-1}{2}\equiv\sum_{i=1}^{t}\frac{p_i-1}{2}\pmod 2,$$

于是

$$\left(\frac{-1}{m}\right)=\prod_{i=1}^{t}\left(\frac{-1}{p_i}\right)=(-1)^{\sum_{i=1}^{t}\frac{p_i-1}{2}}=(-1)^{\frac{m-1}{2}}.$$

证完

定理 3 $\left(\frac{2}{m}\right)=(-1)^{\frac{1}{8}(m^2-1)}$.

证 因为

$$m^2=\prod_{i=1}^{t}(1+p_i^2-1)=1+\sum_{i=1}^{t}(p_i^2-1)+$$

$$+\sum_{1\leqslant i<j\leqslant t}(p_i^2-1)(p_j^2-1)+\cdots,$$

而 $p_i^2\equiv 1(\mathrm{mod}8)(i=1,\cdots,t)$，故得

$$m^2-1\equiv\sum_{i=1}^{t}(p_i^2-1)(\mathrm{mod}64),$$

即

$$\frac{m^2-1}{8}\equiv\sum_{i=1}^{t}\frac{p_i^2-1}{8}(\mathrm{mod}2).$$

于是

$$\left(\frac{2}{m}\right)=\prod_{i=1}^{t}\left(\frac{2}{p_i}\right)=(-1)^{\sum_{i=1}^{t}\frac{p_i^2-1}{8}}=(-1)^{\frac{m^2-1}{8}}.$$

证完

定理 4 若 m 与 n 是二正奇数，且 $(m,n)=1$，则

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

证 设 $m=\prod_{i=1}^{t}p_i$，$n=\prod_{j=1}^{s}q_j$，$p_1,\cdots,p_t,q_1,\cdots,q_s$ 均为素数，则

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)=(-1)^f,$$

$$f=\sum_{i=1}^{t}\sum_{j=1}^{s}\frac{1}{2}(p_i-1)\frac{1}{2}(q_j-1)$$

$$=\sum_{i=1}^{t}\frac{1}{2}(p_i-1)\sum_{j=1}^{s}\frac{1}{2}(q_j-1).$$

在定理 2 中已证 $\sum_{i=1}^{t}\frac{1}{2}(p_i-1)\equiv\frac{1}{2}(m-1)\pmod 2$，故

$$f\equiv\frac{1}{2}(m-1)\cdot\frac{1}{2}(n-1)\pmod 2,$$

得

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

证完

从以上几个定理可以看出，雅可比符号具有勒让德符号一样的计算法则，当 n 是正奇数时，不需要把 n 分解成素因数的乘积，所以计算起来更方便. 在 $t=1$ 时，$\left(\frac{n}{m}\right)$的值与勒让德符号$\left(\frac{n}{m}\right)$的值相等. 在 $t>1$ 时，如果$\left(\frac{n}{m}\right)=-1$，则 $x^2\equiv n\pmod m$ 无解. 但当 $\left(\frac{n}{m}\right)=1$ 时，$x^2\equiv n\pmod m$ 不一定有解. 例如$\left(\frac{2}{9}\right)=1$，而同余式 $x^2\equiv 2\pmod 9$ 无解.

§8 表素数为平方和

不是所有素数都能表成二个整数的平方和，例如由于 $x^2+y^2\equiv 0,1,2\pmod 4$，故 $p\equiv 3\pmod 4$ 时，p 不能表为平方和. 在本节中，我们将证明 $p\equiv 1\pmod 4$ 时，p 可表成平方和.

定义 设整数 n 能表成二个平方和

$$n=x^2+y^2,$$

如果 $(x,y)=1$，则称 n **能本原的表成二个平方和**. 如果由 $n=x^2+y^2(x\geqslant 0,y\geqslant 0)$，$n=a^2+b^2(a\geqslant 0,b\geqslant 0)$，推出 $a=x$，$b=y$ 或 $a=y$，$b=x$，则称表法唯一.

定理 1 设 p 是 m 的一个奇素因子，p 能表成二个平方和，m

能本原的表成二个平方和，则$\frac{m}{p}$也能本原的表成二个平方和.

证 设

$$m=x^2+y^2,\ (x,y)=1,$$
$$p=a^2+b^2,$$

故有

$$(ax-by)(ax+by)=a^2x^2-b^2y^2=a^2(x^2+y^2)-y^2(a^2+b^2)$$
$$\equiv 0(\mathrm{mod}p),$$

因此 $p|ax-by$ 或 $p|ax+by$. 设 $p|ax-by$，因为

$$mp=(ax-by)^2+(ay+bx)^2, \tag{1}$$

故 $p|ay+bx$. 设$(ax-by, ay-bx)=pg$，则有

$$pg|a(ax-by)+b(ay+bx)=xp,$$
$$pg|a(ay+bx)-b(ax-by)=yp,$$

因为$(x,y)=1$，故 $g=1$. 由(1)得

$$\frac{m}{p}=\left(\frac{ax-by}{p}\right)^2+\left(\frac{ay+bx}{p}\right)^2,$$

故$\frac{m}{p}$能本原的表成二个平方的和. $p|ax+by$ 时，可类似地证明.

证完

定理 2 n^2+1 的每一个素因子都能表成二个平方的和.

证 $n=1$ 时，$2=1^2+1^2$，定理成立. 现设定理对 $n\leqslant m-1$ $(m\geqslant 2)$成立，即

$$1^2+1, 2^2+1, 3^2+1, \cdots, (m-1)^2+1$$

的每一个素因子都能表成二个平方的和. 现在，我们来证明定理对 $n=m$ 时成立. 如果 $p|m^2+1$，且 $p<m$，则 $p|(m-p)^2+1$，故由归纳假设 p 能表成二个平方的和. 如果 $p|m^2+1$，且 $p>m$，设

$$m^2+1=fp,\ f<m,\ f=q_1\cdots q_k,\ q_i \text{ 是素数},\ i=1,\cdots,k,$$

则 $q_i<m$. 由归纳假设，$q_i(i=1,\cdots,k)$ 能表成二个平方的和. 再由定理 1 知$\frac{m^2+1}{q_1}$能本原的表成二个平方的和，继续消去 $q_2,\cdots,q_k$，最后可知$\frac{m^2+1}{f}=p$ 可表成二个平方的和. 证完

由定理 2 不难推出定理 3 .

定理 3 每一个形如 $4k+1$ 的素数能表成二个平方的和，且表法唯一.

证 $p\equiv1(\mathrm{mod}4)$，由 $-1\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2(\mathrm{mod}p)$ 和定理 2 知 p 能表成二个平方的和. 现在来证明表法唯一. 设

$$p=x^2+y^2,\ x>0,\ y>0,$$

$$p=a^2+b^2,\ a>0,\ b>0,$$

由定理 1 的证明知 $p\mid ax-by$，或 $p\mid ax+by$. 又有

$$p^2=(ax-by)^2+(ay+bx)^2,$$

如果 $p\mid ax-by$，由于 $ay+bx\neq0$，上式给出 $ax-by=0$，因为 $(a,b)=(x,y)=1$，故有 $a=y,b=x$；如果 $p\mid ax+by$，由

$$p^2=(ax+by)^2+(ay-bx)^2,$$

故 $ay-bx=0$，推出 $a=x,b=y$. 故表法唯一.

证完

设 $p\equiv1(\mathrm{mod}4),(k,p)=1$，$s(k)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right)$，则有

$$p=\left(\frac{1}{2}s(r)\right)^2+\left(\frac{1}{2}s(u)\right)^2,$$

其中$\left(\frac{r}{p}\right)=1,\left(\frac{u}{p}\right)=-1.$

这个结果的证明，这里不准备给出了. 可参看华罗庚的《数论导引》第七章 § 8 的定理 6.

最后，用抽屉原理给出定理 3 的另一个证明.

定理 3 的另一证明：

因为$\left(\frac{-1}{p}\right)=1$，故有整数 s 存在，使

$$s^2+1\equiv 0(\mathrm{mod}\,p),\ (s,p)=1, \tag{2}$$

考虑 $sy-x$，$y=0,1,\cdots,[\sqrt{p}]$，$x=0,1,\cdots,[\sqrt{p}]$. 共有$([\sqrt{p}]+1)^2$个 $sy-x$ 的值产生，而$([\sqrt{p}]+1)^2>p$，由抽屉原理，存在两组 y_1, x_1, y_2, x_2，使

$$sy_1-x_1\equiv sy_2-x_2(\mathrm{mod}\,p).$$

由$(s,p)=1$，易知 $x_1\neq x_2$，$y_1\neq y_2$. 不妨设 $y_1>y_2$. 令 $y=y_1-y_2$，$x=\pm(x_1-x_2)>0$，故有

$$sy\equiv\pm x(\mathrm{mod}\,p), \tag{3}$$

这里 $0<y<\sqrt{p}$，$0<x<\sqrt{p}$.

因为$(y,p)=1$，故有整数 y^{-1} 满足 $yy^{-1}\equiv 1(\mathrm{mod}\,p)$，(3)给出 $s\equiv\pm xy^{-1}(\mathrm{mod}\,p)$，于是，(2)给出 $x^2(y^{-1})^2+1\equiv 0(\mathrm{mod}\,p)$，故$x^2+y^2\equiv 0(\mathrm{mod}\,p)$. 而 $0<x^2+y^2<2p$，便有 $x^2+y^2=p$. 表法唯一同前一证法. 证完

类似的方法可以证明拉格朗日的一个定理：每一个正整数都能表成四个整数的平方和. 下一节，我们就来证明这个定理.

§9 表正整数为平方和

为了证明每一个正整数能表成四个整数的平方和，需要以下的恒等式.

$$(b_1^2+b_2^2+b_3^2+b_4^2)(x_1^2+x_2^2+x_3^2+x_4^2)=y_1^2+y_2^2+y_3^2+y_4^2, \tag{1}$$

此处

$$y_1=b_1x_1+b_2x_2+b_3x_3+b_4x_4,$$

$$y_2=b_1x_2-b_2x_1+b_3x_4-b_4x_3,$$

$$y_3=b_1x_3-b_3x_1+b_4x_2-b_2x_4,$$

$$y_4=b_1x_4-b_4x_1+b_2x_3-b_3x_2.$$

恒等式(1)可以直接验证，也可以用下面的方法推出.

显然，有恒等式

$$(aa'+bb')(cc'+dd')=(ac+bd)(a'c'+b'd')+$$

$$+(ad'-bc')(a'd-b'c). \tag{2}$$

令 $a=b_1+ib_2, b=b_3+ib_4, c=x_1-ix_2, d=x_3-ix_4,$

$a'=b_1-ib_2, b'=b_3-ib_4, c'=x_1+ix_2, d'=x_3+ix_4,$

代入(2)式，即可得出(1)式.

定理 每一个正整数都能表成四个整数的平方和.

证 由于 $1=1^2+0^2+0^2+0^2$, $2=1^2+1^2+0^2+0^2$ 以及恒等式(1)，只需证明每一个奇素数都能表成四个整数的平方和.

先来证明，如果 p 是一个奇素数，则有整数 x, y, m 存在使得

$$1+x^2+y^2=mp,\quad 0<m<p.$$

$\frac{1}{2}(p+1)$个整数 $x^2\left(0\leqslant x\leqslant\frac{1}{2}(p-1)\right)$模 p 不同余，$\frac{1}{2}(p+1)$个整数 $-1-y^2\left(0\leqslant y\leqslant\frac{1}{2}(p-1)\right)$ 模 p 也不同余，这两组数共有 $p+1$ 个，而模 p 只有 p 个剩余，故在这两组中，必然存在着两个彼此模 p 同余的 x^2 和 $-1-y^2$，这就得出了

$$x^2\equiv -1-y^2(\mathrm{mod}\,p),$$

或

$$1+x^2+y^2=mp,$$

又因 $0<1+x^2+y^2<1+2\left(\frac{1}{2}p\right)^2<p^2$，故有 $0<m<p$.

以上证明了 p 有一个正的倍数能表成四个整数的平方和. 因此，p 有一个最小的正倍数能表成四个整数的平方和，记为

$$m_0p=x_1^2+x_2^2+x_3^2+x_4^2,\quad 0<m_0<p. \tag{3}$$

现在来证明 $m_0=1$. 否则，可设 $1<m_0<p$. 先证明，m_0 是奇数. 假定 m_0 是偶数，则 $x_1+x_2+x_3+x_4$ 是偶数，因此或者① x_1, x_2, x_3, x_4 都是偶数，或者②它们全是奇数，或者③它们当中有两个奇数和两个偶数，可设 x_1, x_2 是偶数，x_3，x_4 是奇数. 无论哪一种情形，都给出

$$x_1+x_2, x_1-x_2, x_3+x_4, x_3-x_4$$

全为偶数. 因此，由(3)可得

$$\frac{1}{2}m_0p=\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2,$$

即$\frac{1}{2}m_0p$ 能表成四个整数的平方和，这与 m_0 的定义矛盾，故 m_0 是奇数.

由于 m_0 是奇数，故 $m_0\geqslant 3$. x_1, x_2，x_3，x_4 不能全被 m_0 所除尽，因为，否则由(3)将有 $m_0^2 \mid m_0p$，这与$1<m_0<p$ 矛盾. 于是，由第一章 §2 中的结果知，可选择整数 q_1, q_2, q_3, q_4 使得

$$x_i=q_im_0+y_i \qquad (i=1,2,3,4) \tag{4}$$

满足

$$|y_i|<\frac{1}{2}m_0 (i=1,2,3,4),$$

和

$$y_1^2+y_2^2+y_3^2+y_4^2>0,$$

故有

$$0<y_1^2+y_2^2+y_3^2+y_4^2<4\left(\frac{1}{2}m_0\right)^2=m_0^2.$$

再由(3)和(4)得

$$y_1^2+y_2^2+y_3^2+y_4^2\equiv x_1^2+x_2^2+x_3^2+x_4^2\equiv 0 (\mathrm{mod}\, m_0),$$

即

$$y_1^2+y_2^2+y_3^2+y_4^2=m_0m_1,\ 0<m_1<m_0. \tag{5}$$

由恒等式(1)及(3)、(5)两式即知有四个整数 z_1, z_2, z_3, z_4 使得

$$m_0^2 m_1 p = z_1^2 + z_2^2 + z_3^2 + z_4^2, \tag{6}$$

且由恒等式(1)及(3)、(4)两式得

$$z_1 = \sum_{i=1}^{4} x_i y_i \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 (\mathrm{mod} m_0),$$

$$z_2 = x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 \equiv 0 (\mathrm{mod} m_0),$$

$$z_3 = x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4 \equiv 0 (\mathrm{mod} m_0),$$

$$z_4 = x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2 \equiv 0 (\mathrm{mod} m_0),$$

故可写 $z_i = m_0 t_i (i = 1, 2, 3, 4)$，代入(6)式即得

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2,$$

这与 m_0 的定义矛盾. 这就证明了 $m_0 = 1$. 证完

第四章 习 题

1. 分别求出模 23 和 37 的二次剩余和二次非剩余.

2. 用 § 1 的定理 2 指出下列同余式解的个数:

① $x^2 \equiv 3 (\mathrm{mod} 31)$,

② $x^2 \equiv 2 (\mathrm{mod} 31)$,

③ $x^2 \equiv 6 (\mathrm{mod} 31)$.

3. 用高斯引理计算 $\left(\frac{7}{19}\right)$, $\left(\frac{11}{23}\right)$的值.

4. 求出以 -2 为模 p 二次剩余的素数 p 的一般表达式和以 -2 为模 p 二次非剩余的素数 p 的一般表达式.

5. 在上题中把 -2 换为 -3.

6. 证明: 如果 $p \equiv \pm 1 (\mathrm{mod} 10)$, 则$\left(\frac{5}{p}\right) = 1$; 如果 $p \equiv \pm 3 (\mathrm{mod} 10)$, 则 $\left(\frac{5}{p}\right) = -1$, 其中 p 是一个奇素数.

7. 证明: 如果素数 $p = 4n + 1$, 且 $d | n$, 则$\left(\frac{d}{p}\right) = 1$.

8. 证明: 若 $n > 0$, $4n + 3$ 和 $8n + 7$ 皆为素数, 则麦什涅数 M_{4n+3} 是复合

数，且 $8n+7 \mid M_{4n+3}$.

9. 解下列同余式：

① $x^2 \equiv 3 \pmod{37}$,

② $x^2 \equiv 23 \pmod{101}$,

③ $x^2 \equiv 5 \pmod{41}$,

④ $x^2 \equiv 2 \pmod{311}$,

⑤ $x^2 \equiv 2 \pmod{17}$,

⑥ $x^2 \equiv 89 \pmod{256}$,

⑦ $x^2 = 24 \pmod{25}$,

⑧ $x^2 \equiv 19 \pmod{90}$,

⑨ $8x^2+15x-6 \equiv 0 \pmod{56}$,

⑩ $x^2+x+4 \equiv 0 \pmod{32}$.

10. 设 $f(x)$是一个整值多项式(即当 x 取整数时，$f(x)$取整值)，证明：

① 当$(a,p)=1$时，

$$\sum_{x \bmod p} \left(\frac{f(ax+b)}{p}\right) = \sum_{x \bmod p} \left(\frac{f(x)}{p}\right),$$

$$\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = 0,$$

其中 $x \bmod p$ 表示 x 过模 p 的完全剩余系.

② $$\sum_{x=1}^{p-1} \left(\frac{f(x)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{ax+b}{p}\right) = -\left(\frac{a}{p}\right),$$

其中 $f(x)=x(ax+b)$, $(a,p)=(b,p)=1$.

11. 设 $\alpha=1$ 或 -1, $\beta=1$ 或 -1, $N(\alpha,\beta)$表示 $1,2,\cdots,p-2$ 中使得

$$\left(\frac{x}{p}\right)=\alpha, \quad \left(\frac{x+1}{p}\right)=\beta$$

的整数 x 的个数. 证明

$$4N(\alpha,\beta) = \sum_{x=1}^{p-2} \left(1+\alpha\left(\frac{x}{p}\right)\right)\left(1+\beta\left(\frac{x+1}{p}\right)\right),$$

且用练习 10 推出

$$4N(\alpha,\beta) = p-2-\beta-\alpha\beta-\alpha\left(\frac{-1}{p}\right).$$

特别地，给出

$$N(1,1)=\frac{p-4-\left(\frac{-1}{p}\right)}{4},$$

$$N(-1,-1)=N(-1,\ 1)=\frac{p-2+\left(\frac{-1}{p}\right)}{4},$$

$$N(1,-1)=1+N(1,1).$$

12. 用11题的结论，证明对任一个素数 p，存在整数 x 和 y 使得

$$x^2+y^2+1\equiv 0 \pmod{p}$$

成立.

13. 设 p 是一个奇素数，证明各等式：

① 如果 $p\equiv 1 \pmod 4$，则 $\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)=0$；

② 如果 $p\equiv 1 \pmod 4$，则 $\sum_{\substack{r=1\\(\frac{r}{p})=1}}^{p-1} r=\frac{p(p-1)}{4}$；

③ 如果 $p\equiv 3 \pmod 4$，则

$$\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right)=p\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right);$$

④ 如果 $p\equiv 1 \pmod 4$，则

$$\sum_{r=1}^{p-1} r^3\left(\frac{r}{p}\right)=\frac{3}{2}p\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right);$$

⑤ 如果 $p\equiv 3 \pmod 4$，则

$$\sum_{r=1}^{p-1} r^4\left(\frac{r}{p}\right)=2p\sum_{r=1}^{p-1} r^3\left(\frac{r}{p}\right)-p^2\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right).$$

14. 证明：若素数 $p\equiv 3 \pmod 4$，$q=\frac{p-1}{2}$，则

① $\left(1-2\left(\frac{2}{p}\right)\right)\sum_{r=1}^{q} r\left(\frac{r}{p}\right)=p\frac{1-\left(\frac{2}{p}\right)}{2}\sum_{r=1}^{p}\left(\frac{r}{p}\right)$.

