目　录

第一章　整数的可除性

§1　整除, 带余数除法

以 $a, b, c, q, r, \cdots$ 表示整数.

定义 1　设 a, b 为整数, $b \neq 0$, 若存在整数 c, 使 $a = bc$, 则称 b 可整除 a, 记作 $b|a$. 不然, 就称 b 不可整除 a, 记作 $b \nmid a$. 当 b 可整除 a 时, 称 b 为 a 的除数 (或因数, 约数), a 是 b 的倍数, 以及 c 是 b 除 a 所得的商.

整除的基本性质:

1) $b \neq 0$, 若 $b|a$, 则其商 c 是唯一的.

设 $a = bc_1, a = bc_2$, 则 $bc_1 = bc_2, b(c_1 - c_2) = 0$. 因为 $b \neq 0$, 所以 $c_1 = c_2$.

2) $b|a, a|e$, 则 $b|e$.

3) $b \neq 0$ 的所有倍数为 $0, \pm b, \pm 2b, \pm 3b, \cdots$.

4) $a \neq 0$, 若 $b|a$, 则 $|b| \leqslant |a|$, 等号当且仅当 $b = \pm a$ 时成立. $a\,(\neq 0)$ 的除数只有有限个, a 和 $-a$ 的除数相同. $\pm 1, \pm a$ 是 a 的显然除数. $b|a$,

若 $1<|b|<|a|$, 则称 b 为 a 的真除数.

5) 若 $b|a_1, b|a_2, m_1, m_2$ 为任意整数, 则 $b|(m_1a_1+m_2a_2)$.

定义 2 一个大于 1 的正整数, 如果除了显然除数外, 不存在其他的除数 (即无真除数), 则称为素数. 以 $p, p', p_1, p_2, \cdots$ 表示. 而有真除数的整数称为合数.

由上定义看出全体正整数 (自然数) 分为 1、素数、合数这三类数.

定理 1 任一整数 $a(\neq 0, \neq 1)$ 除 1 以外的最小正除数 d 为素数. 若 a 不是素数, 则必有 $d\leqslant\sqrt{|a|}$.

证 a 的正除数只有有限个, 所以除 1 外必有一最小的, 设为 d. 若 d 不是素数, 则必有它的真除数 d_1, 满足 $d>d_1>1$, 这和 d 为最小矛盾, 所以 d 必为素数. 设 $a=dq$. $|a|\geqslant d^2$, 所以 $d\leqslant\sqrt{|a|}$. □

定理 1 的一个重要应用是: 为了判断一个整数 $a>1$ 是否为合数, 只要用 $\leqslant\sqrt{a}$ 的素数去试除. 例如判断 103 是否为合数, 只要用 $2, 3, 5, 7$ 等去试除.

定理 2 素数有无穷多个.

证 设 $p_1, p_2, \cdots, p_s$ 为所有素数, 令 $n=p_1p_2\cdots p_s+1$. 设 d 为 n 的 >1 的最小正除数, 由定理 1 知 d 必为素数. 但 $d\neq p_i, i=1, 2, \cdots, s$. 因为若 $d=p_i$ 则由 $d|n, d|p_1p_2\cdots p_s$ 推出 $d|(n-p_1p_2\cdots p_s)$, 所以 $d|1$, 矛盾, 定理得证. □

定理 3 设正整数 $n>1$, 则 $n=p_1p_2\cdots p_s, p_1\leqslant p_2\leqslant\cdots\leqslant p_s$.

证 若 n 为素数, 则定理成立. 若 n 为合数. 则其大于 1 的最小正除数必为素数, 记为 $p_1, n=p_1n_1$, 且 n_1 的任一大于 1 的最小正除数 $\geqslant p_1$. 若 n_1 为素数, 则令 $p_2=n_1$, 定理得证. 若 n_1 不是素数, 再这样做下去, 设 n_1 的大于 1 的最小正除数为 $p_2\geqslant p_1$, 则 $n=p_1p_2n_2$. 因为 $p_1\geqslant 2, p_2\geqslant 2$, 所以这样做下去, 必在有限步内结束. 证毕. □

定理 4 (带余数除法) 设 $a, b > 0$ 为整数, 则存在唯一的一对 q 及 r, 使

$$a = qb + r, \quad 0 \leqslant r < b. \tag{1}$$

当 $r = 0$ 时, 即是 b 可整除 a.

证 作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots, \tag{2}$$

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 $r = a - qb$, 则有 $0 \leqslant r < b$.

下面来证明唯一性. 设 r_1, q_1 是满足 (1) 的两个整数, 则

$$a = q_1 b + r_1, \quad 0 \leqslant r_1 < b. \tag{3}$$

由 (1) 及 (3) 得到

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

所以

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

故

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

由于 r 及 r_1 都是小于 b 的正数, 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. 因此必有 $q = q_1$, 从而 $r = r_1$, 得证. □

这个十分简单的定理是整个初等数论的基础. 由带余数除法可证明

定理 5 (算术基本引理) 设 $p|ab$, 且 $p \nmid a$, 则必 $p|b$.

证 不妨设 $a>0,b>0$, 考虑序列

$$a,2a,3a,\cdots,ka,\cdots,$$

则其中必有一些 k 使 $p|ka$, 例如 $k=p,2p,\cdots$. 设 k_0 是使 $p|ak$ 中的最小正整数. 显然, $1<k_0\leqslant p$, 现要证明必有 $k_0=p$. 用反证法. 若 $1<k_0<p$, 则由带余数除法得到

$$p=qk_0+r,\quad 1\leqslant r<k_0$$

(因为 p 为素数, 所以 $r\neq 0$). 由此得到 $p|ar$. 这和 k_0 为最小矛盾, 所以必有 $k_0=p$. 下面来证明 $p|b$.

若不然, $p\nmid b$, 则由带余数除法知

$$b=qp+r\quad (0<r<p),$$

由此推出 $p|ar$, 这和 $k_0=p$ 为最小矛盾, 定理得证. □

推论 1 *若 $p|a_1a_2\cdots a_s$, 则 p 至少能整除某一个 a_i.*

定理 6 (算术基本定理) *设 $n>1$, 则 n 可分解为素数的乘积*

$$n=p_1p_2\cdots p_s.$$

不计这些素数的次序, 则分解式是唯一的, 即

$$n=p_1^{l_1}p_2^{l_2}\cdots p_r^{l_r},\quad p_1<p_2<\cdots<p_r, \tag{4}$$

其中 $l_i\geqslant 1,p_i\,(1\leqslant i\leqslant r)$ 均由 n 所唯一决定.

证 由定理 3 知, $n>1$ 可分解为素数乘积

$$n=p_1p_2\cdots p_s,\quad p_1\leqslant p_2\leqslant\cdots\leqslant p_s.$$

若有另一分解式

$$n=q_1q_2\cdots q_t,\quad q_1\leqslant q_2\leqslant\cdots\leqslant q_t,$$

p_i, q_j 均为素数, 由于 $p_1|q_1q_2\cdots q_t$, 从推论 1 知 p_1 一定能整除某一 q_{j_0}, 所以必有 $p_1 = q_{j_0}$. 同样 $q_1|p_{i_0}$. 所以必有 $q_1 = p_{i_0}$, 从而推出 $p_1 = q_1$.

这样, 依次可证明 $p_2 = q_2, \cdots, p_s = q_s, s = t$. 把相同素数写成方幂即得 (4). □

推论 2 n 的所有正除数 $d = p_1^{i_1}p_2^{i_2}\cdots p_r^{i_r}, 0 \leqslant i_j \leqslant l_j, 1 \leqslant j \leqslant r$.

(4) 叫做 n 的标准分解式. 例如 108 的标准分解式为

$$108 = 2^2 3^3.$$

定理 6 只是一个非构造性定理. 把一个已知数分解成素因数的乘积问题是数学难题之一, 至今还没有一个实用的分解法.

§2 最大公约数, 最小公倍数

定义 3 设 $a_1, a_2, \cdots, a_k$ 是不全为零的整数. 若整数 d 是每一个 $a_i\,(1 \leqslant i \leqslant k)$ 的因数, 则 d 称为 $a_1, a_2, \cdots, a_k$ 的公因数 ($|d| \leqslant \min\limits_{a_i \neq 0}(|a_i|)$). $a_1, a_2, \cdots, a_k$ 的公因数中的最大的称为最大公因数 (或最大公约数), 记作 $(a_1, a_2, \cdots, a_k)$. 若 $(a_1, a_2, \cdots, a_k) = 1$, 则称 $a_1, a_2, \cdots, a_k$ 互素 (互质). 若其中任意两个 $a_i, a_j\,(i \neq j)$ 是互素的, 则称 $a_1, a_2, \cdots, a_k$ 是两两互素的.

定义 4 设 $b_1, b_2, \cdots, b_k$ 均不为零. 若整数 d 是每一个 $b_i\,(1 \leqslant i \leqslant k)$ 的倍数, 则 d 称为 $b_1, b_2, \cdots, b_k$ 的公倍数 ($|d| \geqslant \max\limits_i(|b_i|)$). $b_1, b_2, \cdots, b_k$ 的正的公倍数中的最小的称为最小公倍数, 记作 $[b_1, b_2, \cdots, b_k]$.

由于 a, $-a$ 的因数和倍数均相同, 所以在讨论最大公约数及最小公倍数时为了免去区别正负整数的麻烦, 可以只讨论 a_i, b_i 均大于零的情形, 亦即我们有

$$\begin{aligned}(a_1, a_2, \cdots, a_k) &= (|a_1|, |a_2|, \cdots, |a_k|),\\ [b_1, b_2, \cdots, b_k] &= [|b_1|, |b_2|, \cdots, |b_k|].\end{aligned} \tag{5}$$

由最大公约数及最小公倍数定义可得到

$$\begin{aligned} a_1|a_2, \quad &\text{则 } (a_1,a_2)=|a_1|, \quad a_1\neq 0;\\ b_1|b_2, \quad &\text{则 } [b_1,b_2]=|b_2|, \quad b_2\neq 0. \end{aligned} \tag{6}$$

定理 7 $b_1,b_2,\cdots,b_k$ 的任一公倍数, 必为其最小公倍数的倍数.

证 用反证法. 设 d 为最小公倍数, b 为任一公倍数. 若 $d\nmid b$, 则由带余数除法得到

$$b=qd+r, \quad 0<r<d.$$

然而 $r=b-qd$ 亦为 $b_1,\cdots,b_k$ 的公倍数, 但 $r<d$, 这与 d 为最小公倍数矛盾, 故必有 $d|b$. □

由此可得到下面的推论:

推论 3

$$[[b_1,b_2,\cdots,b_i],[b_{i+1},\cdots,b_k]]=[b_1,\cdots,b_i,b_{i+1},\cdots,b_k]. \tag{7}$$

证

$$[b_1,b_2,\cdots,b_i]|[b_1,b_2,\cdots,b_k],$$
$$[b_{i+1},\cdots,b_k]|[b_1,b_2,\cdots,b_k].$$

由定理 7 知

$$[[b_1,\cdots,b_i],[b_{i+1},\cdots,b_k]]|[b_1,b_2,\cdots,b_k]. \tag{8}$$

另一方面知, 对任一 $1\leqslant l\leqslant k$, 我们有

$$b_l|[b_1,\cdots,b_i], \quad 1\leqslant l\leqslant i,$$
$$b_l|[b_{i+1},\cdots,b_k], \quad i<l\leqslant k,$$

所以对 $1\leqslant l\leqslant k$, 恒有

$$b_l|[[b_1,\cdots,b_i],[b_{i+1},\cdots,b_k]],$$

由定理 7 知

$$[b_1,\cdots,b_k]|[[b_1,\cdots,b_i],[b_{i+1},\cdots,b_k]]. \tag{9}$$

由 (8) 及 (9) 即得 (7). □

由推论 3 知求多个数的最小公倍数可化成求两个数的最小公倍数.

定理 8 $a_1,a_2,\cdots,a_k$ 的任一公因数, 一定是它们的最大公约数的因数.

证 用反证法. 设 d 为最大公约数, d_1 为任一公因数. 若 $d_1\nmid d$, 则 $[d_1,d]>d$. 但另一方面有 $d_1|a_i\,(1\leqslant i\leqslant k), d|a_i\,(1\leqslant i\leqslant k)$, 所以由定理 7 知 $[d_1,d]|a_i\,(1\leqslant i\leqslant k)$, 但这与 d 为最大公约数矛盾. □

推论 4

$$(a_1,a_2,\cdots,a_k)=((a_1,\cdots,a_i),(a_{i+1},\cdots,a_k)). \tag{10}$$

读者可自行证明之. 由此求多个数的最大公约数, 可化成求两个数的最大公约数.

定理 9 设 $m>0$, 则 $[mb_1,mb_2]=m[b_1,b_2]$.

证 因为 $m[b_1,b_2]$ 是 mb_1,mb_2 的公倍数, 所以

$$[mb_1,mb_2]|m[b_1,b_2]. \tag{11}$$

另一方面, 因为 $m|[mb_1,mb_2]$, 故可设 $[mb_1,mb_2]=md$, 这样 $mb_1|md$, $mb_2|md$, 由此推出 $b_1|d,b_2|d$, 所以 $[b_1,b_2]|d$. 由此得到

$$m[b_1,b_2]|[mb_1,mb_2], \tag{12}$$

所以必有

$$[mb_1,mb_2]=m[b_1,b_2]. \qquad \square$$

推论 5 *若* $d|b_1, d|b_2$, 则

$$\left[\frac{b_1}{d}, \frac{b_2}{d}\right] = \frac{1}{d}[b_1, b_2].$$

定理 10 *设* $m > 0$, 则

$$(ma_1, ma_2) = m(a_1, a_2).$$

证 由于

$$m(a_1, a_2)|ma_1, \quad m(a_1, a_2)|ma_2,$$

所以

$$m(a_1, a_2)|(ma_1, ma_2). \tag{13}$$

另一方面, 设

$$(ma_1, ma_2) = md,$$

则 $d|a_1, d|a_2$, 故 $d|(a_1, a_2)$, 所以

$$(ma_1, ma_2)|m(a_1, a_2). \tag{14}$$

由 (13), (14) 定理得证. □

推论 6 *若* $d|a_1, d|a_2$, 则

$$\left(\frac{a_1}{d}, \frac{a_2}{d}\right) = \frac{1}{d}(a_1, a_2).$$

由上面的讨论知, 求最大公约数和最小公倍数时可把它们的公约数提出来, 这样只要讨论互素的情形.

定理 11 *设* $a > 0, b > 0$, 则

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

证 由于 $a|ab, b|ab$, 所以 $[a, b]|ab$, 故可设

$$ab = [a, b]m. \tag{15}$$

上式可写成

$$a=\frac{[a,b]}{b}m,\quad b=\frac{[a,b]}{a}m,$$

亦即

$$m|a,\quad m|b,$$

所以

$$m|(a,b),$$

因此 (15) 式可写成

$$ab=[a,b]\frac{(a,b)}{k}. \tag{16}$$

另一方面, 显有

$$ab=(a,b)M, \tag{17}$$

上式可写成

$$\frac{a}{(a,b)}b=M,\quad \frac{b}{(a,b)}a=M.$$

故 $a|M,b|M$, 所以 $[a,b]|M$.

因此 (17) 式可写成

$$ab=(a,b)[a,b]l. \tag{18}$$

由 (16) 及 (18) 式得到 $k=l=1$. □

利用算术基本定理亦可给出定理的另一个证明.

证 设

$$\begin{aligned}a&=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s},\quad \alpha_i\geqslant 0\quad (1\leqslant i\leqslant s),\\ b&=p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s},\quad \beta_i\geqslant 0\quad (1\leqslant i\leqslant s),\end{aligned}$$

则

$$\begin{aligned}(a,b)&=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_s^{\gamma_s},\quad \gamma_i=\min(\alpha_i,\beta_i)\quad (1\leqslant i\leqslant s),\\ [a,b]&=p_1^{\delta_1}p_2^{\delta_2}\cdots p_s^{\delta_s},\quad \delta_i=\max(\alpha_i,\beta_i)\quad (1\leqslant i\leqslant s).\end{aligned}$$

对于任意整数 c, d 显然有

$$c + d = \max(c, d) + \min(c, d),$$

所以我们得到

$$(a, b)[a, b] = ab. \qquad \square$$

定理 11 表明我们只要求出最大公约数就行了.

下面来证明最大公约数的两个基本性质.

定理 12 *若 a, b, c 不全为零, 且 $a = qb + c$, 则 $(a, b) = (b, c)$.*

证明留给读者.

设 a, b 不全为零, 考虑二元一次线性型 $ax + by$, 显然对任意 x, y, 一定有 $(a, b)|(ax + by)$. 下面我们要证明

定理 13 *设 a, b 不全为零, x_0, y_0 所对应的 $ax_0 + by_0$ 是使 $ax + by$ 能取到的最小正数, 则 $(a, b) = ax_0 + by_0$.*

证 我们只要证明

$$(ax_0 + by_0)|(a, b).$$

设

$$a = q_1(ax_0 + by_0) + r_1, \quad 0 \leqslant r_1 < ax_0 + by_0,$$
$$b = q_2(ax_0 + by_0) + r_2, \quad 0 \leqslant r_2 < ax_0 + by_0.$$

显然, r_1, r_2 均为 $ax + by$ 形式的数, 若 r_1 (或 r_2) $\neq 0$, 则这和 $ax_0 + by_0$ 为最小正数矛盾. 定理得证. $\square$

推论 7 *当 $(a, b) = 1$ 时, 必有 x_0, y_0 存在, 使得 $ax_0 + by_0 = 1$, 反之亦成立.*

定理 13 只是一个 "存在性" 的证明, 没有具体给出最大公约数的求法, 而是把 (a, b) 转化成另一形式 —— 二元一次线性型的最小值问

题, 但这种表达式是有用的, 它要比 (a,b) 的定义容易处理. 另外, 显然 x_0, y_0 不是唯一的, 因为 $x_0 - kb, y_0 - ka$ 也都适合要求.

定理 14 设 $(a,c)=1$, 则 $(ab,c)=(b,c)$.

证 令 $(b,c)=d$, 则 $b=b_1d, c=c_1d, (b_1,c_1)=1$,

$$(ab,c)=(ab_1d,c_1d)=d(ab_1,c_1).$$

所以只要证明 $(ab_1,c_1)=1$ 就行.

若 $(ab_1,c_1)>1$, 则必存在 p, 使得

$$p|ab_1, \quad p|c_1.$$

但由定理 5 知, 若 $p|ab_1$, 则必有 $p|a$ 或 $p|b_1$. 现在 $(a,c_1)=(b_1,c_1)=1$, 所以不可能有

$$p|a, \quad p|c_1 \quad \text{或} \quad p|b_1, \quad p|c_1$$

成立. 定理得证. □

推论 8 设 $(a,b)=1$, 则

$$(ab,d)=(a,d)(b,d). \tag{19}$$

定理 15 设 $(a,c)=1, c|ab$, 则必有 $c|b$.

证 因为 $(ab,c)=(b,c)=c$, 此即 $c|b$. □

§3 辗转相除法

本节要给出一种直接求出最大公约数 (a,b) 的方法, 它是反复应用带余数除法, 通常称之为辗转相除法. 在有限步后求出最大公约数 (a,b). 这种方法不但有应用价值, 且有理论价值, 用它可以来证明最大公约数的基本性质, 这种方法称为构造性方法.

不妨设 $a>0,b>0$, 现在我们按下列方式依次作带余数除法

$$\begin{aligned}
a&=q_1b+r_1,\quad 0<r_1<b\quad (b\nmid a),\\
b&=q_2r_1+r_2,\quad 0<r_2<r_1\quad (r_1\nmid b),\\
r_1&=q_3r_2+r_3,\quad 0<r_3<r_2\quad (r_2\nmid r_1),\\
&\cdots\cdots\cdots\cdots\\
r_{n-2}&=q_nr_{n-1}+r_n,\quad 0<r_n<r_{n-1}\quad (r_{n-1}\nmid r_{n-2}),\\
r_{n-1}&=q_{n+1}r_n\quad (r_n|r_{n-1}).
\end{aligned}\tag{20}$$

由于余数 $r_i\,(1\leqslant i\leqslant n)$ 是正的且逐次减少, 所以这种除法在有限步后必有 $r_n|r_{n-1}$, 这种算法就进行到此为止. 这种算法称为辗转相除法, 亦叫 Euclid 算法.

由定理 12 知

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

定理 16 设 $a>0,b>0$ 并进行辗转相除法 (20), 则

$$Q_ka-P_kb=(-1)^{k-1}r_k,\quad k=1,2,\cdots,n,\tag{21}$$

这里

$$\begin{aligned}
&P_0=1,\quad P_1=q_1,\quad P_k=q_kP_{k-1}+P_{k-2},\\
&Q_0=0,\quad Q_1=1,\quad Q_k=q_kQ_{k-1}+Q_{k-2}.
\end{aligned}\qquad 2\leqslant k\leqslant n\tag{22}$$

证 我们用归纳法来证明之.

由 (20), $a=q_1b+r_1$ 可写成 $Q_1a-P_1b=(-1)^{1-1}r_1$. 由 $b=q_2r_1+r_2=q_2(a-q_1b)+r_2$, $-r_2=q_2a-(q_2q_1+1)b$, 亦即

$$Q_2a-P_2b=(-1)^{2-1}r_2.$$

所以当 $k=1,k=2$ 定理是成立的. 现在来证明由 k 到 $k+1$ 亦成立.

$$\begin{aligned}
&r_{k-1}=q_{k+1}r_k+r_{k+1},\\
&r_{k+1}=(-1)^{k-2}(Q_{k-1}a-P_{k-1}b)-q_{k+1}\cdot(-1)^{k-1}(Q_ka-P_kb),
\end{aligned}$$

所以

$$\begin{aligned}(-1)^k r_{k+1} &= Q_{k-1}a - P_{k-1}b + q_{k+1}Q_k a - q_{k+1}P_k b \\ &= (q_{k+1}Q_k + Q_{k-1})a - (q_{k+1}P_k + P_{k-1})b \\ &= Q_{k+1}a - P_{k+1}b.\end{aligned}$$

定理得证. □

定理 16 给出了定理 13 中的 x_0, y_0 的具体算法.

例 1 求 42823 及 6409 的最大公约数.

解 由辗转相除法得到

$$\begin{aligned}42823 &= 6 \cdot 6409 + 4369, \\ 6409 &= 1 \cdot 4369 + 2040, \\ 4369 &= 2 \cdot 2040 + 289, \\ 2040 &= 7 \cdot 289 + 17, \\ 289 &= 17 \cdot 17,\end{aligned} \tag{23}$$

所以

$$(42823, 6409) = 17.$$

由定理 13 知, 必有 x_0, y_0 存在, 使得

$$42823x_0 + 6409y_0 = 17. \tag{24}$$

现在我们来应用定理 16, 具体地算出 x_0, y_0 的值.

由例 1 知, 此时 $a = 42823, b = 6409, n = 4, r_4 = 17$. 根据上面的等式

$$Q_4 a - P_4 b = -r_4,$$

亦即

$$P_4 b - Q_4 a = r_4, \tag{25}$$

这里, P_4, Q_4 由 (22) 求出. 由 (23) 知, 此时有 $q_1 = 6, q_2 = 1, q_3 = 2, q_4 = 7$, 这样由 (22) 可得到

$$P_4 = 147, \quad Q_4 = 22. \tag{26}$$

由 (25), (26) 即知

$$x_0 = -22, \quad y_0 = 147,$$

亦即

$$-42823 \cdot 22 + 6409 \cdot 147 = 17. \qquad \square$$

§4 一次不定方程

所谓不定方程 (或方程组) 是指变量的数目多于方程的个数, 且未知数须受某种限制 (如整数、正整数或有理数等) 之方程 (或方程组).

本节仅讨论最简单的情形, 以后作进一步的讨论.

设 a, b, c 为整数, 求整数 x, y 满足

$$ax + by = c \tag{27}$$

称为解二元一次不定方程.

定理 17 二元一次不定方程 (27) 有解的充要条件是 $(a, b)|c$. 若 (27) 可解, 且 x_0, y_0 是其一组解, 则 (27) 所有的解为

$$x = x_0 + \frac{b}{(a,b)}t, \quad y = y_0 - \frac{a}{(a,b)}t, \quad t = 0, \pm 1, \pm 2, \cdots. \tag{28}$$

证 必要性是显然的, 下证充分性. 由定理 16 知必存在 u_0, v_0 使

$$au_0 + bv_0 = (a, b), \tag{29}$$

这样

$$x_0 = u_0\frac{c}{(a,b)}, \quad y_0 = v_0\frac{c}{(a,b)} \tag{30}$$

就是 (27) 的一组解.

现设 x_0, y_0 为 (27) 的一组解, 容易直接验证 (28) 中每一组 x, y 为 (27) 的一组解. 反之, 若 x, y 为 (27) 的一组解, 则有

$$a(x - x_0) = -b(y - y_0),$$

进而有

$$\frac{a}{(a,b)}(x - x_0) = \frac{-b}{(a,b)}(y - y_0).$$

因为 $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$, 故由定理 15 得到

$$\frac{b}{(a,b)} \Big| (x - x_0), \quad \frac{a}{(a,b)} \Big| (y - y_0),$$

且有

$$\frac{x - x_0}{\frac{b}{(a,b)}} = -\frac{y - y_0}{\frac{a}{(a,b)}}.$$

令 $t = \frac{x - x_0}{\frac{b}{(a,b)}}$, 由上式即得 (28). □

推论 9 *若 $ax + by = c$ 有解, 则它和*

$$\frac{a}{(a,b)}x + \frac{b}{(a,b)}y = \frac{c}{(a,b)} \tag{31}$$

的解相同.

由上面的讨论知解二元一次不定方程的关键在于:

(1) 验证条件 $(a,b)|c$ 是否成立;

(2) 用定理 16 的方法求出 (29) 式中的 u_0, v_0, 进而得到一组特解 x_0, y_0.

对于较小的 a, b 我们可用观察法求解.

例 2 求解二元一次不定方程

$$15x + 25y = 24.$$

解 因为 $(15, 25) = 5 \nmid 24$, 所以无解. □

例 3 求解二元一次不定方程

$$15x + 25y = 100. \tag{32}$$

解 因为 $(15, 25)|100$, 所以 (32) 有解, 且由推论 7 知只要解

$$3x + 5x = 20. \tag{33}$$

由观察知 $x_0 = 5, y_0 = 1$ 为解之一, 通解为

$$\begin{cases} x = 5 + 5t, \\ y = 1 - 3t, \end{cases} \quad t = 0, \pm 1, \pm 2, \cdots . \qquad \square$$

§5 函数 $[x], \{x\}$

定义 5 设 x 为任意实数, 函数 $[x]$ 等于不超过 x 的最大整数, 函数 $\{x\} = x - [x]$. 我们称 $[x]$ 为 x 的整数部分, $\{x\}$ 为 x 的分数部分.

例如, $[3.4] = 3, [e] = 2, [-5.1] = -6, \{-0.7\} = 0.3$. 由定义立即可得出下面的一些简单性质:

1) $x \geqslant y$, 则 $[x] \geqslant [y]$;

2) $x - 1 < [x] \leqslant x$, $0 \leqslant \{x\} < 1$;

3) $[n + x] = n + [x]$, $\{n + x\} = \{x\}$, n 为整数;

4) $[x + y] = \begin{cases} [x] + [y], & \text{当 } \{x\} + \{y\} < 1, \\ [x] + [y] + 1, & \text{当 } \{x\} + \{y\} \geqslant 1; \end{cases}$

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

下面给出函数 $[x]$ 的几个应用.

引理 设实数 $x > 0$, a 为正整数, 则不超过 x 且被 a 整除的正整数的个数等于 $[\frac{x}{a}]$.

证 能被 a 整除的正整数为

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

而

$$\left[\frac{x}{a}\right] a = \left(\frac{x}{a} - \left\{\frac{x}{a}\right\}\right) a = x - a\left\{\frac{x}{a}\right\} \leqslant x,$$
$$\left(\left[\frac{x}{a}\right] + 1\right) a > \left(\left[\frac{x}{a}\right] + \left\{\frac{x}{a}\right\}\right) a = \frac{x}{a} \cdot a = x.$$

所以不超过 x 能被 a 整除的正整数为

$$a, 2a, \cdots, \left[\frac{x}{a}\right] a,$$

共有 $[\frac{x}{a}]$ 个. □

定理 18 *在 $n!$ 的标准分解式中, 素因子 $p\,(\leqslant n)$ 的指数*

$$h = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]. \tag{34}$$

证 我们用记号 $p^r \| a$ 表示 a 能被 p^r 整除, 但不能被 p^{r+1} 整除. 若能证明 $p^h \| n!$, 则 (34) 成立.

1) 由上面的引理知不超过 n (即在 $1, 2, \cdots, n$ 中) 能被 $p^r (r \geqslant 1)$ 整除的正整数为 $[\frac{n}{p^r}]$.

2) 不超过 n (即在 $1, 2, \cdots, n$ 中) 能被 p^r 整除但不能被 p^{r+1} 整除 $(r \geqslant 1)$ 的正整数个数为 $[\frac{n}{p^r}] - [\frac{n}{p^{r+1}}]$.

3) $n! = 1 \cdot 2 \cdot 3 \cdots n$, 故由 2) 知 $n!$ 的标准分解式中包含 p 的指数 h 为

$$\begin{aligned} h &= 1 \cdot \left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + 2 \cdot \left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right) + \cdots \\ &\quad + \cdots + r \cdot \left(\left[\frac{n}{p^r}\right] - \left[\frac{n}{p^{r+1}}\right]\right) + \cdots \\ &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^r}\right] + \cdots. \end{aligned}$$

□

推论 10 *$n!$ 的标准分解式为*

$$n! = \prod_{p \leqslant n} p^{\sum\limits_{r=1}^{\infty} \left[\frac{n}{p^r}\right]}.$$

例 4 求 100! 中 3 的指数.

解

$$\begin{aligned} h &= \left[\frac{100}{3}\right] + \left[\frac{100}{3^2}\right] + \left[\frac{100}{3^3}\right] + \left[\frac{100}{3^4}\right] \\ &= 33 + 11 + 3 + 1 = 48. \end{aligned}$$

□

定理 19 设 a 为任意整数, k 为自然数, 则

$$\frac{(a+1)(a+2)\cdots(a+k)}{k!}$$

必为整数.

证 不妨设 $a \geqslant 0$.

$$\frac{(a+1)(a+2)\cdots(a+k)}{k!} = \frac{(a+k)!}{a!k!},$$

对任一素数 p, 设 $p^h \| (a+k)!, p^{h_1} \| a!, p^{h_2} \| k!$, 则由定理 18 知

$$h = \sum_{r=1}^{\infty} \left[\frac{a+k}{p^r}\right], \quad h_1 = \sum_{r=1}^{\infty} \left[\frac{a}{p^r}\right], \quad h_2 = \sum_{r=1}^{\infty} \left[\frac{k}{p^r}\right].$$

由于

$$\left[\frac{a+k}{p^r}\right] \geqslant \left[\frac{a}{p^r}\right] + \left[\frac{k}{p^r}\right],$$

所以

$$h \geqslant h_1 + h_2.$$

亦即证明了 $\frac{(a+k)!}{a!k!}$ 为整数. □

推论 11 设 n 为正整数, $n = r + s + \cdots + t, r, s, \cdots, t$ 均大于等于 0, 则

$$\frac{n!}{r!s!\cdots t!}$$

为整数. 且若 $n = p$ 为素数, 则有

$$p \Big| \frac{p!}{r!s!\cdots t!}.$$

证　推论的前半部分是显然的.

因为 $r, s, \cdots, t$ 均小于 p, 所以

$$\frac{p!}{r!s!\cdots t!}$$

为正整数. 但 $(p, r!s!\cdots t!) = 1$, 故

$$(p!, r!s!\cdots t!) = ((p-1)!, r!s!\cdots t!) = r!s!\cdots t!,$$

亦即

$$p \Big| \frac{p!}{r!s!\cdots t!}.$$

由推论知, 对任意 $1 \leqslant i \leqslant p-1, p|C_p^i$, 这里 $C_p^i = \frac{p!}{i!(p-i)!}$　□

定理 20　*设 p 为素数, 则对任意整数 x, 有 $p|(x^p - x)$.*

证　当 $p = 2$ 时定理显然成立. 设 $p > 2$, 对 x 用归纳法, 且不妨设 $x \geqslant 0$ (即为非负整数), $x = 0$ 时显然成立.

设当 $x = k$ 时定理成立, 则当 $x = k+1$ 时

$$\begin{aligned} x^p - x &= (k+1)^p - (k+1) \\ &= k^p + C_p^1 k^{p-1} + C_p^2 k^{p-2} + \cdots + C_p^{p-1} k + 1 - (k+1) \\ &= k^p - k + C_p^1 k^{p-1} + \cdots + C_p^{p-1} k. \end{aligned}$$

由归纳法假设知 $p|(k^p - k)$, 再由前面的推论知 $p|C_p^i\,(1 \leqslant i \leqslant p-1)$, 所以 $p|((k+1)^p - (k+1))$. 定理得证.　□

习题

1. 试证: 对任意整数 n 必有

   (1) $6|n(n+1)(n+2)$;　　(2) $24|n(n+1)(n+2)(n+3)$;

   (3) $30|(n^5 - n)$.

2. 试证: 对任意整数 n,

   (1) 若 $2 \nmid n$, 则 $24|n(n^2-1)$;

   (2) 若 $2 \nmid n, 3 \nmid n$, 则 $24|(n^2+23)$.

3. 设 k 为自然数, 证明: $(n-1)^2|(n^k-1)$ 的充要条件是 $(n-1)|k$.

4. 若 $(a,b)=1, d|(a+b)$, 则 $(d,a)=(d,b)=1$.

5. 若 $(a,4)=(b,4)=2$, 则 $(a+b,4)=4$.

6. 若 $a^2+b^2=c^2$, 则 $2|ab$, 并进一步证明 $6|ab$.

7. 试证有无穷多个自然数, 不能表为 a^2+p 的形式, 其中 p 为素数.

8. 试证

   (1) 有无穷多个自然数为形如 $4m+3$ 的素数;

   (2) 有无穷多个形如 $6m+5$ 的素数.

9. 试证

   (1) 当 $n>1$ 时, $1+\frac{1}{2}+\cdots+\frac{1}{n}$ 都不是整数;

   (2) 当 $n\geqslant 1$ 时, $\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}$ 也不是整数.

10. 若 a,b 为整数, 且 $b\neq 0$, 则存在两个整数 s,t, 使

$$a=bs+t,\quad |t|\leqslant\frac{|b|}{2}$$

    成立. 且当 b 为奇数时, s,t 是唯一的; 而当 b 为偶数时又如何呢?

11. 求出所有满足 $(a,b,c)=10, [a,b,c]=100$ 的自然数 a,b,c.

12. 若 $(a,b)=1, d|ab$, 则存在唯一的一对 d_1,d_2, 使 $d_1|a, d_2|b$, 且 $d=d_1d_2$.

13. 设 $a>0, b>0, (a,b)=1$. 证明 $ab=k^2$ 的充要条件是 $a=k_1^2, b=k_2^2$.

14. 设 a,m,n 为自然数. 若 $(m,n)=1$, 则

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

15. 试证 $((a_1,a_2,\cdots,a_i),(a_{i+1},a_{i+2},\cdots,a_k))=(a_1,\cdots,a_k)$.

16. 试证

   (1) $(a,[b,c])=[(a,b),(a,c)]$;

   (2) $[(m_1,m_n),(m_2,m_n),\cdots,(m_{n-1},m_n)]=([m_1,m_2,\cdots,m_{n-1}],m_n)$.

17. 试证 $(a,b,c)[a,b,c]=|abc|$ 成立的充要条件是

$$(a,b)=(b,c)=(c,a)=1.$$

18. 若整数 a,b,c,d 满足 $ad-bc=\pm1$, 并设 $u=am+bn, v=cm+dn$, 则 $(m,n)=(u,v)$.

19. 设 m,n 为自然数, $2\nmid m$. 证明 $(2^m-1,2^n+1)=1$.

20. 试证: $(n!+1,(n+1)!+1)=1$.

21. 设 a,m,n 为自然数, $m\neq n$, 则

$$(a^{2^m}+1,a^{2^n}+1)=\begin{cases}1, & 2|a,\\ 2, & 2\nmid a.\end{cases}$$

22. 设 x 为实数, 试证

(1) $[x]+[x+\frac{1}{2}]=[2x]$;

(2) $[x-y]\leqslant[x]-[y]\leqslant[x-y]+1$;

(3) $[x+y]=\begin{cases}[x]+[y], & \{x\}+\{y\}<1,\\ [x]+[y]+1, & \{x\}+\{y\}\geqslant1.\end{cases}$

23. 设 n 为自然数, 实数 $a\geqslant0$, 则

(1) $[\frac{[na]}{n}]=[a]$;

(2) $\sum\limits_{k=0}^{n-1}[a+\frac{k}{n}]=[na]$.

24. 试问在 2000! 的十进位表示中, 结尾有多少个零.

25. 设自然数 $m,n,(m,n)=1$, 证明 $\frac{(m+n-1)!}{m!n!}$ 为整数.

26. 设 m,n 为自然数, 证明 $(mn)!$ 可被 $n!(m!)^n$ 整除.

27. 设 m,n 为自然数, 证明 $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ 为整数.

28. 设 k 为正整数, 试证

(1) 每一整数 n 都可唯一地表示为 $n=lm^k$, 其中 m 为正整数, l 没有任何 k 次方因子;

(2) 实数 $A>0$, 则 $\sum\limits'_{1\leqslant z\leqslant A}[\sqrt[k]{\frac{A}{z}}]=[A]$, 其中 $\sum\limits'_{1\leqslant z\leqslant A}$ 表示对所有满足条件 $1\leqslant z\leqslant A$ 且无 k 次方因子的正整数 z 求和.

29. (1) 设 $f(x)$ 在 $Q\leqslant x\leqslant R$ 上连续非负, 则和式 $\sum\limits_{Q<x\leqslant R}[f(x)]$ 表示平面 $Q<x\leqslant R, 0<y\leqslant f(x)$ 内整点 (坐标均为整数的点) 的个数.

(2) 设 p,q 为互素的奇正整数, 则

$$\sum_{0<x<\frac{q}{2}}\left[\frac{p}{q}x\right]+\sum_{0<y<\frac{p}{2}}\left[\frac{q}{p}y\right]=\frac{p-1}{2}\frac{q-1}{2};$$

(3) 设 $r>0, T$ 为圆域 $x^2+y^2 \leqslant r^2$ 内整点的个数, 则

$$T=1+4[r]+8\sum_{0<x\leqslant\frac{r}{\sqrt{2}}}\left[\sqrt{r^2-x^2}\right]-4\left[\frac{r}{\sqrt{2}}\right]^2.$$

30. 设 α,β 为给定的正数, 证明数列 $[\alpha x], x=1,2,\cdots$ 及 $[\beta y], y=1,2,\cdots$ 无公共的正整数, 并且共同组成全体自然数的充要条件是 α,β 为无理数, 且 $\frac{1}{\alpha}+\frac{1}{\beta}=1$.

31. 解下列不定方程

(1) $107x+37y=25$;

(2) $306x-360y=630$.

32. 证明: 二元一次不定方程

$$ax+by=N,\quad a>0,\quad b>0,\quad (a,b)=1$$

的非负解数为 $[\frac{N}{ab}]$ 或 $[\frac{N}{ab}]+1$.

第二章　数论函数

§1 数论函数举例

定义 1 在全体正整数 (或全体整数) 上定义的函数称作数论函数或算术函数.

当然, 更一般些, 也可把数论函数看作是在某一整数集合上定义的函数.

下面来举一些定义在全体自然数集合上的数论函数.

1) $u(n) \equiv 1, \quad n \geqslant 1,$

$e(n) = n, \quad n \geqslant 1,$

$$I(n) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$$

2) n 的所有正除数的个数 $d(n)$,

$$d(n) = \sum_{d|n} 1.$$

显然, $d(1) = 1$, 当 $n > 1$ 时, 我们要利用它的标准分解式来计算 $d(n)$. 设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, 则凡是 n 的除数必有形式 $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$,

$0 \leqslant \beta_i \leqslant \alpha_i\,(1 \leqslant i \leqslant s)$, 所以我们得到

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_s + 1). \tag{1}$$

通常我们称 $d(n)$ 为除数函数.

3) n 的全部素因子的个数 (按重数计) $\Omega(n)$,

$$\begin{aligned} &\Omega(1) = 0, \\ &\Omega(n) = \alpha_1 + \alpha_2 + \cdots + \alpha_s, \quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}. \end{aligned} \tag{2}$$

4) n 的不同的素因子的个数 $\omega(n)$,

$$\begin{aligned} &\omega(1) = 0, \\ &\omega(n) = s, \quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}. \end{aligned} \tag{3}$$

5) n 的正除数的幂和函数 $\sigma_\lambda(n)$, λ 为实数,

$$\sigma_\lambda(n) = \sum_{d|n} d^\lambda. \tag{4}$$

6) 所有不超过 n 且和 n 互素的正整数的个数 $\varphi(n)$,

$$\varphi(n) = \sum_{\substack{1 \leqslant d \leqslant n \\ (d,n)=1}} 1, \tag{5}$$

$\varphi(n)$ 称为 Euler 函数.

7) Möbius 函数 $\mu(n)$,

$$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^s, & n = p_1 p_2 \cdots p_s, \quad p_1 < p_2 < \cdots < p_s, \\ 0, & \text{其他}. \end{cases} \tag{6}$$

8) Mangoldt 函数 $\Lambda(n)$,

$$\Lambda(n) = \begin{cases} \log p, & n = p^k, \quad k \geqslant 1, \\ 0, & \text{其他}. \end{cases} \tag{7}$$

9) Liouville 函数 $\lambda(n)$,

$$\lambda(n) = (-1)^{\Omega(n)}. \tag{8}$$

§2 Dirichlet 乘积

数论函数有一种重要的运算称作 Dirichlet 乘积或卷积, 其定义如下:

定义 2 设 $f(n), g(n)$ 是两个数论函数, 则

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \tag{9}$$

称为 $f(n)$ 和 $g(n)$ 的 Dirichlet 乘积或卷积, 记作

$$h = f * g. \tag{10}$$

下面我们来证明 Dirichlet 乘积满足结合律和交换律.