② $\left(\left(\frac{2}{p}\right)-2\right)\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)-p\sum_{r=1}^{q}\left(\frac{r}{p}\right)$.

15. 证明：设 $q=2h+1$ 是一个素数，$q\equiv 7(\mathrm{mod}8)$，则

$$\sum_{r=1}^{h} r\left(\frac{r}{q}\right)=0.$$

16. 证明：若 $n>0$，且对任意的 $x,y,(x,y)=1$，则

$$x^{2^n}+y^{2^n}$$

的每一个奇因数具有形状 $2^{n+1}k+1, k>0$.

17. 证明：若 $F_n=2^{2^n}+1, n>1$，则 F_n 的任一素因数具有形状 $p=2^{n+2}k+1, k>0$.

*18. 证明：设 $p\neq 2,3,5,11,17$ 是一个素数，则存在 p 的三个不同的二次剩余 r_1,r_2,r_3，使得

$$r_1+r_2+r_3\equiv 0(\mathrm{mod}p).$$

19. 证明：设 $m^2>1$，则对任意的 n,m，

$$\frac{4n^2+1}{m^2+2},\ \frac{4n^2+1}{m^2-2},\ \frac{n^2-2}{2m^2+3},\ \frac{n^2+2}{3m^2+4}$$

没有一个是整数.

*20. 证明：设 $p=4n+1$ 是一个素数，则

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{k^2}{p}\right]=\frac{(p-1)(p-5)}{24}.$$

*21. 证明不定方程

$$4xyz-x-y-t^2=0$$

无正整数解 x,y,z,t.

22. 证明：如果 $n>0$ 适合

$$\sigma(n)=2n+1,$$

则 n 是一个奇数的平方.

*23. 证明：设 $n>1$，则

$$2^n-1\nmid 3^n-1.$$

24. 证明：若 $p\equiv 1(\mathrm{mod}6)$，则 p 可表为 $p=x^2+3y^2$，且表法唯一.

25. 证明：设 q 是一个形如 $4n+1$ 的素数，则存在一个奇素数 $p<q$，使

得$\left(\frac{q}{p}\right)=-1$.

26. 证明：

① 若 $q=8k+3$ 为素数，则 $q\mid 2^{4k+1}+1$.

② 若 $q=8k-3$ 为素数，则 $q\mid 2^{4k-2}+1$.

27. 证明：若 p 是一个形如 $4l+1$ 的素数，则 $p^k(k\geqslant 1)$ 能本原的表为二平方和，且表法唯一.

28. 证明：设 $N=6119=82^2-5\cdot 11^2$，素数 $p\mid N$，则 $\left(\frac{5}{p}\right)=1$，用这个方法把 N 分解成标准分解式.

29. 证明：对任一个素数 p，同余式

$$x^{2^n}\equiv 2^{2^{n-1}}\pmod{p},\quad n\geqslant 3$$

都有解 x.

30. 设 $a>0,b>0,b$ 为奇数，证明雅可比符号

$$\left(\frac{a}{2a+b}\right)=\begin{cases}\left(\frac{a}{b}\right), & \text{如 } a\equiv 0 \text{ 或 } 1\ (\mathrm{mod}4),\\ -\left(\frac{a}{b}\right), & \text{如 } a\equiv 2 \text{ 或 } 3\ (\mathrm{mod}4).\end{cases}$$

31. 证明：若 $a>0,b>0,c>0,(a,b)=1$，且 $2\nmid b,b<4ac$，则

$$\left(\frac{a}{4ac-b}\right)=\left(\frac{a}{b}\right)$$

32. 证明：若 $2\mid m$，m 能本原的表成二平方和，则 $\frac{m}{2}$ 也能本原的表成二平方和.

第五章　原　　根

本章将介绍次数，原根，指数等重要概念，证明原根存在的充分必要条件，原根的某些性质，以及一些求次数和原根的方法等.

§1　整数的次数

设 $m>0,(a,m)=1$，考虑 a 的正方幂

$$a, a^2, a^3, \cdots.$$

由欧拉定理，有 $a^{\varphi(m)} \equiv 1(\mathrm{mod}m)$. 这里，我们感兴趣的是使 $a^l \equiv 1(\mathrm{mod}m)$成立的最小正整数 l.

定义　设 $m>0,(m,a)=1$，l 是使

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

成立的最小正整数，则 l 叫做 a 对模 m 的**次数**.

我们有以下的定理.

定理 1　设 a 对模 m 的次数为 l，$a^n \equiv 1(\mathrm{mod}m)$，$n>0$，则 $l|n$.

证　如果结论不成立，则必有两整数 q 和 r，使

$$n=ql+r,\ 0<r<l,$$

而

$$1 \equiv a^n = a^{ql+r} = a^{ql} \cdot a^r \equiv a^r(\mathrm{mod}m).$$

这就和 l 的定义相违背.　　证完

推论　设 a 对模 m 的次数为 l，则 $l|\varphi(m)$.

定理 2　设 a 对模 m 的次数为 l，则

$$1, a, a^2, \cdots, a^{l-1}$$

对模 m 两两不同余.

证 如果结论不成立，则有某对 $j,k,0\leqslant j<k\leqslant l-1$，使

$$a^j\equiv a^k(\mathrm{mod}m),$$

则有

$$a^{k-j}\equiv 1(\mathrm{mod}m).$$

而 $0<k-j\leqslant l-1$，与 a 对模 m 的次数是 l 矛盾. 证完

定理 3 设 a 对模 m 的次数为 l，$\lambda>0$，a^λ 对模 m 的次数为 l_1，则 $l_1=\dfrac{l}{(\lambda,l)}$.

证 由

$$a^{\lambda l_1}\equiv 1(\mathrm{mod}m),$$

故 $l\mid\lambda l_1$，即得 $\dfrac{l}{(\lambda,l)}\Big|\dfrac{\lambda}{(\lambda,l)}\cdot l_1$，而 $\left(\dfrac{l}{(\lambda,l)},\dfrac{\lambda}{(\lambda,l)}\right)=1$，可得

$$\frac{l}{(\lambda,l)}\Big|l_1. \tag{1}$$

另一方面，

$$(a^\lambda)^{\frac{l}{(\lambda,l)}}=a^{l\cdot\frac{\lambda}{(\lambda,l)}}\equiv 1(\mathrm{mod}m),$$

故

$$l_1\Big|\frac{l}{(\lambda,l)}. \tag{2}$$

由(1)和(2)知 $l_1=\dfrac{l}{(\lambda,l)}$. 证完

推论 设 a 对模 m 的次数为 l，则 $\varphi(l)$ 个数

$$a^\lambda,\ (\lambda,l)=1,\ 0<\lambda\leqslant l.$$

对模 m 的次数均为 l.

显然，同一个模 m 的剩余类中的数，对模 m 的次数都是相同的，以上推论给出的 $\varphi(l)$ 个数虽然次数相同，却对模 m 两两不同余. 对于 $m=p$ 是一个素数，我们有以下定理.

定理 4 设 p 是一个素数，如果存在整数 a，它对模 p 的次数

是 l，则恰有 $\varphi(l)$ 个对模 p 两两不同余的整数，它们对模 p 的次数都为 l.

证 由于 a 对模 p 的次数为 l，定理 2 告诉我们

$$a, a^2, \cdots, a^{l-1}, a^l \tag{3}$$

模 p 两两不同余，因此它们是同余式

$$x^l \equiv 1 (\mathrm{mod} p) \tag{4}$$

的全部解. 由此可见，次数为 l 的对模 p 两两不同余的整数，包含在(3)中.

设(3)中的任一数为

$$a^\lambda, \quad 1 \leqslant \lambda \leqslant l,$$

由定理 3 知，a^λ 的次数为 l，当且仅当 $(\lambda, l)=1$，这就证明了若整数 a 对模 p 的次数为 l，则恰有 $\varphi(l)$ 个整数对模 p 两两不同余，它们的次数均为 l. 证完

设 a 对模 p 的次数为 l，由定理 1 的推论知 $l \mid p-1$. 那么，是否对每一个 l，都有 $\varphi(l)$ 个模 p 互不同余的整数，它们的次数是 l？下面的定理回答了这个问题.

定理 5 设 $l \mid p-1$，则次数是 l 的，模 p 互不同余的整数的个数是 $\varphi(l)$ 个.

证 设 $l \mid p-1$，$\psi(l)$ 代表 $1, 2, \cdots, p-1$ 中对模 p 次数为 l 的个数. 因为 $1, 2, \cdots, p-1$ 中任一个数的次数都等于且只等于 $p-1$ 的某一因数，故 $\psi(l) \geqslant 0$，且

$$\sum_{l \mid p-1} \psi(l) = p-1. \tag{5}$$

另一方面，熟知，对于欧拉函数有

$$\sum_{l \mid p-1} \varphi(l) = p-1, \tag{6}$$

定理 4 告诉我们，$\psi(l)=0$ 或 $\varphi(l)$，从而 $\psi(l) \leqslant \varphi(l)$. 故由

(5),(6)得到和式

$$\sum_{l\mid p-1}(\varphi(l)-\psi(l))=0,$$

它的左端的每一项都是非负的. 所以设 $l\mid p-1$, 必须有 $\psi(l)=\varphi(l)$. 证完

§2 原 根

上一节的定理 5 指出,存在 $\varphi(p-1)$个互不同余的整数,对模 p 的次数为 $p-1$, 这样的整数就叫 p 的原根. 一般地, 有如下的定义.

定义 设整数 $m>0$, $(g,m)=1$, 如果整数 g 对 m 的次数为 $\varphi(m)$,则 g 叫做 m 的一个**原根**.

定理 1 设$(g,m)=1,m>0$, 则 g 是 m 的一个原根的充分必要条件是

$$g,g^2,\cdots,g^{\varphi(m)} \tag{1}$$

组成模 m 的一组缩系.

证 由 §1 的定理 2 知, 若 g 为原根, 则(1)中任意两个数对模 m 不同余,又由$(g,m)=1$,故(1)组成模 m 的一组缩系.

反之,若(1)组成模 m 的一组缩系,故$(g,m)=1$, 进而由第二章 §3 定理 4 得 $g^{\varphi(m)}\equiv 1(\mathrm{mod}m)$,所以对任一 s, $1\leqslant s<\varphi(m)$, $g^s\not\equiv 1(\mathrm{mod}m)$,故 g 是 m 的一个原根. 证完

定理 1 说明了原根的重要性. 如果 g 是 m的一个原根,那么,模 m 的一组缩系可表成形为(1) 的几何级数. 这在处理某些问题时,非常有用. 然而,并非所有的正整数都有原根. 我们有以下的定理.

定理 2 设 $m>1$, 若 m 有原根, 则 m 必为下列诸数之一: 2, $4,p^l,2p^l$,

这里 $l\geqslant 1$，p 是奇素数.

证 设 m 的标准分解式为

$$m=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s},\ p_1<p_2<\cdots<p_s.$$

任一整数 a，$(a,p_i)=1(i=1,\cdots,s)$，必适合

$$a^{\varphi(p_i^{l_i})}\equiv 1(\mathrm{mod}\,p_i^{l_i})\qquad (i=1,\cdots,s).$$

令 $\alpha=[\varphi(p_1^{l_1}),\cdots,\varphi(p_s^{l_s})]$，则

$$a^{\alpha}\equiv 1(\mathrm{mod}\,p_i^{l_i})\ (i=1,\cdots,s).$$

而 $\alpha\leqslant\varphi(n)$，因此，当 $\alpha\neq\varphi(n)$时，则 m 无原根存在. 显然，当且仅当 $\varphi(p_1^{l_1}),\cdots,\varphi(p_s^{l_s})$两两互素时，$\alpha=\varphi(n)$. 当 $p>2$ 时，$\varphi(p^l)$为偶数，故当 m 具有两个不同的奇素因数时，m 没有原根. 即 m 有原根，m 必为 2^{l_1}，p^l，2^tp^l($l_1>0$，$l>0$，$t>0$) 三种形状之一. 若 $t>1$，则 $\varphi(2^t)=2^{t-1}$ 与 $\varphi(p^l)$不互素，故 $t=1$. 若 $m=2^{l_1}$，我们来证 $l_1\geqslant 3$ 时 m 没有原根. 因为 $(2,a)=1$ 时，$a^2\equiv 1(\mathrm{mod}2^3)$. 设 $a^{2^{e-3}}\equiv 1(\mathrm{mod}2^{e-1})$成立，则

$$a^{2^{e-2}}=(1+k2^{e-1})^2=1+k2^e+k^2\cdot 2^{2(e-1)}\equiv 1(\mathrm{mod}2^e).$$

故由归纳法，对任一个奇数 a，当 $e\geqslant 3$ 时，

$$a^{2^{e-2}}\equiv 1(\mathrm{mod}2^e),$$

此时 $\varphi(2^e)=2^{e-1}>2^{e-2}$，故当 $e>2$ 时，$m=2^e$ 没有原根. 这就证明了 $m\neq 2,4,p^l,2p^l$($l\geqslant 1$，p 为奇素数)时，m 没有原根. 证完

定理 3 $m=2,4,p^l,2p^l$($l\geqslant 1$，p 为奇素数)时，m 有原根.

证明定理 3 之前，我们首先证明下面的引理.

引理 设 g 是奇素数 p 的一个原根，满足

$$g^{p-1}\neq 1(\mathrm{mod}p^2),\tag{2}$$

则对于每一个 $\alpha\geqslant 2$，有

$$g^{\varphi(p^{\alpha-1})}\neq 1(\mathrm{mod}p^{\alpha}).\tag{3}$$

证 我们对 α 用归纳法. $\alpha=2$ 时，(3)即(2)，故定理成立. 设定理对 α ($\alpha\geqslant 2$)成立，即(3)成立. 由欧拉定理知

$$g^{\varphi(p^{\alpha-1})}\equiv 1(\mathrm{mod}p^{\alpha-1}).$$

故可设

$$g^{\varphi(p^{\alpha-1})}=1+kp^{\alpha-1},\ p\nmid k,$$

将上式两端自乘 p 次，可得

$$g^{\varphi(p^{\alpha})}=(1+kp^{\alpha-1})^{p}=1+kp^{\alpha}+k^{2}\frac{p(p-1)}{2}p^{2(\alpha-1)}+rp^{3(\alpha-1)},\tag{4}$$

其中 r 是一个整数. 因为 $2\alpha-1\geqslant\alpha+1, 3(\alpha-1)\geqslant\alpha+1$，故由(4)给出

$$g^{\varphi(p^{\alpha})}\equiv 1+kp^{\alpha}(\mathrm{mod}p^{\alpha+1}).$$

因为 $p\nmid k$，故上式给出

$$g^{\varphi(p^{\alpha})}\not\equiv 1(\mathrm{mod}p^{\alpha+1}),$$

故(3)对 $\alpha+1$ 成立. 证完

定理 3 的证明:

$m=2$ 时，1 即为原根. $m=4$ 时，3 即为 4 的原根.

设 $m=p^{l}$，p 是奇素数，$l=1$ 时，已经知道 p 有原根存在，设 g 为 p 的原根. 如果 $g^{p-1}\not\equiv 1(\mathrm{mod}p^{2})$，取 $r=g$；若 $g^{p-1}\equiv 1(\mathrm{mod}p^{2})$，则取 $r=g+p$，也是 p 的元根，且

$$r^{p-1}-1=(g+p)^{p-1}-1\equiv g^{p-1}+(p-1)pg^{p-2}-1$$
$$\equiv -pg^{p-2}\not\equiv 0(\mathrm{mod}p^{2}).$$

现在我们来证明 r 是 $p^{l}(l\geqslant 2)$ 的原根. 设 r 对模 p^{l} 的次数为 t，因为 $r^{t}\equiv 1(\mathrm{mod}p^{l})$，故也有 $r^{t}\equiv 1(\mathrm{mod}p)$，由 r 是 p 的原根，即得 $\varphi(p)\mid t$，写

$$t=\varphi(p)q.\tag{5}$$

因为 $t\mid\varphi(p^{l})$，故 $\varphi(p)q\mid\varphi(p^{l})$. 但是 $\varphi(p^{l})=p^{l-1}(p-1)$，因此 $q\mid p^{l-1}$. 设 $q=p^{\beta}$，这里 $\beta\leqslant l-1$. 如果 $\beta<l-1$，(5)给出 $t=p^{\beta}\varphi(p)$，且 $t\mid\varphi(p^{l-1})$，于是推出

$$r^{\varphi(p^{l-1})}\equiv 1(\mathrm{mod}p^l). \tag{6}$$

但由引理知,(6)是不可能的. 这就证明了 $\beta=l-1$,即 $t=\varphi(p^l)$, r 是 p^l 的一个原根.

设 $m=2p^l$, p 是奇素数,令 g 是 p^l 的一个原根,我们来证明当 g 是奇数时, g 也是 $2p^l$ 的一个原根. 因为 $(g,2p^l)=1$,故

$$g^{\varphi(2p^l)}\equiv 1(\mathrm{mod}2p^l).$$

设 g 对模 $2p^l$ 的次数为 b,则

$$b\mid\varphi(2p^l)=\varphi(p^l). \tag{7}$$

又

$$g^b\equiv 1(\mathrm{mod}p^l),$$

故

$$\varphi(p^l)\mid b. \tag{8}$$

(7)和(8)给出 $b=\varphi(2p^l)$. 如果 g 是偶数,则 $g+p^l$ 是奇数.

证完

以上我们证明了整数 $m>1$ 有一个原根的充分必要条件是 m 为下列诸数中的一个: $2,4,p^l,2p^l$,其中 $l\geqslant 1$, p 是奇素数. 下面的定理告诉我们,对每一个这样的 m,有多少个原根.

定理 4 设 m 有一个原根 g,则 m 恰有 $\varphi(\varphi(m))$ 个对模 m 不同余的原根,它们由集

$$S=\{g^t\mid 1\leqslant t\leqslant\varphi(m),(t,\varphi(m))=1\}$$

中的数给出.

证 由§1的定理3知 S 中的每一个数对模 m 的次数均为 $\varphi(m)$,即都是 m 的原根. 反之,设 a 是 m 的任一个原根,则存在某个 k, $1\leqslant k\leqslant\varphi(m)$,满足

$$g^k\equiv a(\mathrm{mod}m).$$

因为 a 是 m 的原根,故 g^k 的对模次数为 $\varphi(m)$,另一方面,由§1

的定理 3，g^k 对模 m 的次数又为 $\frac{\varphi(m)}{(m,k)}$，故推出 $(m,k)=1$，即 a 与 S 中的一数模 m 同余. 又集 S 中的数模 m 两两不同余，这就证明了 S 给出了 m 的全部互不同余的原根，共 $\varphi(\varphi(m))$ 个. 证完

§3 计算次数的方法

设整数 a 满足 $(a,m)=1$，$m>0$，a 对模 m 的次数为 l. 因为 $l\mid\varphi(m)$，故次数 l 可通过计算

$$a^{d_1},\ a^{d_2},\ \cdots,\ a^{d_s}$$

模 m 的值求出，这里 $d_1,d_2,\cdots,d_s$ 是 $\varphi(m)$ 的诸因子.

现在给出两个便于计算次数的结果.

定理 1 如果 $m=p_1^{l_1}\cdots p_k^{l_k}$ 是 m 的标准分解式，整数 a 对模 m 的次数等于整数 a 对模 $p_i^{l_i}(i=1,\cdots,k)$ 的诸次数的最小公倍数.

证 设 f_i 表示 a 对模 $p_i^{l_i}$ 的次数 $(i=1,\cdots,k)$，$d=[f_1,\cdots,f_k]$，则由

$$a^d\equiv 1(\mathrm{mod}\,p_i^{l_i})\ (i=1,\cdots,k),$$

得

$$a^d\equiv 1(\mathrm{mod}\,m).$$

如果 d 不是 a 对模 m 的次数，则设 a 的次数为 d'，$0<d'<d$，由

$$a^{d'}\equiv 1(\mathrm{mod}\,m),$$

可得

$$a^{d'}\equiv 1(\mathrm{mod}\,p_i^{l_i})\ (i=1,\cdots,k),$$

故 $f_i\mid d'(i=1,\cdots,k)$，与 d 是 $f_1,\cdots,f_k$ 的最小公倍数矛盾. 证完

定理 2 设 p 是一个素数，a 对模 p^j 的次数是 f_j，则 $f_{j+1}=f_j$ 或 $f_{j+1}=pf_j$. 又设 $p^i\parallel a^{f_2}-1$，进而有

$$f_j=\begin{cases}f_2, & \text{如果 } 2\leqslant j\leqslant i;\\ p^{j-i}f_2, & \text{如果 } j>i.\end{cases}$$

证 因为 $a^{f_j}\equiv 1(\mathrm{mod}p^j)$，故$(a^{f_j})^k\equiv 1(\mathrm{mod}p^j)$，且

$$\sum_{k=0}^{p-1}(a^{f_j})^k\equiv\sum_{k=0}^{p-1}1\equiv p(\mathrm{mod}p^j),$$

从而，

$$\sum_{k=0}^{p-1}(a^{f_j})^k\equiv 0(\mathrm{mod}p).$$

故可得

$$a^{pf_j}-1=(a^{f_j}-1)\Big(\sum_{k=0}^{p-1}(a^{f_j})^k\Big)\equiv 0(\mathrm{mod}p^{j+1}).$$

由此得

$$f_{j+1}\mid pf_j, \tag{1}$$

又因 $a^{f_{j+1}}\equiv 1(\mathrm{mod}p^j)$，故

$$f_j\mid f_{j+1}. \tag{2}$$

由(1)和(2)便知 $f_{j+1}=f_j$ 或 pf_j.

由于 $p^i\| a^{f_2}-1$，故 $f_j\mid f_2(j=2,\cdots,i)$. 另一方面，由于 $j=2,\cdots,i$ 时，$a^{f_j}\equiv 1(\mathrm{mod}p^j)$ 可推出 $a^{f_j}\equiv 1(\mathrm{mod}\ p^2)$，故 $f_2\mid f_j$，从而 $f_2=f_j(j=2,\cdots,i)$. 对于 $j>i$，则 $p^j\nmid a^{f_2}-1$，因此，由 $f_{i+1}=f_i$ 或 pf_i，必须有 $f_{i+1}=pf_i$，否则，由 $f_{i+1}=f_i=f_2$，与 $p^{i+1}\nmid a^{f_2}-1$ 矛盾. 由于 $f_{i+2}=f_{i+1}$ 或 pf_{i+1}，必须有 $f_{i+2}=pf_{i+1}$，否则由

$$a^{f_{i+1}}-1=a^{pf_i}-1=(a^{f_i}-1)\Big(\sum_{k=0}^{p-1}(a^{f_i})^k\Big)\equiv 0(\mathrm{mod}p^{i+2})$$

和

$$\sum_{k=0}^{p-1}(a^{f_i})^k\equiv p(\mathrm{mod}p^i),$$

推出

$$a^{f_i}-1\equiv 0(\mathrm{mod}\,p^{i+1}).$$

故 $f_{i+1}\mid f_i$，与 $f_{i+1}=pf_i$ 矛盾. 同理可证 $f_{i+2}=pf_{i+1},\cdots$，故 $f_{i+1}=pf_2, f_{i+2}=pf_{i+1}=p^2f_2, f_{i+3}=pf_{i+2}=p^3f_2,\cdots, f_j=p^{j-i}f_2$.

证完

例 1 设 $a=2$，$m=45=5\cdot 9$，2 对模 5 的次数是 4，2 对模 9 的次数是 6，故 2 对模 45 的次数为 $[4,6]=12$.

例 2 设 $a=7, p=2$，求 7 对模 2^{10} 的次数 f_{10}.

因为 $f_1=1$，$f_2=2$，且 $7^2-1=48$，$2^4\|48$，故 $f_{10}=2^{10-4}\cdot 2=2^7=128$.

§4 计算原根的方法

设 $(g,m)=1, m=p^l$ 或 $2p^l$，p 是一个奇素数，判断 g 是否是 m 的原根，不需要逐一计算 $g^1, g^2,\cdots, g^{\varphi(m)-1}$，而只需计算 $g^t(\mathrm{mod}\,m)$，这里 $t\mid\varphi(m)$. 基于这样的想法，我们有下面的定理.

定理 1 设 $m>2$，$\varphi(m)$ 的所有不同的素因子是 q_1，q_2，$\cdots$，q_s，$(g,m)=1$，则 g 是 m 的一个原根的充分必要条件是

$$g^{\frac{\varphi(m)}{q_i}}\not\equiv 1(\mathrm{mod}\,m)\qquad (i=1,2,\cdots,s). \tag{1}$$

证 若 g 是模 m 的一个原根，则 g 对模 m 的次数是 $\varphi(m)$，但 $0<\frac{\varphi(m)}{q_i}<\varphi(m)\ (i=1,\cdots,s)$，故 (1) 成立.

反之，若 (1) 成立，设 g 对模 m 的次数是 f，假定 $f<\varphi(m)$，因 $f\mid\varphi(m)$，所以 $\frac{\varphi(m)}{f}$ 是大于 1 的整数. 故有某个素因数 $q_i\Big|\frac{\varphi(m)}{f}$，即 $\frac{\varphi(m)}{f}=q_iu$，于是 $\frac{\varphi(m)}{q_i}=fu$，

$$g^{\frac{\varphi(m)}{q_i}}=g^{fu}\equiv 1(\mathrm{mod}\,m).$$

这与(1)矛盾,故 $f=\varphi(m)$,即 g 是 m 的一个原根. 证完

例 1 12 是 41 的一个原根.

设 $m=41, \varphi(41)=2^3\cdot 5, q_1=2, q_2=5, 12^{20}\equiv 40\not\equiv 1 \pmod{41}$, $12^8\equiv 18\not\equiv 1 \pmod{41}$,故由定理 1 知 12 是 41 的一个原根.

我们在§2中证明原根存在的充分必要条件时知道,求 $m=p^l$, $2p^l$ 的原根,归结为求奇素数 p 的原根. 下面我们介绍一种基于定理 2 的求 p 的原根的方法.

定理 2 设 a 对模奇素数 p 的次数是 $d, d<p-1$,则

$$a^\lambda, \lambda=1,2,\cdots,d$$

都不是 p 的原根.

证 因为 $a^\lambda(\lambda=1,\cdots,d)$对模 p 的次数为 $\dfrac{d}{(\lambda,d)}$, 而 $\dfrac{d}{(\lambda,d)}\leqslant d<p-1$,所以 $a^\lambda(\lambda=1,\cdots,d)$都不是 p 的原根. 证完

要求 p 的原根,先列出数

$$1,2,\cdots,p-1. \tag{2}$$

取 $a=2$,计算 2 对 p 的次数 d,如果 $d=p-1$,2 就是 p 的原根. 如果 $d<p-1$,在(2)中除去以下各数

$$\langle 2\rangle_p, \langle 2^2\rangle_p, \cdots, \langle 2^d\rangle_p.$$

在(2)中剩下的数中再取一数, 重复以上方法, 直到(2)中剩下 $\varphi(p-1)$个数, 因为对奇素数 p, 恰有 $\varphi(p-1)$个原根, 因此这 $\varphi(p-1)$个数都是 p 的原根.

例 2 求出 41 的原根.

列出

$$1,2,3,\cdots,40. \tag{3}$$

因为 2 对模 41 的次数为 20,在(3)中除去以下各数

2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25,

9, 18, 36, 31, 21, 1,

其次取 3，因为 3 对模 41 的次数是 8，因此在(3)中除去

3, 9, 27, 40, 38, 32, 14, 1,

其中 1, 9, 32, 40 第一次已除去，(3)中尚剩下 $\varphi(40)$ 个数

6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35,

它们都是 41 的原根.

§5 原根的一个性质

设 p 是一个奇素数，$Q(p)$ 表示 p 的互不同余的 $\varphi(p-1)$ 个原根的和，我们有

定理 1 $Q(p)\equiv\mu(p-1)(\mathrm{mod}p)$,

这里 $\mu(n)$ 表示麦比乌斯函数.

1952 年，莫勒(Moller)推广了定理 1，得到下面的结果.

定理 2 设 p 是一个奇素数，对模 p 次数为 d 的 $\varphi(d)$ 个互不同余的数的 r 次幂和为 S，则

$$S\equiv\frac{\varphi(d)}{\varphi(d_1)}\mu(d_1)(\mathrm{mod}p),$$

这里 $d_1=\dfrac{d}{(r,d)}$.

证明定理 2 之前，先证一个引理.

引理 设 $f(n)$ 是一个数论函数，

$$S'(n)=\sum_{\substack{1\leqslant j\leqslant n\\(j,n)=1}}f(j),$$

则

$$S'(n)=\sum_{d\mid n}\mu(d)(f(d)+f(2d)+\cdots+f(n)).$$

证 设 $\delta_j=(j,n)$，$j=1,\cdots,n$，由第三章 §2 定理 1 知

$$\sum_{d\mid m}\mu(d)=\begin{cases}1,\text{若 } m=1;\\0,\text{若 } m>1.\end{cases}$$

故有

$$S'(n)=\sum_{\substack{1\leqslant j\leqslant n\\(j,n)=1}}f(j)=\sum_{j=1}^{n}f(j)\sum_{d\mid\delta_j}\mu(d)$$

$$=\sum_{j=1}^{n}f(j)\sum_{\substack{d\mid j\\d\mid n}}\mu(d)=\sum_{d\mid n}\mu(d)\sum_{k=1}^{\frac{n}{d}}f(kd).$$

其中最后一个等式，是对和式$\sum_{j=1}^{n}f(j)\sum_{\substack{d\mid j\\d\mid n}}\mu(d)$中具有相同的$\mu(d)$的各项$\mu(d)f(j)$归并在一起，当$j$取$1,\cdots,n$中所有$d$的倍数，便得所有这样的项，把$\mu(d)$提出来便得$\mu(d)\sum_{k=1}^{\frac{n}{d}}f(kd)$，当$d$过$n$的全部因子时，便得到了$\sum_{d\mid n}\mu(d)\sum_{k=1}^{\frac{n}{d}}f(kd)$. 证完

定理2的证明：

设整数t对模p的次数为d，则

$$t^{\lambda},\ 1\leqslant\lambda\leqslant d,\ (\lambda,d)=1 \tag{1}$$

给出$\varphi(d)$个互不同余的对模p次数为d的整数. 由§1的定理3知，t^r模p的次数为d_1，我们来讨论$\varphi(d)$个数

$$t^{r\lambda},\ 1\leqslant\lambda\leqslant d,\ (\lambda,d)=1, \tag{2}$$

对模p，有多少个是相等的. 设

$$t^{rj},\ 1\leqslant j\leqslant d_1,\ (j,d_1)=1. \tag{3}$$

我们来证明，对于(3)中每一个t^{rj}，(2)中恰有$\frac{\varphi(d)}{\varphi(d_1)}$个数和它模$p$同余. 由第二章§9知集

$$\{j+kd_1,\ (j,d_1)=1,\ d_1\geqslant j\geqslant 1,$$

$$k\quad 0,1,\cdots,\frac{d}{d_1}-1\}$$

中与 d 互素的个数为 $\frac{\varphi(d)}{\varphi(d_1)}$ 个，而 $1\leqslant j+kd_1\leqslant d$，可知恰有 $\frac{\varphi(d)}{\varphi(d_1)}$ 个 λ，满足 $1\leqslant\lambda\leqslant d$，$(\lambda,d)=1$，且能表成 $j+kd_1$，对这样的 λ，有

$$t^{r\lambda}=t^{r(j+kd_1)}=t^{rj+krd_1}\equiv t^{rj}\pmod{p}.$$

设 $t^r\equiv a\pmod{p}$，故

$$S=\sum_{\substack{\lambda=1\\(\lambda,d)=1}}^{d}t^{r\lambda}\equiv\frac{\varphi(d)}{\varphi(d_1)}\sum_{\substack{j=1\\(j,d_1)=1}}^{d_1}t^{rj}\equiv\frac{\varphi(d)}{\varphi(d_1)}\sum_{\substack{j=1\\(j,d_1)=1}}^{d_1}a^j,$$

而由引理知

$$\sum_{\substack{j=1\\(j,d_1)=1}}^{d_1}a^j=\sum_{h\mid d_1}\mu(h)\left(a^h+a^{2h}+\cdots+a^{\frac{d_1}{h}\cdot h}\right)$$

$$=\sum_{h\mid d_1}\mu(h)\frac{a^{d_1}-1}{a^h-1}\cdot a^h.$$

而当 $0<h<d_1$ 时，$a^h\not\equiv1\pmod{p}$，$a^{d_1}\equiv1\pmod{p}$，故

$$\sum_{\substack{j=1\\(j,d_1)=1}}^{d_1}a^j\equiv\mu(d_1)a^{d_1}\equiv\mu(d_1)\pmod{p},$$

即得

$$S\equiv\frac{\varphi(d)}{\varphi(d_1)}\mu(d_1)\pmod{p}.$$ 证完

在定理 2 中令 $r=1$，$d=p-1$，便得定理 1。

§6 指 数

如果 m 有一个原根 g，我们知道，数 $1,g,g^2,\cdots,g^{\varphi(m)-1}$ 组成模 m 的一组缩系。由于原根有上述重要性质，我们可以给出下面的定义。

定义 任一整数 n，$(n,m)=1$，必有唯一的整数 k，$0\leqslant k<\varphi(m)$，满足

$$n\equiv g^k(\mathrm{mod}m),$$

k 叫做 n 对模 m 的**指数**，以 $k=\mathrm{ind}_g n$ 表示，在不易引起混淆的情况下，把 $\mathrm{ind}_g n$ 简写成 $\mathrm{ind}n$.

指数具有类似对数的性质. 我们有下面的定理.

定理 1 设 g 是 m 的原根，如果 $(a,m)=(b,m)=1$，我们有

① $\mathrm{ind}(ab)\equiv \mathrm{ind}a+\mathrm{ind}b(\mathrm{mod}\varphi(m))$.

② $\mathrm{ind}a^n\equiv n\mathrm{ind}a(\mathrm{mod}\varphi(m))$，这里 $n\geqslant 1$.

③ $\mathrm{ind}1=0, \mathrm{ind}g=1$.

④ $\mathrm{ind}(-1)=\dfrac{\varphi(m)}{2}$，这里 $m>2$.

⑤ 设 g_1 也是 m 的一个原根，则

$$\mathrm{ind}_g a\equiv \mathrm{ind}_{g_1}a\cdot \mathrm{ind}_g g_1(\mathrm{mod}\varphi(m)).$$

证 ① 设 $ab\equiv g^{\mathrm{ind}(ab)}(\mathrm{mod}m)$，$a\equiv g^{\mathrm{ind}a}(\mathrm{mod}m)$，$b\equiv g^{\mathrm{ind}b}(\mathrm{mod}m)$，则有

$$g^{\mathrm{ind}(ab)}\equiv g^{\mathrm{ind}a+\mathrm{ind}b}(\mathrm{mod}m).$$

故

$$\mathrm{ind}(ab)\equiv \mathrm{ind}a+\mathrm{ind}b(\mathrm{mod}\varphi(m)).$$

② 设 $a^n\equiv g^{\mathrm{ind}a^n}(\mathrm{mod}m)$，$a\equiv g^{\mathrm{ind}a}(\mathrm{mod}m)$，则有

$$g^{\mathrm{ind}a^n}\equiv a^n\equiv (g^{\mathrm{ind}a})^n=g^{n\mathrm{ind}a}(\mathrm{mod}m),$$

故

$$\mathrm{ind}a^n\equiv n\mathrm{ind}a(\mathrm{mod}\varphi(m)).$$

③ 显然.

④ 设 $m>2$，则 $\varphi(m)\equiv 0(\mathrm{mod}2)$. 由于 $m=4$ 时结论是显然的，故只需证 $m=p^\alpha$ 或 $2p^\alpha$（p 是奇素数）时结论成立.

由

$$g^{\varphi(m)}\equiv 1(\mathrm{mod}p^\alpha)$$

得

$$(g^{\frac{\varphi(m)}{2}}-1)(g^{\frac{\varphi(m)}{2}}+1)\equiv 0(\mathrm{mod}p^{\alpha}),$$

由于 $p^{\alpha}\mid g^{\frac{\varphi(m)}{2}}-1$ 或 $p^{\alpha}\mid g^{\frac{\varphi(m)}{2}}+1$，$g$ 是 p^{α} 的原根，故

$$g^{\frac{\varphi(m)}{2}}\equiv -1(\mathrm{mod}p^{\alpha}).$$

对于 $m=2p^{\alpha}$ 的情形，同理可得 $g^{\frac{\varphi(m)}{2}}\equiv -1(\mathrm{mod}p^{\alpha})$，因为 $(2,g)=1$，故 $g^{\frac{\varphi(m)}{2}}\equiv -1(\mathrm{mod}2)$，故得

$$g^{\frac{\varphi(m)}{2}}\equiv -1(\mathrm{mod}2p^{\alpha}).$$

⑤ 由 §2 定理 4，$g_1\equiv g^{l}(\mathrm{mod}m)$，$1\leqslant l\leqslant\varphi(m)$，$(l,\varphi(m))=1$，则

$$g^{\mathrm{ind}_g a}\equiv a\equiv g_1^{\mathrm{ind}_{g_1}a}\equiv g^{l\mathrm{ind}_{g_1}a}(\mathrm{mod}m),$$

故

$$\mathrm{ind}_g a\equiv l\mathrm{ind}_{g_1}a=\mathrm{ind}_g g_1\cdot\mathrm{ind}_{g_1}a(\mathrm{mod}\varphi(m)).$$

证完

利用原根，造出指数表，可以用来解同余式.

下面给出一个造表的简单例子.

例 1 $p=13$，它的全部原根是 2, 6, 7, 11，最小原根是 2，由下列取模得的诸同余式:

$$2^1\equiv 2,\ 2^2\equiv 4,\ 2^3\equiv 8,2^4\equiv 3,2^5\equiv 6,$$
$$2^6\equiv 12,2^7\equiv 11,2^8\equiv 9,2^9\equiv 5,2^{10}\equiv 10,$$
$$2^{11}\equiv 7,2^{12}\equiv 1(\mathrm{mod}13),$$

得出

N	0	1	2	3	4	5	6	7	8	9
0		12	1	4	2	9	5	11	3	8
1	10	7	6							

表 1

I	0	1	2	3	4	5	6	7	8	9
0		2	4	8	3	6	12	11	9	5
1	10	7	1							

表 2

表 1 是已知 N, 查 ind$N$; 表 2 是已知 ind$N$, 查 N.