定理 1 设 f, g, h 为任意三个数论函数, 则

$$f * g = g * f, \tag{11}$$

$$(f * g) * h = f * (g * h). \tag{12}$$

证 由定义知

$$(f * g)(n) = \sum_{ab=n} f(a) g(b),$$

由此看出 (11) 成立.

下面来证明结合律. 为此令 $G = g * h$, 则

$$f * (g * h) = f * G,$$

所以我们有

$$\begin{aligned}(f * G)(n) &= \sum_{ad=n} f(a) G(d) = \sum_{ad=n} f(a) \sum_{bc=d} g(b) h(c) \\ &= \sum_{abc=n} f(a) g(b) h(c).\end{aligned}$$

同样令 $K = f * g$, 考虑卷积 $K * h$, 我们可得到与上面相同的公式, 所以 (12) 成立. □

下面我们来证明一个有用的公式

$$I = \mu * u,$$

亦即

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases} \tag{13}$$

当 $n = 1$ 时 (13) 显然成立. 设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, 则由 $\mu(n)$ 的定义知

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_s) + \mu(p_1 p_2) + \cdots \\ &\quad + \mu(p_{s-1} p_s) + \cdots + \mu(p_1 p_2 \cdots p_s) \\ &= 1 + \binom{s}{1}(-1) + \binom{s}{2}(-1)^2 + \cdots + \binom{s}{s}(-1)^s = (1-1)^s = 0. \end{aligned}$$

亦即我们证明了 (13).

定义 3 *设 $f(n)$ 为数论函数, 若存在一个数论函数 $g(n)$ 使得*

$$f * g = I,$$

则称 $g(n)$ 为 $f(n)$ 的 Dirichlet 逆, 记作 $f^{-1}(n)$.

由定义及交换律知, 如果 g 为 f 的逆, 则 f 亦为 g 的逆. 由 (13) 知 $\mu(n)$ 的逆为 $u(n) \equiv 1$.

定理 2 *I 为卷积中的单位元素, 亦即*

$$f * I = I * f = f. \tag{14}$$

证 $(f * I)(n) = \sum\limits_{d|n} f(d) I(\frac{n}{d}) = f(n).$ □

定义 4 *若 $F = f * u$, 则 F 称为 f 的* Möbius *变换,*
亦即

$$F(n) = \sum_{d|n} f(d). \tag{15}$$

例如 $d(n)$ 为 $u(n)$ 的 Möbius 变换, $I(n)$ 为 $\mu(n)$ 的 Möbius 变换.

定理 3 若 $F = f * u$, 则 $f = F * \mu$.

证 $F * \mu = (f * u) * \mu = f * (u * \mu) = f * I = f$. □

定理 3 表明, 若

$$F(n) = \sum_{d|n} f(d), \tag{16}$$

则有

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right). \tag{17}$$

此时我们称 f 为 F 的 Möbius 反变换. 不难证明 Möbius 反变换是唯一的. 设 $\bar{f}$ 亦为 F 的 Möbius 反变换, 则

$$\bar{f} = F * \mu = (f * u) * \mu = f * (u * \mu) = f * I = f.$$

下面举两个 Möbius 变换的例子:

例 1 $e(n)$ 为 Euler 函数 $\varphi(n)$ 的 Möbius 变换.

证 即要证明

$$n = \sum_{d|n} \varphi(d). \tag{18}$$

设 a 为自然数. $1 \leqslant a \leqslant n$, 令 $d = (n, a)$, 现将不超过 n 的自然数以 $d = (n, a)$ 分类. 令 $n = dk$, 则 $(k, \frac{a}{d}) = 1$, 故对固定的 d, 适合 $(k, \frac{a}{d}) = 1$ 的自然数 a 的个数等于 $\varphi(k) = \varphi(\frac{n}{d})$. 因此我们有下面的公式

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

亦即 $e(n) = n$ 为 $\varphi(n)$ 的 Möbius 变换. 由定理 3 知

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}. \tag{19}$$

我们亦可用 $\varphi(n)$ 的定义来得到公式 (19).

$$\begin{aligned}\varphi(n) &= \sum_{\substack{1\leqslant d\leqslant n\\(d,n)=1}} 1 = \sum_{1\leqslant d\leqslant n}\sum_{l|(d,n)} \mu(l)\\ &= \sum_{l|n}\mu(l)\sum_{\substack{1\leqslant d\leqslant n\\ l|d}} 1 = \sum_{l|n}\mu(l)\frac{n}{l}.\end{aligned}$$

□

例 2 $\log n$ 为 Mangoldt 函数 $\Lambda(n)$ 之 Möbius 变换.

证 亦即要证明

$$\log n = \sum_{d|n}\Lambda(d). \tag{20}$$

当 $n=1$ 时, 因为 $\Lambda(1)=\log 1=0$, 所以 (20) 成立. 现设 $n>1, n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, 由 $\Lambda(d)$ 的定义知

$$\begin{aligned}\sum_{d|n}\Lambda(d) &= \sum_{l_1=0}^{\alpha_1}\sum_{l_2=0}^{\alpha_2}\cdots\sum_{l_s=0}^{\alpha_s}\Lambda(p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s})\\ &= \sum_{l_1=1}^{\alpha_1}\Lambda(p_1^{l_1}) + \sum_{l_2=1}^{\alpha_2}\Lambda(p_2^{l_2}) + \cdots + \sum_{l_s=1}^{\alpha_s}\Lambda(p_s^{l_s})\\ &= \sum_{l_1=1}^{\alpha_1}\log p_1 + \sum_{l_2=1}^{\alpha_2}\log p_2 + \cdots + \sum_{l_s=1}^{\alpha_s}\log p_s\\ &= \alpha_1\log p_1 + \alpha_2\log p_2 + \cdots + \alpha_s\log p_s = \log n,\end{aligned}$$

此即 (20) 式. 由定理 3 可以得到下面的公式

$$\Lambda(n) = \sum_{d|n}\mu(d)\log\frac{n}{d}. \tag{21}$$

□

§3 可乘函数

定义 5 设 $f(n)$ 是定义在全体自然数上且不恒等于零的数论函数, 若它满足条件

$$f(mn) = f(m)f(n), \quad (m,n)=1, \tag{22}$$

则称之为可乘函数 (积性函数). 若对任意自然数 m,n 恒有

$$f(mn)=f(m)f(n),$$

则称之为完全 (绝对) 可乘函数.

例 3 $\mu(n),d(n)$ 为可乘函数, $n^{\lambda},I(n)$ 为完全可乘函数.

证 我们首先来证明

$$\mu(mn)=\mu(m)\mu(n),\quad (m,n)=1. \tag{23}$$

当 $m=n=1$ 时上式显然成立, 若 n (或 m) 中有平方因子时, 上式亦成立, 故只需讨论如下的情形

$$\begin{aligned} &n=p_1p_2\cdots p_k,\quad p_1<p_2<\cdots<p_k,\\ &m=q_1q_2\cdots q_s,\quad q_1<q_2<\cdots<q_s, \end{aligned} \tag{24}$$

这里 $p_i(1\leqslant i\leqslant k),q_j(1\leqslant j\leqslant s)$ 为素数, 且满足

$$p_i\neq q_j. \tag{25}$$

此时我们有

$$\mu(mn)=(-1)^{s+k},\quad \mu(n)=(-1)^k,\quad \mu(m)=(-1)^s,$$

故 (23) 式成立, 亦即 $\mu(n)$ 为可乘函数. 由于 $\mu(4)\neq\mu^2(2)$, 所以它不是完全可乘函数.

其次来证明

$$d(mn)=d(m)d(n),\quad (n,m)=1. \tag{26}$$

当 $m=n=1$ 时上式显然成立, 现设

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s},\quad m=q_1^{\beta_1}q_2^{\beta_2}\cdots q_k^{\beta_k},$$

这里 p_i,q_j 亦满足 (25) 式. 此时有

$$d(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1),\quad d(m)=(\beta_1+1)(\beta_2+1)\cdots(\beta_k+1),$$

而

$$d(mn) = d(p_1^{\alpha_1}\cdots p_s^{\alpha_s}q_1^{\beta_1}\cdots q_k^{\beta_k}),$$
$$= (\alpha_1+1)\cdots(\alpha_s+1)(\beta_1+1)\cdots(\beta_k+1) = d(m)d(n),$$

所以 $d(n)$ 为可乘函数. 由于 $d(9) \neq d^2(3)$, 因此它不是完全可乘函数.

$n^\lambda, I(n)$ 为完全可乘函数是显然的. □

由可乘函数的定义看出, 若 f, g 为可乘 (完全可乘) 函数时, fg 及 $f/g\,(g \neq 0)$ 亦为可乘 (完全可乘) 函数. 下面来证明可乘函数的一些基本性质.

定理 4 可乘函数 $f(n)$ 有如下性质:

1) $f(1) = 1$;

2) $f(n) = f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_s^{\alpha_s}), \quad n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$;

3) $f(n)$ 为完全可乘的充要条件是对任意的 p 及 $k \geqslant 1$, 恒有

$$f(p^k) = f^k(p);$$

4) $f(n)$ 的 Möbius 变换亦为可乘函数.

证 因为 $(1, n) = 1$, 所以 $f(n) = f(1)f(n)$, 因为 $f(n) \neq 0$ 故必有 $f(1) = 1$, 1) 得证. 2), 3) 由定义可立即推出, 下面来证明 4).

设 $(m, n) = 1, F = f * u$, 则

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

因为 $(m, n) = 1$, 所以对 m, n 的每一正除数 d 可以分解为 $d = d_1d_2$ 的形式, 这里 $(d_1, d_2) = 1, d_1|n, d_2|m$, 故

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|n}\sum_{d_2|m} f(d_1d_2)$$
$$= \sum_{d_1|n} f(d_1)\sum_{d_2|m} f(d_2) = F(m)F(n),$$

$F(n)$ 为可乘函数. □

推论 1 设 $f(n)$ 可乘, 则

$$F(n)=\sum_{d|n}f(d)=\prod_{p^\alpha\|n}(1+f(p)+\cdots+f(p^\alpha)). \tag{27}$$

证 因为

$$\begin{aligned}F(n)&=\prod_{p^\alpha\|n}F(p^\alpha)=\prod_{p^\alpha\|n}\sum_{d|p^\alpha}f(d)\\&=\prod_{p^\alpha\|n}(1+f(p)+\cdots+f(p^\alpha)).\end{aligned}$$

□

由 (27) 立即可推出

$$\sum_{d|n}\mu(d)f(d)=\prod_{p|n}(1-f(p)). \tag{28}$$

由 (19) 知

$$\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}=n\prod_{p|n}\left(1-\frac{1}{p}\right). \tag{29}$$

若 $f(n)$ 为完全可乘函数, 则由 (27) 式可得到

$$F(n)=\prod_{p^\alpha\|n}(1+f(p)+f^2(p)+\cdots+f^\alpha(p)).$$

例 4 设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, 则

$$\sigma(n)=\sum_{d|n}d=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}. \tag{30}$$

证 由 (27) 可知

$$\begin{aligned}\sigma(n)&=\sum_{d|n}d=\prod_{p^\alpha\|n}(1+p+\cdots+p^\alpha)\\&=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}.\end{aligned}$$

□

定理 5 设 $f(n)$ 为可乘函数, 则

$$f((m,n))f([m,n])=f(m)f(n). \tag{31}$$

证 设

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_i \geqslant 0,$$
$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}, \quad \beta_i \geqslant 0,$$

则

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_s^{\alpha_s}),$$
$$f(m) = f(p_1^{\beta_1}) f(p_2^{\beta_2}) \cdots f(p_s^{\beta_s}).$$

因为

$$(m,n) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_s^{\min(\alpha_s,\beta_s)},$$
$$[m,n] = p_1^{\max(\alpha_1,\beta_1)} \cdots p_s^{\max(\alpha_s,\beta_s)},$$

所以

$$f((m,n)) = f(p_1^{\min(\alpha_1,\beta_1)}) \cdots f(p_s^{\min(\alpha_s,\beta_s)}),$$
$$f([m,n]) = f(p_1^{\max(\alpha_1,\beta_1)}) \cdots f(p_s^{\max(\alpha_s,\beta_s)}).$$

但是对任意的 i, 恒有

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

故 (31) 式得证. □

当 $(m,n) = 1$ 时 (31) 式即为

$$f(mn) = f(m) f(n).$$

定理 6 我们有

1) 若 f 可乘, g 可乘, 则 $f * g$ 亦可乘;

2) 若 g 可乘, $f * g$ 可乘, 则 f 亦可乘.

证 显然 1) 为定理 4 性质 4) 的推广, 我们把证明留给读者.

2) 我们用反证法, 若 f 不可乘, 则可推出 $f*g$ 亦不可乘. 令 $h=f*g$, 若 f 不可乘, 则必有 m,n 存在, $(m,n)=1$, 但

$$f(mn)\neq f(m)f(n).$$

若 $mn=1$, 则由 $f(1)\neq f(1)f(1)$ 推出 $f(1)\neq 1$, 但 $h(1)=f(1)g(1)=f(1)\neq 1$, 与 h 为可乘矛盾.

我们选取满足上述性质的最小正数 mn, 即当 $d_1d_2<mn$ 时恒有

$$f(d_1d_2)=f(d_1)f(d_2),\quad (d_1,d_2)=1. \tag{32}$$

由 h 的定义知

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

令 $d_1=(d,m), d_2=(d,n)$, 则 $d_1d_2=(d,m)(d,n)=(d,mn)=d$. 故有

$$\begin{aligned}
h(mn)&=\sum_{\substack{d_1\mid m\\ d_2\mid n}} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right)\\
&=\sum_{\substack{d_1\mid m\\ d_2\mid n\\ d_1d_2<mn}} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)+f(mn)g(1)\\
&=\sum_{d_1\mid m} f(d_1)g\left(\frac{m}{d_1}\right)\sum_{d_2\mid n} f(d_2)g\left(\frac{n}{d_2}\right)-f(m)f(n)+f(mn)\\
&=h(m)h(n)+f(mn)-f(m)f(n).
\end{aligned}$$

因为 $f(mn)\neq f(m)f(n)$, 所以由上式推出

$$h(mn)\neq h(m)h(n).$$

这个矛盾就证明了 2). □

推论 2 设 $F=f*\mu$, 若 F 可乘, 则 f 亦可乘.

下面来给出有关数论函数的 Dirichlet 逆的两个结果.

定理 7 设 f 为满足 $f(1)\neq 0$ 的数论函数, 则一定存在唯一的 Dirichlet 逆 f^{-1}, 它由下面的递推公式给出

$$f^{-1}(1)=\frac{1}{f(1)},\quad f^{-1}(n)=\frac{-1}{f(1)}\sum_{\substack{d|n\\ d<n}} f\left(\frac{n}{d}\right)f^{-1}(d),\quad n>1. \tag{33}$$

证 对给定的 f, 我们要证明方程

$$(f*f^{-1})(n)=I(n) \tag{34}$$

只有唯一解 $f^{-1}(n)$.

因为 $f(1)\neq 0$, 所以当 $n=1$ 时, 由

$$f(1)f^{-1}(1)=1$$

即可得到

$$f^{-1}(1)=\frac{1}{f(1)}.$$

设 $n>1$, 假若对于所有的 $k<n$, 函数值 $f^{-1}(k)$ 已经唯一确定.

由 (34) 得到

$$\sum_{d|n} f\left(\frac{n}{d}\right)f^{-1}(d)=0.$$

将上式写成

$$f(1)f^{-1}(n)+\sum_{\substack{d|n\\ d<n}} f\left(\frac{n}{d}\right)f^{-1}(d)=0,$$

所以

$$f^{-1}(n)=\frac{-1}{f(1)}\sum_{\substack{d|n\\ d<n}} f\left(\frac{n}{d}\right)f^{-1}(d).$$

因为上式的右边已经唯一确定, 故 $f^{-1}(n)$ 亦唯一确定, 定理证毕. □

推论 3 可乘函数 f 必有 f^{-1} 存在, 且亦为可乘函数.

定理 8 设 $f(1)\neq 0, g(1)\neq 0$, 则

$$(f*g)^{-1}=f^{-1}*g^{-1}. \tag{35}$$

证 令 $h=f*g$, 由于 $h(1)=f(1)g(1)\neq 0$, 故 h 有逆存在. 因为

$$h^{-1}*h=I,$$

所以

$$h^{-1}*h*f^{-1}=I*f^{-1}=f^{-1}.$$

但

$$h^{-1}*(f*g)*f^{-1}=h^{-1}*(g*f)*f^{-1}=h^{-1}*g*I=h^{-1}*g.$$

由上面两式得到

$$h^{-1}*g=f^{-1},$$

由此推出

$$h^{-1}*g*g^{-1}=f^{-1}*g^{-1},$$

亦即

$$h^{-1}=f^{-1}*g^{-1}. \qquad \square$$

由推论 3 知任意可乘函数都唯一存在 Dirichlet 逆, 且亦为可乘函数, 但利用公式 (33) 来计算 $f^{-1}(n)$ 并不方便. 另一方面我们知道 $u^{-1}=\mu=\mu u$, 因此我们要问对一般的可乘函数, 是否能用下面的公式来得到它的 Dirichlet 逆:

$$f^{-1}(n)=\mu(n)f(n)? \tag{36}$$

我们有下面的

定理 9 设 f 可乘, 则 f 为完全可乘的充要条件是

$$f^{-1}(n)=\mu(n)f(n).$$

证 必要性, 令 $g(n)=\mu(n)f(n)$, 若 f 为完全可乘, 则我们有

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

因此 $g = f^{-1}$.

充分性, 假定 $f^{-1}(n) = \mu(n)f(n)$, 要证对任意自然数 α, 及 p 恒有 $f(p^\alpha) = f^\alpha(p)$. 因为 $f^{-1}(n) = \mu(n)f(n)$, 所以

$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = I(n).$$

现取 $n = p^\alpha$, 则得到

$$\mu(1)f(1)f(p^\alpha) + \mu(p)f(p)f(p^{\alpha-1}) = 0.$$

由上式得到

$$f(p^\alpha) = f(p)f(p^{\alpha-1}),$$

亦即我们证明了

$$f(p^\alpha) = f^\alpha(p),$$

所以 f 为完全可乘函数. □

例 5 设 $n \geqslant 1$, 则

$$\sigma_\lambda^{-1}(n) = \sum_{d|n} d^\lambda \mu(d)\mu\left(\frac{n}{d}\right), \tag{37}$$

$$\varphi^{-1}(n) = \sum_{d|n} d\mu(d), \tag{38}$$

$$d^{-1}(n) = \sum_{d|n} \mu(d)\mu\left(\frac{n}{d}\right). \tag{39}$$

解 因为 $\sigma_\lambda = e^\lambda * u$, 所以 $\sigma_\lambda^{-1} = (e^\lambda)^{-1} * u^{-1} = \mu e^\lambda * \mu$, 这里 e 为函数 $e(n) = n$, 此即 (37).

同样由于 $\varphi = \mu * e$, 故 $\varphi^{-1} = \mu^{-1} * e^{-1} = u * \mu e$, 此即 (38).

$d = u * u$, 所以 $d^{-1} = u^{-1} * u^{-1} = \mu * \mu$, 此即 (39). □

例 6 设 $\lambda(n)$ 为 Liouville 函数, $g = \lambda * u$, 则

$$g(n) = \begin{cases} 1, & \text{若 } n = k^2, \\ 0, & \text{其他}, \end{cases} \tag{40}$$

$$g^{-1}(n) = \sum_{d|n} \mu(d)\lambda(d)\mu\left(\frac{n}{d}\right). \tag{41}$$

证 先证明 (40) 式, 设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$,

$$g(n)=\sum_{d|n}\lambda(d).$$

因为 g 可乘, 所以只要计算 $g(p_i^{\alpha_i})$ 就行,

$$\begin{aligned}g(p_i^{\alpha_i})&=\sum_{d|p_i^{\alpha_i}}\lambda(d)=1+\lambda(p_i)+\lambda(p_i^2)+\cdots+\lambda(p_i^{\alpha_i})\\&=1-1+1-\cdots+(-1)^{\alpha_i}\\&=\begin{cases}0, & \text{若 } \alpha_i \text{ 为奇数},\\ 1, & \text{若 } \alpha_i \text{ 为偶数}.\end{cases}\end{aligned}$$

□

由于 $g(n)=\prod\limits_{i=1}^{k}g(p_i^{\alpha_i})$,

$$g(n)=\prod_{i=1}^{k}g(p_i^{\alpha_i})=\begin{cases}1, & \text{所有 } \alpha_i \text{ 为偶数},\\ 0, & \alpha_i \text{ 中有一个为奇数},\end{cases}$$

上式即为 (40).

由定义知 $\lambda(n)$ 为完全可乘函数, 所以

$$\lambda^{-1}(n)=\mu(n)\lambda(n),$$

因此 $g^{-1}=\lambda^{-1}*u^{-1}=\mu\lambda*\mu$, 亦即

$$g^{-1}(n)=\sum_{d|n}\mu(d)\lambda(d)\mu\left(\frac{n}{d}\right).$$

□

由定理 9 我们可以得到下面的反转公式:

设 g 为完全可乘, $h=f*g$, 则 $f=h*\mu g$.

亦即当

$$h(n)=\sum_{d|n}f(d)g\left(\frac{n}{d}\right)\tag{42}$$

时

$$f(n)=\sum_{d|n}h(d)\mu\left(\frac{n}{d}\right)g\left(\frac{n}{d}\right).\tag{43}$$

令 $g=u$, (42), (43) 就变成 (16), (17).

§4 阶的估计

在进一步研究数论函数的性质之前, 我们先来介绍一下有关阶的概念及其计算, 它是研究数论函数必不可少的工具.

符号 O 及 $\ll$: 设 $x \geqslant 0, f(x)$ 是任一函数, $g(x)$ 为正值函数, 若存在一个正常数 A (与 x 无关) 使不等式

$$|f(x)| \leqslant Ag(x) \tag{44}$$

对所有充分大的 x 都成立, 则我们说, 当 $x \to +\infty$ 时 (严格说是 x 充分大时)

$$f(x) = O(g(x)) \quad \text{或} \quad f(x) \ll g(x).$$

例如:

$$\begin{aligned} \sin x &= O(1), & \sin x &\ll 1, \\ x\cos x &= O(x^2), & x\cos x &\ll x^2, \\ \sqrt{3x^2+7} &= O(x), & \sqrt{3x^2+7} &\ll x. \end{aligned}$$

下面的定理是经常用到的.

定理 10 对任意正整数 n, 我们有

$$x^n = O(e^x). \tag{45}$$

证 因为

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots,$$

所以当 $x \to +\infty$ 时, 有

$$x^n \leqslant n!e^x,$$

此即

$$x^n = O(e^x).$$

证毕. □

设 α 为任一正数, 则必有 n 存在, 使得 $\alpha \leqslant n$, 故对任意正数 α, 有

$$x^{\alpha} = O(e^{x}). \tag{46}$$

现在我们作一变换, 令

$$x = \log y,$$

则 (46) 就变成

$$\log^{\alpha} y = O(y). \tag{47}$$

由于上式中的 α 可任意大, 故从 (47) 式可推出: 对任给 $\varepsilon > 0$, 有

$$\log y = O(y^{\varepsilon}). \tag{48}$$

下面定义符号 $\sim$: 若

$$\lim_{x \to +\infty} \frac{f(x)}{g(x)} = 1,$$

则我们说当 $x \to +\infty$ 时

$$f(x) \sim g(x). \tag{49}$$

例如

$$\frac{1}{x + \log x} \sim \frac{1}{x}, \quad \sqrt{x + x^4} \sim x^2.$$

有了这些符号后我们就可以来研究数论函数 $f(n)$ 当 $n \to \infty$ 时的性质, 例如能否找到一个简单的函数 $g(n)$ (如幂函数、对数函数等) 使得

$$\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1,$$

亦即当 $n \to \infty$ 时

$$f(n) \sim g(n).$$

但是数论函数的值是很不规则的, 例如除数函数 $d(n)$, 当 $n = p$ 时它等于 2, 但当 $n = 2^k$ 时, 它又等于 $k + 1$, 而这里的 k 是很大的:

$$k = \frac{\log n}{\log 2}.$$

下面我们就以 $d(n)$ 为例来给出它的阶的估计.

定理 11 对于任何正数 α, 不可能有

$$d(n) = O(\log^{\alpha} n).$$

成立.

证 对任给的正数 α, 一定有自然数 l 存在, 使得 $l-1 \leqslant \alpha < l$. 设 $p_1, p_2, \cdots, p_l$ 是自然数中前 l 个素数, 令 $n = (p_1 p_2 \cdots p_l)^m$, 这样就有

$$d(n) = (m+1)^l. \tag{50}$$

但 $m = \frac{\log n}{\log(p_1 p_2 \cdots p_l)}$, 所以

$$d(n) > \left(\frac{1}{\log(p_1 p_2 \cdots p_l)}\right)^l \log^l n, \tag{51}$$

而 $c = (\frac{1}{\log(p_1 p_2 \cdots p_l)})^l$ 是仅与 α 有关而与 m 无关的常数, 因此对任意正数 A, 都不可能有

$$c \log^l n < A \log^{\alpha} n$$

成立, 这就证明了定理. □

定理 12 对任给 $\varepsilon > 0$, 一定有

$$d(n) = O(n^{\varepsilon}). \tag{52}$$

证 设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \alpha_i \geqslant 1$, 所以

$$\frac{d(n)}{n^{\varepsilon}} = \frac{\alpha_1 + 1}{p_1^{\alpha_1 \varepsilon}} \frac{\alpha_2 + 1}{p_2^{\alpha_2 \varepsilon}} \cdots \frac{\alpha_s + 1}{p_s^{\alpha_s \varepsilon}}. \tag{53}$$

现在把 n 的素因子 $p_i (1 \leqslant i \leqslant s)$ 分成两类:

$$\text{(i) } p_i^{\varepsilon} \geqslant 2, \quad \text{(ii) } p_i^{\varepsilon} < 2.$$

假若 $p_i \in$ (i), 则此时有

$$p_i^{\alpha_i \varepsilon} \geqslant 2^{\alpha_i} \geqslant 1 + \alpha_i,$$

所以

$$\frac{\alpha_i+1}{p_i^{\alpha_i\varepsilon}}\leqslant 1. \tag{54}$$

假若 $p_i\in$ (ii), 则这种素数的个数不能超过 $2^{\frac{1}{\varepsilon}}$. 因为 $p_i\geqslant 2$, 所以

$$p_i^{\alpha_i\varepsilon}\geqslant 2^{\alpha_i\varepsilon}=e^{\alpha_i\varepsilon\log 2}\geqslant \alpha_i\varepsilon\log 2\geqslant\frac{1}{2}(\alpha_i+1)\varepsilon\log 2,$$

亦即

$$\frac{\alpha_i+1}{p_i^{\alpha_i\varepsilon}}\leqslant\frac{2}{\varepsilon\log 2}, \tag{55}$$

所以我们有

$$\prod_{\substack{p_i\\ p_i^{\varepsilon}<2}}\frac{\alpha_i+1}{p_i^{\alpha_i\varepsilon}}\leqslant\left(\frac{2}{\varepsilon\log 2}\right)^{2^{\frac{1}{\varepsilon}}}. \tag{56}$$

由 (54), (56) 立即得到

$$\frac{d(n)}{n^{\varepsilon}}=\prod_{\substack{p_i\\ p_i^{\varepsilon}\geqslant 2}}\frac{\alpha_i+1}{p_i^{\alpha_i\varepsilon}}\prod_{\substack{p_i\\ p_i^{\varepsilon}<2}}\frac{\alpha_i+1}{p_i^{\alpha_i\varepsilon}}\leqslant\left(\frac{2}{\varepsilon\log 2}\right)^{2^{\frac{1}{\varepsilon}}},$$

亦即

$$d(n)\leqslant\left(\frac{2}{\varepsilon\log 2}\right)^{2^{\frac{1}{\varepsilon}}}n^{\varepsilon}.$$

因此只要取 $A=(\frac{2}{\varepsilon\log 2})^{2^{\frac{1}{\varepsilon}}}$, 就证明了定理. □

由于数论函数值的不规则性, 我们经常去研究它的算术平均值, 即如下的均值估计

$$\bar{f}(n)=\frac{1}{n}\sum_{m\leqslant n}f(m). \tag{57}$$

函数 $\bar{f}(n)$ 的性质比起 $f(n)$ 来要规则得多, 例如取 $f(n)=d(n)$, 在下面我们很容易证明

$$\bar{d}(n)=\frac{1}{n}\sum_{m=1}^{n}d(m)\sim\log n. \tag{58}$$

我们可以说 $d(n)$ 的平均阶为 $\log n$. 为了证明 (58), 我们先来证明一个引理.

引理 1 当 $x \to \infty$ 时, 我们有

$$\sum_{n\leqslant x}\frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right), \tag{59}$$

这里 γ 为常数 —— Euler 常数.

证

$$\begin{aligned}\sum_{n\leqslant x}\frac{1}{n} &= \sum_{n\leqslant x}\int_n^{n+1}\frac{dt}{n} = \sum_{n\leqslant x}\int_n^{n+1}\left(\frac{1}{n}-\frac{1}{t}\right)dt + \int_1^{[x]+1}\frac{dt}{t}\\ &= \log([x]+1) + \sum_{n\leqslant x} a_n,\end{aligned} \tag{60}$$

这里

$$a_n = \int_n^{n+1}\left(\frac{1}{n}-\frac{1}{t}\right)dt = O\left(\frac{1}{n^2}\right) \tag{61}$$

及

$$a_n = \int_n^{n+1}\left(\frac{1}{n}-\frac{1}{t}\right)dt = \int_n^{n+1} O\left(\frac{1}{t^2}\right)dt. \tag{62}$$

由 (61), (62) 得到

$$\sum_{n\leqslant x} a_n = \sum_{n=1}^{\infty} a_n - \sum_{n>x} a_n, \tag{63}$$

而

$$\sum_{n>x} a_n = \int_{[x]+1}^{\infty} O\left(\frac{1}{t^2}\right)dt = O\left(\frac{1}{x}\right). \tag{64}$$

由 (61) 知 $\sum\limits_{n=1}^{\infty} a_n$ 收敛, 令 $\sum\limits_{n=1}^{\infty} a_n = \gamma$, 所以

$$\sum_{n\leqslant x} a_n = \gamma + O\left(\frac{1}{x}\right).$$

由上式及 (60) 得到

$$\begin{aligned}\sum_{n\leqslant x}\frac{1}{n} &= \log x + \gamma + O\left(\frac{1}{x}\right) + \log\frac{[x]+1}{x}\\ &= \log x + \gamma + O\left(\frac{1}{x}\right).\end{aligned}$$

引理得证. □

定理 13 当 x 充分大时, 我们有

$$\sum_{n\leqslant x} d(n) = x\log x + O(x). \tag{65}$$

证

$$\begin{aligned}\sum_{n\leqslant x} d(n) &= \sum_{n\leqslant x}\sum_{d|n} 1 = \sum_{d\leqslant n}\sum_{n\leqslant x/d} 1 = \sum_{d\leqslant x}\left[\frac{x}{d}\right]\\ &= \sum_{d\leqslant x}\frac{x}{d} - \sum_{d\leqslant x}\left\{\frac{x}{d}\right\} = x\sum_{d\leqslant x}\frac{1}{d} + O(x)\\ &= x\left(\log x + \gamma + O\left(\frac{1}{x}\right)\right) + O(x)\\ &= x\log x + \gamma x + O(x) + O(1) = x\log x + O(x),\end{aligned}$$

定理得证. □

显然 (65) 式包含了当 $n\to+\infty$ 时, 有

$$\bar{d}(n) \sim \log n.$$

定理 13 的结果还是很粗糙的 (对误差项 $O(x)$ 而言), 以后我们还要得到更好的估计. 在上述定理的证明过程中, 我们发现 $\sum\limits_{n\leqslant x} d(n)$ 的估计可转化成对和式

$$\sum_{n\leqslant x}\left[\frac{x}{n}\right] \tag{66}$$

的估计, 这里出现的函数 $[x]$ 对全体实数都有实义, 这就引导我们去研究形如下面和式的估计

$$\sum_{n\leqslant x} F\left(\frac{x}{n}\right), \tag{67}$$

这里 $F(x)$ 是定义在 $(0,+\infty)$ 上的函数, 或者更一般地可以研究下面的和式

$$\sum_{n\leqslant x} g(n)F\left(\frac{x}{n}\right), \tag{68}$$

这里 $g(x)$ 为数论函数. 如果令 $g(n)=u(n), F(x)=[x]$, 则 (68) 就变成 (66).

§5 广义 Dirichlet 乘积

本节来研究形如下面的和式

$$\sum f(n)H\left(\frac{x}{n}\right), \tag{69}$$

这里 $f(x)$ 为数论函数, $H(x)$ 为定义的 $(0,+\infty)$ 上的函数, $H(x) = 0\,(0 < x < 1)$. 上式表示定义在 $(0,+\infty)$ 上的一个新的函数 $G(x), G(x) = 0\,(0 < x < 1)$, 记作

$$G = f \circ H, \tag{70}$$

亦即

$$G(x) = (f \circ H)(x) = \sum_{n \leqslant x} f(n)H\left(\frac{x}{n}\right). \tag{71}$$

特别当 $H(x)$ 有性质

$$H(x) = 0, \quad x \text{ 非整数}$$

时, 则

$$(f \circ H)(x) = \begin{cases} 0, & x \text{ 非整数}, \\ (f * H)(x), & x \text{ 为整数}. \end{cases} \tag{72}$$

因此算子 $\circ$ 可以看成是 Dirichlet 乘积的一种推广. 在 (71) 中取 $f(n) = I(n)$, 则得到 $G(x) = H(x)$, 亦即

$$(I \circ H)(x) = H(x). \tag{73}$$

因此对算子 $\circ$ 来说, I 起着单位元素的作用. 一般来说, 算子 $\circ$ 没有交换律与结合律, 但我们有下面的定理.

定理 14 设 f, g 为数论函数, $H(x)$ 为定义在 $(0,+\infty)$ 上的函数, 则

$$f \circ (g \circ H) = (f * g) \circ H. \tag{74}$$

证 设 $x>0$,

$$\begin{aligned}\{f\circ(g\circ H)\}(x)&=\sum_{n\leqslant x}f(x)\sum_{m\leqslant\frac{x}{n}}g(m)H\left(\frac{x}{mn}\right)\\&=\sum_{mn\leqslant x}f(n)g(m)H\left(\frac{x}{mn}\right)\\&=\sum_{d\leqslant x}\left(\sum_{n|d}f(n)g\left(\frac{d}{n}\right)\right)H\left(\frac{x}{d}\right)\\&=\sum_{d\leqslant x}(f*g)(d)H\left(\frac{x}{d}\right)=\{(f*g)\circ H\}(x),\end{aligned}$$

定理证毕. □

我们在 (74) 中取

$$f=g=u,H(x)=U(x)=\begin{cases}0, & 0<x<1,\\1, & x\geqslant 1,\end{cases}$$

则

$$g\circ H=\sum_{n\leqslant x}1=[x],$$

所以

$$\{f\circ(g\circ H)\}(x)=\sum_{n\leqslant x}\left[\frac{x}{n}\right]. \tag{75}$$

而

$$(f*g)(n)=d(n),$$

故

$$\{(f*g)\circ H\}(x)=\sum_{n\leqslant x}d(n). \tag{76}$$

由 (75), (76) 立即得到已知的公式

$$\sum_{n\leqslant x}d(n)=\sum_{n\leqslant x}\left[\frac{x}{n}\right].$$

下面来给出定理 14 的两个重要应用.

定理 15 设 f 有 Dirichlet 逆 f^{-1},

$$G(x)=\sum_{n\leqslant x}f(n)H\left(\frac{x}{n}\right), \tag{77}$$

则

$$H(x)=\sum_{n\leqslant x}f^{-1}(n)G\left(\frac{x}{n}\right); \tag{78}$$

反之, 由 (78) 亦可推出 (77).

证 因为 $G=f\circ H$, 所以 $f^{-1}\circ G=f^{-1}\circ(f\circ H)$, 由定理 14 知

$$f^{-1}\circ(f\circ H)=(f^{-1}*f)\circ H=I\circ H=H,$$

所以 (78) 式成立. 同样的方法可证由 (78) 推出 (77). □

推论 4 若 f 为完全可乘, 则下面两个式子是等价的.

$$G(x)=\sum_{n\leqslant x}f(n)H\left(\frac{x}{n}\right), \tag{79}$$

$$H(x)=\sum_{n\leqslant x}\mu(n)f(n)G\left(\frac{x}{n}\right). \tag{80}$$

定理 16 令 $h=f*g$, 再设

$$H(x)=\sum_{n\leqslant x}h(n),\quad F(x)=\sum_{n\leqslant x}f(n),\quad G(x)=\sum_{n\leqslant x}g(n),$$

则

$$H(x)=\sum_{n\leqslant x}f(n)G\left(\frac{x}{n}\right)=\sum_{n\leqslant x}g(n)F\left(\frac{x}{n}\right). \tag{81}$$

证 由假设知 $F=f\circ U$, $G=g\circ U$, 则我们有

$$f\circ G=f\circ(g\circ U)=(f*g)\circ U=H,$$

$$g\circ F=g\circ(f\circ U)=(g*f)\circ U=H.$$

此即 (81). □

推论 5 设 $F(x)=\sum\limits_{n\leqslant x}f(n)$, 则

$$\sum_{n\leqslant x}\sum_{d|n}f(d)=\sum_{n\leqslant x}F\left(\frac{x}{n}\right). \tag{82}$$

证 在定理 16 中, 令 $g=u$, 即得 (82). □

例 7 设 $x\geqslant 1$, 则

$$\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]=1. \tag{83}$$

解 在定理 16 中令 $f=\mu, g=u$, 则 $h=f*g=\mu*u=I$. 所以

$$\sum_{n\leqslant x}h(n)=\sum_{n\leqslant x}I(n)=1, \tag{84}$$

而

$$\sum_{n\leqslant x}f(n)G\left(\frac{x}{n}\right)=\sum_{n\leqslant x}\mu(n)\sum_{m\leqslant\frac{x}{n}}1=\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]. \tag{85}$$

由 (84), (85) 即得 (83). □

定理 17 设 $h=f*g$, 令

$$F(x)=\sum_{n\leqslant x}f(n),\quad G(x)=\sum_{n\leqslant x}g(n),\quad H(x)=\sum_{n\leqslant x}h(n),$$

则对任意满足 $ab=x$ 的正数 a,b, 恒有

$$H(x)=\sum_{n\leqslant a}f(n)G\left(\frac{x}{n}\right)+\sum_{n\leqslant b}g(n)F\left(\frac{x}{n}\right)-F(a)G(b). \tag{86}$$

证

$$H(x)=\sum_{n\leqslant x}\sum_{d_1d_2=n}f(d_1)g(d_2)=\sum_{d_1d_2\leqslant x}\sum f(d_1)g(d_2), \tag{87}$$

所以

$$\begin{aligned} H(x) &= \sum_{d_1\leqslant a}\sum_{d_2\leqslant \frac{x}{d_1}} f(d_1)g(d_2) \\ &\quad + \sum_{d_2\leqslant b}\sum_{d_1\leqslant \frac{x}{d_2}} f(d_1)g(d_2) - \sum_{d_1\leqslant a}\sum_{d_2\leqslant b} f(d_1)g(d_2) \\ &= \sum_{d_1\leqslant a} f(d_1)G\left(\frac{x}{d_1}\right) + \sum_{d_2\leqslant b} g(d_2)F\left(\frac{x}{d_2}\right) - F(a)G(b). \end{aligned}$$ □

利用定理 17 我们可以改进定理 13 的结果.

定理 18 设 $x \geqslant 1$, 则

$$\sum_{n\leqslant x} d(n) = x\log x + (2\gamma - 1)x + O(\sqrt{x}). \tag{88}$$

证 在定理 17 中令 $f = g = u, d = u * u, a = \sqrt{x}, b = \sqrt{x}$. 由 (86) 得到

$$\begin{aligned} \sum_{n\leqslant x} d(n) &= \sum_{n\leqslant\sqrt{x}} \left[\frac{x}{n}\right] + \sum_{n\leqslant\sqrt{x}} \left[\frac{x}{n}\right] - [\sqrt{x}]^2 \\ &= 2\sum_{n\leqslant\sqrt{x}} \left[\frac{x}{n}\right] - (\sqrt{x} - \{\sqrt{x}\})^2 \\ &= 2\sum_{n\leqslant\sqrt{x}} \left[\frac{x}{n}\right] - x + 2\sqrt{x}\{\sqrt{x}\} - \{\sqrt{x}\}^2 \\ &= 2\sum_{n\leqslant\sqrt{x}} \left[\frac{x}{n}\right] - x + O(\sqrt{x}). \end{aligned} \tag{89}$$

由引理 1 得到

$$\begin{aligned} \sum_{n\leqslant\sqrt{x}} \left[\frac{x}{n}\right] &= \sum_{n\leqslant\sqrt{x}} \frac{x}{n} - \sum_{n\leqslant\sqrt{x}} \left\{\frac{x}{n}\right\} \\ &= x(\log\sqrt{x} + \gamma + O(x^{-\frac{1}{2}})) + O(\sqrt{x}) \\ &= \frac{1}{2}x\log x + \gamma x + O(\sqrt{x}). \end{aligned} \tag{90}$$

由 (89), (90) 定理得证. □

定理 19 设 $x \geqslant 1$, 则

$$\sum_{n\leqslant x}\sigma(n)=\frac{\pi^2}{12}x^2+O(x\log x). \tag{91}$$

证 $\sigma(n)=\sum\limits_{d|n}d$, 在 (82) 中令 $f(d)=d$, 则

$$\begin{aligned}\sum_{n\leqslant x}\sigma(n)&=\sum_{n\leqslant x}F\left(\frac{x}{n}\right)=\sum_{n\leqslant x}\sum_{m\leqslant\frac{x}{n}}m=\sum_{n\leqslant x}\frac{1}{2}\left[\frac{x}{n}\right]\left(\left[\frac{x}{n}\right]+1\right)\\&=\frac{1}{2}\sum_{n\leqslant x}\left(\frac{x}{n}+O(1)\right)\left(\frac{x}{n}+O(1)\right)\\&=\frac{1}{2}\sum_{n\leqslant x}\frac{x^2}{n^2}+O\left(\sum_{n\leqslant x}\frac{x}{n}\right)+O(x)\\&=\frac{x^2}{2}\sum_{n=1}^{\infty}\frac{1}{n^2}-\frac{x^2}{2}\sum_{n>x}\frac{1}{n^2}+O(x\log x),\end{aligned} \tag{92}$$

但

$$\sum_{n>x}\frac{1}{n^2}<\sum_{n=[x]+1}^{\infty}\frac{1}{n(n-1)}=\sum_{n=[x]+1}^{\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right)=\frac{1}{[x]}. \tag{93}$$

由 (92), (93) 得到

$$\sum_{n\leqslant x}\sigma(n)=\frac{\zeta(2)}{2}x^2+O(x\log x),$$

这里

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad s>1. \tag{94}$$

可以证明 $\zeta(2)=\frac{\pi^2}{6}$, 定理得证. □

定理 20 设 $x \geqslant 1$, 则

$$\sum_{n\leqslant x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x). \tag{95}$$

证 因为 $\varphi(n)=\mu*e$, 所以由 (81) 得

$$\begin{aligned}\sum_{n\leqslant x}\varphi(n)&=\sum_{n\leqslant x}\mu(n)\sum_{m\leqslant\frac{x}{n}}m\\&=\sum_{n\leqslant x}\mu(n)\frac{1}{2}\left[\frac{x}{n}\right]\left(\left[\frac{x}{n}\right]+1\right)\\&=\frac{1}{2}\sum_{n\leqslant x}\mu(n)\left(\frac{x}{n}+O(1)\right)^2\\&=\frac{x^2}{2}\sum_{n\leqslant x}\frac{\mu(n)}{n^2}+O\left(\sum_{n\leqslant x}\frac{x}{n}\right)+O(x)\\&=\frac{x^2}{2}\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}-\frac{x^2}{2}\sum_{n>x}\frac{\mu(n)}{n^2}+O(x\log x).\end{aligned}\tag{96}$$

因为

$$\sum_{n=1}^{\infty}\frac{1}{n^2}\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=\sum_{n=1}^{\infty}\frac{a_n}{n^2},$$

这里

$$a_n=\sum_{d|n}\mu(d)=I(n),$$

所以

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=\frac{1}{\zeta(2)}=\frac{6}{\pi^2},\tag{97}$$

而

$$\left|\sum_{n>x}\frac{\mu(n)}{n^2}\right|\leqslant\sum_{n>x}\frac{1}{n^2}=O\left(\frac{1}{x}\right).\tag{98}$$

由 (96), (97), (98) 即得定理. □

定理 21 设 $x\geqslant 1, Q(x)$ 表示不超过 x, 无平方因子的正整数的个数, 则

$$Q(x)=\frac{6}{\pi^2}x+O(\sqrt{x}).\tag{99}$$

证 将不大于 x 的正整数依其最大平方因子 k^2 分类, 显然不大于 x 且以 k^2 为其最大平方因子的正整数的个数为

$$Q\left(\frac{x}{k^2}\right),$$

所以有

$$[x] = Q\left(\frac{x}{1^2}\right) + Q\left(\frac{x}{2^2}\right) + \cdots + Q\left(\frac{x}{k^2}\right) + \cdots,$$

亦即

$$\sum_{k\leqslant\sqrt{x}} Q\left(\frac{x}{k^2}\right) = [x]. \tag{100}$$

另一方面有

$$Q(x) = \sum_{n\leqslant\sqrt{x}} Q\left(\frac{x}{n^2}\right)\sum_{d|n}\mu(d), \tag{101}$$

将上式交换求和次序得到

$$\begin{aligned} Q(x) &= \sum_{d\leqslant\sqrt{x}}\mu(d)\sum_{\substack{n\leqslant\sqrt{x}\\ d|n}} Q\left(\frac{x}{n^2}\right) \\ &= \sum_{d\leqslant\sqrt{x}}\mu(d)\sum_{k\leqslant\sqrt{\frac{x}{d^2}}} Q\left(\frac{x}{d^2k^2}\right). \end{aligned}$$

由上式, (100) 式得到

$$Q(x) = \sum_{d\leqslant\sqrt{x}}\mu(d)\left[\frac{x}{d^2}\right], \tag{102}$$

用 $[\frac{x}{d^2}] = \frac{x}{d^2} + O(1)$ 代入得到

$$\begin{aligned} Q(x) &= \sum_{d\leqslant\sqrt{x}}\frac{x\mu(d)}{d^2} + O(\sqrt{x}) \\ &= x\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + O(\sqrt{x}) \\ &= \frac{6}{\pi^2}x + O(\sqrt{x}). \end{aligned}$$

□

习题

1. 试证 Dirichlet 乘积满足结合律, 即若 f, g, h 为三个数论函数, 则

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

2. 设 $F(n), G(n), H(n)$ 为定义在全体自然数集上的三个数论函数, 且 $G(n)=\sum\limits_{d|n} H(d), F(n)=\sum\limits_{k=1}^{n} G(k)$.

   (1) 试证: $F(n)=\sum\limits_{t=1}^{n} H(t)[\frac{n}{t}]$;

   (2) 若取 $G(n)=\log n$, 由此证明: $H(n)=\Lambda(n)$ 及 $\sum\limits_{d=1}^{n} \Lambda(d)[\frac{n}{d}]=\log n!$.

3. 证明对所有正整数 n, 有 $\sum\limits_{m=1}^{n} \mu(m)[\frac{n}{m}]=1$, 并由此证明对所有的实数 $x \geqslant 1$, 有 $|\sum\limits_{1\leqslant m\leqslant x} \frac{\mu(m)}{m}| \leqslant 1$.

4. (1) 试求函数 $f(n)$, 使其 Möbius 变换为 Möbius 函数;

   (2) 试求函数 $f(n)$, 使其 Möbius 变换为 $\varphi(n)$.

5. 设 $g(n)=\sum\limits_{d|n} f(d), g_1(n)=\sum\limits_{d|n} f_1(d)$.

   (1) 证明: $\sum\limits_{d|n} g(d) f_1(\frac{n}{d})=\sum\limits_{d|n} f(d) g_1(\frac{n}{d})$;

   (2) 求出 $g(n)g_1(n)$ 的 Möbius 反变换.

6. 证明 $f(n)$ 之 Möbius 变换之 Möbius 变换为

$$\sum_{t|n} f(t) d\left(\frac{n}{t}\right),$$

   其中 $d(n)$ 为除数函数.

7. 试证:

   (1) 若 $f(n), g(n)$ 为可乘函数, 则 $\sum\limits_{d^2|n} f(d) g(\frac{n}{d^2})$ 亦为可乘函数;

   (2) $\mu(n)=\sum\limits_{d^2|n} \mu(d)\lambda(\frac{n}{d^2})$.

8. 试证: $\sum\limits_{d^2|n} \mu(d)=\mu^2(n)$ 及 $\sum\limits_{m\leqslant x} \mu^2(m)=\sum\limits_{d\leqslant\sqrt{x}} \mu(d)[\frac{x}{d^2}]$, 并一般地有

$$\sum_{d^k|n} \mu(d)=\begin{cases} 0, & \text{若存在 } m, m^k|n, \\ 1, & \text{其他.} \end{cases}$$

9. 试证: 当 $\omega(n)>1$ 时, $\sum\limits_{d|n} \mu(d)\log d=0$; 一般若 $m \geqslant 1$ 且 $\omega(n)>m$, 则 $\sum\limits_{d|n} \mu(d)\log^m d=0$.

10. 设 $\lambda(n)$ 为 Liouville 函数.

    (1) 求 $\sum\limits_{d|n} \lambda(d)d^s$ 的表达式;

    (2) 证明: $\sum\limits_{k=1}^{[x]} \lambda(k)[\frac{x}{k}]=[\sqrt{x}]$, $x \geqslant 1$.

11. 求 $\sum\limits_{n=1}^{\infty}\mu(n!)$ 之值.

12. 证明: $\sum\limits_{d|n}\mu^2(d)=2^{\omega(n)}$ 及 $\sum\limits_{t|n}\mu(t)d(t)=(-1)^{\omega(n)}$.

13. 试证: $\sum\limits_{d|n}\mu(d)\sigma(d)=(-1)^{\omega(n)}\prod\limits_{p|n}p$ 及 $\sum\limits_{d|n}\mu(d)\varphi(d)=(-1)^{\omega(n)}\prod\limits_{p|n}(p-2)$.

14. 设 $s(n)=\sum\limits_{\substack{j=1\\(j,n)=1}}^{n}j^2$, 证明:

(1) $\sum\limits_{d|n}\frac{s(d)}{d^2}=\frac{1}{n^2}\sum\limits_{j=1}^{n}j^2$;

(2) $s(n)=n^2(\frac{1}{3}\varphi(n)+\frac{1}{2}\sum\limits_{d|n}\mu(d)+\frac{1}{6n}\prod\limits_{p|n}(1-p))$.

15. (1) 设 $n>1$, 证明: $\sum\limits_{\substack{1\leqslant d\leqslant n\\(n,d)=1}}d=\frac{1}{2}n\varphi(n)$;

(2) 设 n 为奇数, 证明: $\sum\limits_{\substack{1\leqslant d\leqslant\frac{n}{2}\\(d,n)=1}}d=\frac{1}{8}n\varphi(n)-\frac{1}{8}\prod\limits_{p|n}(1-p)$.

16. 设 A 为一整数集合, n 为一自然数, $f(a)$ 为定义在 A 上的数论函数, 证明:

(1) $\sum\limits_{a\in A}f(a)=\sum\limits_{d|n}\sum\limits_{\substack{a\in A\\(a,n)=d}}f(a)$;

(2) 若取 $A=\{1,2,3,\cdots,n\}$, $f(a)\equiv 1$ 时, 能得到什么公式?

17. 求出所有使 $\varphi(n)=24$ 的自然数.

18. 证明: (1) $\varphi(n)>\frac{1}{2}\sqrt{n}$; (2) 当 n 为合数时, $\phi(n)\leqslant n-\sqrt{n}$.

19. 试证存在无限多个合数 n, 使 $\varphi(n)>\varphi(n+1)$.

20. 求出所有 $4\nmid\varphi(n)$ 的自然数 n.

21. 设 $x\geqslant a$ 时, $f(x)$ 为一递增非负函数, 则 $x\geqslant a$ 时

$$\left|\sum_{a\leqslant n\leqslant x}f(n)-\int_a^x f(t)dt\right|\leqslant f(x).$$

并由此证明: (1) 当 $\lambda\geqslant 0$ 时, $\sum\limits_{n\leqslant x}n^{\lambda}=\frac{x^{\lambda+1}}{\lambda+1}+O(x^{\lambda})$;

(2) $\sum\limits_{n\leqslant x}\log n=x\log x-x+O(\log x)$.

22. 设 $x\geqslant a$ 时, $f(x)$ 非负递减, 则极限

$$\lim_{N\to\infty}\left(\sum_{n=a}^{N}f(n)-\int_a^N f(x)dx\right)=\alpha$$

存在. 且 $0 \leqslant \alpha \leqslant f(a)$. 若当 $x \to \infty$ 时, $f(x) \to 0$, 则更有

$$\left| \sum_{a \leqslant n \leqslant x} f(n) - \int_a^x f(t)dt - \alpha \right| \leqslant f(x), \quad x \geqslant a+1.$$

并由此证明:

(1) $\sum\limits_{n \leqslant x} \frac{1}{n} = \log x + \gamma + O(\frac{1}{x})$, γ 为 Euler 常数.

(2) 当 $\delta > 1$ 时, $\sum\limits_{n \geqslant x} \frac{1}{n^\delta} = \frac{1}{(\delta-1)x^{\delta-1}} + O(\frac{1}{x^\delta})$.

23. 设 $\Lambda(n)$ 为 Mangoldt 函数, 且 $\psi(x) = \sum\limits_{n \leqslant x} \Lambda(n)$, 则

$$\sum_{n \leqslant x} \psi\left(\frac{x}{n}\right) = \sum_{n \leqslant x} \Lambda(n) \left[\frac{x}{n}\right] = \sum_{n \leqslant x} \log n.$$

24. 试证: 对任意的正整数 n, 有

$$\sum_{k|n} d^3(k) = \left(\sum_{k|n} d(k) \right)^2.$$

25. 设 $\sigma(n)$ 为除数和函数, 证明:

(1) $\sigma(n) = n+1$ 的充要条件是 n 为素数;

(2) 如果 n 为完全数, 即 $\sigma(n) = 2n$, 则

$$\sum_{d|n} \frac{1}{d} = 2.$$

26. 设 d 为自然数. $x \geqslant 1$, 则

$$\sum_{\substack{m \leqslant x \\ (m,d)=1}} \frac{\mu^2(m)}{\varphi(m)} \geqslant \frac{\varphi(d)}{d} \log([x]+1).$$

第三章　素数分布的一些初等结果

§1　函数 $\pi(x)$

素数分布是数论中的一个核心问题, 素数分布中一个最重要的问题是关于区间中素数的个数问题. 设 $x>0$, $\pi(x)$ 表示不超过 x 的素数的个数, 在第一章中我们已经证明了

$$\lim_{x\to\infty}\pi(x)=\infty. \tag{1}$$

进一步我们要问当 $x\to\infty$ 时, $\pi(x)$ 的阶是多大? 一个略为精密一些的结果是

$$\lim_{x\to\infty}\frac{\pi(x)}{x}=0, \tag{2}$$

(2) 式表明了在自然数中素数出现的概率为零.

为了证明 (2) 式我们先来证明几个引理.

引理 1　设 $x>0, p_1, p_2, \cdots, p_s$ 为前 s 个素数, $\phi(x,s)$ 表示不超过 x 且不被 $p_i(1\leqslant i\leqslant s)$ 所整除的自然数的个数, 则

$$\phi(x,s)=\sum_{d|p}\mu(d)\left[\frac{x}{d}\right], \tag{3}$$

这里

$$p = p_1 p_2 \cdots p_s. \tag{4}$$

证 由第二章 (13) 式知道

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

所以

$$\begin{aligned} \phi(x,s) &= \sum_{n \leqslant x} \sum_{d|(n,p)} \mu(d) \\ &= \sum_{d|p} \mu(d) \sum_{\substack{n \leqslant x \\ d|n}} 1 = \sum_{d|p} \mu(d) \left[\frac{x}{d}\right]. \end{aligned}$$

证毕. □

例 1 求不超过 1250 且没有小于 10 的素因子的自然数的个数.

解 因为小于 10 的素因子只有 $2,3,5,7$, 所以只要求出 $\phi(1250,4)$ 就行.

$$\begin{aligned} \phi(1250,4) = & \sum_{d|2\cdot3\cdot5\cdot7} \mu(d) \left[\frac{1250}{d}\right] \\ = & \left[\frac{1250}{1}\right] - \left[\frac{1250}{2}\right] - \left[\frac{1250}{3}\right] - \left[\frac{1250}{5}\right] - \left[\frac{1250}{7}\right] + \left[\frac{1250}{6}\right] \\ & + \left[\frac{1250}{10}\right] + \left[\frac{1250}{14}\right] + \left[\frac{1250}{15}\right] + \left[\frac{1250}{21}\right] + \left[\frac{1250}{35}\right] - \left[\frac{1250}{30}\right] \\ & - \left[\frac{1250}{42}\right] - \left[\frac{1250}{70}\right] - \left[\frac{1250}{105}\right] + \left[\frac{1250}{210}\right] \\ = & \ 237. \end{aligned}$$

□

引理 2 设 s 为自然数, $x > s$, 则

$$\pi(x) < x \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) + 2^{s+1}, \tag{5}$$

这里 $p_1, p_2, \cdots, p_s$ 为前 s 个素数.

证 因为大于 p_s 而又不超过 x 的素数不能被前 s 个素数整除, 所以

$$\pi(x) \leqslant s + \phi(x, s). \tag{6}$$

由 (3) 及 (6) 得到

$$\begin{aligned}
\pi(x) &\leqslant s + \sum_{d|p} \mu(d) \left[\frac{x}{d}\right] \\
&= s + \left(x - \sum_{i=1}^{s} \left[\frac{x}{p_i}\right] + \sum_{1\leqslant i<j\leqslant s} \left[\frac{x}{p_i p_j}\right] + \cdots + \cdots + (-1)^s \left[\frac{x}{p_1 p_2 \cdots p_s}\right] \right) \\
&< s + x\left(1 - \sum_{i=1}^{s} \frac{1}{p_i} + \sum_{1\leqslant i<j\leqslant s} \frac{1}{p_i p_j} + \cdots + (-1)^s \frac{1}{p_1 p_2 \cdots p_s} \right) \\
&\quad + \left(\sum_{i=1}^{s} 1 + \sum_{1\leqslant i<j\leqslant s} 1 + \cdots + \sum_{1\leqslant i_1<i_2<\cdots<i_s\leqslant s} 1 + 1 \right) \\
&< s + x \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) + \left(1 + \binom{s}{1} + \binom{s}{2} + \cdots + \binom{s}{s-1} + 1 \right) \\
&= x \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) + s + (1+1)^s.
\end{aligned}$$

由上式立即推出 (5). □

引理 3

$$\prod_{p} \left(1 - \frac{1}{p}\right) = 0, \tag{7}$$

此处 $\prod\limits_{p}$ 通过全体素数.

证 设 N 为充分大的自然数, 则显然有

$$\prod_{p} \left(1 - \frac{1}{p}\right)^{-1} > \prod_{p\leqslant N} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p\leqslant N} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) > \sum_{n=0}^{N} \frac{1}{n}. \tag{8}$$

由第二章引理 1 知

$$\lim_{N\to\infty} \sum_{n\leqslant N} \frac{1}{n} = \infty,$$

故必有

$$\prod_p \left(1-\frac{1}{p}\right)=0.$$

引理得证. □

有了上面几个引理后, 我们就可以来证明下面的定理.

定理 1 几乎所有自然数皆非素数, 亦即有

$$\lim_{x\to\infty}\frac{\pi(x)}{x}=0.$$

证 由 (5) 式得到

$$\pi(x)<x\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right)+2^{s+1}.$$

现在取 $s+1=[\frac{\log x}{2\log 2}]$, 则由上式得到

$$0<\frac{\pi(x)}{x}<\prod_{i=1}^{[\frac{\log x}{2\log 2}]-1}\left(1-\frac{1}{p_i}\right)+\frac{2^{\frac{\log x}{2\log 2}}}{x},$$

所以

$$\lim_{x\to\infty}\frac{\pi(x)}{x}=0,$$

亦即

$$\pi(x)=o(x),\quad x\to\infty.$$ □

§2 Chebyshev 定理

经过大量的数值计算, Legendre 及 Gauss 都猜测

$$\pi(x)\sim\frac{x}{\log x},\tag{9}$$

这就是著名的 "素数定理", 它是研究素数分布理论的中心问题, 决定素数定理的真伪问题曾吸引了许多数学家的注意.

Chebyshev 首先对这个问题作出了重要的贡献. 1850 年他证明了下面的结果: 存在两个正常数 C_1, C_2 使得不等式

$$C_1\frac{x}{\log x} < \pi(x) < C_2\frac{x}{\log x}, \quad x \geqslant 2 \tag{10}$$

成立. (10) 式就是著名的 Chebyshev 不等式.

引理 4 设 $x > 1, f(t) \in C'[1,x], S(x) = \sum\limits_{n\leqslant x} C_n$, 则

$$\sum_{n\leqslant x} C_n f(n) = S(x)f(x) - \int_1^x S(t)f'(t)dt. \tag{11}$$

证

$$\begin{aligned} S(x)f(x) - \sum_{n\leqslant x} C_n f(n) &= \sum_{n\leqslant x} C_n(f(x) - f(n)) \\ &= \sum_{n\leqslant x} C_n \int_n^x f'(t)dt = \sum_{n\leqslant x} C_n \int_1^x g(n,t)f'(t)dt, \end{aligned}$$

这里

$$g(n,t) = \begin{cases} 1, & \text{若 } n \leqslant t < x, \\ 0, & \text{若 } n > t, \end{cases}$$

所以我们得到

$$S(x)f(x) - \sum_{n\leqslant x} C_n f(n) = \int_1^x \sum_{n\leqslant x} C_n g(n,t)f'(t)dt, \tag{12}$$

但

$$\sum_{n\leqslant x} C_n g(n,t) = \sum_{n\leqslant t} C_n = S(t). \tag{13}$$

将 (13) 代入 (12) 即得 (11). □

利用引理 4 可推出下面的 Euler 求和公式.

定理 2 设 $a > 0, f(x) \in C'[a,b]$, 则

$$\sum_{a<n\leqslant b} f(n) = \int_a^b f(t)dt + \int_a^b \psi_1(t)f'(t)dt + \psi_1(a)f(a) - \psi_1(b)f(b), \tag{14}$$

这里

$$\psi_1(x) = x - [x] - \frac{1}{2}.$$

证 在引理 4 中令 $C_n = 1$, 则

$$\sum_{n\leqslant a} f(n) = [a]f(a) - \int_1^a [t]f'(t)dt, \tag{15}$$

$$\sum_{n\leqslant b} f(n) = [b]f(b) - \int_1^b [t]f'(t)dt. \tag{16}$$

将 (16) 减 (15) 得到

$$\sum_{a<n\leqslant b} f(n) = [b]f(b) - [a]f(a) - \int_a^b [t]f'(t)dt, \tag{17}$$

再利用下式

$$\int_a^b \left(t - \frac{1}{2}\right) f'(t)dt = \left(b - \frac{1}{2}\right) f(b) - \left(a - \frac{1}{2}\right) f(a) - \int_a^b f(t)dt,$$

从 (17) 减去此式即得 (14). □

引理 5 设 $x > 1$, 则

$$\sum_{n\leqslant x} \log n = x\log x - x + O(\log x). \tag{18}$$

证 在定理 2 中取 $f(t) = \log t$, 则得到

$$\sum_{n\leqslant x} \log n = \int_1^x \log t dt - \psi_1(x)\log x + \int_1^x \frac{\psi_1(t)}{t}dt, \tag{19}$$

因为 $|\psi_1(t)| \leqslant \frac{1}{2}$, 所以

$$\left|\int_1^x \frac{\psi_1(t)}{t}dt\right| \leqslant \frac{1}{2}\log x, \quad |\psi_1(x)\log x| \leqslant \frac{1}{2}\log x.$$

将上式代入 (19) 即得 (18). □

Chebyshev 在研究素数定理时引入了两个新函数

$$\theta(x) = \sum_{p\leqslant x} \log p, \tag{20}$$

$$\psi(x) = \sum_{n\leqslant x} \Lambda(n). \tag{21}$$

由 $\Lambda(n)$ 的定义知

$$\begin{aligned}\psi(x)&=\sum_{n\leqslant x}\Lambda(n)=\sum_{m=1}^{\infty}\sum_{p^m\leqslant x}{}^{p}\Lambda(p^m)\\&=\sum_{m\leqslant\frac{\log x}{\log 2}}\sum_{p\leqslant x^{\frac{1}{m}}}\log p=\sum_{m\leqslant\frac{\log x}{\log 2}}\theta(x^{\frac{1}{m}}),\end{aligned}\tag{22}$$

显然

$$\theta(x)=\sum_{p\leqslant x}\log p\leqslant x\log x,$$

所以由 (22) 式得到

$$\begin{aligned}\psi(x)&=\theta(x)+\sum_{2\leqslant m\leqslant\frac{\log x}{\log 2}}\theta(x^{\frac{1}{m}})\\&=\theta(x)+O(x^{\frac{1}{2}}\log^2 x).\end{aligned}\tag{23}$$

利用引理 4 我们可以证明

定理 3 下面几个式子是等价的:

$$\pi(x)\sim\frac{x}{\log x},\quad x\to\infty;\tag{24}$$

$$\psi(x)\sim x,\quad x\to\infty;\tag{25}$$

$$\theta(x)\sim x,\quad x\to\infty.\tag{26}$$

证 由 (23) 式知, 我们只要证明 (24) 与 (26) 等价就行. 在引理 4 中我们令

$$C_n=\begin{cases}1, & n\text{ 为素数},\\0, & \text{其他},\end{cases}$$

则

$$\begin{aligned}\pi(x)&=\sum_{p\leqslant x}1=\sum_{n\leqslant x}C_n,\\\theta(x)&=\sum_{p\leqslant x}\log p=\sum_{n\leqslant x}C_n\log n.\end{aligned}$$

由 (11) 式得到

$$\theta(x)=\pi(x)\log x-\int_1^x\frac{\pi(t)}{t}dt,$$

因为

$$\frac{\pi(t)}{t}=o(1),\quad t\geqslant\sqrt{x},$$

所以

$$\begin{aligned}\theta(x)&=\pi(x)\log x-\int_1^{\sqrt{x}}\frac{\pi(t)}{t}dt-\int_{\sqrt{x}}^x\frac{\pi(t)}{t}dt\\&=\pi(x)\log x+o(x),\end{aligned}\tag{27}$$

亦即

$$\frac{\theta(x)}{x}=\frac{\pi(x)}{\frac{x}{\log x}}+o(1).\tag{28}$$

因此 (24) 与 (26) 是等价的. □

定理 4 设 $x>1$, 则有

$$\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right)=\sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right]=x\log x-x+O(\log x).\tag{29}$$

证 由于

$$\log n=\sum_{d|n}\Lambda(d),$$

所以由第二章定理 16 得到

$$\sum_{n\leqslant x}\log n=\sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right),$$

再由引理 5 即得 (29). □

由定理 4 和引理 5 立即可推出

$$\begin{aligned}
&\sum_{n\leqslant x}\log n-2\sum_{n\leqslant\frac{x}{2}}\log n\\
&\quad=x\log 2+O(\log x)\\
&\quad=\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right)-2\sum_{n\leqslant\frac{x}{2}}\psi\left(\frac{x}{2n}\right)\\
&\quad=\psi(x)+\psi\left(\frac{x}{2}\right)+\psi\left(\frac{x}{3}\right)+\cdots-2\left(\psi\left(\frac{x}{2}\right)+\psi\left(\frac{x}{4}\right)+\psi\left(\frac{x}{6}\right)+\cdots\right)\\
&\quad=\psi(x)-\psi\left(\frac{x}{2}\right)+\psi\left(\frac{x}{3}\right)-\psi\left(\frac{x}{4}\right)+\psi\left(\frac{x}{5}\right)-\cdots<\psi(x),
\end{aligned}$$

因此必存在正常数 A_1, 使得

$$\psi(x)>A_1x. \tag{30}$$

为了证明 $\psi(x)$ 的上界, 我们还需要下面几个引理.

引理 6 设 $x\geqslant 1$, 则有

$$\left|\sum_{n\leqslant x}\frac{\mu(n)}{n}\right|\leqslant 1. \tag{31}$$

证 由第二章 (83) 式知

$$\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]=1,$$

所以

$$x\sum_{n\leqslant x}\frac{\mu(n)}{n}-\sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}=1.$$

由于 $0\leqslant\{t\}<1$, 因此

$$\begin{aligned}
x\left|\sum_{n\leqslant x}\frac{\mu(n)}{n}\right|&=\left|1+\sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}\right|\leqslant 1+\sum_{n\leqslant x}\left\{\frac{x}{n}\right\}\\
&=1+\{x\}+\sum_{2\leqslant n\leqslant x}\left\{\frac{x}{n}\right\}<1+\{x\}+[x]-1=x.
\end{aligned}$$

此即 (31). □

引理 7 设 $x>1$, 则

$$\sum_{n\leqslant x}\frac{\mu(n)}{n}\log\frac{x}{n}=O(1). \tag{32}$$

证 由第二章引理 1 知

$$\sum_{k\leqslant\frac{x}{n}}\frac{1}{k}=\log\frac{x}{n}+\gamma+O\left(\frac{n}{x}\right),$$

所以

$$\begin{aligned}\sum_{n\leqslant x}\frac{\mu(n)}{n}\log\frac{x}{n}&=\sum_{n\leqslant x}\frac{\mu(n)}{n}\left(\sum_{k\leqslant\frac{x}{n}}\frac{1}{k}-\gamma+O\left(\frac{n}{x}\right)\right)\\&=\sum_{n\leqslant x}\frac{\mu(n)}{n}\sum_{k\leqslant\frac{x}{n}}\frac{1}{k}-\gamma\sum_{n\leqslant x}\frac{\mu(n)}{n}+O(1)\\&=\sum_{n\leqslant x}\frac{\mu(n)}{n}\sum_{k\leqslant\frac{x}{n}}\frac{1}{k}+O(1)\\&=\sum_{d\leqslant x}\frac{1}{d}\sum_{n|d}\mu(n)+O(1)\\&=1+O(1)=O(1).\end{aligned}$$

引理得证. □

有了上面几个引理后, 我们可以来证明下面的不等式

$$\psi(x)<A_2x, \tag{33}$$

这里 A_2 为正常数.

因为

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{n}{d},$$

由第二章定理 16 及本章引理 6、引理 7 得到

$$\begin{aligned}\psi(x)&=\sum_{n\leqslant x}\Lambda(n)=\sum_{n\leqslant x}\mu(n)\sum_{m\leqslant\frac{x}{n}}\log m=\sum_{n\leqslant[x]-1}\mu(n)\sum_{m\leqslant\frac{x}{n}}\log m\\&=\sum_{n\leqslant[x]-1}\mu(n)\left(\frac{x}{n}\log\frac{x}{n}-\frac{x}{n}+O\left(\log\frac{x}{n}\right)\right)\\&=x\sum_{n\leqslant[x]-1}\frac{\mu(n)}{n}\log\frac{x}{n}-x\sum_{n\leqslant[x]-1}\frac{\mu(n)}{n}+O\left(\sum_{n\leqslant x}\log\frac{x}{n}\right)\\&=O(x)+O(x)+O(x)=O(x).\end{aligned}$$

此即 (33) 式.

定理 5 *存在正常数 C_1 及 C_2, 使得*

$$C_1\frac{x}{\log x}<\pi(x)<C_2\frac{x}{\log x}. \tag{34}$$

证 由 (23) 及 (28) 得到

$$\frac{\psi(x)}{x}=\frac{\pi(x)}{\frac{x}{\log x}}+o(1), \tag{35}$$

再由 (30), (33), (35) 得到 (34). □

下面给出 Chebyshev 不等式的几个应用.

定理 6 *设 $x>1$, 则*

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1), \tag{36}$$

$$\sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1). \tag{37}$$

证 因为

$$\sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right]=x\log x-x+O(\log x),$$

所以

$$x\sum_{n\leqslant x}\frac{\Lambda(n)}{n}-\sum_{n\leqslant x}\Lambda(n)\left\{\frac{x}{n}\right\}=x\log x+O(x),$$

亦即

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\log x+\frac{1}{x}\sum_{n\leqslant x}\Lambda(n)\left\{\frac{x}{n}\right\}+O(1).$$

由 $\psi(x)=O(x)$ 立即推出 (36). 而

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\sum_{p\leqslant x}\frac{\log p}{p}+\sum_{\substack{p^m\leqslant x\\ m\geqslant 2}}\frac{\log p}{p^m},\tag{38}$$

但

$$\sum_{\substack{p^m\leqslant x\\ m\geqslant 2}}\frac{\log p}{p^m}\leqslant\sum_{p\leqslant x}\log p\sum_{m\geqslant 2}\frac{1}{p^m}=O\left(\sum_{p\leqslant x}\frac{\log p}{p^2}\right)=O(1),$$

所以

$$\sum_{p\leqslant x}\frac{\log p}{p}=\sum_{n\leqslant x}\frac{\Lambda(n)}{n}+O(1)=\log x+O(1).\qquad\square$$

定理 7 设 $x\geqslant 2$, 则存在常数 C_3 使得

$$\sum_{p\leqslant x}\frac{1}{p}=\log\log x+C_3+O\left(\frac{1}{\log x}\right).\tag{39}$$

证 在引理 4 中, 令

$$S(x)=\sum_{n\leqslant x}\frac{C_n\log n}{n},$$

这里

$$C_n=\begin{cases}1, & \text{若 } n \text{ 为素数},\\ 0, & \text{其他},\end{cases}$$

则

$$\begin{aligned}\sum_{p\leqslant x}\frac{1}{p}&=\sum_{p\leqslant x}\frac{\log p}{p}\cdot\frac{1}{\log p}=\sum_{n\leqslant x}\frac{C_n\log n}{n}\cdot\frac{1}{\log n}\\&=\frac{S(x)}{\log x}+\int_2^x\frac{S(t)}{t\log^2 t}dt.\end{aligned}\tag{40}$$

由 (37) 式知

$$S(x)=\log x+R(x),\quad R(x)=O(1),$$

所以

$$\begin{aligned}\sum_{p\leqslant x}\frac{1}{p}&=\frac{\log x+O(1)}{\log x}+\int_2^x\frac{\log t+R(t)}{t\log^2 t}dt\\&=1+O\left(\frac{1}{\log x}\right)+\int_2^x\frac{dt}{t\log t}+\int_2^x\frac{R(t)}{t\log^2 t}dt\\&=\log\log x+1-\log\log 2+\int_2^\infty\frac{R(t)}{t\log^2 t}dt\\&\quad-\int_x^\infty\frac{R(t)}{t\log^2 t}dt+O\left(\frac{1}{\log x}\right).\end{aligned}\tag{41}$$

由于 $R(t)=O(1)$, 所以存在常数 A, 使得

$$\int_2^\infty\frac{R(t)}{t\log^2 t}dt=A,\tag{42}$$

而

$$\int_x^\infty\frac{R(t)}{t\log^2 t}dt=O\left(\int_x^\infty\frac{dt}{t\log^2 t}\right)=O\left(\frac{1}{\log x}\right).\tag{43}$$

由 (41), (42), (43) 即得 (39), 这里

$$C_3=1-\log\log 2+A.$$ □

定理 8 设 $x\geqslant 2$, 则存在常数 C_4 使得

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{C_4}{\log x}+O\left(\frac{1}{\log^2 x}\right).\tag{44}$$

证 令

$$y=\prod_{p\leqslant x}\left(1-\frac{1}{p}\right),$$

则

$$\begin{aligned}\log y &= \log \prod_{p\leqslant x}\left(1-\frac{1}{p}\right) = \sum_{p\leqslant x}\log\left(1-\frac{1}{p}\right)\\ &= \sum_{p\leqslant x}\left(-\frac{1}{p}\right)+\sum_{p\leqslant x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\\ &= -\sum_{p\leqslant x}\frac{1}{p}+\sum_{p}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)-\sum_{p>x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\\ &= -\log\log x - C_3 + O\left(\frac{1}{\log x}\right)+C_5+\sum_{n>x}O\left(\frac{1}{p^2}\right)\\ &= -\log\log x + C_6 + O\left(\frac{1}{\log x}\right), \end{aligned} \tag{45}$$

这里

$$C_6 = -C_3 + C_5, \quad C_5 = \sum_{p}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

由 (45) 式得到

$$y = e^{-\log\log x + C_6 + O(\frac{1}{\log x})},$$

所以

$$\begin{aligned}\prod_{p\leqslant x}\left(1-\frac{1}{p}\right) &= \frac{C_4}{\log x}e^{O(\frac{1}{\log x})} = \frac{C_4}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right)\\ &= \frac{C_4}{\log x}+O\left(\frac{1}{\log^2 x}\right).\end{aligned}$$

得证. □

§3 函数 $\omega(n)$ 与 $\Omega(n)$

$\omega(n)$ 与 $\Omega(n)$ 之值的分布亦很不均匀, 但我们有下面的均值定理.

定理 9

$$\sum_{n\leqslant x}\omega(n) = x\log\log x + C_7 x + O\left(\frac{x}{\log x}\right), \tag{46}$$

$$\sum_{n\leqslant x}\Omega(n) = x\log\log x + C_8 x + O\left(\frac{x}{\log x}\right). \tag{47}$$

证 先来证明 (46) 式

$$\begin{aligned}\sum_{n\leqslant x}\omega(n)&=\sum_{n\leqslant x}\sum_{p|n}1=\sum_{p\leqslant x}\left[\frac{x}{p}\right]=x\sum_{p\leqslant x}\frac{1}{p}+O(\pi(x))\\&=x\left(\log\log x+C_3+O\left(\frac{1}{\log x}\right)\right)+O\left(\frac{x}{\log x}\right)\\&=x\log\log x+C_3x+O\left(\frac{x}{\log x}\right),\end{aligned}$$

而

$$\sum_{n\leqslant x}\Omega(n)=\sum_{n\leqslant x}\sum_{p^k|n}1=\sum_{p^k\leqslant x}\left[\frac{x}{p^k}\right]=\sum_{p\leqslant x}\left[\frac{x}{p}\right]+\sum_{\substack{p^k\leqslant x\\k\geqslant 2}}\left[\frac{x}{p^k}\right],\tag{48}$$

$$\sum_{\substack{p^k\leqslant x\\k\geqslant 2}}\left[\frac{x}{p^k}\right]=\sum_{\substack{p^k\leqslant x\\k\geqslant 2}}\frac{x}{p^k}-\sum_{\substack{p^k\leqslant x\\k\geqslant 2}}\left\{\frac{x}{p^k}\right\},\tag{49}$$

但

$$\sum_{\substack{p^k\leqslant x\\k\geqslant 2}}\frac{x}{p^k}=x\sum_{k=2}^{\infty}\sum_{p}\frac{1}{p^k}+O\left(x\log x\sum_{p>\sqrt{x}}\frac{1}{p^2}\right)=C_9x+O\left(\frac{x}{\log x}\right),\tag{50}$$

$$\sum_{\substack{p^k\leqslant x\\k\geqslant 2}}\left\{\frac{x}{p^k}\right\}\leqslant\sum_{\substack{p^k\leqslant x\\k\geqslant 2}}1\leqslant\log x\sum_{p>\sqrt{x}}1=O\left(\frac{x}{\log x}\right).\tag{51}$$

由 (48)–(51) 得到

$$\sum_{n\leqslant x}\Omega(n)=x\log\log x+C_8x+O\left(\frac{x}{\log x}\right).$$ □

定理 10

$$\sum_{n\leqslant x}\omega^2(n)=x(\log\log x)^2+O(x\log\log x).\tag{52}$$

证 设 $n>1$, 考虑 n 的不同素因子对 p_1,p_2 ($p_1\neq p_2$, 但 p_1,p_2 与 p_2,p_1 算作不同的两对), p_1 可以取 $\omega(n)$ 个值, 对固定的 p_1,p_2 可以取 $\omega(n)-1$ 个值, 所以

$$\omega(n)(\omega(n)-1)=\sum_{\substack{p_1p_2|n\\p_1\neq p_2}}1=\sum_{p_1p_2|n}1-\sum_{p^2|n}1.$$

由上式得到

$$\sum_{n\leqslant x}\omega(n)(\omega(n)-1)=\sum_{n\leqslant x}\left(\sum_{p_1p_2|n}1-\sum_{p^2|n}1\right)$$
$$=\sum_{p_1p_2\leqslant x}\left[\frac{x}{p_1p_2}\right]-\sum_{p^2\leqslant x}\left[\frac{x}{p^2}\right]=\sum_{p_1p_2\leqslant x}\left[\frac{x}{p_1p_2}\right]+O(x). \tag{53}$$

由于

$$\sum_{p_1p_2\leqslant x}\left[\frac{x}{p_1p_2}\right]=x\sum_{p_1p_2\leqslant x}\frac{1}{p_1p_2}+O\left(\sum_{p_1p_2\leqslant x}1\right)$$
$$=x\sum_{p_1p_2\leqslant x}\frac{1}{p_1p_2}+O\left(\sum_{p\leqslant x}\pi\left(\frac{x}{p}\right)\right)$$
$$=x\sum_{p_1p_2\leqslant x}\frac{1}{p_1p_2}+O(x\log\log x), \tag{54}$$

但

$$\left(\sum_{p\leqslant\sqrt{x}}\frac{1}{p}\right)^2\leqslant\sum_{p_1p_2\leqslant x}\frac{1}{p_1p_2}\leqslant\left(\sum_{p\leqslant x}\frac{1}{p}\right)^2,$$

而上式两边都等于

$$(\log\log x+O(1))^2=(\log\log x)^2+O(\log\log x),$$

所以

$$\sum_{p_1p_2\leqslant x}\frac{1}{p_1p_2}=(\log\log x)^2+O(\log\log x). \tag{55}$$

由 (53)–(55) 得到

$$\sum_{n\leqslant x}\omega^2(n)=\sum_{n\leqslant x}\omega(n)+x(\log\log x)^2+O(x\log\log x)$$
$$=x(\log\log x)^2+O(x\log\log x).$$

定理得证. □

定理 11 任给 $\varepsilon>0$, 则在区间 $[1,x]$ 中使得

$$|\omega(n)-\log\log n|>(\log\log n)^{\frac{1}{2}+\varepsilon}$$

的个数为 $o(x)$.

证 将区间 $[1,x]$ 分成 $[1,x^{\frac{1}{e}}]$ 及 $(x^{\frac{1}{e}},x]$ 来考虑. $n\leqslant x^{\frac{1}{e}}$ 的个数显然为 $o(x)$, 而当 $n\in(x^{\frac{1}{e}},x]$ 时有

$$\log\log x-1<\log\log n\leqslant\log\log x,$$

所以我们只要证明使得下式成立

$$|\omega(n)-\log\log x|>(\log\log x)^{\frac{1}{2}+\varepsilon}$$

的 $n\leqslant x$ 的个数为 $o(x)$ 就行. 为此我们来考虑下面的均值估计

$$\begin{aligned}&\sum_{n\leqslant x}(\omega(n)-\log\log x)^2\\&\quad=\sum_{n\leqslant x}\omega^2(n)-2\log\log x\sum_{n\leqslant x}\omega(n)+[x](\log\log x)^2.\end{aligned}$$

将定理 9、定理 10 的结果代入上式即得

$$\sum_{n\leqslant x}(\omega(n)-\log\log x)^2=O(x\log\log x).\tag{56}$$

现在假设在 $[1,x]$ 中有 M 个 n 使得下式成立

$$|\omega(n)-\log\log x|>(\log\log x)^{\frac{1}{2}+\varepsilon},$$

则由 (56) 式得到

$$M\cdot(\log\log x)^{1+2\varepsilon}=O(x\log\log x),$$

所以

$$M=O\left(\frac{x}{(\log\log x)^{2\varepsilon}}\right).$$

定理得证. □

对于 $\Omega(n)$ 定理亦成立, 证明留给读者, 换句话说, 假若我们用 $f(n)$ 表示 $\omega(n)$ 或 $\Omega(n)$, 则在区间 $[1,x]$ 内, 对几乎所有的 n 恒有

$$f(n)\sim\log\log n. \tag{57}$$

§4 Bertrand 假设

本节主要证明在区间 $[n,2n]$ 中必有素数, 它称为 Bertrand 假设或猜想, 此猜想被 Chebyshev 首先证明. 先来证明几个引理.