例 2 解同余式

$$3x\equiv 11(\mathrm{mod}13). \tag{1}$$

解同余式(1)等价于解同余式

$$\mathrm{ind}3+\mathrm{ind}x\equiv \mathrm{ind}11(\mathrm{mod}12).$$

由表 1 得

$$\mathrm{ind}x\equiv 3(\mathrm{mod}12).$$

即得

$$\mathrm{ind}x=3,$$

故由表 2 得 $x=8$, 此即(1)的解.

指数表更重要的作用是解二项同余式.

定义 设 $k>0, m>0$, 一个形如

$$x^k\equiv n(\mathrm{mod}m)$$

的同余式, 叫做**二项同余式**.

定理 2 设 m 有原根 g, $(n, m)=1$, 二项同余式

$$x^k\equiv n(\mathrm{mod}m) \tag{2}$$

有解的充分必要条件是 $d=(k, \varphi(m))\mid \mathrm{ind}_g n$. 如果此同余式有解, 则恰有 d 个解.

证 设 $y=\mathrm{ind}_g x$, 考虑同余式

$$ky\equiv \mathrm{ind}_g n(\mathrm{mod}\varphi(m)). \tag{3}$$

设 x_1, x_2 是(2)的二个解, $x_1\equiv x_2(\mathrm{mod}m)$, 且 $(x_1, m)=(x_2, m)=1$, 由 $\mathrm{ind}_g x_1^k=\mathrm{ind}_g n$, $\mathrm{ind}_g x_2^k=\mathrm{ind}_g n$, 显然 $\mathrm{ind}_g x_1=y_1$, $\mathrm{ind}_g x_2=y_2$ 是

(3)的解. 因为 $\mathrm{ind}_g x_1 \not\equiv \mathrm{ind}_g x_2, 0 \leqslant \mathrm{ind}_g x_1, \mathrm{ind}_g x_2 < \varphi(m)$, 故它们是(3)的不同的解. 反之, 设 y_1, y_2 是(3)的二个解, $y_1 \not\equiv y_2 (\mathrm{mod}\varphi(m))$, $g^{y_1} \equiv x_1 (\mathrm{mod}m)$, 即 $\mathrm{ind}_g x_1 = y_1$, $g^{y_2} \equiv x_2 (\mathrm{mod}m)$, 即 $\mathrm{ind}_g x_2 = y_2$, 故得

$$x_1^k \equiv g^{y_1 k} \equiv g^{\mathrm{ind}_g n} \equiv n (\mathrm{mod}m).$$

同理

$$x_2^k \equiv n (\mathrm{mod}m),$$

且 $x_1 \not\equiv x_2 (\mathrm{mod}m)$. 这就证明了, 由(2)的不同解一定能得到(3)的不同解; 反过来也对. 而(3)有解的充分必要条件是 $d \mid \mathrm{ind}_g n$, 故(2)有解的充分必要条件也是 $d \mid \mathrm{ind}_g n$. 且当(2)有解时, 因为(3)恰有 d 个解, 故(2)也恰有 d 个解. 证完

例 3 解同余式

$$x^3 \equiv 5 (\mathrm{mod}13). \tag{4}$$

由定理 2, 只需解同余式

$$3\mathrm{ind}x \equiv \mathrm{ind}5 (\mathrm{mod}12). \tag{5}$$

由表 1 知 $\mathrm{ind}5 = 9$, 故 $(3, 12) = 3 \mid \mathrm{ind}5$, 便知(5)有三个解 $\mathrm{ind}x \equiv 3, 7, 11 (\mathrm{mod}12)$, 即 $\mathrm{ind}x = 3, 7, 11$. 由表 2 知 $x = 8$, $11, 7$ 是(4)的三个解.

指数表还可以用来解幂同余式

$$a^x \equiv b (\mathrm{mod}m), (b, m) = 1, \tag{6}$$

其中 m 有原根 g.

显然, (6)与同余式

$$x\mathrm{ind}_g a \equiv \mathrm{ind}_g b (\mathrm{mod}\varphi(m))$$

等价. 故(6)有解的充分必要条件是 $(\varphi(m), \mathrm{ind}_g a) \mid \mathrm{ind}_g b$, 且若有解, 恰有 $(\varphi(m), \mathrm{ind}_g a)$ 个解.

例 4 解幂同余式

$$2^x \equiv 3 (\mathrm{mod}13). \tag{7}$$

由(7)得

$$x\mathrm{ind}2\equiv\mathrm{ind}3(\mathrm{mod}12),$$

即得(7)的解 $x\equiv4(\mathrm{mod}12)$.

§7 一般缩系的构造

设 $m>0$, 如果 m 有原根 g, 我们知道模 m 的缩系可经 g 的方幂表出. 那么, 在一般情况下, 整数 $m>0$ 不存在原根, 它的缩系可经多少个数的乘方之积表出呢? 我们先讨论 $m=2^l$, $l\geqslant3$ 的情形.

定理 1 若 $l\geqslant3$, 则 5 对模 2^l 的次数为 2^{l-2}.

证 首先证明, 当 $a\geqslant3$ 时,

$$5^{2^{a-3}}\equiv1+2^{a-1}(\mathrm{mod}2^a). \tag{1}$$

$a=3$ 时, (1)显然成立. 现对 2 的方幂运用归纳法. 设(1)成立, 则有

$$5^{2^{a-2}}=(5^{2^{a-3}})^2=(1+2^{a-1}+k2^a)^2\equiv1+2^a\ (\mathrm{mod}2^{a+1}),$$

其中 k 为整数. 这就证明了, 当 $a\geqslant3$ 时, (1)式成立.

于是, $5^{2^{l-3}}\not\equiv1(\mathrm{mod}2^l)$, 而 $5^{2^{l-2}}\equiv1(\mathrm{mod}2^l)$, 即 5 对模 2^l 的次数为 2^{l-2}. 证完

定理 2 设 $l>2$, 对任一奇数 a, 必有一 $b\geqslant0$, 使

$$a\equiv(-1)^{\frac{a-1}{2}}5^b(\mathrm{mod}2^l),\ b\geqslant0. \tag{2}$$

证 如果 $a\equiv1(\mathrm{mod}4)$, 由定理 1,

$$5^b,\ 0\leqslant b<2^{l-2}$$

给出 2^{l-2} 个模 2^l 的不同数, 且每一个都 $\equiv1(\mathrm{mod}4)$. 因为模 2^l 的缩系 $1,3,5,7,\cdots,2^l-1$ 中, 恰有 2^{l-2} 个数 $\equiv1(\mathrm{mod}4)$, 这 2^{l-2}

个数所在的类，正好是全部 $4k+1$ 形状的数组成，故有 $b\geqslant 0$，使 $a\equiv(-1)^{\frac{a-1}{2}}5^b(\mathrm{mod}2^l)$.

如果 $a\equiv 3(\mathrm{mod}4)$，则 $-a\equiv 1(\mathrm{mod}4)$，有 $b\geqslant 0$，使 $-a\equiv 5^b(\mathrm{mod}2^l)$，即 $a\equiv(-1)^{\frac{a-1}{2}}5^b(\mathrm{mod}2^l)$，(2)仍成立.

证完

定理 3 设 $m=2^l p_1^{l_1}\cdots p_k^{l_k}$ 是 m 的标准分解式，其中 $l\geqslant 0$，$l_j>0(j=1,\cdots,k)$，设

$$\delta=\begin{cases}0, & l=0\text{ 或 }1,\\ 1, & l=2,\\ 2, & l>2,\end{cases}$$

则模 m 的缩系可由 $k+\delta$ 个数的乘方的乘积表出.

证 ① 设 $m=m_1m_2$，$(m_1,m_2)=1$，如果 $a_1,\cdots,a_{\varphi(m_1)}$ 是模 m_1 的一组缩系，由于 $(m_1,m_2)=1$，不妨设 $a_j\equiv 1(\mathrm{mod}m_2)(j=1,\cdots,\varphi(m_1))$. 同样可设 $b_1,\cdots,b_{\varphi(m_2)}$ 是模 m_2 的一组缩系，且 $b_j\equiv 1(\mathrm{mod}m_1)(j=1,\cdots,\varphi(m_2))$，则 $\varphi(m_1m_2)$ 个数

$$a_ib_j,\ i=1,\cdots,\varphi(m_1),\ j=1,\cdots,\varphi(m_2)$$

组成模 m_1m_2 的一组缩系，这是因为 $(a_ib_j,m_1m_2)=1$，且

$$a_ib_j\equiv a_sb_t(\mathrm{mod}m_1m_2),\tag{3}$$

推出

$$a_i\equiv a_s(\mathrm{mod}m_1),\ b_j\equiv b_t(\mathrm{mod}m_2),$$

故 $i=s$，$j=t$，即(3)中 $\varphi(m_1m_2)$ 个数模 m_1m_2 互不同余.

② 由于 p^l 和 $2p^l$（p 是奇素数）的缩系可由一个数的乘方表出，$2^l(l>1)$ 的缩系可由 δ 个数的乘方的乘积表出. 后者是因为当 $l=2$ 时，4 有原根 3，当 $l>2$ 时，由定理 2 可知.

由①和②可知模 m 的缩系可由 $k+\delta$ 个数的乘方的乘积表出.

证完

这个定理告诉我们，$(a,m)=1$，a 与 $k+\delta$ 个数的乘方的乘积

模 m 同余，这 $k+\delta$ 个乘方也叫 a 模 m 的**指数组**.

*§8 原根的一个应用

本节介绍原根在数字信号处理中的一个应用. 在数字信号处理中最重要的计算，是计算离散傅里叶变换.

定义 任给复数序列 $x_n(n=0,1,\cdots,N-1)$，变换

$$\begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N-1} \end{pmatrix} = T \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix} \tag{1}$$

称为离散傅里叶变换(DFT)，其中 T 是一个 n 阶复方阵

$$T=\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N & \cdots & W_N^{(N-1)} \\ 1 & W_N^2 & \cdots & W_N^{2(N-1)} \\ \vdots & \vdots & & \vdots \\ 1 & W_N^{(N-1)} & \cdots & W_N^{(N-1)^2} \end{pmatrix}, W_N=e^{-\frac{2\pi i}{N}}.$$

求出全部 N 个 $X_k(k=0,1,2,\cdots,N-1)$ 大约共需 N^2 次乘法和 N^2 次加法，当 N 很大时，运算量是相当大的. 六十年代出现了一种计算 DFT 的新算法，使乘、加法的次数大致降为 $N\log_2 N$，这就是著名的**快速傅里叶变换**(FFT). 但是，FFT 要求序列的长度 N 是一个 2 的方幂. 1968 年，雷德(Rader)利用原根把 N 是一个奇素数的 DFT 化成两个周期序列的互相关函数，再来计算它. 下面，我们就来介绍这一工作.

定义 设

$$a_0, a_1, \cdots, a_{N-1}, \cdots$$

和

$$b_0, b_1, \cdots, b_{N-1}, \cdots$$

是两个周期为N的序列，它们的**互相关函数**是指

$$B(l)=\sum_{i=0}^{N-1}a_ib_{i+l}\quad(l=0,1,\cdots,N-1).$$

我们把 DFT 写成以下的形状：

$$X_k=\sum_{n=0}^{N-1}x_nW_N^{nk}(k=0,1,\cdots,N-1),\ W_N=e^{-\frac{2\pi i}{N}},\quad(2)$$

定理 设$N=p$，p是一个奇素数，则(2)可化为两个周期为$p-1$的序列的互相关函数，和$2(p-1)$次加法来计算.

证 设$N=p$，

$$\overline{X}_k=\sum_{n=1}^{p-1}x_nW_p^{nk}(k=1,\cdots,p-1),\qquad(3)$$

则有

$$X_0=\sum_{n=0}^{p-1}x_n,\quad X_k=x_0+\overline{X}_k(k=1,\cdots,p-1).\qquad(4)$$

又设g是p的一个原根，则$1,2,\cdots,p-1$，可表为$\langle g^l\rangle_p(l=0,1,\cdots,p-2)$，于是(3)化为

$$X_{\langle g^l\rangle_p}=\sum_{m=0}^{p-2}x_{\langle g^m\rangle_p}W_p^{g^{l+m}},(l=0,1,\cdots,p-2).\qquad(5)$$

由于g是原根，所以(5)是两个周期为$p-1$的序列$a_u=x_{\langle g^u\rangle_p}(u=0,1,\cdots)$和$b_v=W_p^{g^v}(v=0,1,\cdots)$的互相关函数，再由(4)的$2(p-1)$次加法给出全部$X_0,X_1,\cdots,X_{p-1}$. 证完

对于$N=p^l$和$2p^l$(p是一个奇素数)，也有类似的结果.

第五章 习 题

1. 证明：m是一个素数的充分必要条件是存在某个a，a对模m的次

数为 $m-1$.

2. 设 g 是奇素数 p 的一个原根，证明：当 $p\equiv 1 \pmod 4$ 时，$-g$ 也是 p 的一个原根；当 $p\equiv 3 \pmod 4$ 时，$-g$ 对 p 的次数为 $\frac{p-1}{2}$.

3. 证明：若 p 是 $2^n+1 (n>1)$ 形的一个素数，则 3 是 p 的一个原根.

4. 证明：若 p 是 $4q+1$ 形（q 是一个素数）的素数，则 2 是 p 的一个原根.

5. 设 $m>2$，m 有原根存在，整数 a 满足 $(a, m)=1$. 如果存在整数 x 使 $x^2\equiv a \pmod m$，我们写 aRm. 证明：

① aRm 的充分必要条件是 $a^{\frac{\varphi(m)}{2}}\equiv 1 \pmod m$.

② 若 aRm，则同余式 $x^2\equiv a \pmod m$ 恰有两个解.

③ 恰有 $\frac{\varphi(m)}{2}$ 个整数 a，对模 m 互不同余，使得 $(a, m)=1, aRm$.

6. 设 $m>2$，$(a, m)=1$，aRm. 证明同余式 $x^2\equiv a \pmod m$ 恰有两个解的充分必要条件是 m 有一个原根.

7. 设 p 是一个奇素数，$n>1$，$S_n(p)=\sum_{k=1}^{p-1} k^n$，证明

$$S_n(p)\equiv\begin{cases}0 \pmod p, \text{ 如 } n\not\equiv 0 \pmod{p-1},\\ -1 \pmod p, \text{ 如 } n\equiv 0 \pmod{p-1}.\end{cases}$$

8. 证明：若 $p>3$ 是一个奇素数，则模 p 的 $\varphi(p-1)$ 个原根的乘积 $\equiv 1 \pmod p$.

*9. 证明：若 $n>1$，则

$$n\nmid 2^n-1.$$

10. 证明：若 $n>1$，$m>1$ 满足

$$1^n+2^n+\cdots+m^n=(m+1)^n,$$

则有

① p 是 m 的任一素因数时，$p-1\mid n$.

② $m=p_1\cdots p_s$，$p_i\neq p_j$ $(i\neq j)$ 是素数，且有

$$\frac{m}{p_i}+1\equiv 0 \pmod{p_i} \quad (i=1, \cdots, s).$$

11. 证明：设 $n=2^h+1$，$h>1$，则 n 是素数的充分必要条件是

$$3^{\frac{n-1}{2}}\equiv -1(\mathrm{mod}n).$$

12. 设 p 是一个奇素数，求同余式

$$x^{p-1}\equiv 1(\mathrm{mod}p^s),\quad s\geqslant 1$$

的全部解.

13. 求出 41^2 的一个原根.

14. 证明：如果素数 $p=2^\lambda+1$，$\left(\frac{a}{p}\right)=-1$，则 a 是 p 的一个原根.

15. 证明：对于 $a>1, n>0$，有 $n\mid\varphi(a^n-1)$.

16. 证明 7 是形如 $2^{4n}+1(n>0)$ 的素数的原根.

17. 证明：若 p 是奇素数，$2p+1$ 也是一个素数，当 $p\equiv 1(\mathrm{mod}4)$ 时，则 $2p+1$ 有原根 2；当 $p\equiv 3(\mathrm{mod}4)$ 时，$2p+1$ 有原根 -2.

18. 证明：如果 a 对奇素数 p 的次数是奇数，则同余式 $a^x+1\equiv 0(\mathrm{mod}p)$ 没有解.

19. 素数 71 有一个原根 7，求出 71 的所有原根以及求出 71^2 和 $2\cdot 71^2$ 的一个原根.

20. 用指数表解以下同余式：

① $8x\equiv 7(\mathrm{mod}43)$；

② $x^8\equiv 17(\mathrm{mod}43)$；

③ $8^x\equiv 3(\mathrm{mod}43)$.

21. 用指数表求出下列同余式解的个数：

① $x^{65}\equiv 17(\mathrm{mod}97)$；

② $x^{16}\equiv 46(\mathrm{mod}97)$；

③ $7x^7\equiv 11(\mathrm{mod}41)$；

④ $5x^{35}\equiv 37(\mathrm{mod}41)$.

22. 在与模 61 互素的剩余系中指出：

① 对模 61 次数为 10 的数；

② 61 的全部原根.

*23. 证明 3 是下列形式素数的原根：

$$2^np+1,\ n>1,\ p>\frac{3^{2^{n-1}}}{2^n},\ p\text{ 是奇素数}.$$

24. 设 p 是奇素数，$a>1$，证明：

① $q\mid a^n-1$，q 是奇素数，则 $q\mid a-1$ 或 $q\equiv 1(\mathrm{mod}2p)$，

② $q\mid a^n+1$，q 是奇素数，则 $q\mid a+1$ 或 $q\equiv 1(\mathrm{mod}2p)$.

25. 用本章节 § 4 定理 2 后面介绍的方法给出 37 和 73 的全部原根.

第六章　k 次剩余

我们在第四章中已经介绍了二次剩余理论，本章将介绍一般的 k 次($k>1$)剩余的基本性质和某些重要结果，它们不仅在数论的许多方面有用，而且在组合论中也有着重要应用.

§1　k 次剩余

设 $k>1, m>1$，二项同余式

$$x^k \equiv n \pmod{m},\ (n,m)=1. \tag{1}$$

我们有以下的定义.

定义　若(1)有解，则 n 叫做模 m 的 **k 次剩余**；若(1)无解，则 n 叫做模 m 的 **k 次非剩余**.

设 $m=p_1^{\alpha_1}\cdots p_l^{\alpha_l}$ 是 m 的标准分解式，则由第二章§7定理3知，n 是模 m 的 k 次剩余的充分必要条件是 n 是每一个模 $p_i^{\alpha_i}$ ($i=1,\cdots,l$) 的 k 次剩余. 因此，我们只需讨论 $m=p^\alpha$ 的情形，这里 $\alpha\geqslant 1$，p 是素数. 而本章着重讨论 p 是奇素数的情形，对于 $p=2$ 的情形，我们作为习题留给读者.

和二次剩余一样，如果 n 是模 p^α 的 k 次剩余，$n\equiv n_1 \pmod{p^\alpha}$，那么 n_1 也是模 p^α 的 k 次剩余，因此，当我们提到 k 次剩余的个数时，是指对 p^α 不同余的个数.

定理1　**设 p 是一个奇素数，$\alpha>0$，则有 $\varphi(p^\alpha)/(\varphi(p^\alpha),k)$ 个模 p^α 的 k 次剩余.**

证　设 g 是 p^α 的一个原根，由第五章§6定理2知同余式

$$x^k \equiv n \pmod{p^\alpha},\ p\nmid n \tag{2}$$

有解的充分必要条件是 $d=(k,\ \varphi(p^\alpha))\mid \mathrm{ind}_g n$. 于是 $\mathrm{ind}_g n=d$,

$2d, \cdots, \frac{\varphi(p^\alpha)}{d}\cdot d$, 即

$$g^d, g^{2d}, \cdots, g^{\frac{\varphi(p^\alpha)}{d}\cdot d} \tag{3}$$

是模 p^α 的全部 k 次剩余，这是因为(3)中的数对模 p^α 互不同余，且任一 k 次剩余与(3)中的一个数模 p^α 同余. 证完

推论 1 设 p 是一个奇素数，则有 $\frac{p-1}{(p-1,k)}$ 个模 p 的 k 次剩余.