引理 8 设 $x\geqslant 2$, 则

$$\prod_{p\leqslant x}p<4^x. \tag{58}$$

证 当 $2\leqslant x<3$ 时, 引理是显然成立的; 其次, 容易看出, 若当 $x=n$ 为 $\geqslant 3$ 的奇数时引理成立, 则当 $n\leqslant x<n+2$ 时由于

$$\prod_{p\leqslant x}p<4^m\leqslant 4^x,$$

所以引理亦成立. 因此我们只要对 n 为奇数的情况下用归纳法来证明即可.

因为引理在 $n=3$ 时成立, 现假设引理对小于某一奇数 $n\geqslant 5$ 的所有奇数都成立, 我们要证明引理对 $x=n$ 时亦成立.

令

$$K=\frac{n\pm 1}{2},$$

这里正负号的选取要保证 K 为奇数, 所以此时有 $n-K$ 为偶数, 且 $n-K=2K\pm 1-K\leqslant K+1$. 现在假设 p 为满足 $K<p\leqslant n$ 的奇素数, 则显有

$$p|n!,\quad p\nmid K!,\quad p\nmid (n-K)!,$$

所以对 $K<p\leqslant n$ 中的一切素数, 恒有

$$p\Big|\frac{n!}{K!(n-K)!}.$$

由此推出

$$\prod_{K<p\leqslant n} p \leqslant \binom{n}{K}, \tag{59}$$

但是 $\binom{n}{K} = \binom{n}{n-K}$ 皆为 $(1+1)^n$ 展开式之系数, 所以有

$$\binom{n}{K} < 2^{n-1}, \tag{60}$$

因此由归纳假设及上面的不等式得到

$$\prod_{p\leqslant n} p = \prod_{p\leqslant K} p \prod_{K<p\leqslant n} p < 4^K \cdot 2^{n-1} = 2^{n+2K-1} \leqslant 4^n.$$

引理得证. □

定理 12 设 $n>1$, 则在 $[n,2n]$ 中必有素数.

证 首先我们用下面的表来说明当 $n \leqslant 128$ 时定理成立.

$p=3,5$	$2 \leqslant n \leqslant 3$
7	$4 \leqslant n \leqslant 6$
13	$7 \leqslant n \leqslant 12$
23	$13 \leqslant n \leqslant 22$
43	$23 \leqslant n \leqslant 42$
83	$43 \leqslant n \leqslant 82$
131	$83 \leqslant n \leqslant 127$

下面我们用反证法来证明定理, 假设对某一 $n \geqslant 128$ 定理不成立, 即在 $[n,2n]$ 中没有素数, 由第一章定理 18 知

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p\leqslant 2n} p^{\alpha_p},$$

这里

$$\alpha_p = \sum_{j\geqslant 1} \left(\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right] \right).$$

由于假设在 $[n,2n]$ 中没有素数, 所以

$$\binom{2n}{n}=\prod_{p\leqslant 2n}p^{\alpha_p}=\prod_{p\leqslant n}p^{\alpha_p}, \tag{61}$$

但上式可写成

$$\binom{2n}{n}=\prod_{p\leqslant n}p^{\alpha_p}=\prod_{p\leqslant\sqrt{2n}}p^{\alpha_p}\prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n}p^{\alpha_p}\prod_{\frac{2}{3}n<p\leqslant n}p^{\alpha_p}. \tag{62}$$

我们分别处理这三个乘积.

1) 当 $p\leqslant\sqrt{2n}$ 时, 显然有

$$\prod_{p\leqslant\sqrt{2n}}p^{\alpha_p}\leqslant\prod_{p\leqslant\sqrt{2n}}2n. \tag{63}$$

2) 当 $\sqrt{2n}<p\leqslant\frac{2}{3}n$ 时, 因为 $p^2>2n$, 因此

$$\alpha_p=\sum_{j\geqslant 1}\left(\left[\frac{2n}{p^j}\right]-2\left[\frac{n}{p^j}\right]\right)=\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]\leqslant 1,$$

所以

$$\prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n}p^{\alpha_p}\leqslant\prod_{p\leqslant\frac{2}{3}n}p. \tag{64}$$

3) 当 $\frac{2}{3}n<p\leqslant n$ 时, 有

$$p^2>2n,\quad 1<\frac{n}{p}<\frac{3}{2},\quad 2\leqslant\frac{2n}{p}<3,$$

所以

$$\alpha_p=\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]=2-2=0,$$

因此

$$\prod_{\frac{2}{3}n<p\leqslant n}p^{\alpha_p}=1. \tag{65}$$

由 (62)–(65) 得到

$$\binom{2n}{n}\leqslant\prod_{p\leqslant\sqrt{2n}}2n\prod_{p\leqslant\frac{2}{3}n}p. \tag{66}$$

因为当 $n \geqslant 128$ 时, $\sqrt{2n} > 16$, 所以显然有

$$\pi(\sqrt{2n}) < \frac{\sqrt{2n}+1}{2} - 2 \tag{67}$$

(因为 $\pi(y)$ 显然不超过奇数的个数 $\frac{y+1}{2}$, 但当 $y > 16$ 时, $9, 15$ 不是素数, 所以可减去 2). 因此由引理 8 及 (66), (67) 得到

$$\binom{2n}{n} < (2n)^{\sqrt{\frac{n}{2}}-1} 4^{\frac{2n}{3}}. \tag{68}$$

另一方面, 由于 $\binom{2n}{n}$ 为 $(1+1)^{2n}$ 展开式中之系数中的最大者, 由于这 $2n+1$ 项中首项及末项皆为 1, 所以有

$$2n\binom{2n}{n} > 2^{2n},$$

亦即

$$\binom{2n}{n} > \frac{2^{2n}}{2n}. \tag{69}$$

由 (68), (69) 得到

$$\frac{2^{2n}}{2n} < (2n)^{\sqrt{\frac{n}{2}}-1} 4^{\frac{2}{3}n},$$

所以

$$2^{\frac{2}{3}n} < (2n)^{\sqrt{\frac{n}{2}}}.$$

将上式两边取对数, 得到

$$\sqrt{8n}\log 2 - 3\log 2n < 0. \tag{70}$$

令

$$f(n) = \sqrt{8n}\log 2 - 3\log 2n,$$

则有

$$f(128) = 8\log 2, \tag{71}$$

但

$$f'(n) = \frac{\sqrt{2n}\log 2 - 3}{n},$$

显然, 当 $n \geqslant 128$ 时, $f'(n) > 0$, 所以当 $n \geqslant 128$ 时, $f(n)$ 为递增函数, 但这与 (70) 矛盾. 定理得证. □

§5 函数 $M(x)$

设 $x \geqslant 1$, 令

$$M(x) = \sum_{n \leqslant x} \mu(n).$$

本节的目的是要证明

$$\lim_{x \to \infty} \frac{M(x)}{x} = 0 \tag{72}$$

与

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1 \tag{73}$$

等价.

定理 13 (72) 式与下式等价

$$\lim_{x \to \infty} \frac{H(x)}{x \log x} = 0, \tag{74}$$

这里

$$H(x) = \sum_{n \leqslant x} \mu(n) \log n. \tag{75}$$

证 由引理 4 得到

$$\begin{aligned} H(x) &= \sum_{n \leqslant x} \mu(n) \log n = M(x) \log x - \int_1^x \frac{M(t)}{t} dt \\ &= M(x) \log x + O(x), \end{aligned}$$

由上式即可看出 (72) 与 (74) 等价. □

定理 14 *若*

$$\psi(x) \sim x, \quad x \to \infty, \tag{76}$$

则

$$M(x) = o(x), \quad x \to \infty.$$

证 我们只要证明由 (76) 可推出 (74) 就行. 因为

$$\Lambda(n) = -\sum_{d|n} \mu(d)\log d,$$

所以

$$-\mu(n)\log n = \sum_{d|n} \mu(d)\Lambda\left(\frac{n}{d}\right).$$

现在我们在第二章定理 17 中, 取 $a = xe^{-\sqrt{\log x}}, b = e^{\sqrt{\log x}}$, 则

$$-\sum_{n\leqslant x} \mu(n)\log n = \sum_{n\leqslant a} \mu(n)\psi\left(\frac{x}{n}\right) + \sum_{n\leqslant b} \Lambda(n)M\left(\frac{x}{n}\right) - M(a)\psi(b). \quad (77)$$

若 (76) 成立, 则当 $n \leqslant a, x \to \infty$ 时有

$$\psi\left(\frac{x}{n}\right) = \frac{x}{n} + o\left(\frac{x}{n}\right),$$

所以

$$\begin{aligned}\sum_{n\leqslant a} \mu(n)\psi\left(\frac{x}{n}\right) &= x\sum_{n\leqslant a}\frac{\mu(n)}{n} + o\left(x\sum_{n\leqslant x}\frac{1}{n}\right)\\ &= O(x) + o(x\log x) = o(x\log x). \end{aligned} \quad (78)$$

由 (36) 式得到

$$\begin{aligned}\sum_{n\leqslant b} \Lambda(n)M\left(\frac{x}{n}\right) &= O\left(x\sum_{n\leqslant b}\frac{\Lambda(n)}{n}\right) = O(x\log b) + O(x)\\ &= O(x\sqrt{\log x}) + O(x) = o(x\log x), \end{aligned} \quad (79)$$

因为

$$M(a) = O(a), \quad \psi(b) = O(b),$$

所以

$$M(a)\psi(b) = O(ab) = O(x) = o(x\log x). \quad (80)$$

由 (77)–(80) 定理得证. □

定理 15

$$M(x) = o(x), \quad x \to \infty$$

包含

$$\psi(x) \sim x, \quad x \to \infty.$$

证 首先我们来证明下面的公式

$$\psi(x) = x - \sum_{lk \leqslant x} \mu(l) f(k) + O(1), \tag{81}$$

这里

$$f(n) = d(n) - \log n - 2\gamma. \tag{82}$$

为了证明 (81) 式, 我们从下面几个式子出发

$$[x] = \sum_{n \leqslant x} 1; \quad \psi(x) = \sum_{n \leqslant x} \Lambda(n); \quad 1 = \sum_{n \leqslant x} I(n).$$

因为

$$d(n) = \sum_{l|n} 1,$$

所以

$$1 = \sum_{l|n} \mu(l) d\left(\frac{n}{l}\right).$$

另外

$$\Lambda(n) = \sum_{l|n} \mu(l) \log \frac{n}{l},$$
$$I(n) = \sum_{l|n} \mu(l).$$

因此我们有

$$\begin{aligned}
[x] - \psi(x) - 2\gamma &= \sum_{n \leqslant x} (1 - \Lambda(n) - 2\gamma I(n)) \\
&= \sum_{n \leqslant x} \sum_{l|n} \mu(l) \left(d\left(\frac{n}{l}\right) - \log \frac{n}{l} - 2\gamma \right) \\
&= \sum_{lk \leqslant x} \mu(l)(d(k) - \log k - 2\gamma).
\end{aligned}$$

由上式立即推出

$$\psi(x) = x - \sum_{lk\leqslant x} \mu(l)f(k) + O(1),$$

这里 $f(k)$ 由 (82) 式定义, 因此定理的关键是要证明

$$\sum_{lk\leqslant x} \mu(l)f(k) = o(x), \quad x \to \infty. \tag{83}$$

由第二章定理 17 得到

$$\sum_{lk\leqslant x} \mu(l)f(k) = \sum_{n\leqslant a} \mu(n)F\left(\frac{x}{n}\right) + \sum_{n\leqslant b} f(n)M\left(\frac{x}{n}\right) - M(a)F(b), \tag{84}$$

这里

$$F(x) = \sum_{n\leqslant x} f(n),$$

a, b 为满足 $ab = x$ 的任意正数.

设 $\varepsilon > 0$ 为任给的正数, 要证一定存在一个 $x_0 = x_0(\varepsilon)$, 使当 $x > x_0$ 时,

$$\left|\sum_{lk\leqslant x} \mu(l)f(k)\right| < \varepsilon x. \tag{85}$$

为此我们先来求 $F(x)$ 的估计式

$$\begin{aligned} F(x) &= \sum_{n\leqslant x} d(n) - \sum_{n\leqslant x} \log n - 2\gamma \sum_{n\leqslant x} 1 \\ &= x\log x + (2\gamma - 1)x + O(\sqrt{x}) - x\log x + x + O(\log x) - 2\gamma x + O(1) \\ &= O(\sqrt{x}) + O(\log x) + O(1) = O(\sqrt{x}), \end{aligned}$$

所以必有正常数 A 存在, 使得

$$|F(x)| \leqslant A\sqrt{x}, \quad x \geqslant 1. \tag{86}$$

利用 (86) 式我们得到

$$\left|\sum_{n\leqslant a} \mu(n)F\left(\frac{x}{n}\right)\right| \leqslant A\sum_{n\leqslant a} \sqrt{\frac{x}{n}} \leqslant 2A\sqrt{xa} = \frac{2Ax}{\sqrt{b}}. \tag{87}$$

为了估计和式 $\sum\limits_{n\leqslant b} f(n)M(\frac{x}{n})$, 我们首先由 $f(n)$ 的定义看出, 必有 $B>0$ 存在, 使得

$$|f(n)|\leqslant B\sqrt{n}. \tag{88}$$

另外由 $M(x)=o(x)$ 知, 必存在 $x_1=x_1(\varepsilon)$, 使得当 $x>x_1$ 时,

$$|M(x)|\leqslant \frac{1}{36AB}\varepsilon^2 x. \tag{89}$$

现在我们取 $b=\frac{36A^2}{\varepsilon^2}, a=\frac{x}{b}, x_0=x_1 b$, 则当 $x>x_0$ 时,

$$\begin{aligned}\left|\sum_{n\leqslant b} f(n)M\left(\frac{x}{n}\right)\right| &\leqslant \sum_{n\leqslant b}|f(n)|\left|M\left(\frac{x}{n}\right)\right| \\ &\leqslant \frac{\varepsilon^2}{36AB}x\sum_{n\leqslant b}\frac{|f(n)|}{n} \\ &\leqslant \frac{\varepsilon^2}{36A}x\sum_{n\leqslant b}\frac{1}{\sqrt{n}} \\ &\leqslant \frac{\varepsilon^2}{36A}x\cdot 2\sqrt{b}=\frac{\varepsilon}{3}x. \end{aligned}\tag{90}$$

将 b 的选取代入 (87) 式得到

$$\left|\sum_{n\leqslant a}\mu(n)F\left(\frac{x}{n}\right)\right|\leqslant \frac{\varepsilon}{3}x, \tag{91}$$

而

$$|F(b)M(a)|\leqslant A\sqrt{b}a\leqslant \frac{Ax}{\sqrt{b}}\leqslant \frac{\varepsilon}{3}x. \tag{92}$$

由 (84), (90), (91) 及 (92) 式得到, 当 $x>x_0$ 时, 有

$$\left|\sum_{lk\leqslant x}\mu(l)f(k)\right|<\varepsilon x.$$

定理得证. □

§6 函数 $L(x)$

本节主要证明下面的定理.

定理 16 设 $x>1$, 则

$$L(x)=\sum_{n\leqslant x}\lambda(n)=o(x) \tag{93}$$

与

$$\sum_{n\leqslant x}\mu(n)=o(x) \tag{94}$$

等价.

证 先证由 (94) 可推出 (93). 因为 $\lambda=g*\mu$, 所以由第二章 (86) 知

$$\sum_{n\leqslant x}\lambda(n)=\sum_{n\leqslant x^{\frac{2}{3}}}g(n)M\left(\frac{x}{n}\right)+\sum_{n\leqslant x^{\frac{1}{3}}}\mu(n)G\left(\frac{x}{n}\right)-G(x^{\frac{2}{3}})M(x^{\frac{1}{3}}),$$

这里

$$G(x)=\sum_{n\leqslant x}g(n).$$

因为

$$g(n)=\begin{cases}1, & n=K^2,\\ 0, & \text{其他},\end{cases}$$

所以

$$\begin{aligned}\sum_{n\leqslant x}\lambda(n)&=o\left(x\sum_{n\leqslant x^{\frac{2}{3}}}\frac{g(n)}{n}\right)+O\left(\sum_{n\leqslant x^{\frac{1}{3}}}G\left(\frac{x}{n}\right)\right)+o(x)\\&=o\left(x\sum_{n=1}^{\infty}\frac{1}{n^2}\right)+O\left(\sqrt{x}\sum_{n\leqslant x^{\frac{1}{3}}}\frac{1}{\sqrt{n}}\right)+o(x)\\&=o(x)+o(x)+o(x)=o(x).\end{aligned} \tag{95}$$

下面来证由 (93) 可推出 (94).

由第二章习题 7 知

$$\mu(n)=\sum_{d^2|n}\mu(d)\lambda\left(\frac{n}{d^2}\right)=\sum_{n=d^2k}\mu(d)\lambda(k),$$

所以

$$\sum_{n\leqslant x}\mu(n)=\sum_{n\leqslant x}\sum_{n=d^2k}\mu(d)\lambda(k)=\sum_{d^2k\leqslant x}\mu(d)\lambda(k)=\sum_{d\leqslant\sqrt{x}}\mu(d)\sum_{k\leqslant\frac{x}{d^2}}\lambda(k), \tag{96}$$

由上式得到

$$\begin{aligned}\sum_{n\leqslant x}\mu(n)&=\sum_{d\leqslant x^{\frac{1}{3}}}\mu(d)\sum_{k\leqslant\frac{x}{d^2}}\lambda(k)+O\left(\sum_{k\leqslant x^{\frac{1}{3}}}\sum_{d\leqslant\sqrt{\frac{x}{k}}}1\right)\\&=o(x)+o(x)=o(x).\end{aligned}$$

证毕. □

习题

1. 试证 $\prod\limits_{p}\frac{p^2}{p^2-1}=\frac{\pi^2}{6}$.
2. 试证级数 $\sum\limits_{p}\frac{1}{p}$ 发散.
3. 试证数列 $\{6n-1\}$ 中包含无限个素数.
4. 设 $f(x)$ 为一整系数多项式, 则在数列 $\{f(n)\}$ 中有无限个不同的素因子.
5. 利用 $\prod\limits_{p\leqslant x}(1-\frac{1}{p})^{-1}\leqslant\prod\limits_{K=2}^{\pi(x)+1}(1-\frac{1}{K})^{-1}$, 证明:
   (1) $\pi(x)>\log x-1$; (2) $p_n<3^{n+1}$ (p_n 为第 n 个素数).
6. 设 $x>1, s=\pi(\sqrt{x}), p=p_1p_2\cdots p_s$, 则
$$\pi(x)-\pi(\sqrt{x})+1=\sum_{n|p}\mu(n)\left[\frac{x}{n}\right].$$
7. 利用第二章定理 18 及引理 4 证明:
$$\sum_{n\leqslant x}\frac{d(n)}{n}=\frac{1}{2}\log^2x+O(\log x),\quad x\geqslant 2.$$

8. 设 $x \geqslant 2$, 试证:
$$\sum_{n\leqslant x} d^2(n) = O(x\log^3 x).$$

9. 设 $x \geqslant 1$, 则 $\sum\limits_{n\leqslant x} \frac{\varphi(n)}{n} = \frac{6}{\pi^2}x + O(\log x)$.

10. 利用 $\frac{n}{\varphi(n)} = \prod\limits_{p|n}(1-\frac{1}{p})^{-1} = \left(\sum\limits_{d|n}\frac{\mu(d)}{d}\right)^{-1}$, 证明:
(1) $\sum\limits_{n\leqslant x}\frac{n}{\varphi(n)} = O(x)$;　　(2) $\sum\limits_{n\leqslant x}\frac{1}{\varphi(n)} = O(\log x)$.

11. 设 $x \geqslant 1$, 试证存在正常数 B_1, B_2 使
$$B_2 x < \theta(x) < B_1 x.$$

12. 设 p_n 为第 n 个素数, 则存在正常数 C_1, C_2 使
$$C_2 n\log n < p_n < C_1 n\log n.$$

13. 试证级数 $\sum\limits_{p}\frac{1}{p(\log\log p)^\alpha}$ 当 $\alpha > 1$ 时收敛; 当 $\alpha \leqslant 1$ 时发散.

14. 试证 $\prod\limits_{2<p\leqslant x}(1-\frac{2}{p}) = \frac{A+O(1)}{\log^2 x}$, 其中 A 为一绝对常数.

15. 试证 $\sum\limits_{p|x}\frac{\log p}{p} = O(\log\log x)$.

16. 设 $x \geqslant 3$, 则 $\sum\limits_{d|x}\frac{\mu(d)\log d}{d} = O(\log\log x)$.

17. 试证: 存在正常数 C, 使 $n \geqslant 3$ 时
$$\varphi(n) > C\frac{n}{\log\log n}.$$

18. 设 $s > 1$, 记 $\zeta(s) = \sum\limits_{n=1}^{\infty}\frac{1}{n^s}$ (即 Riemann 函数), 试证:
(1) $\sum\limits_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$　　$(s>1)$;
(2) $\sum\limits_{n=1}^{\infty}\frac{d(n)}{n^s} = \zeta^2(s)$　　$(s>1)$;
(3) $\sum\limits_{n=1}^{\infty}\frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$　　$(s>1)$.

19. 试证 $\sum\limits_{n=1}^{\infty}\frac{\mu(n)}{n} = 0$ 与 $M(x) = o(x)$ 是等价的.

20. 试证 $\sum\limits_{n\leqslant x}\frac{1-\Lambda(n)}{n} = 2\gamma + o(1)$ 和素数定理等价.

第四章　同余

§1　概念及基本性质

定义 1　给定正整数 m, 称为模, a, b 为任意两个整数, 若它们被 m 除后所得的余数相同, 即

$$a = q_1 m + \gamma_1, \qquad 0 \leqslant \gamma_1 < m,$$

$$b = q_2 m + \gamma_2, \qquad 0 \leqslant \gamma_2 < m,$$

$$\gamma_1 = \gamma_2,$$

则称 a, b 对模 m 同余, 记作

$$a \equiv b \,(\mathrm{mod}\, m) \tag{1}$$

或简记为 $a \equiv b\ (m)$. 这个式子称为模 m 的同余式.

若所得余数不同, 即 $\gamma_1 \neq \gamma_2$, 则称 a, b 对模 m 不同余, 记作

$$a \not\equiv b \,(\mathrm{mod}\, m)$$

或简记为 $a \not\equiv b\ (m)$.

由定义知, 记号 $a \equiv b\ (m)$ 和 $b \equiv a\ (m)$ 是一样的, 同样 $a \not\equiv b\ (m)$ 和 $b \not\equiv a\ (m)$ 亦是一样的.

定理 1 (1) 式成立的充要条件为

$$m|(a-b). \tag{2}$$

证 若 (1) 式成立, 即有

$$a = q_1 m + \gamma_1,$$
$$b = q_2 m + \gamma_2,$$
$$\gamma_1 = \gamma_2,$$

所以

$$a - b = (q_1 - q_2)m,$$

此即

$$m|(a-b).$$

反之, 若 $m|(a-b)$, 设

$$a = q_1 m + \gamma_1, \quad 0 \leqslant \gamma_1 < m,$$
$$b = q_2 m + \gamma_2, \quad 0 \leqslant \gamma_2 < m,$$

则有

$$a - b = (q_1 - q_2)m + (\gamma_1 - \gamma_2),$$

因为 $m|(a-b)$, 所以必有 $m|(\gamma_1 - \gamma_2)$, 但 $|\gamma_1 - \gamma_2| < m$, 必有 $\gamma_1 = \gamma_2$, 亦即 $a \equiv b\ (m)$. □

同余式有三个最基本的性质:

(1) $a \equiv a \pmod{m}$,

(2) $a \equiv b \pmod{m} \Longleftrightarrow b \equiv a \pmod{m}$,

(3) $a \equiv b \pmod{m},\ b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$.

和等式相类似的性质有

(4) $a_i \equiv b_i \,(\mathrm{mod}\, m),\ i=1,2 \Longrightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \,(\mathrm{mod}\, m)$,

(5) $a_i \equiv b_i \,(\mathrm{mod}\, m),\ i=1,2 \Longrightarrow a_1 a_2 \equiv b_1 b_2 \,(\mathrm{mod}\, m)$,

(6) $c \equiv d \,(\mathrm{mod}\, m),\ (c,m)=1$, 则 $ac \equiv bd \,(\mathrm{mod}\, m)$ 与 $a \equiv b \,(\mathrm{mod}\, m)$ 等价.

从性质 (4) 及 (5) 可得到下面的一般结果.

定理 2 若 $A_{\alpha_1,\alpha_2,\cdots,\alpha_K} \equiv B_{\alpha_1,\alpha_2,\cdots,\alpha_K} \,(\mathrm{mod}\, m),\ x_i \equiv y_i \ (\mathrm{mod}\ m), 1 \leqslant i \leqslant K$, 则

$$\sum_{\alpha_1 \cdots \alpha_K} A_{\alpha_1,\alpha_2,\cdots,\alpha_K} x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_K^{\alpha_K} \equiv \sum_{\alpha_1 \cdots \alpha_K} B_{\alpha_1,\alpha_2,\cdots,\alpha_K} y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_K^{\alpha_K} \,(\mathrm{mod}\, m),$$

特别地, 若 $a_i \equiv b_i \,(\mathrm{mod}\, m),\ 1 \leqslant i \leqslant n, x \equiv y \,(\mathrm{mod}\, m)$, 则

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv b_n y^n + b_{n-1} y^{n-1} + \cdots + b_1 y + b_0 \ (\mathrm{mod}\ m).$$

上面的定理是可用来检验一个数 K 是否是 m 的倍数的简单方法, 而不用具体地去把 m 除 K 计算出来, 有时这种计算是不可能的, 从这一方法也得到了整数被 $3,7,9,11,13$ 等数整除的判别法.

例 1 设 K 为正整数, 试求出它能为 9 整除的判别法.

解 设 K 的十进位表示为

$$K = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^l a_l.$$

因为

$$10^i \equiv 1 \,(\mathrm{mod}\, 9), \quad 1 \leqslant i \leqslant l,$$

所以由定理 2 知

$$K \equiv a_0 + a_1 + \cdots + a_l \,(\mathrm{mod}\, 9),$$

故

$$K \equiv a_0 + a_1 + \cdots + a_l \equiv 0 \,(\mathrm{mod}\, 9),$$

即为整数能被 9 整除的判别法.

例如 $K = 135$ 能被 9 整除, 因为此时 $a_2 = 1, a_1 = 3,\ a_0 = 5,\ 135 \equiv 1 + 3 + 5 \equiv 0 \,(\mathrm{mod}\, 9)$.

而当 $K = 2476$ 不能被 9 整除, 因为此时

$$a_0 + a_1 + a_2 + a_3 = 6 + 7 + 4 + 2 = 19 \not\equiv 0 \,(\mathrm{mod}\, 9). \qquad \square$$

定理 3 设 $K \neq 0$, 则

$$a \equiv b \ (\mathrm{mod}\, m) \Longleftrightarrow aK \equiv bK \,(\mathrm{mod}\, Km). \tag{3}$$

定理 4 设 $aC \equiv bC \ (\mathrm{mod}\, m),\ d = (m, C)$, 则

$$a \equiv b \ \left(\mathrm{mod}\, \frac{m}{d}\right). \tag{4}$$

证 因为 $aC \equiv bC \,(\mathrm{mod}\, m)$, 所以

$$m | C(a - b).$$

由上式推出

$$\frac{m}{d} \left| \frac{C}{d}(a - b), \right.$$

但 $(\frac{m}{d}, \frac{C}{d}) = 1$, 所以

$$\frac{m}{d} \Big| (a - b),$$

此即 (4). $\square$

定理 5 设 $d \neq 0, d|m, a \equiv b \,(\mathrm{mod}\, m)$, 则

$$a \equiv b \,(\mathrm{mod}\, d).$$

定理 6 设 $a \equiv b \,(\mathrm{mod}\, m_1),\ a \equiv b \,(\mathrm{mod}\, m_2)$, 则

$$a \equiv b \,(\mathrm{mod}\, [m_1, m_2]).$$

反之亦然.

定理 7 设 $a \equiv b \pmod{m}$, 则

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

反之则不然.

上面几个定理的证明可以由定义直接得出.

§2 剩余类及剩余系

在同余式的运算中, 两个同余的数所起的作用是一样的, 所以对这些数, 我们可以不加区别. 这就引入剩余类及其代表 —— 剩余系的概念.

定义 2 设 m 为自然数, 称为模, 所有对 m 同余的整数所组成的集合叫做模 m 的一个剩余类 (或同余类), 如果这剩余类中的数和模 m 是互素的, 那么它就称为模 m 的一个互素剩余类.

由剩余类及互素剩余类的定义可以看出, 全体整数可分为 m 个互不相交的模 m 的剩余类 $K_0, K_1, \cdots, K_{m-1}$, 其中 K_γ $(0 \leqslant \gamma \leqslant m-1)$ 为由所有形如

$$qm + \gamma \quad (q = 0, \pm 1, \pm 2, \cdots)$$

的整数组成. 全体和 m 互素的整数可分为 $\varphi(m)$ 个互不相交的模 m 的互素剩余类 K_γ, 这里 K_γ $(0 \leqslant \gamma \leqslant m-1,\ (\gamma, m) = 1)$ 由所有形如

$$qm + \gamma \quad (q = 0, \pm 1, \pm 2, \cdots)$$

的整数组成.

定义 3 在每一个剩余类 K_γ $(0 \leqslant \gamma \leqslant m-1)$ 中任取一数 a_γ, 我们把 $a_0, a_1, \cdots, a_{m-1}$ 叫做模 m 的一个完全剩余系, 在每一个互素剩余类 K_γ $(0 \leqslant \gamma \leqslant m-1, (\gamma, m) = 1)$ 中任取一数 a_γ, 则所有的 a_γ $(0 \leqslant \gamma \leqslant m-1)$ 称为模 m 的一个简化 (互素) 剩余系.

显然, 有无穷多个完全剩余系及简化剩余系.

完全剩余系简称为完全系, 它的一般形式为

$$a_\gamma = q_\gamma m + \gamma, \quad 0 \leqslant \gamma \leqslant m-1.$$

它取决于 q_γ 的选取, 例如取 $q_\gamma = 0$, 得到

$$0, 1, 2, \cdots, m-1,$$

称为模 m 的最小非负完全系.

若当 $\frac{m}{2} > \gamma \geqslant 0$ 时, 取 $q_\gamma = 0$, 当 $m-1 \geqslant \gamma - [\frac{m}{2}]$ 时, 取 $q_\gamma = -1$, 这样得到的完全系叫做模 m 的绝对最小完全系, 此时有

$$-\frac{m}{2}, -\frac{m}{2}+1, \cdots, -1, 0, 1, 2, \cdots, \frac{m}{2}-1 \text{ (当 } m \text{ 为偶数)}$$

及

$$-\frac{m-1}{2}, -\frac{m-1}{2}+1, \cdots, -1, 0, 1, \cdots, \frac{m-1}{2} \text{ (当 } m \text{ 为奇数).}$$

这两种剩余系的取法, 实际上相当于带余除法中余数的取法. 这两种取法是最常用的. 当然应分别对具体问题选取适当的剩余系.

简化剩余系简称为简化系, 它的一般形式为

$$a_\gamma = q_\gamma m + \gamma, \quad 0 \leqslant \gamma \leqslant m-1, \quad (\gamma, m) = 1.$$

q_γ 可任意选取, $q_\gamma = 0$ 是最常用的取法, 此时为

$$\gamma, \quad (\gamma, m) = 1, \quad 0 \leqslant \gamma \leqslant m-1.$$

当 $m = p$ 为素数时, 最常用的简化系为

$$1, 2, \cdots, p-1.$$

由完全系与简化系的定义立即可得出下面的定理.

定理 8 m 个整数组成模 m 的一个完全系的充要条件是这 m 个数两两对模 m 不同余.

定理 9 $\varphi(m)$ 个整数组成模 m 的一个简化系的充要条件是这些数与 m 互素且它们对模 m 两两不同余.

上面两个定理给出了完全系与简化系的判别法. 它们的证明是基于这样的事实: K 样东西放入 K 个匣中, 且不能有两个在同一匣中, 则恰好每个匣中有一个.

定理 10 设 m 为自然数, K,l 为任意数, $(K,m)=1$, 则当 x 通过 m 的完全系时, $Kx+l$ 亦通过 m 的一个完全系.

证 只要证明

$$Kx_0+l, Kx_1+l, \cdots, Kx_{m-1}+l$$

对模 m 两两不同余. 设 $i\neq j$, 若

$$Kx_i+l \equiv Kx_j+l \,(\mathrm{mod}\, m),$$

但 $(K,m)=1$, 所以

$$x_i \equiv x_j \,(\mathrm{mod}\, m).$$

因为 $i\neq j$, 所以上式与 $x_i\,(0\leqslant i\leqslant m-1)$ 为完全系的假设相矛盾. 定理得证. □

定理 11 设 m 为自然数, K, l 为任意整数, $(K,m)=1$, 则当 x 通过 m 的简化系时 $Kx+lm$ 亦通过 m 的一个简化系.

证 设 $x_1, x_2, \cdots, x_{\varphi(m)}$ 为模的一个简化系, 要证明

$$Kx_1+lm, Kx_2+lm, \cdots, Kx_{\varphi(m)}+lm$$

亦为模 m 的一个简化系. 设 $1\leqslant i\leqslant \varphi(m)$, 则

$$(Kx_i+lm, m)=(Kx_i, m)=(x_i, m)=1.$$

再设 $i\neq j$, 且有

$$Kx_i+lm \equiv Kx_j+lm \,(\mathrm{mod}\, m),$$

则由于 $(K,m)=1$, 可推出

$$x_i \equiv x_j \pmod{m}.$$

定理得证. □

例如, x 和 $m-x$ 同时通过模 m 的简化系.

定理 12 设 m_1, m_2 为自然数, $(m_1,m_2)=1$, 则当 x,y 分别通过模 m_1, m_2 的完全 (简化) 系时, m_2x+m_1y 通过模 $m=m_1m_2$ 的完全 (简化) 系.

证 首先来证明当 x,y 通过 m_1,m_2 的完全系时, m_2x+m_1y 通过 m_1m_2 的完全系. 因为 m_2x+m_1y 共有 m_1m_2 个数, 所以由定理 8 知只要证明这些数两两对模 m_1m_2 不同余. 设

$$m_2x+m_1y \equiv m_2x'+m_1y' \pmod{m},$$

所以

$$\begin{aligned} m_2(x-x') &\equiv m_1(y-y') \pmod{m},\\ m_2(x-x') &\equiv m_1(y-y') \pmod{m_1},\\ m_2(x-x') &\equiv m_1(y-y') \pmod{m_2}, \end{aligned}$$

因此

$$\begin{aligned} m_2(x-x') &\equiv 0 \pmod{m_1},\\ m_1(y-y') &\equiv 0 \pmod{m_2}. \end{aligned}$$

由于 $(m_1,m_2)=1$, 故由上面两式得到

$$\begin{aligned} x &\equiv x' \pmod{m_1},\\ y &\equiv y' \pmod{m_2}. \end{aligned}$$

上式即证明了 m_2x+m_1y 当 x,y 通过 m_1,m_2 的完全系时是两两不同余的.

其次来证明当 x, y 分别通过模 m_1, m_2 的简化系时 $m_2x + m_1y$ 通过模 m_1m_2 的简化系. 从上面的证明中, 已经知道这些数对模 m_1m_2 是两两不同余的, 剩下只要证明

$$(m_2x + m_1y, m_1m_2) = 1.$$

设

$$(x, m_1) = (y, m_2) = 1,$$

由于 $(m_1, m_2) = 1$, 所以有

$$(m_2x, m_1) = (m_1y, m_2) = 1,$$

从而有

$$(m_2x + m_1y, m_1) = (m_2x + m_1y, m_2) = 1,$$

所以 $(m_2x + m_1y, m_1m_2) = 1$.

反之, 若 $(m_2x + m_1y, m_1m_2) = 1$, 亦必有

$$(x, m_1) = (y, m_2) = 1.$$

于是定理证毕. □

从定理我们顺便得到下面的已知公式

$$\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2), \quad (m_1, m_2) = 1.$$

从定理 11 还可以得到下面的 Euler 定理.

定理 13 (Euler) 设 $m > 1$, $(a, m) = 1$, 则

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

证 设 $x_1, x_2, \cdots, x_{\varphi(m)}$ 为模 m 的一个简化系. 因为 $(a, m) = 1$, 所以由定理 11 知

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

通过模 m 的一个简化系. 所以有

$$(ax_1)(ax_2)\cdots(ax_{\varphi(m)}) \equiv x_1x_2\cdots x_{\varphi(m)} \pmod m.$$

因为

$$(x_1x_2\cdots x_{\varphi(m)}, m) = 1,$$

因此我们得到

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

定理证毕. □

在 Euler 定理中取 $m = p$ 为素数, 则得到

定理 14 (Fermat) 设 $(a, p) = 1$, 则

$$a^{p-1} \equiv 1 \pmod p.$$

我们再来给出定理 9–11 的一个重要应用. 设 $f(n)$ 为以模 m 为周期的数论函数. 令

$$F(m) = \sum_{x \pmod m} f(x) \text{ 表示对模 } m \text{ 的一个完全系求和,}$$
$$G(m) = \sum_{x \pmod m} f(x) \text{ 表示对模 } m \text{ 的一个简化系求和.}$$

这样由定理 10, 11 得到如下定理.

定理 15 设 l, K 为整数, 则

$$\sum_{x \pmod m} f(x) = \sum_{x \pmod m} f(Kx + l), \quad (K, m) = 1,$$
$$\sum_{x \pmod m}{}' f(x) = \sum_{x \pmod m}{}' f(Kx + lm), \quad (K, m) = 1.$$

定理 16 设 $f(n) = e^{2\pi i \frac{n}{m}}$, 则 $F(m), G(m)$ 均为 m 的可乘函数.

证 设 $m=m_1m_2,\ (m_1,m_2)=1$, 则由定理 10–12 得到

$$\begin{aligned}F(m)&=\sum_{x\,(\mathrm{mod}\,m)}f(x)=\sum_{x_1\,(\mathrm{mod}\,m_1)}\sum_{x_2\,(\mathrm{mod}\,m_2)}f(m_2x_1+m_1x_2)\\&=\sum_{x_1\,(\mathrm{mod}\,m_1)}f(m_2x_1)\sum_{x_2\,(\mathrm{mod}\,m_2)}f(m_1x_2)=F(m_1)F(m_2),\\G(m)&=\sum_{x\,(\mathrm{mod}\,m)}{}'f(x)=\sum_{x_1\,(\mathrm{mod}\,m_1)}{}'\sum_{x_2\,(\mathrm{mod}\,m_2)}{}'f(m_2x_1+m_1x_2)\\&=\sum_{x_1\,(\mathrm{mod}\,m_1)}{}'f(m_2x_1)\sum_{x_2\,(\mathrm{mod}\,m_2)}{}'f(m_1x_2)=G(m_1)G(m_2),\end{aligned}$$

所以 $F(m),G(m)$ 均为可乘函数. □

下面来给出该定理的两个应用.

定理 17 设 m 为自然数, a 为整数, 则

$$\sum_{x\,(\mathrm{mod}\,m)}e^{2\pi i\frac{ax}{m}}=\begin{cases}m, & \text{若 } m|a,\\0, & \text{其他.}\end{cases}$$

证 由定理 15 知, 我们可取一特殊的完全系来求和:

$$\sum_{x\,(\mathrm{mod}\,m)}e^{2\pi i\frac{ax}{m}}=\sum_{x=0}^{m-1}e^{2\pi i\frac{ax}{m}}.$$

当 $m|a$ 时, $e^{2\pi i\frac{ax}{m}}=1$, 所以

$$\sum_{x=0}^{m-1}e^{2\pi i\frac{ax}{m}}=m. \tag{5}$$

今设 $m\nmid a$, 则 $e^{2\pi i\frac{a}{m}}\neq 1$, 因此

$$\sum_{x=0}^{m-1}e^{2\pi i\frac{ax}{m}}=\sum_{x=0}^{m-1}(e^{2\pi i\frac{a}{m}})^x=\frac{1-(e^{2\pi i\frac{a}{m}})^m}{1-e^{2\pi i\frac{a}{m}}}=0.$$

证毕. □

定理 18 设 q,m 为自然数, $(m,q)=1$, 则

$$\sum_{\substack{h=1\\(h,q)=1}}^{q}e^{2\pi i\frac{hm}{q}}=\mu(q). \tag{6}$$

证 由定理 16 知

$$\sum_{\substack{h=1\\(h,q)=1}}^{q} e^{2\pi i\frac{hm}{q}}$$

为 q 的可乘函数.

当 $q=1$, (6) 式显然成立, 现设 $q=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, 则有

$$\sum_{\substack{h=1\\(h,q)=1}}^{q} e^{2\pi i\frac{hm}{q}} = \sum_{\substack{h_1=1\\(h_1,p_1^{\alpha_1})=1}}^{p_1^{\alpha_1}} e^{2\pi i\frac{h_1 m}{p_1^{\alpha_1}}}\cdots\sum_{\substack{h_s=1\\(h_s,p_s^{\alpha_s})=1}}^{p_s^{\alpha_s}} e^{2\pi i\frac{h_s m}{p_s^{\alpha_s}}}. \tag{7}$$

所以, 问题变成计算和式

$$\sum_{\substack{h_j=1\\(h_j,p_j^{\alpha_j})=1}}^{p_j^{\alpha_j}} e^{2\pi i\frac{h_j m}{p_j^{\alpha_j}}}. \tag{8}$$

显然有

$$\begin{aligned}\sum_{\substack{h_j=1\\(h_j,p_j^{\alpha_j})=1}}^{p_j^{\alpha_j}} e^{2\pi i\frac{h_j m}{p_j^{\alpha_j}}} &= \sum_{h_j=1}^{p_j^{\alpha_j}} e^{2\pi i\frac{h_j m}{p_j^{\alpha_j}}} - \sum_{\substack{h_j=1\\(h_j,p_j^{\alpha_j})>1}}^{p_j^{\alpha_j}} e^{2\pi i\frac{h_j m}{p_j^{\alpha_j}}}\\ &= 0-\sum_{h_j=1}^{p_j^{\alpha_j-1}} e^{2\pi i\frac{h_j m}{p_j^{\alpha_j-1}}}.\end{aligned}$$

上式第二项当 $\alpha_j=1$ 时为 1, 当 $\alpha_j>1$ 时为 0, 由此及 (7) 式得到: 当 $q>1$ 时,

$$\sum_{\substack{h=1\\(h,q)=1}}^{q} e^{2\pi i\frac{hm}{q}} = \begin{cases}0, & \text{当 } q \text{ 有平方因子},\\ (-1)^s, & \text{当 } q=p_1\cdots p_s.\end{cases}$$

定理得证. □

§3 同余方程的一般概念, 一次同余方程

设 $f(x)$ 是取整值的数论函数, $m>0$, 若当 $x=a$ 时有

$$f(a)\equiv 0\,(\mathrm{mod}\,m),$$

我们就说 a 是同余方程

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

的一个解.