定理 2 设 p 是一个奇素数，$p\nmid k$，则对所有的 α，当 n 是模 p 的 k 次剩余时，(2)恰有 $(p-1, k)$ 个解；n 是模 p 的 k 次非剩余时，(2)没有解.

证 由第五章 §6 定理 2 知，n 是模 p 的 k 次剩余时，$(k, p-1)\mid \mathrm{ind}_g n$，且 $x^k\equiv n(\mathrm{mod}\,p)$ $(p\nmid n)$ 恰有 $(k, p-1)$ 个解. 由于 $p\nmid k$. 故 $(k, \varphi(p^\alpha))=(k, p-1)$，取 g 为 p 和 p^α 的公共原根，故 $(k, \varphi(p^\alpha))\mid \mathrm{ind}_g n$，即(2)恰有 $(k, p-1)$ 个解. 当 n 是模 p 的 k 次非剩余时，显然，(2)无解. 证完

定理 3 设 p 是一个奇素数，$(k, \varphi(p^\alpha))=d$，则 n 是 p^α 的 k 次剩余的充分必要条件是 n 是 p^α 的 d 次剩余.

证 如果 n 是 p^α 的 k 次剩余，则 $(k, \varphi(p^\alpha))=d\mid \mathrm{ind} n$，而 $(d, \varphi(p^\alpha))=d$，故 n 是 p^α 的 d 次剩余. 反之也真.

证完

我们有下面的定义.

定义 设 $(k, \varphi(p^\alpha))=d$，当 $d=k$ 时，把模 p^α 的 k 次剩余叫做**真 k 次余剩**. 当 $d<k$ 时，把模 p^α 的 k 次剩余叫做**非真 k 次剩余**.

非真 k 次剩余，可归结为真 d 次剩余来讨论. 因此，今后我们只需讨论 p^α 的真 k 次剩余，即假设，总有 $k\mid \varphi(p^\alpha)$.

§2 问题的简化

在这一小节中，我们将指出，对于模 p^α 的真 k 次剩余的研究，可化为模 p 的真 k 次剩余的研究.

定义 设 $A=\{a_1,\cdots,a_t\}$, $B=\{b_1,\cdots,b_s\}$ 是两个整数集，则记

$$A\oplus B=\{a_i+b_j,\ i=1,\cdots,t,\ j=1,\cdots,s\}.$$

这里集 $A\oplus B$ 中的元允许有相同的①.

设 $R_k(m)$ 代表由 1，…，m 中全体 m 的 k 次剩余组成的集.

我们有下面的定理.

定理 1 设 p 是一个奇素数，且 $(k,p)=1$，则对于 $\alpha>1$，

$$R_k(p^\alpha)=R_k(p)\ominus\{tp\mid 0\leqslant t\leqslant p^{\alpha-1}-1\}. \tag{1}$$

证 设 r 是 $R_k(p)$ 中的一个数，则 $r, r+p,\cdots, r+(p^{\alpha-1}-1)p$ 给出了 $(0, p^\alpha)$ 中全体与 r 模 p 同余的 p 的 k 次剩余. 因为每一个模 p^α 的 k 次剩余，也是模 p 的 k 次剩余. 故有

$$R_k(p^\alpha)\subseteq R_k(p)\oplus\{tp\mid 0\leqslant t\leqslant p^{\alpha-1}-1\}. \tag{2}$$

因为(2)的右端的集，共含有 $\dfrac{p-1}{(p-1,k)}\cdot p^{\alpha-1}$ 个数，因为 $k\mid\varphi(p^\alpha)$，$(k,p)=1$，故 $k\mid p-1$，于是有

$$\frac{p-1}{(p-1,k)}\cdot p^{\alpha-1}=\frac{\varphi(p^\alpha)}{k},$$

即(2)的右端含有 $\dfrac{\varphi(p^\alpha)}{k}$ 个数，而 $R_k(p^\alpha)$ 也含 $\dfrac{\varphi(p^\alpha)}{k}$ 个数，故(1)成立.

定理 1 告诉我们，在 $(k,p)=1$ 时，对任一个 $\alpha>1$，求 p^α 的全部 k 次剩余，只需求出 p 的全部真 k 次剩余就行了. 对于 (k,p)

① 本节以及以下 §4—§8 诸节，所讨论的数集均指多重的，即在这样的集中，不要求元不同.

>1 的情形，我们有

定理 2 设 $k=p^{\alpha-1}q, \alpha>1, q|p-1$，则对于 $u>\alpha$，有

$$R_k(p^u)=R_k(p^\alpha)\oplus\{tp^\alpha|0\leqslant t\leqslant p^{u-\alpha}-1\}. \tag{3}$$

证 类似定理 1 的证明，我们有

$$R_k(p^u)\subseteq R_k(p^\alpha)\oplus\{tp^\alpha|0\leqslant t\leqslant p^{u-\alpha}-1\}, \tag{4}$$

而(4)的右端含有

$$\frac{\varphi(p^\alpha)}{(k,p^{\alpha-1}(p-1))}\cdot p^{u-\alpha}$$

个数，而 $k=p^{\alpha-1}q, q|p-1$，即含有 $\frac{\varphi(p^u)}{k}$ 个数. 而 $R_k(p^u)$ 中也含有 $\frac{\varphi(p^u)}{k}$ 个数，故(3)成立. 证完

定理 2 是定理 1 的推广，它指出当 $k=p^{\alpha-1}q, q|p-1$ 时，求出 $p^u(u>\alpha)$ 的全部 k 次剩余，只需求出 p^α 的全部 k 次剩余就行了.

定理 3 设 p 是一个奇素数，$k=p^{\alpha-1}q$，$q|p-1$，则 p^α 的 k 次剩余由 p 的 q 次剩余的 $p^{\alpha-1}$ 次方给出.

证 设 g 是 p^α 的一个原根，p^α 的全部 k 次剩余是

$$g^k, g^{2k}, \cdots, g^{\varphi(p^\alpha)}.$$

不妨设，g 也是 p 的原根，故 p 的全部 q 次剩余是

$$g^q, g^{2q}, \cdots, g^{\varphi(p)},$$

故有

$$g^{tq\cdot p^{\alpha-1}}=g^{tk}\quad\left(t=1,2,\cdots,\frac{\varphi(p)}{q}\right).$$

证完

对于模 p^α 的 k 次剩余，因为我们总假设 $k|\varphi(p^\alpha)$，故在 $(k,p^\alpha)>1$ 时，可设 $k=p^{e-1}q, e\leqslant\alpha, q|p-1$，故由定理 2 和定理 3，我们只需求出模 p 的 q 次剩余就行了. 综上所述，无论 $(k,p)=1$ 或 $(k,p)>1$，下面我们只需讨论模 p 的真 k 次剩余的情形，这里 p 是

一个奇素数.

§3 k 次剩余符号$\left(\frac{n}{p}\right)_k$

在给出 k 次剩余符号之前，我们先证明几个定理. 设 p 是一个奇素数，$k|p-1$，$p-1=kq$.

定理 1 n 是模 p 的一个 k 次剩余的充分必要条件是

$$n^q\equiv 1(\mathrm{mod}p).$$

证 设 n 是模 p 的一个 k 次剩余，则存在整数 x，$(x,p)=1$，满足

$$x^k\equiv n(\mathrm{mod}p),(n,p)=1,$$

故

$$n^q\equiv x^{qk}=x^{p-1}\equiv 1(\mathrm{mod}p).$$

反之，设

$$n^q\equiv 1(\mathrm{mod}p),$$

g 是 p 的一个原根，则有

$$q\mathrm{ind}_g n\equiv 0(\mathrm{mod}(p-1)),$$

即

$$\mathrm{ind}_g n\equiv 0\left(\mathrm{mod}\frac{p-1}{q}\right),$$

因此 $k|\mathrm{ind}_g n$，即 n 是模 p 的一个 k 次剩余. 证完

定理 2 设 $(p,n)=1$，则

$$\sum_{j=0}^{k-1}n^{jq}\equiv\begin{cases}k(\mathrm{mod}p),\text{若 }n\text{ 是模 }p\text{ 的 }k\text{ 次剩余},\\0(\mathrm{mod}p),\text{若 }n\text{ 是模 }p\text{ 的 }k\text{ 次非剩余}.\end{cases}$$

证 因为 $(n,p)=1$，我们有

$$n^{p-1}-1\equiv 0(\mathrm{mod}p),$$

即得

$$(n^q-1)(1+n^q+n^{2q}+\cdots+n^{(k-1)q})\equiv 0(\mathrm{mod}p). \qquad (1)$$

由定理 1，如果 n 是模 p 的一个 k 次剩余，则有

$$\sum_{j=0}^{k-1} n^{jq}\equiv k(\mathrm{mod}p).$$

如果 n 是模 p 的一个 k 次非剩余，由(1)得

$$\sum_{j=0}^{k-1} n^{jq}\equiv 0(\mathrm{mod}p). \qquad \text{证完}$$

在二次剩余理论中，我们曾引入勒让德符号$\left(\frac{n}{p}\right)$，并证明了$\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}}(\mathrm{mod}p)$. 这里，我们引入 k 次剩余符号的定义.

定义 设 $k>1$，p 是一个奇素数，$k\mid p-1$，$q=\frac{p-1}{k}$，符号

$$\left(\frac{n}{p}\right)_k=n^q \mathrm{mod}p,$$

叫做模 p 的 **k 次剩余符号**，这里 $n^q\mathrm{mod}p$ 表示 n^q 模 p 的绝对最小剩余. $\left($模 p 绝对的最小剩余组成的完全剩余系是指：$-\frac{p-1}{2},\cdots,-1,0,1,\cdots,\frac{p-1}{2}\right)$.

对于符号$\left(\frac{n}{p}\right)_k$ 有以下简单性质.

① $p\mid n$ 时，$\left(\frac{n}{p}\right)_k=0$，

② $n\equiv n_1(\mathrm{mod}p)$时，则有$\left(\frac{n}{p}\right)_k=\left(\frac{n_1}{p}\right)_k$.

这是因为

$$\left(\frac{n}{p}\right)_k\equiv n^q\equiv n_1^q\equiv\left(\frac{n_1}{p}\right)_k(\mathrm{mod}p),\text{故有}\left(\frac{n}{p}\right)_k=\left(\frac{n_1}{p}\right)_k.$$

③ 对任意的整数 n_1, n_2，有 $\left(\frac{n_1 n_2}{p}\right)_k \equiv \left(\frac{n_1}{p}\right)_k \left(\frac{n_2}{p}\right)_k \pmod{p}$.

④ 如 $\mathrm{ind}_g n \equiv a \pmod{k}, 0 \leqslant a < k$，则 $\left(\frac{n}{p}\right)_k \equiv g^{aq} \pmod{p}$. 这是因为 $\left(\frac{n}{p}\right)_k \equiv n^q \equiv g^{(\mathrm{ind}_g n) q} \equiv g^{aq}$，故有此结论.

⑤ n 是模 p 的 k 次剩余的充分必要条件是 $\left(\frac{n}{p}\right)_k = 1$.

⑥ 设 $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ 是 n 的标准分解式，则有

$$\left(\frac{n}{p}\right)_k \equiv \left(\frac{p_1}{p}\right)_k^{\alpha_1} \cdots \left(\frac{p_t}{p}\right)_k^{\alpha_t} \pmod{p}.$$

不妨假设 $n < p$，那么只要对每一个小于 p 的素数 p_j，$\left(\frac{p_j}{p}\right)_k$ 的值都知道，$\left(\frac{n}{p}\right)_k$ 的值就不难求出了.

例 设 $p = 19, k = 3, q = 6$，于是

$$\left(\frac{-1}{19}\right)_3 = \left(\frac{1}{19}\right)_3 = 1;$$

$$\left(\frac{2}{19}\right)_3 = 7;$$

$$\left(\frac{3}{19}\right)_3 = \left(\frac{-16}{19}\right)_3 \equiv \left(\frac{-1}{19}\right)_3 \left(\frac{16}{19}\right)_3 \equiv \left(\frac{-1}{19}\right)_3 \left(\frac{2}{19}\right)_3^4 = \left(\frac{2}{19}\right)_3 = 7;$$

$$\left(\frac{5}{19}\right)_3 = \left(\frac{24}{19}\right)_3 \equiv \left(\frac{2}{19}\right)_3^3 \left(\frac{3}{19}\right)_3 = \left(\frac{3}{19}\right)_3 = 7;$$

$$\left(\frac{7}{19}\right)_3 = \left(\frac{45}{19}\right)_3 \equiv \left(\frac{3}{19}\right)_3^2 \left(\frac{5}{19}\right)_3 = 7^3 \equiv 1;$$

$$\left(\frac{11}{19}\right)_3 = \left(\frac{30}{19}\right)_3 \equiv \left(\frac{2}{19}\right)_3 \left(\frac{3}{19}\right)_3 \left(\frac{5}{19}\right)_3 = 7^3 \equiv 1;$$

$$\left(\frac{13}{19}\right)_3 = \left(\frac{32}{19}\right)_3 \equiv \left(\frac{2}{19}\right)_3^5 = -8;$$

$$\left(\frac{17}{19}\right)_3=\left(\frac{-2}{19}\right)_3\equiv\left(\frac{-1}{19}\right)_3\left(\frac{2}{19}\right)_3=7.$$

以上同余式都是取模 19.

由以上计算知，1, 7, 8, 11, 12, 18 是模 19 的六个三次剩余.

对于给定的 p 和 n，计算$\left(\frac{n}{p}\right)_k$是并不困难的. 但是，当 $k>2$ 时，对于给定的 n，$\left(\frac{n}{p}\right)_k=1$，求 p 是什么形状的奇素数是一个很困难的问题. 下面几节，就是讨论这一问题的.

*§ 4 类 C_j 的研究

设

$$S=\{1,2,3,\cdots,p-1\}.$$

因为，若 $n\equiv n_1(\mathrm{mod}\,p)$，则$\left(\frac{n}{p}\right)_k=\left(\frac{n_1}{p}\right)_k$，于是对于同一剩余类中的数，在我们研究$\left(\frac{n}{p}\right)_k$时，可以不加区别. 如无特别声明，在本节及以下各节中，把一个数集中的某一数换成其模 p 同余的数时，仍视为同一个数集，或者我们把一个数集中的数看作模 p 的最小非负剩余.

设 g 是 p 的原根，则

$$S=\{g^0,g^1,\cdots,g^{p-2}\},$$

现在对 S 中的各数，用它们 g 的方幂 $0,1,\cdots,p-2$ 对模 k 分类，这是一个等价分类，即有

$$C_j=\{g^j,g^{j+k},\cdots,g^{j+(q-1)k}\},\ j=0,1,2,\cdots,k-1,$$

这里 $qk=p-1$. 我们称 C_j 是一个类.

设 $c_{j,t}=g^j\cdot g^{tk}$，$t=0,1,\cdots,q-1$，则 C_j 可写成

$$C_j=\{c_{j,0},c_{j,1},\cdots,c_{j,q-1}\},$$

显然，$n\in C_j$，$n_1\in C_j$ 的充分必要条件是$\left(\frac{n}{p}\right)_k=\left(\frac{n_1}{p}\right)_k$.

定理 1

① C_0 由 p 的全体 k 次剩余组成.

② 设 $r_j\in C_j$，则

$$C_j=\{r_j, r_jg^k, r_jg^{2k}, \cdots, r_jg^{(q-1)k}\}.$$

证 ① 因为 $C_0=\{g^k, g^{2k}, \cdots, g^{\frac{p-1}{k}\cdot k}\}$，故 C_0 正好由 p 的全体 k 次剩余组成.

② 设 $r_j=g^{j+uk}$，$0\leqslant u\leqslant q-1$，则

$$g^{j+uk}, r_jg^k=g^{j+(u+1)k}, \cdots, r_jg^{(q-1)k}=g^{j+(u+q-1)k},$$

而

$$u, u+1, \cdots, u+q-1$$

过模 q 的一个完全剩余系，故

$$C_j=\{r_j, r_jg^k, \cdots, r_jg^{(q-1)k}\}.$$ 证完

为了研究各 C_j 之间的某些关系，我们需要引进某些记号.

设 A, B 是两个数集，在 §2 中，我们曾定义

$$A\oplus B=\{a+b\mid a\in A, b\in B\}.$$

显然对于数集来说，运算$\oplus$是可换的，也是满足结合律的. 例如，设 $A=\{1,2,2\}$，$B=\{1,2,3,4\}$，且 $p=5$，则在 $\bmod p$ 时，有

$$A\oplus B=\{2,3,4,5,3,4,5,6,3,4,5,6\}$$

$$=\{0,0,0,1,1,2,3,3,3,4,4,4\}.$$

设 t 是一个数，记

$$tA=\{ta\mid a\in A\},$$

于是有

$$t(A\oplus B)=tA\oplus tB.$$

设 $A=\{a_1, \cdots, a_m\}$，

$$A(t)=\{a_1,\cdots,\underbrace{a_{\cdot},\cdots,a_{m}}_{t\text{个}},\underbrace{\cdots,a_m}_{t\text{个}}\},$$

$$A(1)=A,A(0)=\varnothing(\text{空集}).$$

如果

$$A(t)\subset S_1,$$

且 S_1 中除 $A(t)$外，不再含其他 A 的元，则称 A 在 S_1 中的**频率为** t.

如果 S_1 正好由 $A(t_1)$的全体元和 $B(t_2)$的全体元组成，则记

$$S_1=A(t_1)+B(t_2).$$

如果 $A\cap B=\varnothing$，则 A 在 S_1 中的频率为 t_1，B 在 S_1 中频率为 t_2.

当 $A=B+C$ 时，记

$$A-B=C.$$

例如，当 $A=\{1,1,2,3,3,4,5,5,5\}$，和 $B=\{1,2,5,5\}$，则

$$C=\{1,3,3,4,5\}.$$

设 A 是一个数集，x 是一个实变量，则

$$F(A)=F(A,x)=\sum_{a\in A}x^a$$

称为 A 的**母函数**. 显然

$$F(A)F(B)=F(A\oplus B).$$

当我们把集 A 和集 B 间的关系，用它们的母函数来替代时，自然会遇到以上等式，这就是我们定义运算①的原因.

例 1 取 $p=13,k=3,g=2$，我们有

$$C_0=\{2^0,2^3,2^6,2^9\}=\{1,5,8,12\},$$

$$C_1=\{2,2\cdot5,2\cdot8,2\cdot12\}=\{2,3,10,11\},$$

$$C_2=\{2\cdot2,2\cdot3,2\cdot10,2\cdot11\}=\{4,6,7,9\}.$$

我们用 C 代表恰含 q 个 0 的集，则

$$C_0\oplus C_0=\{2,6,9,0,6,10,0,1,\ 9,0,3,7,0,\ 4,7,\ 11\}=C(1)$$

$+C_1(1)+C_2(2)$.

定理 2 设

$$C_j=\{g^j, g^{j+k}, \cdots, g^{j+(q-1)k}\},$$

则有

① $C_r=C_s$ 的充分必要条件是 $r\equiv s(\mathrm{mod}k)$;

② $g^kC_j=C_{j+k}$;

③ $g^k(C_0\ominus C_{j-k})=C_k\oplus C_j$;

④ 任一 $r_0\in C_0$, $r_0(C_k\oplus C_j)=C_k\oplus C_j$;

⑤ $C\oplus C_j=C_j(q)$.