例如

$$2x + 5 \equiv 0 \,(\mathrm{mod}\, 7),$$
$$x^2 + x + 1 \equiv 0 \,(\mathrm{mod}\, 2),$$
$$2^x \equiv 1 \,(\mathrm{mod}\, 3)$$

都是同余方程.

在一般情况下, 求解同余方程是很复杂的, 没有一般方法. 我们在这里仅讨论 $f(x)$ 是整系数多项式的情形, 关于这种同余方程, 有下面最简单的性质.

定理 19 *设 $f(x)$ 为整系数多项式. $m > 0$, 若 a 是*

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

的一个解, 则所有 $x \equiv a \,(\mathrm{mod}\, m)$ 都是解, 即和 a 对模 m 同余的数均是解.

定理的证明是显然的, 由定理知, 我们可将所有对模的同余的解看作是相同的, 仅把对模 m 不同余的解, 才看作是不同的.

定义 4 *$f(x) \equiv 0 \,(\mathrm{mod}\, m)$ 的所有对模 m 不同余的解的个数称为方程 $f(x) \equiv 0 \,(\mathrm{mod}\, m)$ 的解数, 记作 $\rho(f, m)$.*

例 2 求同余方程

$$x^5 + x + 1 \equiv 0 \,(\mathrm{mod}\, 7)$$

的解.

解 我们只要直接验证模 7 的一个完全剩余系

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6.$$

将上面 7 个数代入验证, 知 $x=2,4$ 为两个解答, 亦即 $\rho(x^5+x+1,7)=2$. 这两个解答可表示为

$$x\equiv 2\,(\mathrm{mod}\,7),\qquad x\equiv 4\,(\mathrm{mod}\,7).\qquad\square$$

由上例知道, 当模不大时, 定理 19 实际上给出了一种解法. 通常我们总是取绝对值最小的完全剩余系来验证其是否解答. 例如在上例中我们可取如下的完全系

$$-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3.$$

设 $m=m_1m_2,\ (m_1,m_2)=1$, 则同余方程

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

与同余方程组

$$\begin{cases} f(x)\equiv 0\,(\mathrm{mod}\,m_1),\\ f(x)\equiv 0\,(\mathrm{mod}\,m_2) \end{cases}$$

等价. 由此可推出下面的定理.

定理 20 设 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ 为其标准分解, 则同余方程

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

与同余方程组

$$\begin{cases} f(x)\equiv 0\,(\mathrm{mod}\,p_1^{\alpha_1}),\\ f(x)\equiv 0\,(\mathrm{mod}\,p_2^{\alpha_2}),\\ \qquad\cdots\cdots\cdots\cdots\\ f(x)\equiv 0\,(\mathrm{mod}\,p_s^{\alpha_s}) \end{cases}$$

等价.

定理 21 同余方程 $f(x) \equiv 0 \pmod{p^\alpha}$ 的解一定是 $f(x) \equiv 0 \pmod{p}$ 的解.

以上三个简单的定理指出, 研究同余方程可先从素数模的同余方程的解开始讨论.

下面先来讨论最简单的一项同余方程.

定理 22 设 $a \neq 0, m > 0$, 则同余方程 $ax \equiv b \pmod{m}$ 有解的充要条件是 $(a,m)|b$, 在有解的条件下, 它有 (a,m) 个解.

证 显见, 同余方程

$$ax \equiv b \pmod{m} \tag{9}$$

与二元一次不定方程

$$ax + my = b \tag{10}$$

是等价的, 亦即同余方程的解 x 与不定方程的解 (x,y) 相对应. 由第一章定理 17 知, $ax + my = b$ 有解的充要条件是 $(a,m)|b$, 而且它所有的解为

$$x = x_0 + \frac{m}{(a,m)}t, \quad y = y_0 - \frac{a}{(a,m)}t, \quad t = 0, \pm 1, \pm 2, \cdots,$$

这里 x_0, y_0 为不定方程 (10) 的一个解.

因此, 同余方程 (9) 的所有解为

$$x = x_0 + \frac{m}{(a,m)}t, \quad t = 0, \pm 1, \pm 2, \cdots. \tag{11}$$

现在来求出对模 m 不同余的全部 x. 设

$$x_1 = x_0 + \frac{m}{(a,m)}t_1, \quad x_2 = x_0 + \frac{m}{(a,m)}t_2.$$

下面的等价是显然的

$$\begin{aligned} m \nmid (x_1 - x_2) &\Longleftrightarrow m \nmid \frac{m}{(a,m)}(t_1 - t_2) \\ &\Longleftrightarrow (a,m) \nmid (t_1 - t_2), \end{aligned}$$

即

$$x_1 \neq x_2 \,(\mathrm{mod}\, m)$$

与

$$t_1 \neq t_2 \,(\mathrm{mod}\, (a, m))$$

等价.

所以对模 m 不同余的解有

$$x = x_0 + \frac{m}{(a,m)}t, \quad t = 0, 1, 2, \cdots, (a,m) - 1, \tag{12}$$

即

$$\rho(ax - b, m) = (a, m), \quad (a, m)|b.$$

特别当 $(a, m) = 1$ 时有唯一解. □

注 不难看出, 我们一定可找到 (9) 的解 x 的适当条件

$$0 \leqslant x < \frac{m}{(a,m)}.$$

定理 23 设 $(a, m) = 1$, 则同余方程 $ax \equiv b \,(\mathrm{mod}\, m)$ 的解为

$$x \equiv ba^{\varphi(m)-1} \,(\mathrm{mod}\, m). \tag{13}$$

证 由 Euler 定理得到

$$a(ba^{\varphi(m)-1}) \equiv ba^{\varphi(m)} \equiv b \,(\mathrm{mod}\, m),$$

所以由定理 22 知, 它的唯一解即为 (13). □

例 3 解同余方程

$$9x \equiv 8 \,(\mathrm{mod}\, 34). \tag{14}$$

解 此时 $(9, 34) = 1, \varphi(34) = 16$, 所以其唯一解为

$$x \equiv 8 \cdot 9^{15} \,(\mathrm{mod}\, 34),$$

但

$$8 \cdot 9^{15} \equiv 8 \cdot 3^{30} \equiv 8 \cdot 3^{14} \equiv 8 \cdot (2187)^2 \equiv 8 \cdot 11^2 \equiv 16 \,(\mathrm{mod}\, 34),$$

所以 (14) 的解为

$$x \equiv 16 \,(\mathrm{mod}\, 34). \qquad \square$$

当模 m 不大时, 这种方法是可行的.

定理 24 设 $(a, m) = 1$, 若存在整数 s, 使得 $a|(b + sm)$, 则

$$x \equiv \frac{b + sm}{a} \,(\mathrm{mod}\, m) \tag{15}$$

为同余方程 (9) 的唯一解.

证 因为 $a(\frac{b+sm}{a}) = b + sm \equiv b \,(\mathrm{mod}\, m)$. $\square$

下面来探讨下 s 的选取问题.

设 $a > 0$, 因为 $a|(b + sm)$, 即为

$$ms \equiv -b \,(\mathrm{mod}\, a)$$

当 $(a, m) = 1$ 时必有唯一解 s 存在, 我们当然可以在模 a 的绝对最小完全剩余系中找这种 s.

例 4 解同余方程

$$3x \equiv 20 \,(\mathrm{mod}\, 161). \tag{16}$$

解 因为 $(3, 161) = 1$, 此时 $a = 3$, 所以可在 $-1, 0, 1$ 三个值中去找我们所需的 s, 此有 $3|(20 - 161)$ (即 $s = -1$).

由定理 24 知, 此时同余方程 (16) 的解为

$$x \equiv -47 \,(\mathrm{mod}\, 161). \qquad \square$$

定理 25 设 $m > 0$, $(a, m) = 1$, $(b, m) = 1$, 以 $x = x(a, b, m)$ 记作 $ax \equiv b \,(\mathrm{mod}\, m)$ 的解, 则当 a 通过 m 的简化系时, x 亦通过模 m 的简化系.

证 设 $(a_1,m)=1$, $(a_2,m)=1, x_1, x_2$ 分别表示 $a_1x\equiv b\,(\mathrm{mod}\,m)$ 及 $a_2x\equiv b(\mathrm{mod}\,m)$ 的解答, 要证当 $a_1\not\equiv a_2\,(\mathrm{mod}\,m)$ 时, 必有 $x_1\not\equiv x_2\,(\mathrm{mod}\,m)$. 用反证法. 若 $x_1\equiv x_2\,(\mathrm{mod}\,m)$, 则由 $a_1x_1\equiv a_2x_2(\mathrm{mod}\,m)$ 推出 $a_1x_1\equiv a_2x_1\,(\mathrm{mod}\,m)$. 因为 $(b,m)=1$, 所以 $(x_1, m)=1$, 因此必有

$$a_1\equiv a_2\,(\mathrm{mod}\,m).$$

矛盾, 定理得证. □

特别当 $b=1$ 时, 我们经常用 a^{-1} 来表示 $ax\equiv 1\,(\mathrm{mod}\,m)$ 的解.

§4 孙子定理

现在来研究一次同余方程式组的解法. 先来考虑形如下面的方程组

$$\begin{cases} x\equiv C_1\,(\mathrm{mod}\,m_1), \\ x\equiv C_2\,(\mathrm{mod}\,m_2). \end{cases} \tag{17}$$

定理 26 设 $d=(m_1,m_2), M=[m_1,m_2]$. 若 $d\nmid(C_2-C_1)$, 则同余式组 (17) 无解. 若 $d|(C_2-C_1)$, 则 (17) 对模 M 有唯一解.

证 由 (17) 的第一式得到

$$x=C_1+m_1t, \tag{18}$$

这里 t 为任意整数. 现在要选取适当的 t, 使得 (18) 适合 (17) 的第二式, 亦即要使

$$C_1+m_1t\equiv C_2\,(\mathrm{mod}\,m_2).$$

所以问题变成解下面的一项同余式

$$m_1t\equiv C_2-C_1\,(\mathrm{mod}\,m_2). \tag{19}$$

由定理 22 知, 当 $d\nmid(C_2-C_1)$ 时它无解, 当 $d|(C_2-C_1)$ 时它的解有下面的形式

$$t=t_0+\frac{m_2}{d}y,\quad y=0,\pm1,\pm2,\cdots. \tag{20}$$

将 (20) 代入 (18) 得到

$$\begin{aligned} x &= C_1 + m_1\left(t_0 + \frac{m_2}{d}y\right) \\ &= C_1 + m_1 t_0 + \frac{m_1 m_2}{d}y \\ &= C_1 + m_1 t_0 + My, \quad y = 0, \pm 1, \pm 2, \cdots, \end{aligned}$$

所以 (17) 的解可写成下面的形式

$$x \equiv x_0 \,(\mathrm{mod}\, M), \tag{21}$$

这里 $x_0 = C_1 + m_1 t_0$, t_0 为 (19) 的任一解. 定理证毕. □

例 5 试解同余式组

$$\begin{cases} x \equiv 9 \,(\mathrm{mod}\, 34), \\ x \equiv 4 \,(\mathrm{mod}\, 19). \end{cases} \tag{22}$$

解 因为 $(34, 19) = 1$, 所以 (22) 有解.

$$\begin{aligned} x = 9 + 34t &\equiv 4 \,(\mathrm{mod}\, 19), \\ 15t &\equiv -5 \,(\mathrm{mod}\, 19), \\ 3t &\equiv -1 \,(\mathrm{mod}\, 19), \\ t &\equiv 6 \,(\mathrm{mod}\, 19), \end{aligned}$$

所以得到解为

$$x = 9 + 34(6 + 19y) = 213 + 646y,$$

即

$$x \equiv 213 \,(\mathrm{mod}\, 646). \qquad \square$$

由定理 26 知, 当 $(m_1, m_2) = 1$ 时 (17) 恒有唯一解.

现在来研究下面的同余方程组

$$\begin{cases} x \equiv C_1 \,(\mathrm{mod}\, m_1), \\ x \equiv C_2 \,(\mathrm{mod}\, m_2), \\ \quad \cdots\cdots\cdots\cdots \\ x \equiv C_s \,(\mathrm{mod}\, m_s). \end{cases} \tag{23}$$

我们有下面的定理.

定理 27 令 $d_{ij}=(m_i,m_j), M_k=[m_1,m_2,\cdots,m_k], 1\leqslant k\leqslant s$, 则 (23) 有解的充要条件为

$$C_i\equiv C_j\,(\mathrm{mod}\,d_{ij}),\quad 1\leqslant i\leqslant j\leqslant s. \tag{24}$$

当条件 (24) 满足时, 同余方程组对模 M_s 有唯一解.

证 必要性. 设 x_0 为 (23) 的解, 任取 $1\leqslant i\leqslant j\leqslant s$, 则有

$$x_0\equiv C_i\,(\mathrm{mod}\,d_{ij}),$$
$$x_0\equiv C_j\,(\mathrm{mod}\,d_{ij}),$$

所以

$$C_i\equiv C_j\,(\mathrm{mod}\,d_{ij}).$$

假若 x_1,x_2 为 (23) 的两个解, 则有

$$x_1\equiv x_2\,(\mathrm{mod}\,m_1),$$
$$x_1\equiv x_2\,(\mathrm{mod}\,m_2),$$
$$\cdots\cdots\cdots\cdots$$
$$x_1\equiv x_2\,(\mathrm{mod}\,m_s),$$

所以

$$x_1\equiv x_2\,(\mathrm{mod}\,M_s).$$

必要性得证.

充分性. 令 $M_0=1$, 我们要在 $0\leqslant N<M_s$ 中找出形如

$$N=a_1M_0+a_2M_1+\cdots+a_sM_{s-1} \tag{25}$$

的解. 这里 $a_i\,(1\leqslant i\leqslant s)$ 满足条件 $0\leqslant a_i\leqslant\frac{M_i}{M_{i-1}}$.

由于当 $i\geqslant j$ 时

$$M_i\equiv 0\,(\mathrm{mod}\,m_j),$$

所以要使由 (25) 式确定的 N 为同余方程组 (23) 的解, 可用下面的方法依次求出 $a_i\,(1\leqslant i\leqslant s)$.

首先, 由同余方程

$$a_1M_0\equiv C_1\,(\mathrm{mod}\,m_1)$$

定出 a_1, 显然可取 $a_1=C_1$, 满足 $0\leqslant C_1<m_1=\frac{M_1}{M_0}$, 这样就有

$$N\equiv C_1\,(\mathrm{mod}\,m_1).$$

再从同余方程

$$a_1M_0+a_2M_1\equiv C_2\,(\mathrm{mod}\,m_2)$$

定出 a_2. 因为由定理假设知

$$C_2\equiv C_1\,(\mathrm{mod}\,d_{12}),$$

所以 a_2 有解, 且可取 a_2 满足条件 (定理 22 的注)

$$0\leqslant a_2<\frac{m_2}{(M_1,m_2)}=\frac{[m_1,m_2]}{M_1}=\frac{M_2}{M_1}.$$

现在假设对所有的 $i<n$, a_i 已经确定, 即 N 已经满足同余方程组

$$\begin{cases}x\equiv C_1\,(\mathrm{mod}\,m_1),\\ x\equiv C_2\,(\mathrm{mod}\,m_2),\\ \quad\cdots\cdots\cdots\cdots\\ x\equiv C_{n-1}\,(\mathrm{mod}\,m_{n-1}).\end{cases}$$

现在要来解同余方程

$$a_1M_0+a_2M_1+\cdots+a_{n-1}M_{n-2}+a_nM_{n-1}=C_n\,(\mathrm{mod}\,m_n).\tag{26}$$

为此令

$$\gamma_n=a_1M_0+a_2M_1+\cdots+a_{n-1}M_{n-2},\quad n\geqslant 2,$$

则要使 (26) 有解的充要条件为

$$C_n\equiv\gamma_n\,(\mathrm{mod}\,(M_{n-1},m_n)).\tag{27}$$

但现在

$$\gamma_n \equiv C_i \,(\mathrm{mod}\, m_i), \quad i = 1, 2, \cdots, n-1,$$

且由定理假设

$$C_i \equiv C_n \,(\mathrm{mod}\, d_{in}), \quad 1 \leqslant i \leqslant n,$$

亦即

$$\gamma_n \equiv C_n \,(\mathrm{mod}\, [d_{1n}, d_{2n}, \cdots, d_{n-1,n}]),$$

但由第一章习题 16 知

$$[d_{1n}, d_{2n}, \cdots, d_{n-1,n}] = (M_{n-1}, m_n),$$

所以在定理的假设下, (27) 式满足, 亦即可唯一确定 a_n 满足

$$0 \leqslant a_n < \frac{m_n}{(M_{n-1}, m_n)} = \frac{M_n}{M_{n-1}}.$$

这样我们就证明了由 (25) 式确定的 N 满足同余方程 (23), 充分性得证. □

定理 27 的证明方法亦是构造性的, 它的优点是确保它的解 N 一定小于 M_s, 这一点是有用的 (从计算的观点来说). 解同余方程组的步骤如下:

1) 验证条件 (24) 是否满足, 若不满足则无解.

2) 若满足条件 (24), 则令

$$a_1 = C_1.$$

当 $n > 2$ 时, 依次解同余方程

$$a_n M_{n-1} \equiv C_n - \gamma_n \,(\mathrm{mod}\, m_n),$$

这里

$$\gamma_n = a_1 M_0 + a_2 M_1 + \cdots + a_{n-1} M_{n-2}, \quad n \geqslant 2,$$

求出 $a_2, a_3, \cdots, a_s$, 即得到如下形式的解

$$N = a_1 M_0 + a_2 M_1 + \cdots + a_s M_{s-1} = \gamma_s + a_s M_{s-1}.$$

例 6 试解同余方程组

$$\begin{cases} x \equiv 2 \,(\mathrm{mod}\, 7), \\ x \equiv 5 \,(\mathrm{mod}\, 9), \\ x \equiv 11 \,(\mathrm{mod}\, 15). \end{cases} \tag{28}$$

解 因为 $(15, 9) = 3$, 而

$$11 \equiv 5 \,(\mathrm{mod}\, 3),$$

所以 (28) 可解, 其解为

$$N = a_1 + a_2 M_1 + a_3 M_2,$$

这里 $a_1 = 2, M_1 = 7, M_2 = 63$.

解

$$7a_2 \equiv 5 - 2 \,(\mathrm{mod}\, 9),$$

得

$$a_2 \equiv 3 \,(\mathrm{mod}\, 9).$$

解

$$63a_3 \equiv 11 - (2 + 3 \cdot 7) \equiv -12 \equiv 3 \,(\mathrm{mod}\, 15),$$

$$21a_3 \equiv 1 \,(\mathrm{mod}\, 15),$$

$$a_3 \equiv 1 \,(\mathrm{mod}\, 5),$$

所以

$$N = 2 + 3 \times 7 + 1 \times 63 = 86,$$

即 (28) 的解为

$$N \equiv 86 \,(\mathrm{mod}\, 315). \qquad \square$$

由定理 27 知, 当 $m_i \,(1 \leqslant i \leqslant s)$ 两两互素时, 同余方程组 (23) 对模 M 恒有唯一解, 这里 $M = m_1 m_2 \cdots m_s$.

定理 28 (孙子定理) 设 $m_1, m_2, \cdots, m_s$ 为两两互素的正整数, $m = m_1 m_2 \cdots m_s$, $M_i = \frac{m}{m_i} (1 \leqslant i \leqslant s)$, 则同余方程组 (23) 对模 m 有唯一解, 且解为

$$x \equiv M_1^{-1} M_1 C_1 + M_2^{-1} M_2 C_2 + \cdots + M_s^{-1} M_s C_s \,(\mathrm{mod}\, m), \tag{29}$$

这里 M_i^{-1} 为

$$M_i^{-1} M_i \equiv 1 \,(\mathrm{mod}\, m_i), \quad 1 \leqslant i \leqslant s \tag{30}$$

的解.

证 我们只要证明 (29) 为解就行. 令

$$x_i = M_i^{-1} M_i C_i, \quad 1 \leqslant i \leqslant s,$$

则有

$$x_i \equiv C_i \,(\mathrm{mod}\, m_i), \quad 1 \leqslant i \leqslant s,$$
$$x_i \equiv 0 \,(\mathrm{mod}\, M_i), \quad 1 \leqslant i \leqslant s,$$

故

$$x = x_1 + x_2 + \cdots + x_s$$

满足

$$x \equiv C_i \,(\mathrm{mod}\, m_i), \quad 1 \leqslant i \leqslant s.$$

得证. □

利用定理 28 的关键是求 $M_i^{-1} (1 \leqslant i \leqslant s)$, 它的优点是形式对称, 但可能出现较大的数.

定理 29 设 $m_i (1 \leqslant i \leqslant s)$ 两两互素, $m = m_1 m_2 \cdots m_s$, $m = m_i M_i (1 \leqslant i \leqslant s)$. 令

$$C = M_1^{-1} M_1 C_1 + M_2^{-1} M_2 C_2 + \cdots + M_s^{-1} M_s C_s,$$

这里 M_i^{-1} 为

$$M_i^{-1}M_i \equiv 1 \,(\mathrm{mod}\, m_i), \quad 1 \leqslant i \leqslant s$$

的解, 则当 $C_1, C_2, \cdots, C_s$ 分别过 $m_1, m_2, \cdots, m_s$ 的完全 (简化) 剩余系时, C 通过 m 的完全 (简化) 剩余系.

证 设

$$C = M_1^{-1}M_1C_1 + \cdots + M_s^{-1}M_sC_s,$$
$$\overline{C} = M_1^{-1}M_1\overline{C}_1 + \cdots + M_s^{-1}M_s\overline{C}_s.$$

要证

$$C \equiv \overline{C} \,(\mathrm{mod}\, m)$$

与同余式组

$$C_i \equiv \overline{C}_i \,(\mathrm{mod}\, m_i), \quad 1 \leqslant i \leqslant s$$

等价. 因为

$$\begin{aligned} C = \overline{C} &\Longleftrightarrow M_i^{-1}M_iC_i \equiv M_i^{-1}M_i\overline{C}_i \,(\mathrm{mod}\, m_i), \quad 1 \leqslant i \leqslant s \\ &\Longleftrightarrow C_i \equiv \overline{C}_i \,(\mathrm{mod}\, m_i), \quad 1 \leqslant i \leqslant s, \end{aligned}$$

所以当 $C_i\,(1 \leqslant i \leqslant s)$ 通过 m_i 的完全系时, C 通过 m 的完全系. 其次要证明

$$(C, m) = 1 \Longleftrightarrow (C_i, m_i) = 1, \quad 1 \leqslant i \leqslant s.$$

因为

$$\begin{aligned} (C, m) = 1 &\Longleftrightarrow (C, m_i) = 1, \quad 1 \leqslant i \leqslant s \\ &\Longleftrightarrow (M_i^{-1}M_iC_i, m_i) = 1, \quad 1 \leqslant i \leqslant s \\ &\Longleftrightarrow (C_i, m_i) = 1, \quad 1 \leqslant i \leqslant s. \end{aligned}$$

定理证毕. □

下面来给出孙子定理的一个应用.

定理 30 若 $m=m_1m_2$, $(m_1,m_2)=1$. 设同余方程

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

的解数为 $\rho(f,m)$, 则有

$$\rho(f,m)=\rho(f,m_1)\cdot\rho(f,m_2),$$

即解数为 m 的可乘函数.

证 设 $f(x)\equiv 0\,(\mathrm{mod}\,m_1)$ 对模 m_1 不同余的解为

$$x\equiv a_i\,(\mathrm{mod}\,m_1),\quad 1\leqslant i\leqslant\rho(f,m_1)=T_1,$$

$f(x)\equiv 0\,(\mathrm{mod}\,m_2)$ 对模 m_2 不同余的解为

$$x\equiv b_j\,(\mathrm{mod}\,m_2),\quad 1\leqslant j\leqslant\rho(f,m_2)=T_2.$$

因为

$$f(x)\equiv 0\,(\mathrm{mod}\,m)\Longleftrightarrow\begin{cases}f(x)\equiv 0\,(\mathrm{mod}\,m_1),\\ f(x)\equiv 0\,(\mathrm{mod}\,m_2),\end{cases}$$

但

$$f(x)\equiv 0\,(\mathrm{mod}\,m_1)\Longleftrightarrow\begin{cases}x\equiv a_1\,(\mathrm{mod}\,m_1),\\ \cdots\cdots\cdots\cdots\\ x\equiv a_{T_1}\,(\mathrm{mod}\,m_1),\end{cases}$$

$$f(x)\equiv 0\,(\mathrm{mod}\,m_2)\Longleftrightarrow\begin{cases}x\equiv b_1\,(\mathrm{mod}\,m_2),\\ \cdots\cdots\cdots\cdots\\ x\equiv b_{T_2}\,(\mathrm{mod}\,m_2),\end{cases}$$

所以

$$f(x)\equiv 0\,(\mathrm{mod}\,m)\Longleftrightarrow\begin{cases}x\equiv a_i\,(\mathrm{mod}\,m_1),\,1\leqslant i\leqslant T_1,\\ x\equiv b_j\,(\mathrm{mod}\,m_2),\,1\leqslant j\leqslant T_2,\end{cases}$$

即 $f(x) \equiv 0 \,(\mathrm{mod}\, m)$ 等价于 T_1T_2 个一次同余方程组. 由孙子定理知每一个方程组给出一解

$$x \equiv M_1^{-1}M_1a_i + M_2^{-1}M_2b_j \,(\mathrm{mod}\, m), \quad 1 \leqslant i \leqslant T_1, \quad 1 \leqslant j \leqslant T_2,$$

但由定理 29, $a_i \,(1 \leqslant i \leqslant T_1)$ 对模 m_1 两两不同余, $b_j \,(1 \leqslant j \leqslant T_2)$ 对模 m_2 亦两两不同余. 此即

$$\rho(f, m) = \rho(f, m_1) \cdot \rho(f, m_2).$$

定理证毕. □

下面我们简要介绍一下有关多项式恒等同余的一些基本概念.

§5 多项式的 (恒等) 同余

设 p 为素数, $f(x), g(x)$ 为整数多项式, 若多项式 $f(x) - g(x)$ 的所有系数均被 p 整除, 则称 $f(x)$ 对模 p 恒等同余于 $g(x)$, 记作

$$f(x) \quad g(x) \,(\mathrm{mod}\, p), \tag{31}$$

或简记为

$$f \quad g \,(p),$$

这关系式称为模 p 的恒等同余式.

要注意的是, 对所有 x 均有 $f(x) \equiv g(x) \,(\mathrm{mod} p)$, 并不一定能推出

$$f(x) \quad g(x) \,(\mathrm{mod}\, p).$$

例如

$$x^p - x \equiv 0 \,(\mathrm{mod}\, p),$$

但

$$x^p - x \quad 0 \,(\mathrm{mod}\, p);$$

$$x^2 + x \equiv 0 \,(\mathrm{mod}\, 2),$$

但

$$x^2+x \quad 0\,(\mathrm{mod}\,2).$$

当然, 反过来是对的.

恒等同余的一些基本性质:

(1) $f(x) \quad f(x)\,(\mathrm{mod}\,p)$.

(2) $f(x) \quad g(x)\,(\mathrm{mod}\,p) \Longleftrightarrow g(x) \quad f(x)\,(\mathrm{mod}\,p)$.

(3) $f(x) \quad g(x)\,(\mathrm{mod}\,p), g(x) \quad h(x)\,(\mathrm{mod}\,p)$, 则

$$f(x) \quad h(x)\,(\mathrm{mod}\,p).$$

(4) 若 $f_1(x) \quad g_1(x)\,(\mathrm{mod}\,p), f_2(x) \quad g_2(x)\,(\mathrm{mod}\,p)$, 则

$$\begin{aligned} f_1(x)+f_2(x) &\quad g_1(x)+g_2(x)\,(\mathrm{mod}\,p),\\ f_1(x)f_2(x) &\quad g_1(x)g_2(x)\,(\mathrm{mod}\,p). \end{aligned}$$

(5) 对每一 $f(x)$, 必存在唯一的 $\overline{f}(x)=\overline{a}_Kx^K+\cdots+\overline{a}_1x+\overline{a}_0$ 满足 $0<\overline{a}_K<p, 0\leqslant\overline{a}_i<p\,(0\leqslant i\leqslant K-1)$, 使得 $\overline{f}(x) \quad f(x)\,(\mathrm{mod}\ p)$. $\overline{f}(x)$ 称为 $f(x)$ 的对模 p 的标准多项式, K 称为 $f(x)$ 对模 p 的次数, 记作 $\partial_p^0 f=K$.

由次数的定义看出, 模 p 的 K 次标准多项式有 $(p-1)p^K$ 个.

例如

$$f(x)=12x^5+7x^3+2x+3,$$

$$\partial_3^0 f=3, \quad \partial_7^0 f=5.$$

(6) 若 $f(x) \quad g(x)\cdot h(x)\,(\mathrm{mod}\,p)$, 则

$$\partial_p^0 f \quad \partial_p^0 g+\partial_p^0 h. \tag{32}$$

若存在 $c\not\equiv 0\,(\mathrm{mod}\,p)$, 使得 $f(x) \quad cg(x)\,(\mathrm{mod}\,p)$, 则称 $f(x)$ 与 $g(x)$ 相互结合 $\mathrm{mod}\,p$.

(7) 任一多项式 $f(x) \quad 0\,(\mathrm{mod}\,p)$, 有且仅有 $p-1$ 个对模 p 互不同余的标准多项式与之相结合, 且其中有一个首项系数为 1.

因此推出首项系数为 1 且互不结合的标准多项式有 p^K 个.

(8) 若 $f(x)|g(x)\,(\mathrm{mod}\,p), g(x)|h(x)\,(\mathrm{mod}\,p)$, 则

$$f(x)|h(x)\,(\mathrm{mod}\,p).$$

通常的多项式的带余除法可推广到模 p 的带余除法.

(9) 任给二多项式 $f(x), g(x)$, 且 $g(x) \not\equiv 0\,(\mathrm{mod}\,p)$. 则必有唯一的对模 p 的标准多项式 $q(x)$ 及 $\gamma(x)$, 使得

$$f(x) \equiv q(x)g(x) + \gamma(x)\,(\mathrm{mod}\,p),$$

这里 $\gamma(x) \not\equiv 0\,(\mathrm{mod}\,p)$, 或 $\partial_p^0\gamma < \partial_p^0 g$.

例如

$$\begin{aligned} x^3 + x^2 + 1 \equiv\ & (2x+2)(2x^2+1) + (-2x-1)\,(\mathrm{mod}\,3) \\ \equiv\ & (2x+2)(2x^2+1) + (x+2)\,(\mathrm{mod}\,3). \end{aligned}$$

定义 5 *若一多项式 $f(x), \partial_p^0 f = n$, 不能分解为两个次数小于 n 的多项式之积 mod p, 则此多项式称为模 p 的不可化多项式或模 p 的素多项式.*

例如, 当 $p = 3$ 时, 一次互不结合的标准多项式有 3 个:

$$x, x+1, x+2,$$

且皆不可化. 二次的互不结合的标准多项式有 3^2 个:

$$\begin{gathered} x^2, x^2+x, x^2+2x, \\ x^2+1, x^2+x+1, x^2+2x+1, \\ x^2+2, x^2+x+2, x^2+2x+2, \end{gathered}$$

但不可化的仅有 3 个 (除去将 3 个一次互不结合的两两相乘可得多项式, 剩下的 3 个即为二次不可化多项式).

显然, 对模 p 的不可化多项式, 原来一定不可化, 但反之则不然, 如

$$x^2+2 \quad (x+1)(x+2)\,(\mathrm{mod}\,3),$$

但 x^2+2 却不可化.

所有有关多项式的最大公约式、最小公倍式、多项式的分解定理均可推广到这里模 p 的情形, 特别有下面的定理.

定理 31 任一多项式均可分解为模 p 的首项系数为 1 的标准不可化多项式的乘积, 除去次序外, 这种分解式是唯一的.

$$f(x) \quad Cq_1^{\alpha_1}(x)q_2^{\alpha_2}(x)\cdots q_s^{\alpha_s}(x)\,(\mathrm{mod}\,p), \tag{33}$$

$$\partial_p^0 f=\alpha_1\partial_p^0 q_1+\alpha_2\partial_p^0 q_2+\cdots+\alpha_s\partial_p^0 q_s,$$

这里 $q_i(x)(1\leqslant i\leqslant s)$ 是首项系数为 1 的两两不同余的标准素多项式.

定理 31 中的 $q_i(x)(1\leqslant i\leqslant s)$ 为 $f(x)$ 的 α 重因子 $\mathrm{mod}\,p$, 亦即一个多项式 $q(x)$, 若有 $q^k(x)|f(x)\,(\mathrm{mod}\,p)$, 则我们称 $q(x)$ 为 $f(x)$ 的重因子 $\mathrm{mod}\,p$.

§6 模 p 的高次同余方程

设 p 为素数, $f(x)=a_nx^n+\cdots+a_1x+a_0$ 为 n 次多项式, 讨论同余方程

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

因为 $a_n\not\equiv 0\,(\mathrm{mod}\,p)$, 所以必有 a_n^{-1} 存在, 使 $a_n^{-1}a_n\equiv 1\,(\mathrm{mod}\,p)$, 所以我们只要考虑首项系数为 1 的多项式

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad \partial_p^0 f=n.$$

定理 32 设 C 为同余方程 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 的解, 则

$$f(x) \quad (x-C)g(x)\,(\mathrm{mod}\,p),$$

这里 $g(x)$ 为 $n-1$ 次多项式 $g(x)$.

证 对任意整数 C, 有 $n-1$ 次多项式 $g(x)$ 存在, 使

$$f(x)-f(C)=(x-C)g(x).$$

由此即得定理. □

定义 6 若 $f(x)\equiv(x-C)^{\alpha}g(x)\,(\mathrm{mod}\,p)$, 这里 $g(C)\not\equiv 0\,(\mathrm{mod}\,p)$, 则称 C 为同余方程 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 的 α 重解.

由定理 31 及定理 32 立即可推出如下定理.

定理 33 设 $\partial_p^0 f=n$, f 对模 p 的标准多项式为

$$f(x)\equiv C(x-C_1)^{\alpha_1}(x-C_2)^{\alpha_2}\cdots(x-C_K)^{\alpha_K}g(x)\,(\mathrm{mod}\,p),$$

其中 $C_i\,(1\leqslant i\leqslant K)$ 对模 p 两两不同余, $g(x)$ 为二次以上的模 p 不可化多项式的乘积.

$$\alpha_1+\alpha_2+\cdots+\alpha_K+\partial_p^0 g=n,$$

则 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 的所有按重数记的解数 $\leqslant\partial_p^0 f$.

推论 1 设 $f(x)\equiv 0\,(\mathrm{mod}\,p)$, 则同余方程 $f(x)\equiv 0\,(\mathrm{mod}\,p)$ 对模 p 不同余的解数 $\rho(f,p)\leqslant\min(p,\partial_p^0 f)$.

推论 2

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-(p-1))\,(\mathrm{mod}\,p).$$

推论 3 (Wilson)

$$(p-1)!+1\equiv 0\,(\mathrm{mod}\,p).$$

在推论 2 中令 $x=p$ 即可得证.

定理 34 设 $\partial_p^0 f=n$, 由多项式除法得

$$f(x)=(x^p-x)q(x)+\gamma(x),\quad \partial_p^0\gamma<p,$$

则同余方程

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

与同余方程

$$\gamma(x) \equiv 0 \,(\mathrm{mod}\, p)$$

等价.

所以对同余方程不同余的解来说, 我们只要考虑首项系数为 1, 次数 $< p$ 的多项式 $f(x)$.

由此可推出

推论 4 同余式 $f(x) \equiv 0 \,(\mathrm{mod}\ p)$ 有 p 个不同余解与 $(x^p - x) | f(x)$ $(\mathrm{mod}\, p)$ 等价, 亦即与 $\gamma(x) \quad 0 \,(\mathrm{mod}\, p)$ 等价.

定理 35 设 $f(x) \quad 0 \,(\mathrm{mod} p)$, 则 $\rho(f, p) = \partial_p^0 f$ 与 $f(x) | (x^p - x) \,(\mathrm{mod}\, p)$ 等价.

证 若 $\rho(p, f) = \partial_p^0 f = p$, 则由推论 4 知 $\gamma(x) \quad 0 \,(\mathrm{mod}\, p)$, 所以 $f(x)$ 和 $x^p - x$ 互相结合. 若 $\partial_p^0 f < p$, 不妨设 $K = \partial_p^0 f < p$, 同余式 $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ 有 K 个不同余解 $C_1, C_2, \cdots, C_K$. 则由定理 33 知

$$f(x) \quad C(x - C_1) \cdots (x - C_K) \,(\mathrm{mod}\, p).$$

设 $CC^{-1} \equiv 1 \,(\mathrm{mod}\, p)$, 则由推论 2 知

$$x^p - x \quad C^{-1} f(x) \quad \prod_{\substack{0 \leqslant b < p \\ b \neq C_i \,(\mathrm{mod}\ p) \\ 1 \leqslant i \leqslant K}} (x - b),$$

此即

$$f(x) | (x^p - x) \,(\mathrm{mod}\, p).$$

反之, 若有

$$x^p - x \quad f(x) g(x) \,(\mathrm{mod}\, p).$$

显见, $f(x)$, $g(x)$ 本身不可能有重解, 且 $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ 与 $g(x) \equiv 0 \,(\mathrm{mod}\, p)$ 不能有相同的解, 并且 $x^p - x \equiv 0 \,(\mathrm{mod}\, p)$ 的每一个解一定是 $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ 或 $g(x) \equiv 0 \,(\mathrm{mod}\, p)$ 中的一个解, 所以

$$p = \rho(x^p - x, p) = \rho(f, p) + \rho(g, p),$$

但由于

$$\partial_p^0 f + \partial_p^0 g = p$$

及

$$\rho(f, p) \leqslant \partial_p^0 f, \quad \rho(g, p) \leqslant \partial_p^0 g,$$

所以必有

$$\rho(f, p) = \partial_p^0 f, \quad \rho(g, p) = \partial_p^0 g.$$

证毕. □

下面我们来研究同余方程

$$f(x) \equiv 0 \,(\mathrm{mod}\, p^\alpha). \tag{34}$$

显然, $f(x) \equiv 0 \,(\mathrm{mod}\, p^\alpha)$ 的解一定是 $f(x) \equiv 0 \,(\mathrm{mod}\, p^{\alpha-1})$ 的解, 反过来, 若同余式

$$f(x) \equiv 0 \,(\mathrm{mod}\, p^{\alpha-1}) \tag{35}$$

有 L 个对模 $p^{\alpha-1}$ 两两不同余的解 $\xi_1, \xi_2, \cdots, \xi_L$, 设 x_0 是 $f(x) \equiv 0 \,(\mathrm{mod}\, p^\alpha)$ 的解, 则必有一 ξ_{i_0} 存在, 使得

$$x_0 \equiv \xi_{i_0} \,(\mathrm{mod}\, p^{\alpha-1}).$$

当然可以有多于一个 x_0 (它们对模 p^α 两两不同余) 对应于同一个 ξ_{i_0}, 对应于不同 ξ_i 的 x 当然对模 p^α 不同余 (事实上, 它们对模 $p^{\alpha-1}$ 两两不同余). 所以为了求同余方程 (34) 的解, 只要对同余方程 (35) 的每一个解, 去找出所有和它对应且对模 p^α 两两不同余的解来, 即找出下面同余式

$$x_i \equiv \xi \,(\mathrm{mod}\, p^{\alpha-1}), \quad 1 \leqslant i \leqslant K;$$
$$x_{k_1} \equiv x_{k_2} \,(\mathrm{mod}\, p^\alpha), \quad \text{当 } k_1 \neq k_2$$

的全部解来.

定理 36 设 $\alpha>1,\xi$ 为同余方程 (35) 的一个解, 则同余方程 (34) 所有满足 $x=\xi\,(\mathrm{mod}\,p^{\alpha-1})$ 且对模 p^{α} 两两不同余的解的个数为

(i) 若 $f'(\xi)\not\equiv 0\,(\mathrm{mod}\,p)$, 则有一个解,

$$x\equiv\xi+Kp^{\alpha-1}\,(\mathrm{mod}\,p^{\alpha}),\quad Kf'(\xi)=-\frac{f(\xi)}{p^{\alpha-1}}\,(\mathrm{mod}\,p).$$

(ii) 若 $f'(\xi)\equiv 0\,(\mathrm{mod}\,p)$, 且 $f(\xi)\not\equiv 0\,(\mathrm{mod}\,p^{\alpha})$, 则无解.

(iii) 若 $f'(\xi)\equiv 0\,(\mathrm{mod}\,p)$, 且 $f(\xi)\equiv 0\,(\mathrm{mod}\,p^{\alpha})$, 则有 p 个解,

$$x\equiv\xi+Kp^{\alpha-1},\quad K=0,1,2,\cdots,p-1.$$

证 设 $x=\xi+Kp^{\alpha-1}$ 为 (34) 的解, 要确定 K 的值, 由多项式展开得

$$f(\xi+Kp^{\alpha-1})=f(\xi)+f'(\xi)Kp^{\alpha-1}+\frac{f''(\xi)}{2!}K^2p^{2\alpha-1}+\cdots.$$

因为 $\alpha>1$, 所以 $2\alpha-2\geqslant\alpha$, 因此我们得到

$$f(\xi+Kp^{\alpha-1})\equiv f(\xi)+f'(\xi)Kp^{\alpha-1}\,(\mathrm{mod}\,p^{\alpha}).\tag{36}$$

由上式看出 $\xi+Kp^{\alpha-1}$ 为 (34) 的解, 等价于 K 为下面的一次同余式的解,

$$f(\xi)+f'(\xi)Kp^{\alpha-1}\equiv 0\,(\mathrm{mod}\,p^{\alpha}).\tag{37}$$

因为

$$f(\xi)\equiv 0\,(\mathrm{mod}\,p^{\alpha-1}),$$

所以 (37) 等价于同余方程

$$f'(\xi)K\equiv-\frac{f(\xi)}{p^{\alpha-1}}\,(\mathrm{mod}\,p).\tag{38}$$

若 $f'(\xi)\not\equiv 0\,(\mathrm{mod}\,p)$, 则 K 对模 p 有唯一解, 所以

$$x=\xi+Kp^{\alpha-1}$$

对模 p^α 有唯一解. (i) 得证.