证 ① 设 $C_r=C_s$, 故 $g^r\equiv g^{s+tk}(\mathrm{mod}p)$, 对于某个 t, $0\leqslant t\leqslant q-1$, 即

$$r\equiv s+tk(\mathrm{mod}p-1),$$

即 $r\equiv s(\mathrm{mod}k)$. 反之, 如 $r\equiv s(\mathrm{mod}k)$, 不失一般, 可设 $r=s+tk$, $t\geqslant 0$, 故 $g^r\in C_s$, 由定理 1 的②知, $C_r=C_s$.

②、③、④、⑤由定义直接可得. 证完

例 1 告诉我们, $C_0\oplus C_0$ 可表成 $C(1)$, $C_1(1)$, $C_2(2)$之和. 一般地, $C_i\oplus C_j$ 也具有这一性质, 由定理 2 知, 只需证明 $C_0\oplus C_j$ 的情形. 下一节就来讨论这一情形.

*§5 $C_0\oplus C_j$ 的讨论

设 g 是模 p 的一个原根,

$$C_j=\{g^j, g^{j+k}, \cdots, g^{j+(q-1)k}\},$$

因为

$$g^{\frac{p-1}{2}}\equiv -1(\mathrm{mod}p),$$

故

$$\{-g^j, -g^{j+k}, \cdots, -g^{j+(q-1)k}\}=C_{j+\frac{p-1}{2}}$$

也是一个类. 我们有下面的定义.

定义 称类 $C_{j+\frac{p-1}{2}}$ 是 C_j 的**共轭类**, 记为 C_j^*.

定理 1

$$C_j^*=\begin{cases}C_j, \text{如果 } q\equiv 0 \pmod 2,\\ C_{j+\frac{k}{2}}, \text{如果 } q\equiv 1 \pmod 2.\end{cases}$$

证 因为

$$\frac{p-1}{2}=\frac{kq}{2}\equiv\begin{cases}0 \pmod k, \text{如果 } q\equiv 0 \pmod 2,\\ \frac{k}{2} \pmod k, \text{如果 } q\equiv 1 \pmod 2,\end{cases}$$

由 §4 的定理 2 的①知定理成立. 证完

定理 2 集

$$C_0\oplus C_j=C(e_{j,0})+\sum_{t=0}^{k-1}C_t(a_{j,t}), \tag{1}$$

这里 $a_{j,t}\geqslant 0$ 是某个整数,

$$e_{j,0}=\begin{cases}1, \text{如 } C_j=C_0^*,\\ 0, \text{如 } C_j\neq C_0^*.\end{cases}$$

证 设

$$C_j=\{C_{j,0}, C_{j,1}, \cdots, C_{j,q-1}\}, j=0, 1, \cdots, k-1.$$

则

$$\begin{aligned}C_0\oplus C_j=\{&C_{0,0}+C_{j,0}, C_{0,0}+C_{j,1}, \cdots, C_{0,0}+C_{j,q-1},\\ &C_{0,1}+C_{j,0}, C_{0,1}+C_{j,1}, \cdots, C_{0,1}+C_{j,q-1}, \cdots,\\ &C_{0,q-1}+C_{j,0}, \cdots, C_{0,q-1}+C_{j,q-1}\},\end{aligned}$$

令

$$\begin{aligned}T_r&=\{c_{0,r-1}+c_{j,t+r-2}, t=1, 2, \cdots, q\},\\ &=\{g^{(r-1)k}+g^j\cdot g^{(t+r-2)k}, t=1, 2, \cdots, q\}\\ &=\{g^{(r-1)k}(1+g^{j+(t-1)k}), t=1, 2, \cdots, q\}\end{aligned}$$

$$=\{g^{(r-1)k}(c_{0,0}+c_{j,t-1}),t=1,2,\cdots,q\}.$$

又因为 $t=1,2,\cdots,q$ 时，$t+r-2$ 过 q 的一组完全剩余系，故

$$\begin{aligned}T_r&=\{g^{(r-1)k}+g^j\cdot g^{(t+r-2)k},t=1,2,\cdots,q\}\\&=\{g^{(r-1)k}+g^jg^{tk},t=1,2,\cdots,q\}\\&=\{c_{0,r-1}+c_{j,t},t=1,2,\cdots,q\}.\end{aligned}$$

于是可设

$$S=\sum_{i=1}^{q}T_i=C_0\oplus C_j.$$

对某个 t 值，如果 $c_{0,0}+c_{j,t-1}$ 属于某个类(包括类 C)，则对于每一个 $0<r\leqslant q$，由§4的定理1知 $g^{(r-1)k}(c_{0,0}+c_{j,t-1})$ 属于同一类．故对 $t=1,\cdots,q$，S 由 q 个类组成，但其中可能重复．C 或 C_e 在 S 中的频率，就看 C 或 C_e 中有多少个数属于集

$$U=\{c_{0,0}+c_{j,t-1},t=1,\cdots,q\}.$$

首先计算 C 在 S 中的频率，就看 U 中有多少个 0，而 $c_{0,0}+c_{j,t-1}=0$，当且仅当 $C_j=C_0^*$．由于 $C_0^*=C_{\frac{p-1}{2}}$，故 $j=\dfrac{p-1}{2}$，由 $c_{j,t-1}=-c_{0,0}$，得 $g^{\frac{p-1}{2}}\cdot g^{(t-1)k}\equiv g^{\frac{p-1}{2}}\pmod p$，即 $g^{(t-1)k}\equiv 1\pmod p$，故 $qk|(t-1)k$，$q|t-1$，$t=1$．

现设 C_e 在 S 中的频率为 $a_{j,e}$，即 U 中有 $a_{j,e}$ 个值属于 C_e，也就是 $a_{j,e}$ 是使得下式成立的 t 的个数：

$$c_{0,0}+c_{j,t-1}=c_{e,s-1},\quad \text{对于某个 } s,1\leqslant s\leqslant q.$$

故

$$S=C_{(e_j,0)}+\sum_{e=0}^{k-1}C_e(a_{j,e}),$$

即(1)式成立．　　证完

推论　我们有

$$\sum_{e=0}^{k-1} a_{j,e} = \begin{cases} q-1, & \text{如 } C_j = C_0^*, \\ q, & \text{如 } C_j \neq C_0^*. \end{cases}$$

证 因为每一个类有 q 个元，所以，当 $C_j = C_0^*$ 时，$e_{j,0} = 1$，故

$$q^2 = q + q\sum_{e=0}^{k-1} a_{j,e},$$

$$\sum_{e=0}^{k-1} a_{j,e} = q-1.$$

当 $C_j \neq C_0^*$ 时，$e_{j,0} = 0$，故

$$q^2 = q\sum_{e=0}^{k-1} a_{j,e},$$

$$\sum_{e=0}^{k-1} a_{j,e} = q.$$ 证完

从定理 2 的证明可以看出，C 或 C_e 在 $C_0 \oplus C_j$ 中的频率，等于 C 或 C_e 属于集

$$\{1 + c_{j,t-1}, t = 1, \cdots, q\}$$

中数的个数.

例 1 $p = 31, k = 5, g = 3,$

$C_0 = \{1, 26, 25, 30, 5, 6\},$

$C_1 = \{3, 16, 13, 28, 15, 18\},$

$C_2 = \{9, 17, 8, 22, 14, 23\},$

$C_3 = \{27, 20, 24, 4, 11, 7\},$

$C_4 = \{19, 29, 10, 12, 2, 21\}.$

我们把矩阵

$$\begin{pmatrix} 1 & 26 & 25 & 30 & 5 & 6 \\ 3 & 16 & 13 & 28 & 15 & 18 \\ 9 & 17 & 8 & 22 & 14 & 23 \\ 27 & 20 & 24 & 4 & 11 & 7 \\ 19 & 29 & 10 & 12 & 2 & 21 \end{pmatrix}$$

称为**类矩阵**.

为了求出 C 或 C_e 在 $C_0 \oplus C_j$ 中的频率，只需把类矩阵加上一个全幺矩阵，得

$$\begin{pmatrix} 2 & 27 & 26 & 0 & 6 & 7 \\ 4 & 17 & 14 & 29 & 16 & 19 \\ 10 & 18 & 9 & 23 & 15 & 24 \\ 28 & 21 & 25 & 5 & 12 & 8 \\ 20 & 30 & 11 & 13 & 3 & 22 \end{pmatrix}.$$

如果这矩阵中的任一元素 $b_{ij} \in C_r (0 \leqslant r \leqslant k-1)$，则将 b_{ij} 处换成 r，如 $b_{ij} \in C$，则将 b_{ij} 处换成记号 $*$，即得矩阵

$$\begin{pmatrix} 4 & 3 & 0 & * & 0 & 3 \\ 3 & 2 & 2 & 4 & 1 & 4 \\ 4 & 1 & 2 & 2 & 1 & 3 \\ 1 & 4 & 0 & 0 & 4 & 2 \\ 3 & 0 & 3 & 1 & 1 & 2 \end{pmatrix}.$$

这样 C 或 C_e 在 $C \oplus C_j$ 中的频率就是上面矩阵中第 j 行中 $*$ 或 e 的个数，故有

$$C_0 \oplus C_0 = C(1) + C_0(2) + C_1(0) + C_2(0) + C_3(2) + C_4(1),$$
$$C_0 \oplus C_1 = C(0) + C_0(0) + C_1(1) + C_2(2) + C_3(1) + C_4(2),$$
$$C_0 \oplus C_2 = C(0) + C_0(0) + C_1(2) + C_2(2) + C_3(1) + C_4(1),$$
$$C_0 \oplus C_3 = C(0) + C_0(2) + C_1(1) + C_2(1) + C_3(0) + C_4(2),$$
$$C_0 \oplus C_4 = C(0) + C_0(1) + C_1(2) + C_2(1) + C_3(2) + C_4(0).$$

不列 C 在 $C_0 \oplus C_j$ 中的频率，而把 C_0, C_1, C_2, C_3, C_4 在 $C_0 \oplus C_j$ 中的频

率作为下面矩阵的第 $j+1$ 行，即得

$$A_0=\begin{pmatrix}2&0&0&2&1\\0&1&2&1&2\\0&2&2&1&1\\2&1&1&0&2\\1&2&1&2&0\end{pmatrix}.$$

A_0 称为频率阵.

例2 取 $p=31$，$k=6$，和 $g=3$，重复例 1 的步骤，依次得以下四个矩阵：

$$\begin{pmatrix}1&16&8&4&2\\3&17&24&12&6\\9&20&10&5&18\\27&29&30&15&23\\19&25&28&14&7\\26&13&22&11&21\end{pmatrix},$$

$$\begin{pmatrix}2&17&9&5&3\\4&18&25&13&7\\10&21&11&6&19\\28&30&0&16&24\\20&26&29&15&8\\27&14&23&12&22\end{pmatrix},$$

$$\begin{pmatrix}0&1&2&2&1\\0&2&4&5&4\\2&5&5&1&4\\4&3&*&0&1\\2&5&3&3&0\\3&4&3&1&5\end{pmatrix},$$

$$A_0=\begin{pmatrix}1&2&2&0&0&0\\1&0&1&0&2&1\\0&1&1&0&1&2\\1&1&0&1&1&0\\1&0&1&2&0&1\\0&1&0&2&1&1\end{pmatrix}.$$

*§6 频率间的关系

可以看出，例1中的A_0是对称矩阵，而例2中 A_0的数满足$a_{j,h}=a_{h-s,j-s}$. 下面将证明这在一般情形下也是正确的.

定理1 C_h在$C_0\oplus C_j$中的频率和C_j在$C_0^*\oplus C_h$的频率相等.

证 在上节定理2的证明中，我们看到C_h在$C_0\oplus C_j$中的频率$a_{j,h}$为$1+C_{j,t-1}$, $t=1,\cdots,q$中，使$1+C_{j,t-1}\in C_h$的t的个数，换句话说，$a_{j,h}$是满足方程

$$1+C_{j,t-1}=C_{h,s-1},\quad 1\leqslant t,\quad s\leqslant q \tag{1}$$

的有序数对(t,s)的个数.

写(1)为

$$-1+C_{h,s-1}=C_{j,t-1},\quad 1\leqslant t,\quad s\leqslant q, \tag{2}$$

那么，在上节定理2的证明中，令

$$T_r=\{C_{\frac{p-1}{2},r-1}+C_{h,t+r-2},\ t=1,2,\cdots,q\}=\{g^{(r-1)k}(g^{\frac{p-1}{2}}+g^{h+(t-1)k}),\ t=1,\cdots,q\}=\{g^{(r-1)k}(-1+c_{h,t-1}),\ t=1,\cdots,q\},$$

因为$C_0^*=C_{\frac{p-1}{2}}$，故类似定理2的证明可知，C_j在$C_0^*\oplus C_h$中的频率为(2)的有序对(t,s)的个数，即为C_h在$C_0\oplus C_j$中的频率. 证完

推论1 设$q\equiv 0(\mathrm{mod}2)$，则$a_{j,h}=a_{h,j}$.

证 $q\equiv 0(\mathrm{mod}2)$时，因为$C_0^*=C_0$，故$a_{j,h}=a_{h,j}$.

证完

推论2 设$q\equiv 1(\mathrm{mod}2)$，则 $a_{j,h}=a_{h-\frac{k}{2},j-\frac{k}{2}}$.

证 当$q\equiv 1(\mathrm{mod}2)$时，有$C_0^*=C_{\frac{k}{2}}$，故

$$C_0^*\oplus C_h=C_{\frac{k}{2}}\oplus C_h=g^{\frac{k}{2}}(C_0\oplus C_{h-\frac{k}{2}})$$

$$=g^{\frac{k}{2}}\left(C(e_{h-\frac{k}{2},0})+\sum_{t=0}^{k-1}C_t(a_{h-\frac{k}{2},t})\right)$$

$$=C(e_{h-\frac{k}{2},0})+\sum_{t=0}^{k-1}C_{t+\frac{k}{2}}(a_{h-\frac{k}{2},t}). \qquad (3)$$

设$\langle t+\frac{k}{2}\rangle_k=r$，则当$t=0,1,\cdots,k-1$时，$r=0,1,\cdots,k-1$，且$t+\frac{k}{2}=fk+r$，$f$是整数，代入(3)得

$$C_0^*\oplus C_h=C(e_{h-\frac{k}{2},0})+\sum_{r=0}^{k-1}C_r(a_{h-\frac{k}{2},\,r-\frac{k}{2}}).$$

因此，C_j在$C_0^*\oplus C_h$中的频率为$a_{h-\frac{k}{2},\,j-\frac{k}{2}}$，即$a_{j,h}=a_{h-\frac{k}{2},\,j-\frac{k}{2}}$.

证完

定理2 我们有

$$a_{j,h}=a_{k-j,h-j}.$$

证 因为

$$g^j(C_0\oplus C_{k-j})=C_j\oplus C_k=C_j\oplus C_0=C_0\oplus C_j,$$

且

$$g^j(C_0\oplus C_{k-j})=g^j\left(C(e_{k-j,0})+\sum_{t=0}^{k-1}C_t(a_{k-j,t})\right)$$

$$=C(e_{k-j,0})+\sum_{t=0}^{k-1}C_{t+j}(a_{k-j,t})$$

$$=C(e_{k-j,0})+\sum_{r=0}^{k-1}C_r(a_{k-j,r-j}),$$

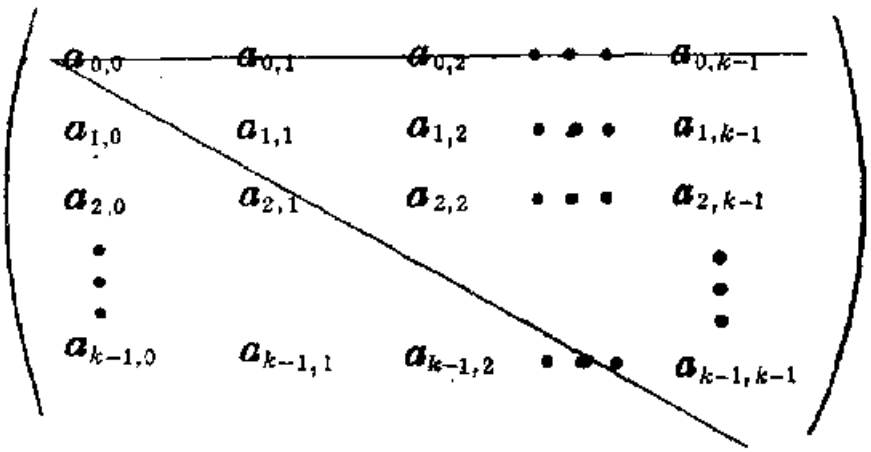
故

$$C_0\oplus C_j=C(e_{k-j,0})+\sum_{r=0}^{k-1}C_r(a_{k-j,r-j}).$$

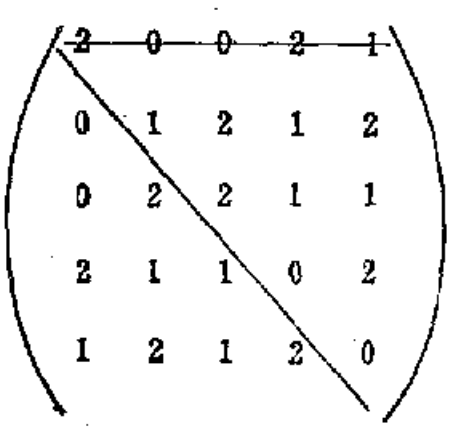
因$C_0\oplus C_j$表成诸C之和，表法是唯一的，故$a_{j,k}=a_{k-j,k-j}$.

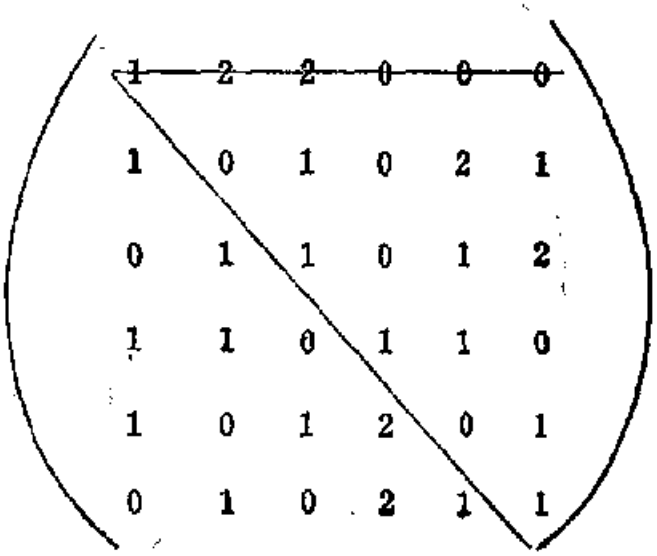
证完

定理 2 可如下形象地表示出来，在频率阵 A_0 中紧挨主对角线



下方画一平行直线，然后去掉第一行后，即可分成恒等的二块：上面一块的第一行就是下面一块的最后一行. 现以前一节的两个频率矩阵为例，有





对于频率阵

$$A_0=\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & \cdots & a_{0,k-1} \\ a_{1,0} & a_{1,1} & a_{1,2} & \cdots & a_{1,k-1} \\ \vdots & & & & \\ a_{k-1,0} & a_{k-1,1} & a_{k-1,2} & \cdots & a_{k-1,k-1} \end{pmatrix},$$

由定理 1 和定理 2 可知其中肯定有相同的元，因此，不需要k^2个符号来表A_0. 当$k=9, q\equiv 0(\mathrm{mod}2)$时，不难验证，反复用定理 1 和定理2，$A_0$只需$a_{0,j}(j=0,1,2,3,4,5,6,7,8)$，$a_{1,j}(j=2,3,4,5,6,7)$，$a_{2,j}(j=4,5,6)$，$a_{3,6}$，共 19 个符号就能把$A_0$表出了，依次用1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 来代表以上各记号(注意，这里不是频率的具体数字)，那么$k=9$时的频率阵可表为

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

一般地，设$N(k)$代表在一个k行k列频率阵A_0中不同记号的最大个数. 我们有下面的定理.

定理3 我们有

$$N(k)=\begin{cases} \dfrac{k^2+3k+6}{6}, & \text{若}k\equiv 0(\mathrm{mod}3), \\ \dfrac{k^2+3k+2}{6}, & \text{若}k\not\equiv 0(\mathrm{mod}3). \end{cases}$$

证 设$q\equiv 0(\mathrm{mod}2)$，我们有

$$a_{j,k}=a_{k,j}=a_{k-j,k-j}=a_{k-j,k-j}=a_{k-k,j-k}=a_{j-k,k-k}. \qquad (5)$$

下面我们将指出，对于(5)中的脚标可以都仅表某一个或二个或三个频率.

(5) 中的脚标都仅表一个频率的充分必要条件是$j=h=0$. 这是因为，当$j=h=0$时，显然(5)中的诸频率都为$a_{0,0}$. 反之，由$j\equiv j-h(\mathrm{mod}k)$，和$k-h\equiv j-h(\mathrm{mod}k)$，可推得$h\equiv j\equiv 0(\mathrm{mod}k)$. 不妨设$0\leqslant h, j<k$，故$h=j=0$.

对于$a_{0,j}(j=1, \cdots, k-1)$，(5) 中仅出现三个不同的频率$a_{j,0}=a_{0,j}=a_{k-j,k-j}$.

现设$a_{j,h}$, $j\neq 0$, $h\neq 0$, $j\neq h$，易知除开$3\mid k$的情形外，(5)均给出六个不同的频率. 因为矩阵含k^2个元，因此，当$k\neq 3$时，

$$N(k)=1+(k-1)+\frac{k^2-3(k-1)-1}{6}$$

$$=\frac{k^2+3k+2}{6}.$$

当$3\mid k$时，设$k=3t$, $j=t$, $h=2t$，(5)给出

$$a_{t,2t}=a_{2t,t},$$

而$j\neq t$时，(5)仍给出六个不同的频率. 所以当$3\mid k$时，

$$N(k)=1+(k-1)+1+\frac{k^2-1-3(k-1)-2}{6}$$

$$=\frac{k^2+3k+6}{6}.$$

当$q\equiv 1(\mathrm{mod}2)$时，用关系式

$$a_{j,h}=a_{h-\frac{k}{2},\ j-\frac{k}{2}}=a_{k-j,h-j}=a_{\frac{k}{2}-h,j-h}=a_{h-j-\frac{k}{2},\ \frac{k}{2}-j}=a_{j-h-\frac{k}{2},\ k-h}. \quad (6)$$

可类似证明. 此时，可设$k\equiv 0(\mathrm{mod}2)$. 在$j=0$, $h=\frac{k}{2}$时，(6)中恰

给出一个记号，在 $j=0$，$h\neq\frac{k}{2}$时，(6)中恰给出三个不同记号，此外，仅当$k=6t$，$j=2t$，$h=t$ 时，(6)中给出二个不同的记号 $a_{2t,t}=a_{4t,5t}$，其余，(6)均给出六个不同的记号. 证完

*§7 广频率阵

为简便起见，我们写

$$F_j=F(C_j)=\sum_{t\in C_j}x^t. \tag{1}$$

当我们处理母函数(1)时，我们采用以下规定：

① 当 $u\equiv v(\mathrm{mod}p)$时，$x^u=x^v$.

② 当$v+u\equiv s(\mathrm{mod}p)$时，$x^ux^v=x^s$.

③ 当$j\equiv h(\mathrm{mod}k)$时，$F_j=F_h$.

于是，运用前节的结果，我们可以证明下面的结果.

定理1

$$F_jF_h=F_hF_j=\sum_{t=0}^{k-1}a_{j-h,k-h+t}F_t+qe_{j,h} \tag{2}$$

这里$e_{j,h}=1$或 0 取决于 C_j和 C_h是否彼此共轭，$a_{u,t}$表示 C_t在 $C_0\oplus C_u$中的频率，满足：当$u\equiv v(\mathrm{mod}k)$，$t\equiv s(\mathrm{mod}k)$时，$a_{u,t}=a_{v,s}$.

证 由母函数的性质知

$$F_jF_h=F_hF_j=F(C_h\oplus C_j),$$

而

$$C_h\oplus C_j=g^h(C_0\oplus C_{j-h})=g^h\left(C(e_{j-h,0})+\sum_{r=0}^{k-1}C_r(a_{j-h,r})\right)$$

$$=C(e_{j-h,0})+\sum_{r=0}^{k-1}C_{r+h}(a_{j,h,r})$$

$$=C(e_{j-h,0})+\sum_{t=0}^{k-1}C_t(a_{j-h,t-k})$$

$$=C(e_{j-h,0})+\sum_{t=0}^{k-1}C_t(a_{j-h,k-h+t}).$$

因此

$$F(C_h\oplus C_j)=\sum_{t\in C_{h\oplus C_j}}x^t$$

$$=\sum_{t\in C(e_{j-h,0})}x^t+\sum_{t=0}^{k-1}\sum_{t\in C_t(a_{j-h,k-h+t})}x^t$$

$$=\sum_{t\in C(e_{j-h,0})}x^t+\sum_{t=0}^{k-1}a_{j-h,k-h+t}\sum_{t\in C_t}x^t$$

$$=\sum_{t\in C(e_{j-h,0})}x^t+\sum_{t=0}^{k-1}a_{j-h,k-h+t}F_t$$

$$=e_{j-h,0}q+\sum_{t=0}^{k-1}a_{j-h,k-h+t}F_t,$$

其中 $e_{j-h,0}=1$ 或 0 取决于 $C_{j-h}=C_0^*$ 或 $C_{j-h}\neq C_0^*$. 由 $C_{j-h}=C_0^*=C_{\frac{p-1}{2}}$，得 $C_j=C_{\frac{p-1}{2}+h}$，即 $C_j=C_h^*$，故令 $e_{j,h}=e_{j-h,0}$，则 $e_{j,h}=1$ 或 0 取决于 $C_j=C_h^*$ 或 $C_j\neq C_h^*$，这就证明了(2).

证完

为了计算上的方便，利用(2)，我们定义运算关系：

$$\begin{pmatrix}q\\F_0\\\vdots\\F_h\\\vdots\\F_{k-1}\end{pmatrix}F_j=$$

$$\begin{pmatrix} 0 & 0 & \cdots & q & \cdots & 0 \\ e_{j,0} & a_{j,0} & \cdots & a_{j,j} & \cdots & a_{j,-1} \\ \vdots & & & & & \\ e_{j,k} & a_{j-k,-k} & \cdots & a_{j-k,j-k} & \cdots & a_{j-k,-k-1} \\ \vdots & & & & & \\ e_{j,k-1} & a_{j+1,1} & \cdots & a_{j+1,j+1} & \cdots & a_{j+1,0} \end{pmatrix} \begin{pmatrix} q \\ F_0 \\ \vdots \\ F_k \\ \vdots \\ F_{k-1} \end{pmatrix}$$

设Q代表右边的列矩阵，M_j代表右边的$k+1$阶方阵，上式可改写成

$$QF_j = M_jQ,$$

其中M_j的右下角k阶子阵包含频率阵A_j的诸元，第一行的第$j+2$列处为q，某余皆为0，第1列的$r+2$行处为1，其余皆为0，这里C_r与C_j是相互共轭的. 我们称M_j为**广频率阵**.

利用矩阵乘法可群，即知

$$QF_{j_1}F_{j_2}\cdots F_{j_m} = M_{j_1}M_{j_2}\cdots M_{j_m}Q.$$

特别地

$$QF_0^u = M_0^uQ.$$

例 设$k=4$，$q\equiv 0(\mathrm{mod}2)$，因为$C_0^* = C_0$，$C_2^* = C_2$，故

$$M_0 = \begin{pmatrix} 0 & q & 0 & 0 & 0 \\ 1 & a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ 0 & a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \\ 0 & a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ 0 & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 0 & 0 & 0 & q & 0 \\ 0 & a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ 0 & a_{1,3} & a_{1,0} & a_{1,1} & a_{1,2} \\ 1 & a_{0,2} & a_{0,3} & a_{0,0} & a_{0,1} \\ 0 & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,0} \end{pmatrix}.$$

实际上，只需写出M_j的最后一行，其诸a的脚标分别加1就可得

倒数第二行，分别加 2 就可得倒数第三行，……．

母函数和广频率阵可以作为研究模 p 高次剩余的工具，下面我们说明这一点．

首先，证明

定理 2 设 p 是一个奇素数，$kq=p-1$，$C_j=\{g^{j+tk}, t=0,1,\cdots,q-1\}$，$p_1$ 是一个素数，$p_1\neq p$，则 $p_1\in C_j$ 的充分必要条件是

$$F_0^{p_1}\equiv F_j(\mathrm{mod}\ p_1).$$

证 我们有

$$F_0^{p_1}=\left(\sum_{t\in C_1}x^t\right)^{p_1}\equiv\sum_{t\in C_0}x^{tp_1}(\mathrm{mod}p_1).$$

因此，如果 $p_1\in C_j$，则 $\sum_{t\in C_0}x^{tp_1}=\sum_{t\in C_j}x^t=F_j$．反之，$\sum_{t\in C_0}x^{tp_1}=\sum_{t\in C_j}x^t$，则 $tp_1\in C_j$，$t\in C_0$，$tp_1=g^{uk}p_1=g^{j+vk}$，$0\leqslant u,\ v\leqslant q-1$，故 $p_1=g^{j+(v-u)k}\in C_j$．

证完

显然有

推论 把 $F_0^{p_1}$ 表成 $1, F_0, F_1,\cdots,F_{k-1}$ 的整系数的线性组合，则 $p_1\in C_j$ 的充分必要条件是 F_j 的系数模 p_1 同余 1，其余的系数模 p_1 同余 0．

现在，我们举例说明，以上定理在二次剩余上的应用．

例 设 $p=4m+1$，求使 $\left(\frac{7}{p}\right)=1$ 的全体素数 p．由于 $k=2$，故 $p-1=kq$，$q=2m$，$C_0^*=C_0$，$N(2)=2$．设 $a_{0,0}=a$，$a_{1,0}=a_{0,1}=a_{1,1}=b$，则

$$M_0=\begin{pmatrix}0 & 2m & 0\\ 1 & a_{0,0} & a_{0,1}\\ 0 & a_{1,1} & a_{1,0}\end{pmatrix}=\begin{pmatrix}0 & 2m & 0\\ 1 & a & b\\ 0 & b & b\end{pmatrix},$$

由 § 5 定理 2 的推论知

$$a_{0,0}+a_{0,1}=2m-1,\quad a_{1,0}+a_{1,1}=2m,$$

即

$$1+a+b=2m=2b.$$

因此

$$\begin{pmatrix}2m\\F_0\\F_1\end{pmatrix}F_0=\begin{pmatrix}0&2m&0\\1&m-1&m\\0&m&m\end{pmatrix}\begin{pmatrix}2m\\F_0\\F_1\end{pmatrix},$$

给出

$$F_0^2=2m+(m-1)F_0+mF_1,$$
$$F_0F_1=\qquad\qquad mF_0+mF_1.$$

运用这两个关系式，便可求出 F_0^3，F_0^4，…，直至 F_0^7 的表达式. 还可用

$$QF_0^6=M_0^6Q,$$

求出 F_0^7 的表达式，M_0^6 中的第二行即 F_0^7 表成 $1,F_0,\cdots,F_6$ 的线性组合的系数. 下面我们介绍一个更简单的计算方法. 写

$$I=1+F_0+F_1=1+x+x^2+\cdots+x^{p-1},$$

根据我们的约定，对所有的整数 t，均有

$$x^tI=I.$$

因此

$$F_0I=(\sum_{t\in C_0}x^t)(1+x+\cdots+x^{p-1})=2mI.$$

设

$$F_0^t=u_t+v_tF_0+w_tI,$$

则

$$F_0^{t+1}=(u_t+v_tF_0+w_tI)F_0$$
$$=u_tF_0+v_tF_0^2+w_t\cdot 2mI$$

$$=u_tF_0+v_t(2m+(m-1)F_0+mF_1)+w_t2mI$$
$$=mI(v_t+2w_t)+mv_t+(u_t-v_t)F_0.$$

故 $t\geqslant 2$ 时，有

$$u_{t+1}=mv_t,\quad v_{t+1}=u_t-v_t,\quad w_{t+1}=m(v_t+2w_t),$$

最后，我们有

$$F_0^7=u_7+v_7F_0+w_7(1+F_0+F_1)$$
$$=u_7+(v_7+w_7)F_0+w_7+w_7F_1.$$

故$\left(\frac{7}{4m+1}\right)=1$的充分必要条件是

$$u_7\equiv 0(\mathrm{mod}7),\quad v_7\equiv 1(\mathrm{mod}7),\quad w_7\equiv 0(\mathrm{mod}7).$$

	u_t	v_t	w_t
2	m	-1	m
3	$-m$	$m+1$	$m(2m-1)$
4	m^2+m	$-2m-1$	$m(4m^2-m+1)$
5	$-2m^2-m$	m^2+3m+1	$8m^4-2m^3-m$
6	m^3+3m^2+m	$-3m^2-4m-1$	$16m^5-4m^4+m^3+m^2+m$
7	$-3m^3-4m^2-m$	m^3+6m^2+5m+1	$32m^6-8m^5+2m^4-m^3-2m^2-m$

易知 $m\equiv 0,2,6(\mathrm{mod}7)$时，

$$u_7\equiv 0(\mathrm{mod}7),\quad v_7\equiv 1(\mathrm{mod}7),\quad w_7\equiv 0(\mathrm{mod}7).$$

故

$\left(\frac{7}{4m+1}\right)=1$，$p=4m+1$是素数，当且仅当 p 形为 $28t+1,28t+9,28t+25$.

*§8 广频率阵在高次剩余上的应用

本节将把以上的结果应用到三次剩余和四次剩余上去，对于小的素数p_1，可以给出满足$\left(\frac{p_1}{p}\right)_3=1$或$\left(\frac{p_1}{p}\right)_4=1$的所有 p 的形状.

我们有

定理1 设素数 $p=8m+5$, 则

$$\left(\frac{3}{p}\right)_4=1$$

的充分必要条件是 p 表成形状

$$(12t+9)^2+4(6s+1)^2$$

或

$$(12t+9)^2+4(6s-1)^2.$$

证 已知 $p=8m+5, k=4$, 则 $q=2m+1, N(4)=5, C_0^*=C_2$, $C_1^*=C_3$, 广频率阵

$$M_0=\begin{pmatrix} 0 & q & 0 & 0 & 0 \\ 0 & a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ 0 & a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \\ 1 & a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ 0 & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \end{pmatrix},$$

$$M_1=\begin{pmatrix} 0 & 0 & q & 0 & 0 \\ 0 & a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ 0 & a_{0,3} & a_{0,0} & a_{0,1} & a_{0,2} \\ 0 & a_{3,2} & a_{3,3} & a_{3,0} & a_{3,1} \\ 1 & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,0} \end{pmatrix}.$$

设 $a_{0,2}=a_1, a_{0,3}=a_{3,1}=a_{1,2}=a_2, a_{0,0}=a_{2,2}=a_{2,0}=a_3, a_{0,1}=a_{3,2}=a_{1,3}=a_4, a_{3,3}=a_{3,0}=a_{2,3}=a_{2,1}=a_{1,1}=a_{1,0}=a_5$, 故

$$M_0=\begin{pmatrix} 0 & q & 0 & 0 & 0 \\ 0 & a_3 & a_4 & a_1 & a_2 \\ 0 & a_5 & a_5 & a_2 & a_4 \\ 1 & a_3 & a_5 & a_3 & a_5 \\ 0 & a_5 & a_2 & a_4 & a_5 \end{pmatrix},$$

$$M_1=\begin{pmatrix}0 & 0 & q & 0 & 0\\ 0 & a_5 & a_5 & a_2 & a_4\\ 0 & a_2 & a_3 & a_4 & a_1\\ 0 & a_4 & a_5 & a_5 & a_2\\ 1 & a_5 & a_3 & a_5 & a_3\end{pmatrix}.$$

用§5定理2的推论知

$$a_1+a_2+a_3+a_4=2m+1,$$
$$2a_5+a_2+a_4=2m+1,$$
$$a_3+a_5=m,$$

故

$$\begin{aligned}a_5&=m-a_3,\\ a_2+a_4&=1+2a_3,\\ a_1&=2m-3a_3.\end{aligned}\tag{1}$$

因为$QF_0F_1=QF_1F_0$，故$M_0M_1Q=M_1M_0Q$. 再由

$$\sum_{i=1}^{p-1}b_ix^i=\sum_{i=1}^{p-1}d_ix^i\text{推出}b_i=d_i(i=1,\cdots,p-1),$$

可知

$$M_0M_1=M_1M_0.$$

比较位于第二行第三列交叉处的元，可得

$$a_3a_5+a_4a_3+a_1a_5+a_2a_3=a_5a_5+a_5a_2+a_2a_4+a_4a_5.$$

将(1)代入上式得

$$\begin{aligned}&a_3(m-a_3)+a_4a_3+(m-a_3)(2m-3a_3)+a_3(1+2a_3-a_4)\\ &=(m-a_3)^2+(m-a_3)(1+2a_3)+a_4(1+2a_3-a_4).\end{aligned}$$

故得

$$m^2+5a_3^2-2a_3a_4-m-a_4-4ma_3+2a_3+a_4^2=0,$$

即

$$(8a_3-4m+1)^2+4(2a_3-2a_4+1)^2=p.\tag{2}$$

现在

$$QF_0^2=M_0^2Q,$$

因此

$$F_0^3=a_1q+u_0F_0+u_1F_1+u_2F_2+u_3F_3,$$

这里(a_1,u_0,u_1,u_2,u_3)是 M_0^2 的第二行，即

$$u_0=a_3^2+a_4a_5+a_1a_3+a_2a_5=a_3^2+(m-a_3)(1+2a_3)+a_3(2m-3a_3)\equiv m+a_3(m-1)-a_3^2(\mathrm{mod}3).$$

$$u_1=a_3a_4+a_4a_5+a_1a_5+a_2^2=a_3a_4+a_4(m-a_3)+(m-a_3)(2m-3a_3)+(1+2a_3-a_4)^2\equiv(a_3+a_4-m-1)^2+m^2-2m(\mathrm{mod}3).$$

$$u_2=a_3a_1+a_4a_2+a_1a_3+a_2a_4\equiv 2ma_3+2a_4(1+2a_3-a_4)\equiv a_4^2+a_3a_4-a_4+ma_3(\mathrm{mod}3).$$

$$u_3=a_3a_2+a_4a_4-a_1a_5+a_2a_5\equiv a_4^2+2m^2-2ma_3+a_2m\equiv(a_4+m)^2+m^2+m(\mathrm{mod}3).$$

因为

$$\left(\frac{3}{8m+5}\right)_4=1,$$

故

$$\left(\frac{3}{p}\right)=\left(\frac{8m+5}{3}\right)=\left(\frac{2(m+1)}{3}\right)=1,$$

便知

$$\left(\frac{m+1}{3}\right)=-1,$$

$m\equiv 1(\mathrm{mod}3)$，于是 $u_0\equiv 1-a_3^2$，$u_1\equiv(a_3+a_4+1)^2+2$，$u_2\equiv a_4^2+a_3a_4-a_4+a_3$，$u_3\equiv(a_4+1)^2+2(\mathrm{mod}3)$.