若 $f'(\xi) \equiv 0 \pmod p$, 则 $\xi + Kp^{\alpha-1}$ 是 $f(x) \equiv 0 \pmod{p^\alpha}$ 的解, 等价于 $f(\xi) \equiv 0 \pmod{p^\alpha}$, 即得出 (ii) 与 (iii) 的结论.

定理证毕. □

上面的定理给出了求所有素数幂为模的高次同余式的解法: 从 $f(x) \equiv 0 \pmod p$ 开始解起, 依次解 $f(x) \equiv 0 \pmod{p^2}, \cdots$.

由定理 36 可得出下面的推论.

推论 5 *若 $f(x) \equiv 0 \pmod{p^\alpha}$ 和 $f'(x) \equiv 0 \pmod p$ 无公共解, 则对任意 α, $f(x) \equiv 0 \pmod{p^\alpha}$ 的解数和 $f(x) \equiv 0 \pmod p$ 的解数相同, 即*

$$\rho(f, p^\alpha) = \rho(f, p).$$

例 7 试证同余式

$$x^2 + p \equiv 0 \pmod{p^2} \tag{39}$$

无解.

证 显见 $x^2 + p \equiv 0 \pmod p$ 只有一个解 $x = 0$, 且它是 $2x \equiv 0 \pmod p$ 的解, 但 $x = 0$ 不是同余式 (39) 的解. 所以由定理 36 知 (39) 无解. □

如果将同余式 (39) 换成

$$x^2 + px \equiv 0 \pmod{p^2}, \tag{40}$$

则容易证明 (40) 有 p 个解

$$0, p, 2p, \cdots, (p-1)p.$$

习题

1. 若 $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, 则

$$a_1 a_2 \equiv b_1 b_2 \pmod m.$$

2. 若 $C \equiv d \,(\mathrm{mod}\, m)$, $(C, m) = 1$, 则

$$aC \equiv bd \,(\mathrm{mod}\, m)$$

与

$$a \equiv b \,(\mathrm{mod}\, m)$$

等价.

3. 若 $a \equiv b \,(\mathrm{mod}\, m_1)$, $a \equiv b \,(\mathrm{mod}\, m_2)$, 则 $a \equiv b \,(\mathrm{mod}\, [m_1, m_2])$.

4. 设素数 $p \geqslant 3$, 若 $a^2 \equiv b^2 \,(\mathrm{mod} p)$, $p \nmid a$, 则 $a \equiv b \,(\mathrm{mod} p)$ 或 $a \equiv -b \,(\mathrm{mod}\, p)$ 且仅有一个成立.

5. 设正整数

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0, \quad 0 \leqslant a_i < 10,$$

则 11 整除 a 的充要条件是

$$11 \Big| \sum_{i=1}^{n} (-1)^i a_i.$$

6. 试找出整数能被 37, 101 整除的判别条件来.

7. 试证: $641 | (2^{32} + 1)$.

8. 若 a 是一奇数, 则 $a^{2^n} \equiv 1 \,(\mathrm{mod}\, 2^{n+2})$, $\quad n \geqslant 1$.

9. 证明:

$$x = u + p^{s-t} v, \quad u = 0, 1, 2, \cdots, p^{s-t} - 1, \quad v = 0, 1, 2, \cdots, p^t - 1, \quad t \leqslant s$$

是模 p^s(p 为素数) 的一个完全剩余系.

10. (1) 若 $2 \nmid m$, 则 $2, 4, 6, \cdots, 2m$ 是 m 的完全剩余系;
(2) 若 $m > 2$, 则 $1^2, 2^2, 3^2, \cdots, m^2$ 不是 m 的完全剩余系.

11. 若 $m_1, m_2, \cdots, m_k$ 两两互素, $x_1, x_2, \cdots, x_k$ 分别通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余系, 则

$$x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 m_2 \cdots m_{k-1} x_k$$

通过模 $m_1 m_2 \cdots m_k$ 的完全剩余系.

12. 若 m 是大于 1 的正整数, a 为整数, $(a,m)=1$, 则

(1) $\sum\limits_{\xi\,(\mathrm{mod}\,m)}\{\frac{a\xi+b}{m}\}=\frac{m-1}{2}$;

(2) $\sum\limits_{\xi\,(\mathrm{mod}\,m)}{}'\{\frac{a\xi}{m}\}=\frac{1}{2}\varphi(m)$.

13. (1) 求 3^{400} 的最后一位数字;

(2) 求 $(12371^{56}+34)^{28}$ 被 111 除以后所得的余数.

14. (1) 求 3^{400} 的最后两位数字;

(2) 求 9^{9^9} 的最后两位数字.

15. (1) 设 p 为素数, 不用 Fermat 定理, 直接证明

$$(h_1+h_2+\cdots+h_n)^p\equiv h_1^p+h_2^p+\cdots+h_n^p\,(\mathrm{mod}\,p);$$

(2) 证明上述同余式和 Fermat 定理等价.

16. 证明 Euler 定理: $a^{\varphi(m)}\equiv 1\,(\mathrm{mod}\,m)$, $(a,m)=1$ 和 Fermat 定理: $a^p\equiv a\,(\mathrm{mod}\,p)$ 是等价的.

17. 证明:

(1) 若 $(n,13)=(a,13)=1$, 则 $n^{12}\equiv a^{12}\,(\mathrm{mod}\,13)$;

(2) 若 $(n,91)=(a,91)=1$, 则 $n^{12}\equiv a^{12}\,(\mathrm{mod}\,91)$.

18. 设 a,γ 为正整数, $(a,\gamma)=1$, 证明算术 (等差) 数列 $a+K\gamma\,(K=0,1,2,\cdots)$ 中一定可以选出一个几何 (等比) 数列.

19. 试证: 若 $f(x_1,x_2,\cdots,x_n)$ 为一整值函数, 则方程

$$f(x_1,x_2,\cdots,x_n)=N,\quad a_i\leqslant x_i\leqslant b_i$$

的整数解的个数为

$$\sum_{a_1\leqslant x_1\leqslant b_1}\sum_{a_2\leqslant x_2\leqslant b_2}\cdots\sum_{a_n\leqslant x_n\leqslant b_n}\int_0^1 e^{2\pi i(f(x_1,x_2,\cdots,x_n)-N)x}dx.$$

(提示: 利用 $\int_0^1 e^{2\pi i\alpha x}dx=\begin{cases}1, & \text{若 } \alpha=0,\\ 0, & \text{若 } \alpha\neq 0,\end{cases}$ α 为整数.)

20. 直接求同余方程 $x^5-3x^2+2\equiv 0\,(\mathrm{mod}\,7)$ 的所有解.

21. 当 a 为何值时 $x^3\equiv a\,(\mathrm{mod}\,9)$ 有解.

22. 判断下列同余方程是否有解, 若有解求其解:

(1) $20x \equiv 4 \pmod{30}$;　　(2) $15x \equiv 25 \pmod{35}$;

(3) $15x \equiv 0 \pmod{35}$.

23. 解二元一次同余方程组

$$\begin{cases} x + 4y - 29 \equiv 0 \pmod{143}, \\ 2x - 9y + 84 \equiv 0 \pmod{143}. \end{cases}$$

24. 设 p 为素数, $0 < a < p$, 证明: $ax \equiv b \pmod{p}$ 的解为

$$x \equiv b(-1)^{a-1} \frac{(p-1)(p-2)\cdots(p-a+1)}{a!} \pmod{p}.$$

25. 判断下列同余方程组是否有解, 若有解求其解:

(1) $x \equiv 1 \pmod{4}$,　$x \equiv 0 \pmod{3}$,　$x \equiv 5 \pmod{7}$;

(2) $x \equiv 2 \pmod{4}$,　$x \equiv 7 \pmod{10}$,　$x \equiv 1 \pmod{3}$;

(3) $x \equiv 2 \pmod{3}$,　$x \equiv 3 \pmod{5}$,　$x \equiv 5 \pmod{2}$;

(4) $x \equiv 3 \pmod{8}$,　$x \equiv 11 \pmod{20}$,　$x \equiv 1 \pmod{15}$.

26. 解同余方程组:

$$x \equiv b_1 \pmod{4}, \quad x \equiv b_2 \pmod{5}, \quad x \equiv b_3 \pmod{7}.$$

27. 解同余方程组:

$$2x \equiv 3 \pmod{5}, \quad 3x \equiv 1 \pmod{7}.$$

28. 设 $m_1, m_2, \cdots, m_K$ 两两互素, 则同余方程组 $a_i x \equiv b_i \pmod{m_i}, 1 \leqslant i \leqslant K$ 有解的充要条件是每一个同余方程 $ax_i \equiv b_i \pmod{m_i}$ 均可解.

29. 设 $(a, b) = 1, C > 0$, 证明一定存在整数 x, 使 $(a + bx, C) = 1$.

第五章　二次剩余与 Gauss 互反律

§1　二次剩余

前一章告诉我们, 解多项式同余方程

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

的问题可以化成求解一系列的素数模的同余方程.

本章主要研究下面形式的二次同余式

$$x^2 \equiv a \,(\mathrm{mod}\, p), \tag{1}$$

这里 p 为奇素数, 且 $(a, p) = 1$.

因为 p 为素数, 所以同余式 (1) 最多有两个解答, 容易看出, 若 x 为 (1) 的解, 则 $-x$ 亦为其解, 所以同余式 (1) 若有解, 则必有二解.

定义 1　*若同余式* (1) *有解, 则称* a *为二次剩余* $\mathrm{mod}\ p$, *记作* $a\,\mathrm{R}\,p$; *若* (1) *无解, 则称* a *为二次非剩余* $\mathrm{mod}\, p$, *记作* $a\,\overline{\mathrm{R}}\,p$.

本章主要研究下面两个基本问题:

1) 给定奇素数 p, 要问哪些 a 是二次剩余 $\bmod p$, 哪些是二次非剩余 $\bmod p$?

2) 给定 a, 要问对哪些 p, a 是二次剩余 $\bmod p$; 对哪些 p, a 是二次非剩余 $\bmod p$?

下面首先来研究问题 1.

例 1 试求模 5 的二次剩余.

解 模 5 的简化系为 $1,2,3,4$, 将其平方得到

$$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1 \,(\mathrm{mod}\, 5).$$

因此看出 $1,4$ 为二次剩余, $2,3$ 为二次非剩余, 如果我们取模 5 的简化系为 $-1,-2,1,2$, 则将其平方得到

$$(-1)^2 \equiv 1,\ (-2)^2 \equiv 4, 1^2 \equiv 1, 2^2 \equiv 4 \,(\mathrm{mod}\, 5),$$

由此亦看出 1,4 为二次剩余. □

一般我们常取

$$-\frac{p-1}{2}, \cdots, -2, -1, 1, 2, \cdots, \frac{p-1}{2} \tag{2}$$

为模 p 的简化系, 将其平方得到 $\frac{p-1}{2}$ 个数,

$$1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

显然与 (3) 中 $\frac{p-1}{2}$ 个数同余的数必为二次剩余 $\bmod p$, 因为这 $\frac{p-1}{2}$ 个数是模 p 的简化系平方后得到的全体数. 我们很容易证明这 $\frac{p-1}{2}$ 个数两两不同余, 所以模 p 的二次剩余与二次非剩余各占一半. 因为若成立

$$k^2 \equiv l^2 \,(\mathrm{mod}\, p), \qquad 0 < k < l \leqslant \frac{p-1}{2},$$

则

$$(l-k)(l+k) \equiv 0 \,(\mathrm{mod}\, p),$$

但

$$0 < l + k < p, \quad 0 < l - k < p,$$

所以这是不可能的. 由以上讨论, 我们得到了下面的定理.

定理 1 *在模 p 的简化系中, 二次剩余与二次非剩余各占一半, 且 (3) 中的 $\frac{p-1}{2}$ 个数皆为二次剩余.*

§2 Legendre 符号

为了研究二次剩余的性质, Legendre 引进了下面的所谓 Legendre 符号.

定义 2 *设 p 为奇素数, $(a,p)=1$, 定义 Legendre 符号如下*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{若 } a \,\mathrm{R}\, p, \\ -1, & \text{若 } a \,\overline{\mathrm{R}}\, p. \end{cases} \tag{4}$$

为了方便起见, 我们可定义当 $p|a$ 时, 有

$$\left(\frac{a}{p}\right) = 0.$$

例如 $(\frac{1}{p}) = 1$, $(\frac{a^2}{p}) = 1$, $(\frac{3}{17}) = -1$, $(\frac{22}{11}) = 0$.

由定义可以看出

$$\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right). \tag{5}$$

定理 2 *设 $(a,p)=1$, 则有*

$$-\left(\frac{a}{p}\right)(p-1)! \equiv a^{\frac{1}{2}(p-1)} \,(\mathrm{mod}\, p). \tag{6}$$

证 设

$$S = \{1, 2, 3, \cdots, p-1\} \tag{7}$$

为模 p 的简化系组成的集合, $x \in S$, 则由第四章定理 25 知: 对每一 x 必存在唯一的 $y \in S$ 为下面同余式的解

$$yx \equiv a \,(\mathrm{mod}\, p). \tag{8}$$

当 $(\frac{a}{p}) = -1$ 时, 同余式

$$x^2 \equiv a \pmod{p}$$

无解, 所以 $y \neq x$. 因此集合 S 中的元素可以分成 $\frac{p-1}{2}$ 对, 每一对元素适合同余式 (8), 这样我们就得到

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

或

$$-\left(\frac{a}{p}\right)(p-1)! \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

当 $(\frac{a}{p}) = 1$ 时, 同余式

$$x^2 \equiv a \pmod{p}$$

有二解 x_0 与 $p - x_0$. 在 S 中除去这两个数外, 剩下的 $p-3$ 个数分成 $\frac{p-3}{2}$ 对, 它们都适合同余式 (8), 所以有

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots (p-1) &\equiv a^{\frac{1}{2}(p-3)} x_0 (p - x_0) \pmod{p} \\ &\equiv -a^{\frac{1}{2}(p-3)} x_0^2 \pmod{p} \\ &\equiv -a^{\frac{1}{2}(p-1)} \pmod{p}, \end{aligned}$$

上式可写成

$$-\left(\frac{a}{p}\right)(p-1)! \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

定理得证. □

由定理 2, 我们可以得到一系列有用的推论.

推论 1 (Wilson 定理)

$$(p-1)! \equiv -1 \pmod{p}. \tag{9}$$

证 在 (6) 式中取 $a = 1$, 即得 (9) □

推论 2 (Euler 判别法) 设 $(a,p)=1$, 则

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\,(\mathrm{mod}\,p). \tag{10}$$

证 将 (9) 代入 (6) 即得 (10). □

推论 3 (Fermat 小定理) 设 $(a,p)=1$, 则

$$a^{p-1}\equiv 1\,(\mathrm{mod}\,p). \tag{11}$$

证 将 (10) 式平方, 即得 (11). □

推论 4

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}. \tag{12}$$

证 在 (10) 中取 $a=-1$, 得

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}\,(\mathrm{mod}\,p). \tag{13}$$

因为

$$-1\not\equiv 1\,(\mathrm{mod}\,p),$$

所以由 (13) 推出 (12). □

推论 5

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right). \tag{14}$$

证 当 a,b 有一个是 p 的倍数时, 上式显然成立, 当 $(a,p)=(b,p)=1$ 时, 由 (10) 式得到

$$\begin{aligned}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)&\equiv (ab)^{\frac{p-1}{2}}\,(\mathrm{mod}\,p)\\ &\equiv\left(\frac{ab}{p}\right)\,(\mathrm{mod}\,p).\end{aligned} \tag{15}$$

再由 $1\not\equiv -1\,(\mathrm{mod}\,p)$, 推出 (14). □

推论 5 告诉我们, Legendre 符号为一完全可乘函数.

推论 6 设 $(a,p)=1, a=\pm q_1q_2\cdots q_sb^2$, 这里 $q_i\,(1\leqslant i\leqslant s)$ 为互不相同的素数, 则

$$\left(\frac{a}{p}\right)=\left(\frac{\pm1}{p}\right)\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_s}{p}\right). \tag{16}$$

证 由 (14) 及 $(\frac{b^2}{p})=1$, 即得 (16). □

由推论 6 知, 要计算 $(\frac{a}{p})$ 只要计算

$$\left(\frac{2}{p}\right)\ 及\ \left(\frac{q}{p}\right)$$

即可, 这里 q 为小于 p 的奇素数.

定理 3 设 p 为奇素数, 则

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & p\equiv\pm1,\,(\mathrm{mod}\,8),\\ -1, & p\equiv\pm3,\,(\mathrm{mod}\,8).\end{cases} \tag{17}$$

证 考虑下面 $(p-1)/2$ 个同余式

$$\begin{aligned}p-1&\equiv1\cdot(-1)^1\,(\mathrm{mod}\,p),\\ 2&\equiv2\cdot(-1)^2\,(\mathrm{mod}\,p),\\ p-3&\equiv3\cdot(-1)^3\,(\mathrm{mod}\,p),\\ 4&\equiv4\cdot(-1)^4\,(\mathrm{mod}\,p),\\ \gamma&\equiv\frac{p-1}{2}\cdot(-1)^{\frac{p-1}{2}}\,(\mathrm{mod}\,p),\end{aligned}$$

这里

$$\gamma=\begin{cases}\dfrac{p-1}{2}, & p\equiv1\,(\mathrm{mod}\,4),\\ p-\dfrac{p-1}{2}, & p\equiv3\,(\mathrm{mod}\,4).\end{cases}$$

将这 $\frac{p-1}{2}$ 个同余式相乘, 得到

$$2\cdot4\cdot6\cdot8\cdots(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}}\,(\mathrm{mod}\,p),$$

亦即

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}}\,(\mathrm{mod}\,p).$$

由此及 (10) 式即得 (17). □

上面求得 $(\frac{2}{p})$ 的思想对于计算一般的 $(\frac{a}{p})$ 是有所启发的, 下面来证明一个重要的定理, 即 Gauss 引理.

定理 4 (Gauss 引理) *设 p 为奇素数, $(a,p)=1$, 若在*

$$a,2a,\cdots,\left(\frac{p-1}{2}\right)a \tag{18}$$

的各个最小非负剩余 $\mathrm{mod}\,p$ 中, 恰有 k 个大于 $\frac{p-1}{2}$, 则

$$\left(\frac{a}{p}\right)=(-1)^k. \tag{19}$$

证 设 $r_1,r_2,\cdots,r_l$ 表示在 (18) 中的最小非负剩余 $\mathrm{mod}\,p$ 中, 不超过 $\frac{p-1}{2}$ 的那些数, 以 $s_1,s_2,\cdots,s_k$ 表示它们中大于 $\frac{p-1}{2}$ 的那些数, 由推论 2 知, 我们只要证明下式就行了,

$$a^{\frac{p-1}{2}}\equiv(-1)^k\,(\mathrm{mod}\,p). \tag{20}$$

由 $r_i\,(1\leqslant i\leqslant l)$ 及 $s_j\,(1\leqslant j\leqslant k)$ 的定义知下面的 $\frac{p-1}{2}$ 个数

$$r_1,r_2,\cdots,r_l,p-s_1,p-s_2,\cdots,p-s_k \tag{21}$$

都是不超过 $\frac{p-1}{2}$ 的, 若能证明 (21) 中的数对模 p 两两不同余, 则它们必为

$$1,2,\cdots,\frac{p-1}{2} \tag{22}$$

的一个排列. 由此可以推出 (19) 式.

现在来证明 (21) 中的数对模 p 两两不同余. 首先证明任意两个 $r_i,r_j\,(i\neq j)$ 对模 p 不同余, 这是因为若 $r_i\equiv r_j\,(\mathrm{mod}\,p)$, 则必有 k_i, k_j 存在, 使得

$$k_ia\equiv k_ja\,(\mathrm{mod}\,p),$$

因为 $(a,p)=1$, 所以必有 $k_i \equiv k_j \pmod p$, 但 k_i, k_j 都不超过 $\frac{p-1}{2}$, 因此 $k_i = k_j$, 即 $i=j$. 同样的方法可以证明当 $i \neq j$ 时 $p-s_i \not\equiv p-s_j \pmod p$.

最后来证明对任意的 i,j 恒有 $r_i \not\equiv p-s_j \pmod p$, 因为由 r_i 和 s_j 的定义可知, 必有 u,v 存在, $1 \leqslant u,v \leqslant \frac{p-1}{2}$, 使得

$$r_i \equiv ua \pmod p, \qquad s_j \equiv va \pmod p.$$

若有 $r_i \equiv p-s_j \pmod p$, 则得到

$$a(u+v) \equiv 0 \pmod p,$$

由于 $(a,p)=1$, 所以

$$(u+v) \equiv 0 \pmod p.$$

但 $1 \leqslant u+v < p-1$, 矛盾, 这样我们证明了 (21) 中的数对模 p 是两两不同余的, 所以它们是 (22) 的一个排列, 于是

$$r_1 r_2 \cdots r_l (p-s_1)(p-s_2)\cdots(p-s_k) = 1\cdot 2\cdot 3 \cdots \frac{p-1}{2}.$$

但当 $1 \leqslant i \leqslant k$ 时, 有

$$p - s_i \equiv -s_i \pmod p,$$

所以

$$r_1 r_2 \cdots r_l s_1 s_2 \cdots s_k (-1)^k \equiv \left(\frac{p-1}{2}\right)! \pmod p, \tag{23}$$

但 $r_1, r_2, \cdots, r_l, s_1, s_2, \cdots, s_k$ 为

$$a, 2a, \cdots, \frac{p-1}{2}a$$

的最小非负剩余, 所以

$$r_1 r_2 \cdots r_l s_1 s_2 \cdots s_k \equiv a\cdot(2a)\cdots\left(\frac{p-1}{2}a\right) \pmod p. \tag{24}$$

由 (23), (24) 得到

$$(-1)^k a(2a)\cdots\left(\frac{p-1}{2}a\right)\equiv\left(\frac{p-1}{2}\right)!\,(\mathrm{mod}\,p),$$

消去 $(\frac{p-1}{2})!$ 得到

$$a^{\frac{p-1}{2}}\equiv(-1)^k\,(\mathrm{mod}\,p).$$

定理得证. □

例 2 求 $(\frac{5}{17})$.

解 现在 $a=5,p=17,\frac{p-1}{2}=8$, 整数 $5,10,15,20,25,30,35,40$ 的最小非负剩余 $\mathrm{mod}\,17$ 为

$$5,\ 10,\ 15,\ 3,\ 8,\ 13,\ 1,\ 6,$$

其中 3 个大于 8, 因此由定理 4 知 $(\frac{5}{17})=-1$. □

定理 5 设 a 为奇数, $(a,p)=1$, 则

$$\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{j=1}^{\frac{p-1}{2}}[\frac{ja}{p}]}. \tag{25}$$

证 与定理 4 相同, 我们将

$$a,2a,\cdots,\ \left(\frac{p-1}{2}\right)a$$

的最小非负剩余分成两类, 将不超过 $\frac{p-1}{2}$ 的归入一类, 记为

$$r_1,r_2,\cdots,r_l,$$

将大于 $\frac{p-1}{2}$ 的数归入另一类, 记为

$$s_1,s_2,\cdots,s_k.$$

上面我们已经证明了

$$r_1,r_2,\cdots,r_l,p-s_1,p-s_2,\cdots,p-s_k$$

为

$$1, 2, \cdots, \frac{p-1}{2}$$

的一个排列, 所以

$$\sum_{j=1}^{l} r_j + \sum_{i=1}^{k} (p - s_i) = \sum_{n=1}^{\frac{p-1}{2}} n = \frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right) = \frac{p^2-1}{8}. \tag{26}$$

另一方面, 我们知道 $ja\,(j = 1, 2, \cdots, \frac{p-1}{2})$ 的最小非负剩余 $\bmod p$ 就是 ja 用 p 相除所得的余数, 即

$$ja = \left[\frac{ja}{p}\right] \cdot p + \left\{\frac{ja}{p}\right\} p, \quad j = 1, 2, \cdots, \frac{p-1}{2}.$$

将上式对 $j\,(1 \leqslant j \leqslant \frac{p-1}{2})$ 相加得到

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] p + \sum_{j=1}^{\frac{p-1}{2}} \left\{\frac{ja}{p}\right\} p,$$

上式亦可写成

$$\frac{p^2-1}{8} a = a \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + \sum_{j=1}^{l} r_j + \sum_{j=1}^{k} s_j. \tag{27}$$

将 (26) 代入 (27) 得到

$$\frac{p^2-1}{8} a = p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + 2\sum_{j=1}^{k} s_j - pk + \frac{p^2-1}{8}$$

或

$$\frac{p^2-1}{8}(a-1) = p\left(\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - k\right) + 2\sum_{j=1}^{k} s_j. \tag{28}$$

因为 $\frac{p^2-1}{8}$ 为整数, $a-1$ 为偶数, 所以 $\sum\limits_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}] - k$ 一定亦为偶数, 亦即

$$(-1)^{\sum\limits_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}] - k} = 1. \tag{29}$$

由上式及 Gauss 引理, 定理得证. □

推论 7 设 p,q 为不同的奇素数, 则有

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^k, \tag{30}$$

这里

$$k=\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{q}\right]+\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{jq}{p}\right]. \tag{31}$$

证 由定理 5 立即可推出 (30). □

由上面的推论我们就可得到下面的二次互反律定理.

定理 6 (二次互反律) 设 p,q 为不同的奇素数, 则有

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}. \tag{32}$$

证 由推论 7 知

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^k,$$

这里 k 由 (31) 式确定, 因此问题变成要证明

$$k=\frac{(p-1)(q-1)}{4}. \tag{33}$$

我们采用几何图形的思想来证明上式.

令 $P=\frac{p-1}{2}, Q=\frac{q-1}{2}$, 因为 $p\neq q$ 为奇素数, 所以在直线 OD 上除 O 点外无其他整点. 因为不存在整数 h, 使得

$$Q<h<\frac{q}{p}P<\frac{q}{2}=Q+\frac{1}{2},$$

所以在 DF 上除了 F 外亦无其他整点, 而

$$\sum_{j=1}^{P}\left[\frac{qj}{p}\right]=\triangle ODP \text{ 上的整点个数 } -OP \text{ 上的整点个数},$$

$$\sum_{j=1}^{Q}\left[\frac{pj}{q}\right]=\triangle OEQ \text{ 上的整点个数 } -OQ \text{ 上的整点个数},$$

所以

$$\begin{aligned}k&=\sum_{j=1}^{P}\left[\frac{qj}{p}\right]+\sum_{j=1}^{Q}\left[\frac{pj}{q}\right]\\&=\text{矩形 } OPFQ \text{ 上的整点个数 } -OP \text{ 及 } OQ \text{ 上的整点个数}=PQ.\end{aligned}$$

定理得证. □

有了上面的定理之后, 我们就可以来计算任意的 $(\frac{a}{p})$ 了.

例 3 试计算 $(\frac{-42}{61})$.

解

$$\left(\frac{-42}{61}\right)=\left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right),$$

而

$$\left(\frac{-1}{61}\right)=(-1)^{\frac{61-1}{2}}=1,$$

$$\left(\frac{2}{61}\right)=(-1)^{\frac{61^2-1}{8}}=(-1)^{\frac{3^2-1}{8}}=-1,$$

$$\left(\frac{3}{61}\right)=\left(\frac{61}{3}\right)(-1)^{\frac{61-1}{2}\cdot\frac{3-1}{2}}=\left(\frac{1}{3}\right)=1,$$

$$\begin{aligned}\left(\frac{7}{61}\right)&=\left(\frac{61}{7}\right)(-1)^{\frac{61-1}{2}\cdot\frac{7-1}{2}}=\left(\frac{-2}{7}\right)=\left(\frac{-1}{7}\right)\left(\frac{2}{7}\right)\\&=(-1)^{\frac{7-1}{2}}\cdot(-1)^{\frac{7^2-1}{8}}=-1,\end{aligned}$$

所以

$$\left(\frac{-42}{61}\right)=1.$$

另一种更快的计算是

$$\left(\frac{-42}{61}\right)=\left(\frac{19}{61}\right)=\left(\frac{61}{19}\right)=\left(\frac{4}{19}\right)=1. \qquad \square$$

§3 Jacobi 符号

定义 3 设 $Q>0$ 为奇数, $Q=q_1q_2\cdots q_s$ $(1\leqslant i\leqslant s)$ 为奇素数, Jacobi 符号是定义在全体整数 a 上的函数,

$$\left(\frac{a}{Q}\right)=\left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\cdots\left(\frac{a}{q_s}\right),$$

这里 $(\frac{a}{q_i})(1\leqslant i\leqslant s)$ 是 Legendre 符号.

由 Jacobi 符号的定义可以看出 $(\frac{a}{Q})$ 只能取 1, -1 或 0 (当 $(a,Q)>1$ 时), 由定义可以看出下面几点:

(1) 当 Q 为奇素数时, Jacobi 符号就是 Legendre 符号.

(2) $(\frac{a}{Q})=1$ 并不意味着同余式

$$x^2\equiv a\,(\mathrm{mod}\,Q) \tag{34}$$

有解.

因为当 Q 为一完全平方时, 恒有 $(\frac{a}{Q})=1$, $(a,Q)=1$, 但当 $Q=9, a=2$ 时, (34) 式无解.

(3) Jacobi 符号的特点, 就是不要求 Q 为奇素数, 如果对它我们能有一种直接的计算方法, 即不要化成 Legendre 符号后再计算的方法, 那么就避免了应用互反律时, 一定需要分解为素因子乘积的麻烦. 因此首先要研究它的性质, 即 Legendre 符号的那些性质, 特别是互反律, 能否对 Jacobi 符号亦成立.

Jacobi 符号的性质:

1) $(\frac{a}{Q})$ 是 a 的可乘函数, 周期函数, 周期为 Q (其实为 $Q', Q = l^2Q', Q'$ 无平方因子);

2) $(\frac{1}{Q}) = 1,\ (\frac{a^2}{Q}) = 1,\ (a, Q) = 1$;

3) $(\frac{-1}{Q}) = (-1)^{\frac{Q-1}{2}}$;

4) $(\frac{2}{Q}) = (-1)^{\frac{Q^2-1}{8}}$;

5) $(\frac{Q}{P}) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}(\frac{P}{Q})$, P, Q 为奇数.

1), 2) 的证明是基于 Legendre 符号的性质, 3), 4) 的证明是基于下面的引理.

引理 若 $m = p_1p_2\cdots p_s, p_i\,(1 \leqslant i \leqslant s)$ 为奇素数, 则

$$\frac{m-1}{2} = \frac{p_1-1}{2} + \frac{p_2-1}{2} + \cdots + \frac{p_s-1}{2} + 2K, \tag{35}$$

$$\frac{m^2-1}{8} = \frac{p_1^2-1}{8} + \frac{p_2^2-1}{8} + \cdots + \frac{p_s^2-1}{8} + 2L, \tag{36}$$

这里 K, L 为整数.

证

$$\frac{m-1}{2} = \frac{p_1p_2\cdots p_s-1}{2} = \frac{1}{2}\left(\left(1+2\cdot\frac{p_1-1}{2}\right)\left(1+2\cdot\frac{p_2-1}{2}\right)\cdots\left(1+2\cdot\frac{p_s-1}{2}\right)-1\right),$$

$$\frac{m^2-1}{8} = \frac{1}{8}\left(\left(1+8\cdot\frac{p_1^2-1}{8}\right)\left(1+8\cdot\frac{p_2^2-1}{8}\right)\cdots\left(1+8\cdot\frac{p_s^2-1}{8}\right)-1\right).$$

由上面二式立即推出 (35) 及 (36). □

现在我们利用 (36) 来证明

$$\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}.$$

设 $Q = q_1q_2\cdots q_s, q_i\,(1 \leqslant i \leqslant s)$ 为奇素数, 所以

$$\left(\frac{2}{Q}\right) = \prod_{i=1}^{s}\left(\frac{2}{q_i}\right) = \prod_{i=1}^{s}(-1)^{\frac{q_i^2-1}{8}} = (-1)^{\sum\limits_{i=1}^{s}\frac{q_i^2-1}{8}} = (-1)^{\frac{Q^2-1}{8}}.$$

下面来证明

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{Q-1}{2}\cdot\frac{P-1}{2}}\left(\frac{P}{Q}\right),\quad P,Q\text{ 为奇数.}$$

若 $(P,Q)>1$, 则上式显然成立, 现设 $(P,Q)=1$, 并设

$$P=p_1p_2\cdots p_s,\quad Q=q_1q_2\cdots q_r,$$

这里 $p_i\,(1\leqslant i\leqslant s)$, $q_j\,(1\leqslant j\leqslant r)$ 为奇素数, 且满足

$$(p_i,q_j)=1,\quad 1\leqslant i\leqslant s,\quad 1\leqslant j\leqslant r,$$

所以

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=\prod_{i=1}^{s}\prod_{j=1}^{r}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)=(-1)^k.$$

由 Legendre 符号的二次互反律知

$$k=\sum_{i=1}^{s}\sum_{j=1}^{r}\frac{1}{2}(p_i-1)\cdot\frac{1}{2}(q_j-1)=\sum_{i=1}^{s}\frac{1}{2}(p_i-1)\sum_{j=1}^{r}\frac{1}{2}(q_j-1).$$

由上式及 (35) 立即得到

$$(-1)^k=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

例 4 判断二次同余式

$$x^2\equiv 888\,(\mathrm{mod}\,1999)\tag{37}$$

有无解?

解

$$\left(\frac{888}{1999}\right)=\left(\frac{4}{1999}\right)\left(\frac{2}{1999}\right)\left(\frac{111}{1999}\right).$$

因为

$$\left(\frac{4}{1999}\right)=1,$$
$$\left(\frac{2}{1999}\right)=(-1)^{\frac{1999^2-1}{8}}=1,$$

所以

$$\left(\frac{888}{1999}\right)=\left(\frac{111}{1999}\right).$$

现在我们把 $\left(\frac{111}{1999}\right)$ 看成 Jacobi 符号来计算它,

$$\left(\frac{111}{1999}\right)=(-1)^{\frac{111-1}{2}\cdot\frac{1999-1}{2}}\left(\frac{1999}{111}\right)=-\left(\frac{1}{111}\right)=-1,$$

所以

$$\left(\frac{888}{1999}\right)=-1,$$

即同余方程 (37) 不可解. □

例 5　计算 $\left(\frac{33}{73}\right)$.

解

$$\left(\frac{33}{73}\right)=(-1)^{16\cdot 36}\left(\frac{73}{33}\right)=\left(\frac{73}{33}\right)=\left(\frac{7}{33}\right),$$
$$\left(\frac{7}{33}\right)=(-1)^{3\cdot 16}\left(\frac{33}{7}\right)=\left(\frac{33}{7}\right)=\left(\frac{5}{7}\right),$$
$$\left(\frac{5}{7}\right)=(-1)^{2\cdot 3}\left(\frac{7}{5}\right)=\left(\frac{7}{5}\right)=\left(\frac{2}{5}\right)=-1,$$

所以

$$\left(\frac{33}{73}\right)=-1.$$ □

习题

1. 设整数 $\alpha\geqslant 1$, p 是奇素数, 若 $p^{\alpha}\nmid a$, 求

$$x^2\equiv a\,(\mathrm{mod}\,p^{\alpha})$$

的一切解.

2. 证明同余式

$$ax^2+bx+c\equiv 0\,(\mathrm{mod}\,m),\quad (2a,m)=1$$

有解的充要条件是

$$x^2 \equiv q \,(\mathrm{mod}\, m), \quad q = b^2 - 4ac$$

有解, 并且前一同余式的一切解可由后一同余式的解导出.

3. 分别写出 7, 13, 29, 37 的全体二次剩余和非剩余.

4. 设 $p > 2$ 为奇素数, 证明:
(1) $(\frac{-1}{p}) = 1$ 的充要条件是 $p = 4n + 1$;
(2) $(\frac{2}{p}) = 1$ 的充要条件是 $p = 8n \pm 1$;
(3) $(\frac{-2}{p}) = 1$ 的充要条件是 $p = 8n + 1, 8n + 3$; 并由此进一步证明对任意素数 $p, -1, -2, 2$ 中必有一个是 p 的平方剩余.

5. 利用上题证明: 对任意素数 p, 必有整数 x, 使

$$p | x^8 - 16.$$

6. 证明: 同余式 $x^2 + 1 \equiv 0 \,(\mathrm{mod}\, p),\ p = 4m + 1$ 的解是

$$x \equiv (2m)! \,(\mathrm{mod}\, p).$$

7. 设 x, y 为整数, $(x, y) = 1$, 问: $x^2 + y^2$ 的大于 2 的素因子一定具有什么形式? $x^2 + 2y^2$ 的大于 2 的素因子一定具有什么形式?

8. 计算: $(\frac{-23}{83}), (\frac{51}{71}), (\frac{71}{73}), (\frac{-35}{97})$.

9. 设 $p > 3$ 为素数, 证明:
(1) $(\frac{3}{p}) = 1$ 之充要条件为 $p = 12n \pm 1$;
(2) $(\frac{-3}{p}) = 1$ 之充要条件为 $p = 6n + 1$.

10. 设 $m > 3,\ (a, m) = 1$. 若 a 为 m 的二次剩余, 则必有

$$m \Big| \Big(a^{\frac{\varphi(m)}{2}} - 1 \Big).$$

反过来对吗? 举例说明.

11. 设 $m > 3, m | ab - 1$, 则 a, b 同为 m 的平方剩余或非剩余.

12. 设 $p > 2$ 为素数, $(a, p) = 1$, 则

$$\sum_{x=1}^{p} \left(\frac{ax + b}{p} \right) = 0.$$

13. 设 n 为正整数, $4n+3$ 及 $8n+7$ 都是素数, 则

$$2^{4n+3} \equiv 1 \,(\mathrm{mod}\, 8n+7),$$

并由此证明

$$23|2^{11}-1, \quad 47|2^{23}-1, \quad 503|2^{251}-1.$$

14. 设素数 $p \geqslant 3$.

(1) 求出使 $(\frac{5}{p}) = 1$ 的全体素数;

(2) 求出使 $(\frac{10}{p}) = 1$ 的全体素数;

(3) 求出使 $(\frac{11}{p}) = 1$ 的全体素数.

15. 求出下列同余式的解数:

(1) $x^2 \equiv 3766 \pmod{5987}$;

(2) $x^2 \equiv 3149 \pmod{5987}$, 其中 5987 是素数.

16. 设 a, b 为自然数, $(a,b) = 1, 2 \nmid b$ 及 $b < 4ac$, 证明:

$$\left(\frac{a}{4ac-b}\right) = \left(\frac{a}{b}\right).$$

17. 设 a, b 为自然数, $(a,b) = 1, 2 \nmid b$, 证明对 Jacobi 符号有公式

$$\left(\frac{a}{2a+b}\right) = \begin{cases} \left(\frac{a}{b}\right), & \text{当 } a = 4n \text{ 或 } 4n+1 \text{ 时,} \\ -\left(\frac{a}{b}\right), & \text{当 } a = 4n+2 \text{ 或 } 4n+3 \text{ 时.} \end{cases}$$

18. 设 n 为奇数, a 为给定整数, 证明 $a^n - 1$ 的大于 2 的素因子 p 满足

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

19. 设 a, b, x_0, y_0 为整数, $(ax_0, by_0) = 1$, p 为奇素数, 若 $N = ax_0^2 + by_0^2$, 且 $p|N$, 则

$$\left(\frac{ab}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

20. 若 $(\frac{r}{p}) = 1$, $(\frac{n}{p}) = -1$, 则 $r \cdot 1^2, r \cdot 2^2, \cdots, r(\frac{p-1}{2})^2, n \cdot 1^2, \cdots, n\left(\frac{p-1}{2}\right)^2$ 为模 p 的简化剩余系.

第六章　指数、原根和指标

§1　指数和原根

设 $n>1,(a,n)=1$, 则由 Euler 定理知道

$$a^{\varphi(n)}\equiv 1\,(\mathrm{mod}\,n), \tag{1}$$

所以, 可能存在自然数 $d<\varphi(n)$, 使得

$$a^{d}\equiv 1\,(\mathrm{mod}\,n). \tag{2}$$

定义 1　使得 (2) 式成立的最小正整数 d, 称为 a 对模 n 的次数, 并称 a 是属于指数 $d\,(\mathrm{mod}\ n)$. 我们把这个最小正整数 d 记作 $\delta_n(a)$. 为方便起见, 当 $(a,n)\neq 1$ 时, 令 $\delta_n(a)=0$, 由 (1) 式看出, $\delta_n(a)\leqslant\varphi(n)$.

定义 2　若 $\delta_n(a)=\varphi(n)$, 则 a 称为模 n 的原根.

由定义知, 对任意的 $\lambda<\delta_n(a)$, a 不是二项同余式

$$x^{\lambda}-1\equiv 0\,(\mathrm{mod}\,n) \tag{3}$$

的解. 若 a 是同余方程

$$x^d - 1 \equiv 0 \,(\mathrm{mod}\, n) \tag{4}$$

的解, 而对任一 $\lambda < d$, a 不是同余方程

$$x^\lambda - 1 \equiv 0 \,(\mathrm{mod}\, n)$$

的解, 则称 a 是方程 (4) 的原解. 显然, (4) 的原解 a 对模 n 的次数为 $\delta_n(a) = d$, 若 a 是模 n 的原根, 则 a 是

$$x^{\varphi(n)} - 1 \equiv 0 \,(\mathrm{mod}\, n)$$

的原解.

我们现在可以从讨论 (4) 出发, 而直接讨论指数、原根的性质, 先来考察几个例子.