而$\left(\frac{3}{8m+5}\right)_4=1$ 的充分必要条件是

$$u_0-1\equiv u_1\equiv u_2\equiv u_3\equiv 0(\mathrm{mod}3), \tag{3}$$

而(3)成立的充分必要条件是$a_3\equiv 0(\mathrm{mod}3)$, $a_4\equiv 0(\mathrm{mod}3)$或$a_4\equiv 1(\mathrm{mod}3)$. 令$2a_3-m=3t+2$, $a_3-a_4=3s$ 或 $3s-1$, 即得

$$p=(12t+9)^2+4(6s+1)^2 \tag{4}$$

或

$$p=(12t+9)^2+4(6s-1)^2. \tag{5}$$

反之, 若 p 可表成(4)或(5), 第五章已证, 由 p 表成两个平方和的表法唯一, 结合(2)式, 则可推出(3)式成立.

证完

完全类似地可证

定理2 设 $p=6m+1$, 那么

$$\left(\frac{2}{p}\right)_3=1$$

的充分必要条件是 $p=u^2+27v^2$.

证 我们有$p-1=3\cdot 2m$, $q=2m$, $a_{0,0}=a$, $a_{0,1}=a_{1,0}=a_{2,2}=b$, $a_{0,2}=a_{2,0}=a_{1,1}=c$, $a_{1,2}=a_{2,1}=d$, 以及$C_3^*=C_0$, $C_1^*=C_1$,

$$M_0=\begin{pmatrix}0&q&0&0\\1&a&b&c\\0&b&c&d\\0&c&d&b\end{pmatrix},$$

$$M_1=\begin{pmatrix}0&0&q&0\\0&b&c&d\\1&c&a&b\\0&d&b&c\end{pmatrix},$$

$$a+b+c=2m-1,$$

$$b+c+d=2m. \tag{6}$$

由$M_0M_1=M_1M_0$, 得

$$b^2+c^2+d^2=2m+ac+bc+ba, \tag{7}$$

由(6)和(7)推出

$$3a^2+3ab+3b^2-(6m-5)a-(6m-3)b+4m^2-6m+2=0.$$

上式两端乘 36，得

$$(9a-6m+7)^2+27(a+2b-2m+1)^2=4p. \tag{8}$$

因为$\left(\frac{2}{p}\right)_3=1$的充分必要条件是 $F_0^2\equiv F_0(\mathrm{mod}2)$，由 $QF_0=M_0Q$ 知 $F_0^2=q\mid aF_0+bF_1+cF_2$，故$\left(\frac{2}{p}\right)_3=1$ 的充分必要条件为 $q\equiv 0(\mathrm{mod}2), a\equiv 1(\mathrm{mod}2), b\equiv c\equiv 0(\mathrm{mod}2)$. 而 $a\equiv 1(\mathrm{mod}2)$，由(6)推出$b+c\equiv 0(\mathrm{mod}2), d\equiv 0(\mathrm{mod}2)$，再由 $b^2+c^2+d^2=2m+ac+ba+cb$推出$bc\equiv 0(\mathrm{mod}2)$，故$b\equiv c\equiv 0(\mathrm{mod}2)$. 故$\left(\frac{2}{p}\right)_3=1$ 的充分必要条件为$a\equiv 1(\mathrm{mod}2)$. 由$a\equiv 1(\mathrm{mod}2)$，显然可得 $p=u^2+27v^2$. 再由$p=u^2+27v^2$表成 $p=x^2+3y^2$ 的表法唯一(见第四章习题 24)，由(8)可推出$a\equiv 1(\mathrm{mod}2)$.

证完

§9 高斯引理的推广

设$p=2qk+1$是一个奇素数，我们知道，n 是模 p 的 $2k$ 次剩余的充分必要条件是$\left(\frac{n}{p}\right)_{2k}=1$. 如果，设$\left(\frac{n}{p}\right)_k=1$，那么此时容易证明：$n$ 是模 p 的 $2k$ 次非剩余的充分必要条件是$\left(\frac{n}{p}\right)_{2k}=-1$(留作习题). 这里，实际上与勒让德符号具有更相似的性质. 我们还可以把高斯引理作如下的推广.

引理 设 $p=2qk+1$是一个素数，$0<a_1<a_2<\cdots<a_{2q}<p$，$S=\{a_1,a_2,\cdots,a_{2q}\}$ 是 p 的 k 次剩余组成的集，$\left(\frac{n}{p}\right)_k=1$. 再设

$$S_1=\{a'_1,a'_2,\cdots,a'_q\},\ a'_i\neq a'_j,\ a'_i\neq p-a'_j,$$
$$1\leqslant i<j\leqslant q$$

和

$$S_n=\{a''_1,a''_2,\cdots,a''_q\},\ a''_i\equiv na'_i\ (\mathrm{mod}p),$$
$$i=1,\cdots,q$$

是S的两个子集. 如果S的q个数$a_{i_1},\cdots,a_{i_q}$具有某个性质P,但$p-a_{i_t}(t=1,\cdots,q)$不具有性质P,且S_1和S_n中分别恰有u_1和u_n个数不具有性质P,则

$$\left(\frac{n}{p}\right)_{2k}=(-1)^{u_1+u_n}. \tag{1}$$

证 因为$a'_i\neq p-a'_j$,则有$a''_i\neq p-a''_j(\mathrm{mod}p)$,否则由$a''_i\equiv p-a''_j(\mathrm{mod}p)$,推出$n(a'_i+a'_j)\equiv 0(\mathrm{mod}p)$,即$a'_i+a'_j=p$,与所设不合. 不失一般,设$S_1$中$a'_1,\cdots,a'_{u_1}$不具有性质$P$,因为$\{p-a'_1,\cdots,p-a'_{u_1}\}\subset S$,所以$p-a'_1,\cdots,p-a'_{u_1}$都具有性质$P$;同理,可设$S_n$中$a''_1,\cdots,a''_{u_n}$不具有性质$P$,而$p-a''_1,\cdots,p-a''_{u_n}$都具有性质$P$. 于是,$p-a'_1,\cdots,p-a'_{u_1},a'_{u_1+1},\cdots,a'_q$是$S$中具有性质$P$的数的全体;同理,$p-a''_1,\cdots,p-a''_{u_n},a''_{u_n+1},\cdots,a''_q$也是$S$中具有性质$P$的数的全体. 于是,设$S$中全体具有性质$P$的数的乘积为$h$,则有

$$\prod_{i=1}^{q}a''_i\equiv n^q\prod_{s=1}^{q}a'_i\equiv(-1)^{u_1}n^q h\equiv(-1)^{u_n}h(\mathrm{mod}p),$$

故

$$\left(\frac{n}{p}\right)_{2k}\equiv n^q\equiv(-1)^{u_1+u_n}(\mathrm{mod}p).$$

因为此时$\left(\frac{n}{p}\right)_{2k}=\pm 1$,故(1)式成立.

证完

在这个引理中,设$k=1$,$\left(\frac{n}{p}\right)_k=1$,表示$p\nmid n$,$S_1=\{1,\ 2,\ \cdots,$

$\frac{p-1}{2}\}$，性质 P 指小于 $\frac{p}{2}$，故 $u_1=0,\left(\frac{n}{p}\right)=(-1)^{u_n}$，这就是高斯引理.

推论 在引理的条件下，如果设 $2\nmid k$，则有 $\left(\frac{n}{p}\right)_{2k}=\left(\frac{n}{p}\right)=(-1)^{u_1+u_n}$. （留作习题）

现在，我们用引理，来证明几个定理.

定理 1 设 $p=2kq+1,\left(\frac{2}{p}\right)_k=1$，$S_1$ 和 S 的定义如引理所述，则 $\left(\frac{2}{p}\right)_{2k}=1$ 的充分必要条件是 $u\equiv v(\mathrm{mod}2)$，这里 u 和 v 分别表 S_1 中大于 $\frac{p}{2}$ 的个数和 S_1 中奇数的个数.

证 设性质 P_1 表示数小于 $\frac{p}{2}$，性质 P_2 表示数是偶数，设 $a\in S$，由于 $\left(\frac{-1}{p}\right)_k=1$，故 $p-a\in S$，这说明 S 中大于 $\frac{p}{2}$ 的数和小于 $\frac{p}{2}$ 的数各占一半，S 中的奇数和偶数也是各占一半，即 P_1 和 P_2 都合引理中的性质 P 的要求. 设 u_1 和 u_2 分别表示 S_1 和 S_2 中不具有性质 P_1 的数，u_1' 和 u_2' 分别表示 S_1 和 S_2 中不具有性质 P_2 的数，此处 S_2 的定义见引理，于是由引理可得

$$\left(\frac{2}{p}\right)_{2k}=(-1)^{u_1+u_2}=(-1)^{u_1'+u_2'}. \tag{2}$$

易知 $u_1=u,u_1'=v$，现在我们来证明 $u=u_2'$. 设 a_i' 是 S_1 中任一个大于 $\frac{p}{2}$ 的数，如果 $a_i''=2t,t<\frac{p}{2}$，则由 $a_i'=2t\equiv 2a_i'\ (\mathrm{mod}p)$，可得 $a_i=t$，与 $a_i>\frac{p}{2}$ 矛盾，故 a_i'' 是奇数. 而如果 a_i'' 是奇数，由 $a_i''\equiv 2a_i(\mathrm{mod}\ p)$ 知 $a_i>\frac{p}{2}$，否则由 $a_i<\frac{p}{2}$，可得 $a_i''=2a_i$，这是不可能的. 这就证明了 $u=u_2'$. 由(2)知 $u+u_2\equiv v+u_2'(\mathrm{mod}2)$，故 $u_2\equiv v(\mathrm{mod}2)$，再

由(2)得

$$\left(\frac{2}{p}\right)_{2k}=(-1)^{u+v}.$$

这就证明了$\left(\frac{2}{p}\right)_{2k}=1$的充分必要条件是$u\equiv v(\mathrm{mod}2)$. 证完

推论 在定理1的条件下，如果$2\nmid k$，则$u\equiv v(\mathrm{mod}2)$的充分必要条件是$p\equiv\pm1(\mathrm{mod}8)$.

这个推论的证明，留给读者.

例1 设$p=31, k=3$，已知$g=3$是31的一个原根，那么$a_i'=\langle 3^{3i}\rangle_{31}, i=1,2,3,4,5, S_1=\{27,16,29,8,30\}$. 因此$u=4, v=2$.

定理2 设$p=2qk+1, \left(\frac{2}{p}\right)_k=1$，$S$的定义如引理，

$$S_1=\{a_1', a_2', \cdots, a_q'\},\ a_i'<\frac{p}{2}$$

是S的一个子集，v_k代表S_1中小于$\frac{p}{4}$的整数的个数，则

$$\left(\frac{2}{p}\right)_{2k}=(-1)^{q+v_k}.$$

证 在引理中，取性质P指数小于$\frac{p}{2}$，故$u_1=0$. 现在我们来证明$n-v_k=u_2$，这里u_2的定义如引理所述. 设$a_i'\in S_1, a_i'>\frac{p}{4}$，则由$a_i''\equiv 2a_i'(\mathrm{mod}p)$知$a_i''>\frac{p}{2}$，否则，由$a_i'=2a_i'$可推出$a_i'=\frac{a_i''}{2}<\frac{p}{4}$，与所设矛盾. 反之，类似地由$a_i''>\frac{p}{2}$可推出$a_i'>\frac{p}{4}$. 这就证明$q-v_k=u_2$. 于是由引理得

$$\left(\frac{2}{p}\right)_{2k}=(-1)^{u_2}=(-1)^{q+v_k}.$$ 证完

易知有如下推论.

推论　在定理 2 的条件下，设 $k=2$，即 $p=4q+1,\left(\frac{2}{p}\right)=1$，则有

$$\left(\frac{2}{p}\right)_4=(-1)^{v_2}.$$

例2　设 $p=73$，可知 $S=\{1,4,9,16,25,36,49,64,8,27,48,71,23,50,6,37,70,32,96,35,3,46,18,65,41,19,72,54,38,24,11,2,67,61,57,55\}$，故 $v_2=10,\left(\frac{2}{p}\right)_4=1$.

利用高斯引理，可以推出二次互反律，这里也有类似的结果.

定理 3　设 $p=2tk+1$，$q=2fk+1$ 是二个素数，且 $\left(\frac{p}{q}\right)_k=\left(\frac{q}{p}\right)_k=1$，$u_q(p)$ 表示 $\{\langle a_1q\rangle_p,\langle a_2q\rangle_p,\cdots,\langle a_tq\rangle_p\}$ 中大于 $\frac{p}{2}$ 的个数，其中 $a_1,a_2,\cdots,a_t$ 表示模 p 全体 k 次剩余 $a_j(a_j<p,\ j=1,\cdots,2t)$ 的前 t 个数，即 $a_j<\frac{p}{2}(j=1,\ \cdots,\ t)$；$u_p(q)$ 表示 $\{\langle b_1p\rangle_q,\langle b_2p\rangle_q,\cdots,\langle b_fp\rangle_q\}$ 中大于 $\frac{q}{2}$ 的个数，其中 $b_1,b_2,\cdots,b_f$ 表示模 q 的全体 k 次剩余 $b_j(b_j<q,j=1,\cdots,2f)$ 的前 f 个数，即 $b_j<\frac{q}{2}(j=1,\cdots,f)$，则有

$$\left(\frac{p}{q}\right)_{2k}\left(\frac{q}{p}\right)_{2k}=(-1)^{u_p(q)+u_q(p)}$$

利用引理，这个定理的证明是容易的，我们留给读者去做.

最后，我们给出高斯关于 $\left(\frac{2}{p}\right)_4$ 的一个结果，它的证明更简单，用起来也较为方便.

定理 4　设 $p\equiv1(\mathrm{mod}8),p=m_1^2+m_2^2,4\mid m_1$，则

$$\left(\frac{2}{p}\right)_4=(-1)^{\frac{m_1}{4}}.$$

证 显然，$(m_1, m_2)=1$，故有 j 使得 $m_1 \equiv jm_2 \pmod{p}$，由此可得 $m_1^2 \equiv j^2 m_2^2 \pmod{p}$，$p \equiv (j^2+1)m_2^2 \pmod{p}$，$j^2+1 \equiv 0 \pmod{p}$，于是 $(j+1)^2 \equiv 2j \pmod{p}$，以及

$$j^{\frac{p-1}{4}} \equiv j^{2\frac{p-1}{8}} \equiv (-1)^{\frac{p-1}{8}} \pmod{p},$$

故有

$$2^{\frac{p-1}{4}} j^{\frac{p-1}{4}} = (2j)^{\frac{p-1}{4}} \equiv (j+1)^{\frac{p-1}{2}} \equiv \left(\frac{j+1}{p}\right) \pmod{p},$$

$$2^{\frac{p-1}{4}} (-1)^{\frac{p-1}{8}} \equiv \left(\frac{j+1}{p}\right) \pmod{p}, \tag{3}$$

而 $(m_1+m_2)^2+(m_1-m_2)^2=2p$，故 $\left(\frac{2p}{m_1+m_2}\right)=1$，由此得

$$\left(\frac{2}{m_1+m_2}\right)=\left(\frac{p}{m_1+m_2}\right)=\left(\frac{m_1+m_2}{p}\right)$$

$$=\left(\frac{j+1}{p}\right)\left(\frac{m_2}{p}\right)$$

$$=\left(\frac{j+1}{p}\right)\left(\frac{p}{m_2}\right)=\left(\frac{j+1}{p}\right).$$

代入(3)得

$$2^{\frac{p-1}{4}} \equiv \left(\frac{2}{m_1+m_2}\right)(-1)^{\frac{p-1}{8}}$$

$$=(-1)^{\frac{(m_1+m_2)^2-1+p-1}{8}} \pmod{p},$$

由于 $\frac{(m_1+m_2)^2-2+p}{8} \equiv \frac{m_1 m_2}{4} \pmod{2}$，故上式得出

$$\left(\frac{2}{p}\right)_4 \equiv 2^{\frac{p-1}{4}} \equiv (-1)^{\frac{m_1 m_2}{4}} = (-1)^{\frac{m_1}{4}} \pmod{p},$$

故得

$$\left(\frac{2}{p}\right)_4 = (-1)^{\frac{m_1}{4}}.$$

证完

第六章 习 题

1. 求出 17 和 19 的三次剩余的个数.

2. 证明：若 $p\equiv 5(\mathrm{mod}6)$ 是一个素数，则任一与 p 互素的整数是模 p 的三次剩余.

3. 已知 13 的一个原根 2，求出 13 的三次剩余和四次剩余.

4. 证明整数 x^4+1 没有形如 $8t+5$ 的素因子.

5. 求出 17 和 17^2 的四次剩余.

6. 求出 53^2 的 26 次剩余.

7. 证明：设 $\alpha\geqslant 3$，当 $2\nmid k$ 时，2^α 的 k 次剩余的个数是 $2^{\alpha-1}$；当 $2|k$ 时，2^α 的 k 次剩余的个数是 $\frac{2^{\alpha-2}}{(k,2^{\alpha-2})}$.

8. 证明，若 $k=2^b$，$\alpha\geqslant 3$，则 2^α 的 k 次剩余由下式给出：

$$R_{2^b}(2^\alpha)=\begin{cases}\{1\}, & \text{当 } b\geqslant \alpha-2\geqslant 1,\\ \{1+j2^{b+2}:\ 0\leqslant j\leqslant 2^{\alpha-b-2}-1\}, & \text{当 } 1\leqslant b<\alpha-2.\end{cases}$$

9. 证明：若 p 是一个素数，则同余式 $x^5\equiv 16(\mathrm{mod}\,p)$ 有解.

*10. 已知 $p=37$ 的一个原根 2，分别求出 $k=2,3,4,6$ 的频率阵，并验证与频率阵有关的诸定理.

*11. 证明 $g^j(C_0\ominus C_{j-k})=g^j(C_j\oplus C_{k-j})$.

*12. 求出全部 $6m+1$ 形的素数，使得 3 是一个三次剩余.

*13. 补出 §8 定理 2 的计算过程.

14. 给出 §9 引理推论的证明.

15. 给出 §9 定理 1 推论的证明.

16. 证明 §9 引理中的诸 $a_i(i=1,\cdots,2q)$ 满足

$$a_{2q+1-i}=p-a_i(i=1,\cdots q).$$

17. 补出 §9 定理 3 的证明.

18. 证明 $\left(\frac{2}{73}\right)_8=1$.

19. 证明同余式 $x^4\equiv 4(\mathrm{mod}37)$ 和同余式 $x^4\equiv 37(\mathrm{mod}41)$ 之中至少有一个有解.

*20. 用广频率阵的方法重新给出§9定理4的证明.

21. 证明：设 $p=2qk+1$ 是一个奇素数，$\left(\frac{n}{p}\right)_k=1$，则 n 是模 p 的 $2k$ 次非剩余的充分必要条件是

$$\left(\frac{n}{p}\right)_{2k}=-1.$$

名词索引

名词后面的节号，表示该名词出现的章节号，比如§1.1 表示第一章§1，下同.

十五画以上