例 1 求模 7 的原根.

解 此时, $n = 7$, $\varphi(n) = 6$, 模 7 的简化剩余系为: 1, 2, 3, 4, 5, 6, 现在, 列表如下

a	1	2	3	4	5	6
$\delta_n(a)$	1	3	6	3	6	2

由此看出, 3, 5 为模 7 的全部原根. □

例 2 求模 15 的原根

解 此时, $n = 15$, $\varphi(n) = 8$, 模 15 的简化系为 1, 2, 4, 7, 8, 11, 13, 14, 列表如下

a	1	2	4	7	8	11	13	14
$\delta_n(a)$	1	4	2	4	4	2	4	2

所以模 15 无原根存在. □

例 3 求模 9 的原根.

解 $n=9=3^2,\ \varphi(n)=6,$ 模 9 的简化系为 1, 2, 4, 5, 7, 8, 列表如下

a	1	2	4	5	7	8
$\delta_n(a)$	1	6	3	6	3	2

所以, 2, 5 为模 9 的全部原根. □

例 4 求模 8 的原根.

解 $n=8=2^3,\ \varphi(n)=4,$ 模 8 的简化系为 1, 3, 5, 7, 列表如下

a	1	3	5	7
$\delta_n(a)$	1	2	2	2

所以模 8 不存在原根. □

例 5 试证模 $n=2^k\ (k\geqslant 3)$ 必无原根.

证 因为当 $n=2^k$ 时, $\varphi(n)=2^{k-1},$ 所以只需证明对于 $(a,2)=1,$ 必有

$$a^{2^{k-2}}\equiv 1\,(\mathrm{mod}\,2^k),\quad k\geqslant 3 \tag{5}$$

就行.

我们用归纳法来证明, 当 $k\geqslant 3$ 时, (5) 式成立. 设 $k=3,\ a=2m+1,$ 则

$$a^2=(2m+1)^2=4m(m+1)+1\equiv 1\,(\mathrm{mod}\,8).$$

若 (5) 式对 $k_0\geqslant 3$ 成立, 则当 $k=k_0+1$ 时, 有

$$a^{2^{k_0-1}}-1=(a^{2^{k_0-2}}-1)(a^{2^{k_0-2}}+1)\equiv 0\,(\mathrm{mod}\,2^{k_0+1}),$$

证毕. □

当 $n=2$ 时原根为 1, $n=4$ 时原根为 3.

下面来证明有关指数的一些基本性质.

定理 1 设

$$a \equiv b \,(\mathrm{mod}\, n),$$

则

$$\delta_n(a) = \delta_n(b).$$

证明是显然的.

定理 2

$$a^k \equiv 1 \,(\mathrm{mod}\, n) \tag{6}$$

与

$$\delta_n(a) | k \tag{7}$$

等价.

证 由 (7) 推 (6) 是显然的, 现假设 (6) 式成立, 令

$$k = q\delta_n(a) + r, \quad 0 \leqslant r < \delta_n(a).$$

若 $r \neq 0$, 则得到

$$a^k = a^{q\delta_n(a)} \cdot a^r,$$

所以,

$$a^r \equiv a^k \equiv 1 \,(\mathrm{mod}\, n).$$

这与 $\delta_n(a)$ 为次数的定义矛盾, 故必有 $r=0$. □

由上面两个定理可得到下面的几个推论.

推论 1 $\delta_n(a) | \varphi(n)$.

推论 2 设 $(a,n)=1$, 则

$$a^{k_1} \equiv a^{k_2} \,(\mathrm{mod}\, n)$$

与

$$\delta_n(a)|(k_1-k_2)$$

等价.

推论 3 设 $(a,n)=1$, 则

$$a^0,a^1,\cdots,a^{\delta_n(a)-1}$$

对模 n 两两不同余, 特别当 a 为原根时,

$$a^0,a^1,\cdots,a^{\delta_n(a)-1}$$

组成模 n 的一个简化系 (因为此时 $\delta_n(a)=\varphi(n)$).

定理 3 设 $\lambda|\delta_n(a)$, 则 $\delta_n(a^\lambda)=\frac{\delta_n(a)}{\lambda}$.

证 设 $\delta_n(a^\lambda)=d$, 由于

$$(a^\lambda)^{\frac{\delta_n(a)}{\lambda}}\equiv 1\,(\mathrm{mod}\,n),$$

所以由定理 2 知 $d|\frac{\delta_n(a)}{\lambda}$. 若 $d<\frac{\delta_n(a)}{\lambda}$, 则 $\lambda d<\delta_n(a)$, 但 $a^{\lambda d}\equiv 1\,(\mathrm{mod}\,n)$, 这与 $\delta_n(a)$ 为次数矛盾, 所以 $\lambda d\geqslant\delta_n(a)$, 因此, 必有 $d=\frac{\delta_n(a)}{\lambda}$. □

定理 4 若 $(c,\delta_n(a))=1$, 则 $\delta_n(a^c)=\delta_n(a)$.

证 设 $\delta_n(a^c)=d$, 由定理 2 知 $\delta_n(a)|cd$. 因为 $(\delta_n(a),c)=1$, 所以 $\delta_n(a)|d$, 但另一方面, 仍有 $(a^c)^{\delta_n(a)}\equiv 1\,(\mathrm{mod}\,n)$, 由定理 2 知 $d|\delta_n(a)$, 因此必有 $\delta_n(a)=d$, 定理得证. □

结合定理 3 与定理 4 可以得到下面的定理.

定理 5

$$\delta_n(a^c)=\frac{\delta_n(a)}{(\delta_n(a),c)}. \tag{8}$$

证

$$a^c=a^{(c,\delta_n(a))\cdot\frac{c}{(c,\delta_n(a))}}.$$

令

$$b = a^{(c,\delta_n(a))},$$

则由定理 3 知 b 的次数为 $\frac{\delta_n(a)}{(c,\delta_n(a))}$, 因为 $(\frac{c}{(c,\delta_n(a))}, \frac{\delta_n(a)}{(c,\delta_n(a))}) = 1$, 由定理 4 知 $a^c = b^{\frac{c}{(c,\delta_n(a))}}$ 的次数为 $\frac{\delta_n(a)}{(c,\delta_n(a))}$. 证毕. □

定理 6 若 $(\delta_n(a), \delta_n(b)) = 1$, 则 $\delta_n(ab) = \delta_n(a) \cdot \delta_n(b)$.

证 设 $\delta_n(ab) = d$, 则

$$(ab)^d \equiv 1 \,(\mathrm{mod}\, n),$$

所以

$$1 \equiv (ab)^d \equiv (ab)^{d\delta_n(b)} \equiv a^{d\delta_n(b)} \,(\mathrm{mod}\, n),$$

由此推出

$$\delta_n(a) | d\delta_n(b).$$

因为 $(\delta_n(a), \delta_n(b)) = 1$, 故

$$\delta_n(a) | d. \tag{9}$$

同样可得

$$1 \equiv (ab)^d \equiv (ab)^{d\delta_n(a)} \equiv b^{d\delta_n(a)} \,(\mathrm{mod}\, n),$$

所以 $\delta_n(b) | d\delta_n(a)$, 因此

$$\delta_n(b) | d. \tag{10}$$

由 (9), (10) 得到 $\delta_n(a) \cdot \delta_n(b) | d$, 但显然有

$$(ab)^{\delta_n(a)\delta_n(b)} \equiv 1 \,(\mathrm{mod}\, n),$$

所以, $d | \delta_n(a)\delta_n(b)$, 故必有 $d = \delta_n(a) \cdot \delta_n(b)$. 得证. □

若条件 $(\delta_n(a), \delta_n(b)) = 1$ 不满足, 则在一般情形下, 并不能推出

$$\delta_n(ab) = [\delta_n(a), \delta_n(b)].$$

现举例说明如下: 设 $n=10$, 简化系为 1, 3, 7, 9, 列表如下

a	1	3	7	9
$\delta_n(a)$	1	4	4	2

由上表立即可得到

$$\begin{aligned}
&\delta_n(3\times 3)=\delta_n(9)=2\neq[\delta_n(3),\delta_n(3)]=4,\\
&\delta_n(3\times 7)=\delta_n(1)=1\neq[\delta_n(3),\delta_n(7)]=4,\\
&\delta_n(3\times 9)=\delta_n(7)=4=[\delta_n(3),\delta_n(9)]=4,\\
&\delta_n(7\times 9)=\delta_n(3)=4=[\delta_n(7),\delta_n(9)]=4,
\end{aligned}$$

但我们有下面的定理

定理 7 对任意的 a,b, 一定存在 c, 使得 $\delta_n(c)=[\delta_n(a),\delta_n(b)]$.

证 显然只要证明 $(a,n)=(b,n)=1$ 的情形.

令

$$\delta=[\delta_n(a),\delta_n(b)]=q_{q_1}^{\alpha_1}\cdot q_{q_2}^{\alpha_2}\cdots q_{q_s}^{\alpha_s},$$

这里 $q_i\,(1\leqslant i\leqslant s)$ 为素数. 由最小公倍数的定义知, 对每一个 $i, q_i^{\alpha_i}|\delta_n(a)$ 及 $q_i^{\alpha_i}|\delta_n(b)$ 至少有一个成立, 不妨设 $q_i^{\alpha_i}|\delta_n(a)$ 成立, 则有 $\delta_n(a)=q_i^{\alpha_i}\gamma_i$, 令 $c_i=a^{\gamma_i}$, 则由定理 3 知, $\delta_n(c_i)=q_i^{\alpha_i}$, 这样我们证明了有 $c_1,c_2,\cdots,c_s$ 存在, 使得 $\delta_n(c_i)=q_i^{\alpha_i}\,(1\leqslant i\leqslant s)$. 令 $c=c_1c_2\cdots c_s$, 由定理 6, 得到

$$\begin{aligned}
\delta_n(c)&=\delta_n(c_1)\delta_n(c_2)\cdots\delta_n(c_s)\\
&=q_1^{\alpha_1}\cdot q_2^{\alpha_2}\cdots q_s^{\alpha_s}=[\delta_n(a),\delta_n(b)].
\end{aligned}$$

定理得证. □

上面的定理在证明原根存在性时, 将显出其用处.

下面来讨论两个以上模出现的情况.

定理 8 设 $(n_1,n_2)=1$, 则 $\delta_{n_1n_2}(a)=[\delta_{n_1}(a),\delta_{n_2}(a)]$.

证 设 $\delta_{n_1n_2}(a)=d$, 显然

$$a^d\equiv 1\,(\mathrm{mod}\,n_1n_2)$$

与

$$\begin{cases} a^d\equiv 1\,(\mathrm{mod}\,n_1),\\ a^d\equiv 1\,(\mathrm{mod}\,n_2) \end{cases}$$

等价, 所以

$$\delta_{n_1}(a)|d,\ \delta_{n_2}(a)|d,$$

由此推出

$$[\delta_{n_1}(a),\delta_{n_2}(a)]|d. \tag{11}$$

但另一方面有

$$a^{[\delta_{n_1}(a),\delta_{n_2}(a)]}\equiv 1\,(\mathrm{mod}\,n_1),$$
$$a^{[\delta_{n_1}(a),\delta_{n_2}(a)]}\equiv 1\,(\mathrm{mod}\,n_2),$$

所以

$$a^{[\delta_{n_1}(a),\delta_{n_2}(a)]}\equiv 1\,(\mathrm{mod}\,n_1n_2),$$

因此

$$d|[\delta_{n_1}(a),\delta_{n_2}(a)]. \tag{12}$$

由 (11), (12) 得到 $d=[\delta_{n_1}(a),\delta_{n_2}(a)]$, 得证. □

定理 9 设 $(n_1,n_2)=1$, 则对于任意的 a_1,a_2 必存在 a, 使得

$$\delta_{n_1n_2}(a)=[\delta_{n_1}(a_1),\delta_{n_2}(a_2)].$$

证 考虑同余式组

$$\begin{cases} x\equiv a_1\,(\mathrm{mod}\,n_1),\\ x\equiv a_2\,(\mathrm{mod}\,n_2). \end{cases}$$

由孙子定理知存在唯一解

$$x\equiv a\,(\mathrm{mod}\,n_1n_2),$$

由定理 1 知 $\delta_{n_1}(a)=\delta_{n_1}(a_1)$, $\delta_{n_2}(a)=\delta_{n_2}(a_2)$, 所以由定理 8 得到

$$\delta_{n_1n_2}(a)=[\delta_{n_1}(a_1),\delta_{n_2}(a_2)].$$

证毕. □

§2 原根存在定理

定理 10 设 $n=2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$,

$$\varepsilon(n)=[\Phi(2^{\alpha_0}),\varphi(p_1^{\alpha_1}),\cdots,\varphi(p_s^{\alpha_s})],$$
$$\Phi(2^{\alpha_0})=\begin{cases}\varphi(2^{\alpha_0}), & \alpha_0\leqslant 2,\\ \varphi(2^{\alpha_0})/2, & \alpha_0\geqslant 3,\end{cases}$$

则对任一 $a,(a,n)=1$ 必有 $\delta_n(a)|\varepsilon(n)$.

证 由定理 8 知 $\delta_n(a)=[\delta_{2^{\alpha_0}}(a),\delta_{p_1{}^{\alpha_1}}(a),\cdots,\delta_{p_s{}^{\alpha_s}}(a)]$, 再由定理 2 及例 5 知 $\delta_n(a)|\varepsilon(n)$. □

推论 4 当 $n\neq 2,4,p^{\alpha},2p^{\alpha}\ (p>2)$ 时一定不存在原根.

因为由 $\varepsilon(n)$ 的定义知必有 $\varepsilon(n)|\varphi(n)$, 但当 n 不是上述四种情形时, 必有 $\varepsilon(n)\leqslant\frac{1}{2}\varphi(n)$, 所以对这种 n, 对所有的 $(a,n)=1$, 恒有 $\delta_n(a)<\varphi(n)$, 即不存在原根. □

本节的主要内容是要证明当 $n=2,4,p^{\alpha},2p^{\alpha}$ 时, 必有原根存在. 先来证明几个引理.

引理 1 设素数 $p>2$, 则对模 p 必有原根存在.

证 设 $1,2,\cdots,p-1$ 对模 p 的指数为 $\delta_p(1),\cdots,\delta_p(p-1)$, 由定理 7 知, 必有 g 使得

$$\delta_p(g)=[\delta_p(1),\delta_p(2),\cdots,\delta_p(p-1)]. \tag{13}$$

因为

$$g^{p-1}\equiv 1\,(\mathrm{mod}\,p), \tag{14}$$

所以, $\delta_p(g)|(p-1)$, 但另一方面同余方程

$$x^{\delta_p(g)} \equiv 1 \,(\mathrm{mod}\, p) \tag{15}$$

有 $p-1$ 个解 $1, 2, \cdots, p-1$, 又同余方程解答的个数不大于方程的次数, 所以, $p-1 \leqslant \delta_p(g)$, 故必有 $\delta_p(g) = p-1$, 即 g 为模 p 的原根. □

引理 2 设 $\alpha \geqslant 2$, 若 g 是 p^α 的原根, 则 g 一定亦为 $p^{\alpha-1}$ 的原根.

证 设 $d = \delta_{p^{\alpha-1}}(g)$, 要证 $d = \varphi(p^{\alpha-1})$. 因为 $g^d \equiv 1 \,(\mathrm{mod}\, p^{\alpha-1})$, 所以 $g^d = 1 + kp^{\alpha-1}$, $g^{dp} = (1 + kp^{\alpha-1})^p = 1 + k'p^\alpha$, 所以 $g^{dp} \equiv 1 \,(\mathrm{mod}\, p^\alpha)$. 因为 g 是 p^α 的原根, 所以 $\varphi(p^\alpha)|dp$, 因此 $\varphi(p^{\alpha-1})|d$. 但另一方面由 d 的定义知 $d|\varphi(p^{\alpha-1})$, 所以必有 $d = \varphi(p^{\alpha-1})$. 这样, 要找 p^α 的原根可以在 p 的原根中去找. □

引理 3 设 g 为 p 的原根, 则一定存在 t_0, 使得 $g + t_0 p$ 是所有 $p^\alpha\,(\alpha \geqslant 1)$ 的原根.

证 考虑 $g+tp$, 设其对模 p^2 的次数为 δ 所以, $\delta|\varphi(p^2) = p(p-1)$, 由于

$$(g + tp)^\delta \equiv 1 \,(\mathrm{mod}\, p^2),$$

所以

$$(g + tp)^\delta \equiv 1 \,(\mathrm{mod} p).$$

但 g 是 p 的原根, 因此 $(p-1)|\delta$, 所以 $\delta = (p-1)p^r$, 这里 $r = 0$ 或 1. 假若我们能找到一个 t_0, 使得 $r \neq 0$, 则 $\delta = (p-1)p = \varphi(p^2)$, 即 $g + t_0 p$ 为 p^2 的原根. 下面来指出这种 t_0 是一定存在的.

$$(g + tp)^{p-1} = g^{p-1} + (p-1)g^{p-2}tp + p^2 T,$$

因为 $g^{p-1} = 1 + T_1 p$, 所以

$$(g + tp)^{p-1} = 1 + p(T_1 - g^{p-2}t) + P^2 T_2. \tag{16}$$

由 (16) 式看出, 只要选取 t_0, 使得

$$g^{p-2}t_0 \not\equiv T_1 \,(\mathrm{mod}\, p), \tag{17}$$

这时就有

$$(g + t_0 p)^{p-1} \not\equiv 1 \,(\mathrm{mod}\, p^2), \tag{18}$$

从而推出 $g + t_0 p$ 对模 p^2 的次数 $\delta = p(p-1)$. 容易看出满足 (17) 的 t_0 是显然存在的, 因为同余方程

$$g^{p-2}t \equiv T_1 \,(\mathrm{mod}\, p)$$

只有唯一解, 所以除了一个 t 外, 剩下的 $p-1$ 个 $t(\mathrm{mod}\, p)$ 均使 (17) 式成立. 所以我们可以用 g 或 $g+p$ 去试算, 看其是否为 p^2 的原根, 因为两者必有一个是 p^2 的原根. 下面来证明这样的 $g + t_0 p$ 是所有的 $p^\alpha\,(\alpha \geqslant 1)$ 的原根. 从 (16) 式容易看出, 这样的 t_0 一定满足下面的 $\alpha - 1$ 个式子,

$$\begin{gathered}
(g + t_0 p)^{p-1} \not\equiv 1 \,(\mathrm{mod}\, p^2),\ \text{所以为 } p^2 \text{ 的原根},\\
(g + t_0 p)^{p(p-1)} \not\equiv 1 \,(\mathrm{mod}\, p^3),\ \text{所以为 } p^3 \text{ 的原根},\\
\cdots\cdots\cdots\cdots\\
(g + t_0 p)^{p^{\alpha-2}(p-1)} \not\equiv 1 \,(\mathrm{mod}\, p^\alpha),\ \text{所以为 } p^\alpha \text{ 的原根}.
\end{gathered}$$

引理证毕. □

引理 4 *设 $\alpha \geqslant 1$, 若 g 为 $p^\alpha\,(p > 2)$ 的原根, 则 g 和 $g + p^\alpha$ 中为奇数者是 $2p^\alpha$ 的原根.*

证 因为 g 和 $g + p^\alpha$ 均为 p^α 的原根, 所以不妨假设 g 为奇数, $(g, 2p^\alpha) = 1$. 设 g 对 $2p^\alpha$ 的次数为 d, 所以 $d | \varphi(2p^\alpha) = \varphi(p^\alpha)$, 但另一方面从 $g^d \equiv 1 \,(\mathrm{mod}\, 2p^\alpha)$ 推出 $g^d \equiv 1 \,(\mathrm{mod}\, p^\alpha)$, 所以 $\varphi(p^\alpha) | d$. 因此必有 $d = \varphi(p^\alpha) = \varphi(2p^\alpha)$, 亦即 g 为 $2p^\alpha$ 的原根, 证毕. □

由上面几个引理立即得到下面的定理.

定理 11 *当 $n = 2, 4, p^\alpha, 2p^\alpha\ (p > 2)$ 时, 必有原根存在.*

定理 12 若模 n 有原根存在, 则对模 n 次数为 d 的数的个数为 $\varphi(d)$, 特别地, 对模 n 有 $\varphi(\varphi(n))$ 个原根.

证 因为 g 为模 n 的原根, 所以

$$g^0, g^1, \cdots, g^{\varphi(n)-1}$$

为模 n 的一个简化系, 我们要在这 $\varphi(n)$ 个数中去找出次数为 d 的数, 即在 $g^\lambda, 0\leqslant\lambda\leqslant\varphi(n)-1$ 中找出有多少个 λ, 使得 g^λ 的次数为 d, 由定理 5, 得到

$$\delta_n(g^\lambda)=\delta_n(g)/(\delta_n(g),\lambda)=\varphi(n)/(\varphi(n),\lambda).$$

所以 $\delta_n(g^\lambda)=d$ 的数的个数, 即为当 $0\leqslant\lambda\leqslant\varphi(n)-1$ 且满足

$$(\varphi(n),\lambda)=\varphi(n)/d \tag{19}$$

的 λ 的个数, 由 (19) 式看出 λ 必有形式 $\lambda=(\varphi(n)/d)k,\ 0\leqslant k\leqslant d-1$, 所以

$$\frac{\varphi(n)}{d}=\left(\varphi(n),\frac{\varphi(n)}{d}k\right)=\frac{\varphi(n)}{d}(d,k),$$

因此 k 必须满足 $(d,k)=1, 0\leqslant k\leqslant d-1$, 由此推出 k 的个数为 $\varphi(d)$ 个, 亦即 λ 有 $\varphi(d)$ 个. 定理得证. □

§3 模 $p^\alpha\,(p\geqslant 2)$ 简化系的改造

我们知道, 若能找到模 n 的原根 g, 则

$$g^0,\ g^1,\cdots,g^{\varphi(n)-1}$$

即为模 n 的简化系. 所以关键在于找原根, 下面我们来提供一个寻找模 p 的原根的方法. 这种方法称为 "消去法", 它是基于下面的事实: 若 a 对模 p 的次数为 d, $d<\varphi(p)$, 则 $a^1, a^2, \cdots, a^d$ 不可能为模 p 的原根. 设模 p 的简化系为

$$1,\ 2,\ 3\cdots,\ p-1, \tag{20}$$

首先取 $a=2$, 求得其次数为 d, 若 $d=p-1$, 则 2 即为原根, 若 $d<p-1$, 则在 (20) 中消去与下列的数对模 p 同余的数

$$2^1,\ 2^2,\cdots,\ 2^d, \tag{21}$$

这种方法可继续下去, 直到剩下 $\varphi(p-1)$ 个数为止, 这些数全部为模 p 的原根.

例 6　试求模 41 的原根.

解　模 41 的简化系为

$$1,\ 2,\ 3,\cdots,39,\ 40. \tag{22}$$

首先求得 2 的次数为 20, 所以应消去与

$$2^1,\ 2^2,\ 3^3,\cdots,\ 2^{20}$$

对模 41 同余的数, 这些数为

$$2,\ 4,\ 8,\ 16,\ 32,\ 23,\ 5,\ 10,\ 20,\ 40,\ 39,\ 37,\ 33,\ 25,\ 9,\ 18,\ 36,\ 31,\ 21,\ 1.$$

因此, 在模 41 的简化系中还剩下 20 个数, 但 $\varphi(40)=16<20$, 所以再来考虑 3, 它对模 41 的次数为 8, 所以, 应消去与

$$3^1,\ 3^2,\cdots,\ 3^8$$

对模 41 同余的数, 这些数为

$$3,\ 9,\ 27,\ 40,\ 38,\ 32,\ 14,\ 1,$$

其中 1, 9, 32, 40 这 4 个数已被消去, 所以实际上第二次只消去了 4 个数, 剩下的 $\varphi(40)$ 个数

$$6,\ 7,\ 11,\ 12,\ 13,\ 15,\ 17,\ 19,\ 22,\ 24,\ 26,\ 28,\ 29,\ 30,\ 34,\ 35$$

即为模 41 的原根. □

求得模 p 的原根, 则 $n = p^\alpha$ 的原根 g 都能找到, 所以其简化系都可以从 $g^0, g^1, \cdots, g^{\varphi(n)-1}$ 得到. 但对于 $n = 2^\alpha$, $\alpha > 2$ 时无原根, 那么如何来表示其简化系呢?

定理 13 设 $\alpha \geqslant 3$, 则 5 及 3 对 2^α 的次数为 $2^{\alpha-2}$, 且

$$\pm 5^0,\ \pm 5^1, \cdots,\ \pm 5^{2^{\alpha-2}-1} \tag{23}$$

及

$$\pm 3^0,\ \pm 3^1, \cdots,\ \pm 3^{2^{\alpha-2}-1} \tag{24}$$

均构成 2^α 的一个简化系.

证 由例 5 知, 当 $\alpha \geqslant 3$ 时, 对任一 a, $(a, 2) = 1$, 有

$$a^{2^{\alpha-2}} \equiv 1 \,(\mathrm{mod}\, 2^\alpha),$$

所以任一 a 的次数 $\delta_{2^\alpha}(a) | 2^{\alpha-2}$, 且一定为 2^λ 的形式. 下面来证明 5 对模 2^α 的次数为 $2^{\alpha-2}$, 这只要证明当 $\alpha \geqslant 3$ 时

$$5^{2^{\alpha-3}} \not\equiv 1 \,(\mathrm{mod}\, 2^\alpha). \tag{25}$$

现在用归纳法来证明 (25) 式.

当 $\alpha = 3$ 时, 由于

$$5^{2^0} \not\equiv 1 \ (\mathrm{mod}\, 8),$$

所以 (25) 式成立, 现设当 $\alpha = k \geqslant 3$ 时成立, 要证当 $\alpha = k+1$ 时 (25) 式亦成立. 由于当 $k \geqslant 3$ 时, 有

$$5^{2^{k-3}} \equiv 1 \,(\mathrm{mod}\, 2^{k-1})$$

($k = 3$ 可直接验证, $k > 3$ 即 $\delta_{2^{k-1}}(5) / 2^{k-3}$). 由上式及归纳假设, 知

$$5^{2^{k-3}} = 1 + (2L+1)2^{k-1},$$

所以

$$5^{2^{k-2}} = 1 + (2L+1)2^k + (2L+1)^2 2^{2k-2}.$$

因为当 $k \geqslant 3$ 时 $2k-2 \geqslant k+1$, 所以由上式推出

$$5^{2^{k-2}} \not\equiv 1 \,(\mathrm{mod}\, 2^{k+1}),$$

此即证明了 (25) 式当 $\alpha = k+1$ 时亦成立, 因此我们证明了

$$\delta_{2^\alpha}(5) = 2^{\alpha-2}, \quad \alpha \geqslant 3.$$

下面来证明当 $\alpha \geqslant 3$ 时,

$$\pm 5^0,\ \pm 5^1, \cdots,\ \pm 5^{2^{\alpha-2}-1}$$

为 2^α 的简化系.

首先由 $\delta_{2^\alpha}(5) = 2^{\alpha-2}$ 知 $5^0,\ 5^1,\ 5^2, \cdots, 5^{2^{\alpha-2}-1}$ 对模 2^α 两两不同余, 同样, $-5^0, -5^1, -5^2, \cdots, -5^{2^{\alpha-2}-1}$ 对模 2^α 两两不同余; 其次, 显然有

$$\begin{aligned} 5^{\alpha_1} &\equiv 1 \,(\mathrm{mod}\, 4), \\ -5^{\alpha_2} &\equiv -1 \,(\mathrm{mod}\, 4), \end{aligned} \tag{26}$$

所以

$$5^{\alpha_1} \not\equiv -5^{\alpha_2} \,(\mathrm{mod}\, 4),$$

此即证明了 (23) 构成 2^α 的一个简化系, 同样 (24) 亦构成 2^α 的简化系. □

定理 14 设 $n = 2^\alpha$ $(\alpha \geqslant 3)$, 则在模 n 的简化系中次数为 d 的个数 $\psi(d)$ 为

$$\psi(d) = \begin{cases} 1, & d = 1, \\ 3, & d = 2, \\ 2\varphi(d), & d > 2. \end{cases} \tag{27}$$

证 由定理 13 知, 当 $\alpha \geqslant 3$ 时, $1 \leqslant a \leqslant 2^\alpha, (a, 2) = 1$ 可由简化系

$$5^0, 5^1, \cdots, 5^{2^{\alpha-2}-1}, -5^0, -5^1, \cdots, -5^{2^{\alpha-2}-1} \tag{28}$$

来表示. 再由定理 9 及定理 13 知

$$\delta_{2^\alpha}(5^k)=\delta_{2^\alpha}(5)/(\delta_{2^\alpha}(5),k)=2^{\alpha-2}/(2^{\alpha-2},k),$$

因此和定理 12 相同, 在 $5^0,5^1,\cdots,5^{2^{\alpha-2}-1}$ 中次数为 d 的个数有 $\varphi(d)$ 个, 而在 $-5^0,-5^1,\cdots,-5^{2^{\alpha-2}-1}$ 中, 除了 -5^0 的次数为 2 外, $-5^k,1\leqslant k\leqslant 2^{\alpha-2}-1$ 和 5^k 的次数相同, 所以有 $\psi(1)=1,\psi(2)=1+2\varphi(2),\psi(d)=2\varphi(d),\ 2<d|2^{\alpha-2},$ 且容易验证

$$\sum_{d|2^{\alpha-2}}\psi(d)=1+1+2\sum_{2\leqslant d|2^{\alpha-2}}\varphi(d)=2\sum_{d|2^{\alpha-2}}\varphi(d)=2^{\alpha-1}.\qquad\square$$

定理 15 设 $n=2^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s},\varepsilon(n)$ 由定理 10 给出, 则一定存在 a, 使得 $\delta_n(a)=\varepsilon(n)$.

证 因为 p^α 有原根存在, 次数为 $\varphi(p^\alpha)$, 而当 $\alpha_0\geqslant 3$ 时, 5 的次数为 $\Phi(2^{\alpha_0})$,

$$\Phi(2^{\alpha_0})=\begin{cases}\varphi(2^{\alpha_0}), & \alpha_0\leqslant 2,\\ \dfrac{1}{2}\varphi(2^{\alpha_0}), & \alpha_0>2.\end{cases}$$

再由定理 9, 即得定理. $\square$

为了解决任意模 n 的简化系的构造问题, 我们引进指标与指标组的概念.

§4 指标与指标组

定义 3 设 $n>1$ 有原根存在, 则对任一 $a,(a,n)=1$, 有唯一的 r 存在, 使得

$$g^r\equiv a\,(\mathrm{mod}\,n),\quad 0\leqslant r\leqslant\varphi(n)-1.\tag{29}$$

r 称为以 g 为底的 a 对模 n 的指标, 记作

$$\mathrm{ind}_{n,g}a=\mathrm{ind}_g a=\mathrm{ind}\,a.$$

由定义看出, 指标和所取的原根 g 有关.

下面来证明指标的一些基本性质.

定理 16 对任意的 r',

$$g^{r'} \equiv a \pmod{n}$$

与

$$r' \equiv \operatorname{ind} a \pmod{\varphi(n)} \tag{30}$$

等价.

证 因为原根的次数为 $\varphi(n)$, 由推论 2 立即得到 (30). □

下面为简单起见, 我们令 $c = \varphi(n)$.

定理 17

$$\operatorname{ind}(a_1 a_2) \equiv \operatorname{ind} a_1 + \operatorname{ind} a_2 \pmod{c}. \tag{31}$$

证 由 g 为原根及推论 2 即得上式. □

定理 18

$$\operatorname{ind}_{g_1} g_2 \cdot \operatorname{ind}_{g_2} g_1 \equiv 1 \pmod{c}. \tag{32}$$

证 设 $r_1 = \operatorname{ind}_{g_1} g_2, r_2 = \operatorname{ind}_{g_2} g_1$, 即

$$g_1^{r_1} \equiv g_2 \pmod{n}, \quad g_2^{r_2} \equiv g_1 \pmod{n},$$

所以

$$g_2^{r_1 r_2} \equiv g_2 \pmod{n}.$$

由推论 2 得到

$$r_1 r_2 \equiv 1 \pmod{c},$$

由 (32) 显然可推出

$$(\operatorname{ind}_{g_1} g_2, c) = 1. \tag{33}$$

证毕. □

定理 19

$$\mathrm{ind}_{g_1} a = \mathrm{ind}_{g_1} g_2 \cdot \mathrm{ind}_{g_2} a \,(\mathrm{mod}\, c). \tag{34}$$

证

$$a \equiv g_2^{\mathrm{ind}_{g_2} a} \equiv g_1^{\mathrm{ind}_{g_1} g_2 \cdot \mathrm{ind}_{g_2} a} \,(\mathrm{mod}\, n).$$

由上式及 (30) 即得 (34). □

从上面几个定理可以看出指标有和对数一样的运算法则.

定理 20 对模 n 的任意原根 g, 下面的公式成立

$$\delta_n(a) = \frac{c}{(\mathrm{ind}_g a, c)}. \tag{35}$$

证 因为 $\delta_n(g) = c,\ a \equiv g^{\mathrm{ind}_g a} \,(\mathrm{mod}\, n)$, 由定理 5 即得 (35). □

公式 (35) 给出了次数与指标间的关系. 由于对模 $p^\alpha\,(p > 2)$ 存在原根, 所以我们实质上是解决了简化系结构的研究问题, 但对 $2^\alpha\,(a \geqslant 3)$ 不存在原根, 我们采用类似的方法, 需要引进指标组的概念.

定义 4 设 $n = 2^\alpha\,(\alpha \geqslant 3)$, 对任一 $a, (a, 2) = 1$, 存在唯一的一对 r_{-1} 和 $r_0, 0 \leqslant r_{-1} < 2, 0 < r_0 < 2^{\alpha-2}$, 使得

$$a \equiv (-1)^{r_{-1}} 5^{r_0} \,(\mathrm{mod}\, 2^\alpha), \tag{36}$$

(r_{-1}, r_0) 称为以 -1, 5 为底的 a 对模 2^α 的指标组.

为了使上面的定义也包含当 $\alpha \leqslant 2$ 的情形, 我们引入下面的记号,

$$C_{-1} = \begin{cases} 1, & \alpha = 1, \\ 2, & \alpha \geqslant 2, \end{cases} \qquad C_0 = \begin{cases} 1, & \alpha = 1, \\ 2^{\alpha-2}, & \alpha \geqslant 2. \end{cases} \tag{37}$$

定义 5 设 $n = 2^\alpha\,(\alpha \geqslant 1)$, 对任一 $a, (a, 2) = 1$ 存在唯一的一对 r_{-1}, 和 $r_0, 0 \leqslant r_{-1} < C_{-1}, 0 \leqslant r_0 < C_0$ 使得

$$a \equiv (-1)^{r_{-1}} 5^{r_0} \,(\mathrm{mod}\, 2^\alpha), \tag{37'}$$

(r_{-1}, r_0) 称为以 -1, 5 为底的 a 对模 2^α 的指标组.

它有下面的基本性质.

定理 21

$$r_{-1} \equiv \frac{a-1}{2} \pmod{C_{-1}}. \tag{38}$$

证 当 $\alpha \geqslant 3$ 时, $C_{-1}=2$, 由 (26) 知, 当 $a \equiv 1 \pmod 4$ 时, $r_{-1}=0$, 当 $a \equiv -1 \pmod 4$ 时, $r_{-1}=1$, 所以, 当 $\alpha \geqslant 3$ 时, (38) 是成立的. 当 $\alpha=1$ 时, $C_{-1}=1$, $C_0=1$; 当 $\alpha=2$ 时, $C_0=1$, $C_{-1}=2$, 直接验证即得 (38). □

定理 22 对任意的 r'_{-1}, r'_0,

$$(-1)^{r'_{-1}} 5^{r'_0} \equiv a \pmod{2^\alpha} \tag{39}$$

与

$$r'_{-1} \equiv r_{-1} \pmod{C_{-1}}, \quad r'_0 \equiv r_0 \pmod{C_0} \tag{40}$$

等价.

证 可假定 $\alpha \geqslant 2$, 此时 $C_{-1}=2$, 由 (38) 知

$$r'_{-1} \equiv r_{-1} \equiv \frac{a-1}{2} \pmod{C_{-1}}, \tag{41}$$

所以 (40) 的第一式得证. 这样就有

$$5^{r'_0} \equiv 5^{r_0} \pmod{2^\alpha}.$$

由于 $\delta_{2^\alpha}(5)=C_0$, 因此由推论 2 得到

$$r'_0 \equiv r_0 \pmod{C_0}.$$

证毕. □

定理 23 设 $(a_1a_2, 2)=1$, 则

$$\begin{aligned} r_{-1}(a_1a_2) &\equiv r_{-1}(a_1)+r_{-1}(a_2) \pmod{C_{-1}}, \\ r_0(a_1a_2) &\equiv r_0(a_1)+r_0(a_2) \pmod{C_0}. \end{aligned} \tag{41'}$$

证 可假定 $\alpha \geqslant 2$, $C_{-1}=2$. 先来证明第一式, 因为

$$\begin{aligned}\frac{a_1a_2-1}{2} &= \frac{1}{2}\left(\left(1+2\cdot\frac{a_1-1}{2}\right)\left(1+2\cdot\frac{a_2-1}{2}\right)-1\right)\\ &= \frac{a_1-1}{2}+\frac{a_2-1}{2}+\frac{1}{2}(a_1-1)(a_2-1)\\ &\equiv \frac{a_1-1}{2}+\frac{a_2-1}{2}\ (\mathrm{mod}\,2).\end{aligned}$$

由上式及 (38) 式即得 (41′) 的第一式. 由

$$\begin{aligned}a_1a_2 &\equiv (-1)^{r_{-1}(a_1a_2)}5^{r_0(a_1a_2)}\ (\mathrm{mod}\,2^\alpha),\\ a_1 &\equiv (-1)^{r_{-1}(a_1)}5^{r_0(a_1)}\ (\mathrm{mod}\,2^\alpha),\\ a_2 &\equiv (-1)^{r_{-1}(a_2)}5^{r_0(a_2)}\ (\mathrm{mod}\,2^\alpha)\end{aligned}$$

及 (41′) 的第一式并注意 $C_{-1}=2$, 就可得到

$$5^{r_0(a_1a_2)} \equiv 5^{r_0(a_1)}5^{r_0(a_2)}\ (\mathrm{mod}\,2^\alpha).$$

由此及推论 2 并注意 $\delta_{2^\alpha}(5)=C_0$, 即得 (41′) 的第二式. □

对模 2^α 的指标组当然亦依赖于底的选取, 我们这里取的是 -1 和 5, 显然只要任一 g_0 对模 2^α 的次数为 $2^{\alpha-2}$, 则 $-1, g_0$ 亦构成 2^α 的一组基. 对于指标组的其他一些性质, 我们就不在这里讨论了.

现在我们来证明下面的重要定理.

定理 24 设 $n=2^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$, $g_1,\cdots,g_s$ 分别为模 $p_1^{\alpha_1},\cdots,p_s^{\alpha_s}$ 的原根 [由原根存在定理知, 可取 $g_i\,(1\leqslant i\leqslant s)$ 为 p_i^k (对所有 $k\geqslant 1$) 的原根], 则对任给一组数 $(r_{-1},r_0,r_1,\cdots,r_s), 0\leqslant r_{-1}<C_{-1}, 0\leqslant r_0<C_0, 0\leqslant r_i<C_i=\varphi(p_i^{\alpha_i}), 1\leqslant i\leqslant s$, 一定存在一 a, $(a,n)=1$, 使 a 对 2^{α_0} 的指标组为 (r_{-1},r_0), 对 $p_i^{\alpha_i}$ 的指标为 r_i, 且当 $r_{-1},r_0,r_1,\cdots,r_s$ 分别通过 $C_{-1},C_0,C_1,\cdots,C_s$ 的完全系时 a 通过 n 的简化系, 反之亦然.

证 由孙子定理知, 同余方程组

$$\begin{cases} x \equiv (-1)^{r_{-1}} 5^{r_0} \pmod{2^{\alpha_0}}, \\ x \equiv g_1^{r_1} \pmod{p_1^{\alpha_1}}, \\ \quad \cdots\cdots\cdots\cdots \\ x \equiv g_s^{r_s} \pmod{p_s^{\alpha_s}} \end{cases} \tag{42}$$

对模 n 有唯一解

$$x \equiv a \pmod{n}. \tag{42'}$$

此即为所求.

首先, $(a,n)=1$, 由指标定义知 a 满足要求. 其次只要 $r_{-1}, r_0, r_1, \cdots, r_s$ 和 $r'_{-1}, r'_0, r'_1, \cdots, r'_s$ 对模 $C_{-1}, C_0, C_1, \cdots, C_s$ 两两不恒同余, 则对应的解 a, a' 一定对模 n 不同余. 所以当 $r_{-1}, r_0, r_1, \cdots, r_s$ 过 $C_{-1}, C_0, C_1, \cdots, C_s$ 的完全系时, 对应的共 $C_{-1}C_0C_1\cdots C_s = \varphi(n)$ 个 a 对模 n 两两不同余, 且 $(a,n)=1$, 所以是一个简化系. 反之, 若 a 通过模 n 的简化系, 则不同的 a, a' 所对应的 $(r_{-1}, r_0, r_1, \cdots, r_s)$ 及 $(r'_{-1}, r'_0, r'_1, \cdots, r'_s)$ 一定不可能使得同余式

$$r_i \equiv r'_i \pmod{C_i}, \quad -1 \leqslant i \leqslant s$$

全部成立, 因为 a 共有 $\varphi(n) = C_{-1}C_0C_1\cdots C_s$ 个, 而 r_i 最多能取 C_i 个值, 所以一定要全取到, 即 r_i 通过 C_i 的完全系 $(-1 \leqslant i \leqslant s)$. □

§5 二项同余方程

设 $n = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_s^{\alpha_s}, k \geqslant 1, (a,n)=1$, 则二项同余方程

$$x^k \equiv a \pmod{n} \tag{43}$$

与

$$\begin{cases} x^k \equiv a \,(\mathrm{mod}\, 2^{\alpha_0}), \\ x^k \equiv a \,(\mathrm{mod}\, p_1^{\alpha_1}), \\ \quad \cdots\cdots\cdots\cdots \\ x^k \equiv a \,(\mathrm{mod}\, p_s^{\alpha_s}) \end{cases} \tag{44}$$

等价.

利用原根可以解 (44) 的一个二项同余方程, 当 $n = p, k = 2$ 时, 我们已在第五章进行了讨论.

定理 25 设 $n \geqslant 1$, 且有原根 $g, (a, n) = 1, k \geqslant 1$, 则 $x^k \equiv a \,(\mathrm{mod}\, n)$ 有解的充要条件为 $(k, \varphi(n))|\mathrm{ind}\, a$, 若有解, 则恰有 $(k, \varphi(n))$ 个解.

证 设 $x = g^y$, $a = g^{\mathrm{ind}\, a}$. 则

$$x^k \equiv a \,(\mathrm{mod}\, n)$$

与

$$g^{ky} \equiv g^{\mathrm{ind}\, a} \,(\mathrm{mod}\, n) \tag{45}$$

等价.

由推论 2 知 (45) 与

$$ky \equiv \mathrm{ind}\, a \,(\mathrm{mod}\, \varphi(n)) \tag{46}$$

等价, 而 (46) 有解的充要条件是 $(k, \varphi(n))|\mathrm{ind}\, a$, 若有解, 则恰有 $(k, \varphi(n))$ 个解. □

定义 6 设 $k \geqslant 1, n > 1, (a, n) = 1$, 若 $x^k \equiv a \,(\mathrm{mod}\, n)$ 有解, 则称 a 为模 n 的 k 次剩余.

定理 26 设 $k \geqslant 1, n > 1, (a, n) = 1$, 模 n 有原根, 则 a 是模 n 的 k 次剩余的充要条件是

$$a^{\frac{\varphi(n)}{(\varphi(n), k)}} \equiv 1 \,(\mathrm{mod}\, n), \tag{47}$$

且模 n 的 k 次剩余的个数为 $\frac{\varphi(n)}{(\varphi(n),k)}$.

证 由定理 25 知, a 是 k 次剩余的充要条件为 $(k,\varphi(n))|\operatorname{ind} a$, 而在 $g^0,g^1,\cdots,g^{\varphi(n)-1}$ 中, 指标能被 $(k,\varphi(n))$ 整除的个数恰有 $\frac{\varphi(n)}{(k,\varphi(n))}$ 个. 下面来证 (47) 式, 因为

$$a^{\frac{\varphi(n)}{(k,\varphi(n))}}\equiv 1\,(\mathrm{mod}\,n)\text{ 与 }\delta_n(a)|\frac{\varphi(n)}{(k,\varphi(n))}\text{ 等价,}$$

但 $\delta_n(a)=\frac{\varphi(n)}{(\operatorname{ind} a,\varphi(n))}$, 所以 (47) 式与

$$\frac{\varphi(n)}{(\operatorname{ind} a,\varphi(n))}\Big|\frac{\varphi(n)}{(k,\varphi(n))}$$

等价, 亦即

$$\frac{\varphi(n)}{(k,\varphi(n))}=\lambda\frac{\varphi(n)}{(\operatorname{ind} a,\varphi(n))}.$$

上式等价于

$$(k,\varphi(n))|(\operatorname{ind} a,\varphi(n)),$$

显然亦等价于

$$(k,\varphi(n))|\operatorname{ind} a.$$

再由刚才证明的结论定理得证. □

定理 27 设 $n=2^\alpha,\alpha\geqslant 3,\ 2\nmid a,a\equiv(-1)^{r_{-1}}5^{r_0}\,(\mathrm{mod}\,2^\alpha)$, 则二项同余方程

$$x^k\equiv a\,(\mathrm{mod}\,2^\alpha)\tag{48}$$

当 $2\nmid k$ 时恰有一解, 当 $2|k$ 时, 有解的充要条件是 $r_{-1}=0,(k,2^{\alpha-2})|r_0$, 且有解时恰有 $2(k,2^{\alpha-2})$ 个解.

证 设 $x\equiv(-1)^u5^v\ (\mathrm{mod}\,2^\alpha)$, 则 (48) 与

$$(-1)^{ku}5^{kv}\equiv(-1)^{r_{-1}}5^{r_0}\,(\mathrm{mod}\,2^\alpha)\tag{49}$$

等价, 而 (49) 又等价于同余方程组

$$ku\equiv r_{-1}\ (\mathrm{mod}\,2),\quad kv\equiv r_0\,(\mathrm{mod}\,2^{\alpha-2})\tag{50}$$

(因为当 $\alpha \geqslant 3$ 时, $C_1 = 2, C_0 = 2^{\alpha-2}$). 由此看出当 $(k,2) = 1$ 时, u, v 有唯一解; 当 $2|k$ 时, 首先 $r_{-1} = 0$, 所以此时 u 有两个解, $u = 0, 1$, 而 $kv \equiv r_0 \pmod{2^{\alpha-2}}$ 有解的充要条件为 $(k, 2^{\alpha-2})|r_0$, 且此时有 $(k, 2^{\alpha-2})$ 个解, 所以总共有 $2(k, 2^{\alpha-2})$ 个解, 证毕. □

下面我们举例说明如何用指标来解同余方程.

例 7 试解同余方程

$$x^9 \equiv 6 \pmod{7}. \tag{51}$$

解 设 $n = 7, \varphi(n) = 6$, 此时原根 $g = 3$, 列表如下

a	1	2	3	4	5	6
$\operatorname{ind} a$	6	2	1	4	5	3

令 $x = 3^y$, 则同余方程 (51) 等价于

$$3^{9y} \equiv 3^3 \pmod{7}.$$

上面的同余方程等价于

$$9y \equiv 3 \pmod{6},$$

它有三个解答, $y = 1,\ 3,\ 5$, 由此得到同余方程 (51) 的解答为 $x \equiv 3,\ 6,\ 5 \pmod{7}$. □

习题

1. 写出模 3, 5, 11, 13, 19 的指数表, 并指出它们的所有原根.
2. 求 $\delta_{43}(7)$, $\delta_{41}(10)$.
3. 设 p 为素数, $n \geqslant 1, (n, p-1) = 1$. 证明: 当 x 通过模 p 的完全系时, x^n 亦通过模 p 的完全系.

4. 设 $m>1, n\geqslant 1, (n,\varphi(m))=1$，证明：当 x 通过 m 的简化系，x^n 亦通过 m 的简化系.

5. 设素数 $p>2$，证明：$\delta_p(a)=2$ 的充要条件是 $a\equiv -1(\mathrm{mod}\, p)$.

6. m 为素数的充要条件是存在一个整数 a，使

$$\delta_m(a)=m-1.$$

7. 设 p 为素数. 若 $\delta_p(a)=3$，则 $1+a+a^2\equiv 0\,(\mathrm{mod}\, p)$ 及 $\delta_p(1+a)=6$.

8. (1) p 为素数, 若 $\delta_p(a)=h, 2|h$，则

$$a^{\frac{h}{2}}\equiv -1\,(\mathrm{mod}\, p);$$

(2) p 为素数, 若 $\delta_p(a)=2\lambda, 2\nmid\lambda$，则 $\delta_p(-a)=\lambda$;

(3) 素数 $p=4n+1$，若 g 为原根, 则 $-g$ 亦为原根.

9. 设 $n=2^k$，$k\geqslant 3$，证明：$\delta_n(a)=2^{k-2}$ 的充要条件是 $a\equiv\pm 3\,(\mathrm{mod}\, 8)$.

10. 设 $m>2$ 并有原根存在, 证明:

(1) a 是模 m 的二次剩余的充要条件是

$$a^{\varphi(m)/2}\equiv 1\,(\mathrm{mod}\, m);$$

(2) 若 a 是 m 的二次剩余, 则 $x^2\equiv a\,(\mathrm{mod}\, m)$ 恰有二解;

(3) 模 m 恰有 $\frac{1}{2}\varphi(m)$ 个二次剩余.

11. 设素数 $p>2$，若 g 为模 p 的原根, 且

$$g^{p-1}\equiv 1\,(\mathrm{mod}\, p^2),$$

则 g 不是 p^k 的原根，$k\geqslant 2$.

12. (1) 若 $q=4k+1$，$p=2q+1$ 均为素数, 则 2 是 p 的原根;

(2) 若 $q=2k+1$，$p=2q+1$ 均为素数, 则 $-3, 4$ 均为 p 的原根.

13. 设 p 为素数. s 为模 p 所有正原根 g $(1<g<p)$ 之和. 证明：$s\equiv\mu(p-1)\,(\mathrm{mod}\, p)$，其中 μ 为 Möbius 函数.

14. 设素数 $p>3$. 证明：模 p 的所有正原根 g $(1<g<p)$ 之积对模 p 同余于 1.

15. 设 p 为素数, $n \geqslant 1, d=(n, p-1)$, 证明: 模 p 的 n 次剩余和 d 次剩余是由相同的一些数组成的.

16. 设 p 为素数, 若 $2 \nmid \delta_p(a)$, 则同余方程

$$a^x + 1 \equiv 0 \,(\mathrm{mod}\, p)$$

无解.

17. 求同余方程

$$5^x \equiv 3^x + 2 \,(\mathrm{mod}\, 11)$$

的所有解.

18. 设 $n \geqslant 2$, a 为整数, 若 $n | a^{n-1} - 1$, 但对任何 $d, 0 < d < n-1$, 均有 $n \nmid a^d - 1$, 则 n 为素数.

19. 设 $n > 1, (a, n) = (b, n) = 1$, 再设 $\lambda = (\delta_n(a), \delta_n(b))$.
证明: (1)

$$\delta_n((ab)^\lambda) = \frac{1}{\lambda^2}\delta_n(a)\delta_n(b);$$

(2) 设 $d = \delta_n(ab)$, 则 d 必满足

$$\lambda^2 d = \delta_n(a)\delta_n(b)(d, \lambda).$$

20. 利用原根证明 Wilson 定理.

21. (1) 求一个 g, 它是 5 的原根, 但不是 5^2 的原根;
(2) 证明: 10 是 487 的原根, 但不是 487^2 的原根.

22. 设 $a > 1, n > 0$, 证明: $n | \varphi(a^n - 1)$.

23. 设 $n > 1$, 存在原根, 证明: g 为模 n 的原根的充要条件是 g 为模 n 的 q_i $(i = 1, 2, \cdots, k)$ 次非剩余, 其中 q_i 是 $\varphi(n)$ 的全部不同的素因子.

24. (1) 写出模 41 以原根 6 为底的指标表;
(2) 写出模 17 以原根 3 为底的指标表.

25. 设模 $n > 2$ 存在原根, 证明: 对任一原根, -1 的指标总是 $\frac{1}{2}\varphi(n)$.

26. 设 g_1, g_2 是模 m 的两个原根, 证明:

$$\mathrm{ind}_{g_1} g_2 \cdot \mathrm{ind}_{g_2} g_1 \equiv 1 \,(\mathrm{mod}\, \varphi(m)).$$

27. 利用指标表解高次同余方程:

(1) $x^{12} \equiv 16 \pmod{17}$; (2) $5x^{11} \equiv -6 \pmod{17}$; (3) $x^{15} \equiv 14 \pmod{41}$;

(4) $7x^{7} \equiv 11 \pmod{41}$; (5) $x^{6} \equiv -15 \pmod{64}$; (6) $x^{5} \equiv 13 \pmod{68}$.

28. 设素数 $p > 2$, 利用原根及指标来讨论同余方程 $ax^n \equiv b \pmod{p}$, 分 (1) $(n, p-1) = 1$; (2) $(n, p-1) > 1$ 两种情形.

第七章　Dirichlet 特征

类似于自然数列中的素数分布问题, 我们可以讨论在算术 (等差) 数列中的素数分布. 这个问题之所以重要, 不仅由于它是经典的素数分布问题的推广, 更由于它在许多著名的数论问题的研究中起着重要作用. 研究这一问题的主要工具是 Dirichlet 所引进的一类称之为特征的完全可乘函数 $\chi(n)$, 通常称为 Dirichlet 特征. 本章所讨论的特征均为 Dirichlet 特征.

§1　模为素数幂的特征的定义及其性质

首先我们来定义以素数幂为模的特征.

设 $k=p^{\alpha}, p>2, \alpha \geqslant 1$, 设 g 是所有模 p^{α} (即 p 给定, α 任意) 的最小正原根. $(n,k)=1,\ r=\operatorname{ind} n$, 即

$$n \equiv g^{r} \pmod{k}.$$

此处为方便起见, 令

$$e(x)=e^{2\pi i x}.$$

定义 1 设 $k=p^{\alpha},p>2,\alpha\geqslant 1$, 定义在全体自然数 n 上的函数

$$\chi(n)=\chi(n;k)=\chi(n;k,m)=\begin{cases}0, & (n,k)>1,\\ e\left(\dfrac{m\cdot \operatorname{ind} n}{\varphi(k)}\right), & (n,k)=1\end{cases}\tag{1}$$

称为模 k 的特征, 这里参数 m 为整数.

由定义可看出, 对同一个 k, 特征为 m 的周期函数, 周期为 $\varphi(k)$, 所以对应于模 k 的全部特征可由 m 取值 $0,1,\cdots,\varphi(k)-1$ 得到. 再设 $k=2^{\alpha}$, 当 $\alpha\geqslant 3$ 时模 k 没有原根. 但对任一奇数 n, 可引进指标组, 即

$$n\equiv(-1)^{r_{-1}}5^{r_0}\pmod{2^{\alpha}}.$$

定义 2 设 $k=2^{\alpha},\ \alpha\geqslant 1$, 由下列公式给出定义在全体自然数 n 上的函数, 称为模 k 的特征:

$$\chi(n)=\chi(n;2)=\chi(n;2,0,0)=\begin{cases}0, & (n,2)>1,\\ 1, & (n,2)=1;\end{cases}\tag{2}$$

$$\chi(n)=\chi(n;4)=\chi(n;4,m_{-1},0)=\begin{cases}0, & (n,2)>1,\\ (-1)^{m_{-1}r_{-1}}, & (n,2)=1,\end{cases}\tag{3}$$

这里 $n\equiv(-1)^{r_{-1}}\pmod 4$, 参数 m_{-1} 为整数;

$$\begin{aligned}\chi(n)&=\chi(n;2^{\alpha})=\chi(n;2^{\alpha},m_{-1},m_0)\\ &=\begin{cases}0, & (n,2)>1,\\ (-1)^{m_{-1}r_{-1}}e\left(\dfrac{m_0r_0}{2^{\alpha-2}}\right), & (n,2)=1,\end{cases}\end{aligned}\tag{4}$$

这里 $\alpha\geqslant 3$, 参数 m_{-1},m_0 为整数.

由定义及指标的性质可得到下面的定理.

定理 1 设 $k=p^{\alpha},p\geqslant 2,\alpha\geqslant 1$, 则有

(1) $\begin{cases} \chi(n;p^\alpha)=0, & (n,p)>1, \\ |\chi(n;p^\alpha)|=1, & (n,p)=1, \\ \chi(1;p^\alpha)=1; \end{cases}$

(2) $\chi(n;p^\alpha)$ 是 n 的周期函数, 周期为 p^α;

(3) $\chi(n;p^\alpha)$ 是 n 的完全可乘函数, 即

$$\chi(n_1n_2;p^\alpha)=\chi(n_1;p^\alpha)\chi(n_2;p^\alpha).$$

定理 2 对每一个模 $k=p^\alpha, p\geqslant 2, \alpha\geqslant 1$, 恰好有 $\varphi(k)$ 个不同的特征.

证 首先设 $k=p^\alpha, p>2, \alpha\geqslant 1$, 由定义 1 知模 k 所有的特征由 m 取值 $0,\ 1,\ 2,\cdots,\varphi(k)-1$ 得到, 故要证明这 $\varphi(k)$ 个特征两两不相同就行.

设 $0\leqslant m,\ m'<\varphi(k), m\neq m'$, 用反证法, 若

$$\chi(n;k,m)=\chi(n;k,m'),$$

则由定理 1 的 (1) 及当 n 遍历模 k 的简化系时, 其指标 r 就遍历模 $\varphi(k)$ 的完全系, 故得

$$\varphi(k)=\sum_{\substack{n=1\\(n,k)=1}}^{k}\frac{\chi(n;k,m)}{\chi(n;k,m')}=\sum_{r=0}^{\varphi(k)-1}e\left(\frac{m-m'}{\varphi(k)}r\right)=0.$$

矛盾, 故定理对 $k=p^\alpha, p>2$ 的情形已证.

现设 $k=2^\alpha, \alpha\geqslant 3$, 由定义 2 知, m_{-1}, m_0 和 $m_{-1}+2, m_0+2^{\alpha-2}$ 对应同一个特征, 所以模 k 的所有特征由 m_{-1} 取值 $0,1$ 及 m_0 取值 $0,1,2,\cdots,2^{\alpha-2}-1$ 给出, 共有 $2\cdot 2^{\alpha-2}=\varphi(2^\alpha)$ 个, 因此只要证明这些特征两两不相同就行. 用反证法, 设 $0\leqslant m_{-1}, m'_{-1}<2$, $0\leqslant m_0, m'_0<2^{\alpha-2}$, 且 $m_{-1}=m'_{-1}, m_0=m'_0$ 不能同时成立, 若

$$\chi(n;k,m_{-1},m_0)=\chi(n;k,m'_{-1},m'_0),$$

则由定理 1 的 (1) 及当 n 遍历模 k 的简化系时, 其指标组 r_{-1}, r_0 分别遍历模 2 及 $2^{\alpha-2}$ 的完全系, 由此得到

$$\begin{aligned}\varphi(2^\alpha) &= \sum_{\substack{n=1\\(n,2)=1}}^{2^\alpha} \frac{\chi(n;k,m_{-1},m_0)}{\chi(n;k,m'_{-1},m'_0)}\\ &= \sum_{r_{-1}=0}^{1} (-1)^{r_{-1}(m_{-1}-m'_{-1})} \times \sum_{r_0=0}^{2^{\alpha-2}-1} e\left(\frac{m_0-m'_0}{2^{\alpha-2}} r_0\right) = 0.\end{aligned}$$

上式最后一步是用到了对参数的限制. 这个矛盾就证明了 $k = 2^\alpha$, $\alpha \geqslant 3$ 的情形.

最后当 $k=2$ 时只有 1 个特征, $k=4$ 时有 2 个不同特征, 所以定理全部得证. □

我们把下面的特征称为主特征

$$\chi(n;k) = \begin{cases} 0, & (n,k) > 1,\\ 1, & (n,k) = 1. \end{cases} \tag{5}$$

主特征可简记为 $\chi^0(n;k) = \chi^0(n) = \chi^0$.

定理 3 (正交性) 设 $k = p^\alpha, p \geqslant 2, \alpha \geqslant 1$, 则有

$$\frac{1}{\varphi(k)} \sum_{\chi(\bmod k)} \chi(n) = \begin{cases} 1, & n \equiv 1 \,(\bmod k),\\ 0, & n \not\equiv 1 \,(\bmod k), \end{cases} \tag{6}$$

这里的求和号表示对模 k 的所有 $\varphi(k)$ 个特征求和, 及

$$\frac{1}{\varphi(k)} \sum_{n=1}^{k} \chi(n) = \begin{cases} 1, & \chi = \chi^0,\\ 0, & \chi \neq \chi^0. \end{cases} \tag{6'}$$

证 我们只证明 (6) 式的第二个式子. 因为当 $n \not\equiv 1 \,(\bmod k)$ 时, $\operatorname{ind} n \not\equiv 0 \,(\bmod\ \varphi(k))$, 故

$$\sum_{\chi(\bmod k)} \chi(n) = \sum_{m=0}^{\varphi(k)-1} e\left(\frac{m \cdot \operatorname{ind} n}{\varphi(k)}\right) = 0.$$

其他几个式子可从定义直接推出. □

特征 $\chi(n)$ 的一个重要性质是周期性. 对模 k 的特征来说, k 当然是它的周期, 但是特征可以有小于 k 的周期, 例如对模 $k=p^{\alpha}\,(\alpha>1)$ 来说, 显有 $\chi^0(n;p^{\alpha})=\chi^0(n;p)$, 因此 $\chi^0(n+p;p^{\alpha})=\chi^0(n;p^{\alpha})$, 所以对每一个模 k 的特征 $\chi(n;k)$ 一定有一个最小正周期 e, 利用带余数除法很容易证明 $e|k$, 我们把非主特征中最小正周期恰好等于其模的特征称为原特征, 其他的称为非原特征. 这样模 k 的特征就被分为原特征、非原特征两类, 而最重要的是原特征. 显然模 $p\,(p>2)$ 的非主特征均为原特征, 模 2 没有原特征, 模 4 的原特征为 $\chi(n;4,-1,0)$.

定理 4 设 $k=p^{\alpha},p>2$, 则 $\chi(n;p^{\alpha},m)$ 是原特征的充要条件为 $(m,p)=1$; 当 $k=2^{\alpha},\alpha\geqslant 3$ 时, $\chi(n;2^{\alpha},m)$ 为原特征的充要条件为 $(m_0,2)=1$.

证 设 $k=p^{\alpha},p>2$. 先证必要性, 设

$$\chi(n;p^{\alpha},m)=e\left(\frac{m\cdot\operatorname{ind}n}{\varphi(p^{\alpha})}\right),\quad 0<m<\varphi(p^{\alpha})$$

为非主特征, 若 $(m,p)>1$, 则 $m=m'p^{\beta},(m',p)=1,1\leqslant\beta<\alpha$, 这样就有

$$\chi(n;p^{\alpha},m)=e\left(\frac{m'\cdot\operatorname{ind}n}{\varphi(p^{\alpha-\beta})}\right)=\chi(n;p^{\alpha-\beta},m'),$$

这与原特征的定义矛盾, 所以必有 $(m,p)=1$.

现证充分性, 因为对模 $k=p$ 来说, 当 $(n,p)=1$ 时均为原特征, 现设 $k=p^{\alpha},\alpha>1$, 因为最小正周期 $e|k$, 所以我们只要证明当 $(m,p)=1$ 时, 模 k 的非主特征对任意的 $1\leqslant\lambda<\alpha$, 不可能以模 p^{λ} 为其周期. 设 $(m,p)=1$,

$$\chi(n;p^{\alpha},m)=e\left(\frac{m\cdot\operatorname{ind}n}{\varphi(p^{\alpha})}\right),$$

对任意的 $1\leqslant\lambda<\alpha$, 考虑 $n=1+p^{\lambda}$, 显然 $n\not\equiv 1\pmod{p^{\alpha}}$, 所以

$$\operatorname{ind}n\equiv 0\pmod{\varphi(p^{\lambda})},$$
$$\operatorname{ind}n\not\equiv 0\pmod{\varphi(p^{\alpha})},$$

因此 $\chi(n;p^\alpha,m)\neq 1$, 即 p^λ 不是周期, 所以为原特征.

下面来证明 $k=2^\alpha,\alpha\geqslant 1$ 的情形. $k=2$ 时, 仅有一主特征 $\chi^0(n;2)$; $k=4$ 时, 非主特征为 $\chi(n;4,-1,0)$, 因为 $\chi(3;4,-1,0)=-1$, 所以它是原特征. 当 $\alpha\geqslant 3$ 时, 其非主特征为

$$\chi(n;2^\alpha,m_{-1},m_0)=(-1)^{m_{-1}r_{-1}}e\left(\frac{m_0r_0}{2^{\alpha-2}}\right),$$

这里参数 $m_{-1},\ m_0$ 满足 $0\leqslant m_{-1}<2,\ 0\leqslant m_0<2^{\alpha-2},m_{-1},m_0$ 不同时为 0.

先证必要性, 若 $(m_0,2)>1$, 如果 $m_0=0$, 则 $m_{-1}=1$, 此时有

$$\chi(n;2^\alpha,m_{-1},m_0)=\chi(n;4,1,0).$$

因为 $\alpha\geqslant 3$, 所以这和 χ 为原特征矛盾, 如果 $m_0>0$, 则可设 $m_0=m_0'2^\beta,1\leqslant\beta<\alpha-2,(m_0',2)=1$, 故有

$$\chi(n;2^\alpha,m_{-1},m_0)=(-1)^{m_{-1}r_{-1}}e\left(\frac{m_0'r_0}{2^{\alpha-\beta-2}}\right),$$

这里 $\alpha-\beta\geqslant 3$, 由指标组性质知, 当 $n=\bar{n}\pmod{2^{\alpha-\beta}},(n,2)=1$ 时有

$$r_{-1}(n)\equiv\bar{r}_{-1}(\bar{n})\,(\mathrm{mod}\,2),\quad r_0(\bar{n})=r_0(n)\pmod{2^{\alpha-\beta-2}},$$

故当 $n=\bar{n}\pmod{2^{\alpha-\beta}}$ 时有

$$\chi(n;2^\alpha,m_{-1},m_0)=\chi(\bar{n};2^\alpha,m_{-1},m_0),$$

此即表明 $2^{\alpha-\beta}$ 为其周期, 故不可能, 因此必有 $(m_0,2)=1$.

再证充分性, 若 $(m_0,2)=1$, 则对任意 $\lambda,2\leqslant\lambda<\alpha$, 考虑 $n=1+2^\lambda$, 显然 $n\not\equiv 1\pmod{2^\alpha}$, 此时由指标组性质知, $r_{-1}(n)=0,r_0(n)\not\equiv 0\pmod{2^{\alpha-2}}$, 所以

$$\chi(n;2^\alpha,m_{-1},m_0)=e\left(\frac{m_0r_0}{2^{\alpha-2}}\right)\neq 1,$$

即任意 2^λ, $(\lambda<2)$ 均不为其周期, 所以是原特征, 定理证毕. □

定理 5 设 $k=p^{\alpha},\ p\geqslant 2$, 则对模 k 的每一个非主特征, 必有唯一的一个模 $k^*=p^{\lambda},\ \lambda\leqslant\alpha$ 及唯一的一个模 k^* 的原特征与它恒等. 反过来, 对模 $k^*=p^{\lambda}$ 的每一个原特征, 对每一个模 $k=p^{\alpha},\alpha\geqslant\lambda$, 必有唯一的一个模 k 的非主特征与它恒等.

证 先证 $k=p^{\alpha},\ p>2$ 的情形, 若 $\chi(n;p^{\alpha},m)$ 非原特征, 则必有 $\alpha\geqslant 2$, 且 $0<m<\varphi(p^{\alpha}),(m,p)>1$, 因此由 (1) 式得到

$$\chi(n;p^{\alpha},m)=\chi(n;p^{\alpha-\beta},\overline{m}),$$

这里 $m=\overline{m}p^{\beta},1\leqslant\beta<\alpha,(\overline{m},p)=1$, 由定理 4 知 $\chi(n;p^{\alpha-\beta},\overline{m})$ 为模 $p^{\alpha-\beta}$ 的原特征, 唯一性由原特征的定义推出. 反过来, 只要取 $m=\overline{m}p^{\alpha-\lambda}$ 即可 $(\lambda=\alpha-\beta)$, 当 $\chi(n;p^{\alpha},m)$ 为原特征时, 可取 $k^*=k$.

下面来证 $k=2^{\alpha}$ 的情形, 若 $\chi(n;2^{\alpha},m_{-1},m_0)$ 为非原特征, 则必有 $\alpha\geqslant 3$, 且 $(m_0,2)>1,0\leqslant m_0<2^{\alpha-2}$. 当 $m_0=0$ 时, 必有 $m_{-1}=1$, 而

$$\chi(n;2^{\alpha},1,0)=\chi(n;4,1,0),$$

即为对应模 4 的原特征, 当 $m_0>0$ 时可取 $m_0=\overline{m}_0 2^{\beta},1\leqslant\beta<\alpha-2,(\overline{m}_0,2)=1$, 由特征定义及指标组性质知

$$\chi(n;2^{\alpha},m_{-1},m_0)=\chi(n;2^{\alpha-\beta},m_{-1},\overline{m}_0),$$

而上式右边为模 $2^{\alpha-\beta}$ 的原特征, 所以 $k^*=2^{\lambda},\ \lambda=\alpha-\beta$. 反过来, 模 4 的原特征对应于模 $2^{\alpha}\,(\alpha\geqslant 3)$ 的非原特征为 $\chi(n;2^{\alpha},1,0)$, 而模 $2^{\lambda}\,(\lambda>2)$ 的原特征 $\chi(n;2^{\lambda},m_{-1},m_0)$ 对应于模 $2^{\alpha}\,(\alpha>\lambda)$ 的非原特征为 $\chi(n;2^{\alpha},m_{-1},\overline{m}_0 2^{\alpha-\lambda})$, 定理证毕. □

仅取实值的特征称为实特征, 其他称为复特征, 主特征显然为实特征.

定理 6 设 $k=p^{\alpha},\ p>2$, 则 $\chi(n;p^{\alpha},m)$ 为实特征的充要条件是 $m=0,\frac{1}{2}\varphi(p^{\alpha})$, 模 2, 模 4 的特征均为实特征; 当 $k=2^{\alpha}\,(\alpha\geqslant 3)$ 时, $\chi(n;2^{\alpha},m_{-1},m_0)$ 为实特征的充要条件为 $m_0=0,2^{\alpha-3}$.

证 由特征的定义可推出定理的论断. □

定理 7 设 $k=p^{\alpha}$, 那么当且仅当模 $k=4,8$ 及 $p\,(p>2)$ 时才有实原特征存在.

证 当 $k=2$ 时无原特征, $k=4$ 时其非主特征为

$$\chi(n;4,1,0)=\begin{cases}0, & (n,2)>1,\\ (-1)^{r_{-1}}, & (n,2)=1.\end{cases}$$

由第五章知 $r_{-1}\equiv\frac{n-1}{2}\,(\mathrm{mod}\,2)$, 故有

$$\chi(n;4,1,0)=\begin{cases}0, & (n,2)>1,\\ (-1)^{\frac{n-1}{2}}, & (n,2)=1,\end{cases}$$

显然为实原特征.

当 $k=2^{\alpha},\ \alpha\geqslant 3$ 时, 由定理 6 知, 仅当 $m_0=2^{\alpha-3}$ 时才是实的非主特征, 且当 $(m_0,2)=1$ 时才为原特征. 所以一定有 $\alpha=3$, 即 $k=8$, 此时有两个实原特征, 它们是

$$\chi(n;8,0,1)\quad 及\quad \chi(n;8,1,1).$$

不难验证

$$\chi(n;8,0,1)=\begin{cases}0, & (n,2)>1,\\ (-1)^{\frac{n^2-1}{8}}, & (n,2)=1\end{cases}\qquad\left(\frac{n^2-1}{8}\equiv r_0\,(\mathrm{mod}\,2)\right)$$

及

$$\chi(n;8,1,1)=\chi(n;4,1,0)\ \chi(n;8,0,1).$$

当 $k=p^{\alpha},\ \alpha>2$ 时, 由定理 6 知仅当 $m=\frac{1}{2}\varphi(p^{\alpha})$ 时才是实的非原特征, 且当 $(m,p)=1$ 时才是原特征, 故必有 $\alpha=1, m=\frac{1}{2}(p-1)$, 即实原特征为

$$\chi\left(n;p,\frac{p-1}{2}\right)=(-1)^{r},\quad r=\mathrm{ind}\,n.$$

因为原根一定是二次非剩余, 所以 $(\frac{g}{p})=-1$. 故有

$$\chi\left(n;p,\frac{p-1}{2}\right)=\left(\frac{g^r}{p}\right)=\left(\frac{g}{p}\right)^r=\left(\frac{n}{p}\right). \qquad \square$$

以上我们定义了以素数幂为模的特征, 并讨论了它们的基本性质. 下面我们来定义任意正整数 $k\,(k\geqslant 2)$ 为模的特征, 并把以上的定理推广到任意模的情形.

§2 任意模的特征的定义及其性质

定义 3 设 $k\geqslant 2$, 其标准分解式为 $k=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, 由等式

$$\chi(n)=\chi(n;k)=\prod_{j=1}^{s}\chi(n;p_j^{\alpha_j}) \tag{7}$$

所确定的函数 $\chi(n)$ 称为模 k 的特征, 这里 $\chi(n;p_j^{\alpha_j})$ 为以素数幂 $p_j^{\alpha_j}$ 为模的特征.

不难看出, 定理 1 对一般模的特征也是成立的, 即有

定理 1′ 设 $\chi(n;k)$ 为模 k 的特征, 则有

(1) $\begin{cases}\chi(n;k)=0, & (n,k)>1,\\ |\chi(n;k)|=1, & (n,k)=1,\\ \chi(1;k)=1;\end{cases}$

(2) $\chi(n+k;k)=\chi(n;k)$;

(3) $\chi(n_1n_2;k)=\chi(n_1;k)\chi(n_2;k)$.

现在来证明下面的定理.

定理 8 对每一个模 k, 恰好有 $\varphi(k)$ 个不同的特征.

证 由于对每一个模 $p_j^{\alpha_j}$ 恰好有 $\varphi(p_j^{\alpha_j})$ 个不同的特征, 所以对模 k 来说至多有 $\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_s^{\alpha_s})$ 个两两不同的特征.

设

$$\chi(n;k)=\prod_{j=1}^{s}\chi(n;p_j^{\alpha_j}),\quad \chi'(n;k)=\prod_{j=1}^{s}\chi'(n;p_j^{\alpha_j}). \tag{8}$$

我们要证明: $\chi(n;k)=\chi'(n;k)$ 的充要条件是

$$\chi(n;p_j^{\alpha_j})=\chi'(n;p_j^{\alpha_j}),\quad 1\leqslant j\leqslant s. \tag{9}$$

充分性是显然的, 下面来证明必要性, 为此设

$$k_jp_j^{\alpha_j}=k,\quad k_j^{-1}k_j\equiv 1\,(\mathrm{mod}\ p_j^{\alpha_j}),\quad 1\leqslant j\leqslant s; \tag{10}$$

$$n=k_1^{-1}k_1n_1+k_2^{-1}k_2n_2+\cdots+k_s^{-1}k_sn_s, \tag{11}$$

由第四章定理 29 知, 当 $n_1,n_2,\cdots,n_s$ 分别遍历模 $p_1^{\alpha_1},p_2^{\alpha_2},\cdots,p_s^{\alpha_s}$ 的完全 (简化) 系时, n 亦遍历模 k 的完全 (简化) 系, 由 (10), (11) 知对 $1\leqslant j\leqslant s$ 有

$$n\equiv n_j\,(\mathrm{mod}\ p_j^{\alpha_j}), \tag{12}$$

所以由定理 1 得到

$$\chi(n;k)=\prod_{j=1}^{s}\chi(n;p_j^{\alpha_j})=\prod_{j=1}^{s}\chi(n_j;p_j^{\alpha_j}), \tag{13}$$

$$\chi'(n;k)=\prod_{j=1}^{s}\chi'(n;p_j^{\alpha_j})=\prod_{j=1}^{s}\chi'(n_j;p_j^{\alpha_j}). \tag{14}$$

由 (13), (14) 我们可以证明对任一 $j_0,1\leqslant j_0\leqslant s$, 恒有

$$\chi(n_{j_0};p_{j_0}^{\alpha_{j_0}})=\chi'(n_{j_0};p_{j_0}^{\alpha_{j_0}}). \tag{15}$$

为此我们取 $n_j=1\,(j\neq j_0)$, 这样由 (9), (13), (14) 就推出 (15), 这就证明了必要性, 定理得证. □

我们把下面的特征称为主特征

$$\chi(n;k)=\begin{cases}0, & (n,k)>1,\\ 1, & (n,k)=1.\end{cases} \tag{16}$$

主特征可简记为 $\chi^0(n;k)=\chi^0(n)=\chi^0$.

定理 9 (正交性) 设 $k \geqslant 2$, 则有

$$\frac{1}{\varphi(k)} \sum_{\chi(\bmod k)} \chi(n) = \begin{cases} 1, & n \equiv 1 \,(\bmod k), \\ 0, & n \not\equiv 1 \,(\bmod k), \end{cases} \tag{17}$$

这里的求和号表示对模 k 的所有 $\varphi(k)$ 个特征求和, 及

$$\frac{1}{\varphi(k)} \sum_{n \leqslant k} \chi(n) = \begin{cases} 1, & \chi = \chi^0, \\ 0, & \chi \neq \chi^0. \end{cases} \tag{18}$$

证 设 $k = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$,

$$C_{-1} = \begin{cases} 1, & \alpha_0 = 1, \\ 2, & \alpha_0 \geqslant 2, \end{cases} \quad C_0 = \begin{cases} 1, & \alpha_0 = 1, \\ 2^{\alpha_0 - 2}, & \alpha_0 \geqslant 2, \end{cases} \tag{19}$$

$$C_i = \varphi(p_i^{\alpha_i}), \quad 1 \leqslant i \leqslant s.$$

所以当 $(n, k) = 1$ 时,

$$\chi(n; k) = e\left(\frac{m_{-1} r_{-1}}{C_{-1}}\right) e\left(\frac{m_0 r_0}{C_0}\right) e\left(\frac{m_1 r_1}{C_1}\right) \cdots e\left(\frac{m_s r_s}{C_s}\right), \tag{20}$$

这里 r_{-1}, r_0 为 n 对模 2^{α_0} 的指标组, r_i 为 n 对模 $p_i^{\alpha_i}$ 的指标, $0 \leqslant r_i < C_i,\ 0 \leqslant m_i < C_i, -1 \leqslant i \leqslant s$, 这样就有

$$\begin{aligned} \sum_{\chi(\bmod\ k)} \chi(n) = & \sum_{m_{-1}=0}^{C_{-1}-1} \sum_{m_0=0}^{C_0-1} \sum_{m_1=0}^{C_1-1} \cdots \sum_{m_s=0}^{C_s-1} e\left(\frac{m_{-1} r_{-1}}{C_{-1}}\right) e\left(\frac{m_0 r_0}{C_0}\right) \cdot \\ & e\left(\frac{m_1 r_1}{C_1}\right) \cdots e\left(\frac{m_s r_s}{C_s}\right) \\ = & \sum_{m_{-1}=0}^{C_{-1}-1} e\left(\frac{m_{-1} r_{-1}}{C_{-1}}\right) \sum_{m_0=0}^{C_0-1} e\left(\frac{m_0 r_0}{C_0}\right) \cdot \\ & \sum_{m_1=0}^{C_1-1} e\left(\frac{m_1 r_1}{C_1}\right) \cdots \sum_{m_s=0}^{C_s-1} e\left(\frac{m_s r_s}{C_s}\right), \end{aligned}$$

并且仅当 $n \equiv 1 \,(\bmod k)$ 时, 才有 $r_i = 0, -1 \leqslant i \leqslant s$, 此时有

$$\sum_{m_{-1}=0}^{C_{-1}-1} e\left(\frac{m_{-1} r_{-1}}{C_{-1}}\right) \sum_{m_0=0}^{C_0-1} e\left(\frac{m_0 r_0}{C_0}\right) = \varphi(2^{\alpha_0})$$

及

$$\sum_{m_i=0}^{C_i-1} e\left(\frac{m_i r_i}{C_i}\right) = \varphi(p_i^{\alpha_i}), \quad 1 \leqslant i \leqslant s.$$

而当 $n \not\equiv 1 \pmod{k}$ 时, 至少存在一个 i, 使 $r_i \neq 0$, 此时有

$$\sum_{m_i=0}^{C_i-1} e\left(\frac{m_i r_i}{C_i}\right) = 0,$$

这就证明了 (17). 为了证明 (18) 式, 我们有下面类似的公式

$$\sum_{k=1}^{n} \chi(n) = \sum_{r_{-1}=0}^{C_{-1}-1} e\left(\frac{m_{-1} r_{-1}}{C_{-1}}\right) \sum_{r_0=0}^{C_0-1} e\left(\frac{m_0 r_0}{C_0}\right) \cdot \sum_{r_1=0}^{C_1-1} e\left(\frac{m_1 r_1}{C_1}\right) \cdots \sum_{r_s=0}^{C_s-1} e\left(\frac{m_s r_s}{C_s}\right),$$

并且仅当 $\chi = \chi^0$ 时, 才有 $m_i = 0, -1 \leqslant i \leqslant s$, 这时上式等于 $\varphi(k)$, 而当 $\chi \neq \chi^0$ 时至少存在一个 $m_i \neq 0$, 此时相应的和式为零, 至此定理证毕. □

从定理的证明中可以看出 (17) 式可写成下面的更为一般的形式

$$\frac{1}{\varphi(k)} \sum_{\chi (\bmod k)} \overline{\chi}(n)\chi(l) = \begin{cases} 1, & n \equiv l \pmod{k}, \\ 0, & n \not\equiv l \pmod{k}, \end{cases} \tag{17'}$$

这里的求和号表示对模 k 的所有 $\varphi(k)$ 个特征求和.

特征和模 k 的简化系之间有一种对偶关系, 可解释如下: 显然, 由 (20) 式知模 k 的特征由数组 $m_{-1}, m_0, m_1, \cdots, m_s$, $0 \leqslant m_i < C_i$, $-1 \leqslant i \leqslant s$ 所完全确定, 我们以 $\chi(n; k, h), (h, k) = 1$ 表示模 k 的这样一个特征, 即它所对应的组数 $m_{-1}, m_0, m_1, \cdots, m_s$ 恰好是 h 对模 $2^{\alpha_0}, p_1^{\alpha_1}, \cdots, p_s^{\alpha_s}$ 的指标组和指标. 这样, 当 h 过模 k 的简化系时, $\chi(n; k, h)$ 就给出了模 k 的全部特征.

对于模 k 的特征亦可分为实特征与复特征. $\overline{\chi}(n)$ 亦为一特征, 称为 $\chi(n)$ 的共轭复特征. 在定理 8 的证明中我们很容易看出有下面的定理成立.

定理 10 $\chi(n;k)$ 为主 (实) 特征的充要条件是所有的 $\chi(n;p_j^{\alpha_j})$ $(1\leqslant j\leqslant s)$ 均为主 (实) 特征.

对模 k 我们同样可引进原特征的概念, 但是由于在 (7) 式中可能有主特征出现, 所以我们不采用以前模为素数幂的原特征的定义, 而引进下面的定义.

定义 4 设 $k\geqslant 2$, $\chi(n;k)$ 是模 k 的一个非主特征, 如果在条件 $(n,k)=1$ 下, 不存在 $k_1<k$, 使得当 $n\equiv n'\pmod{k_1}$ 时, 恒有

$$\chi(n;k)=\chi(n';k),$$

则 $\chi(n;k)$ 称为模 k 的原特征.

显然当 k 为素数幂时, 这里的定义和原来的定义是一致的.

由定义看出原特征是这样的特征, 它在条件 $(n,k)=1$ 之下, 不存在比 k 更小的正周期, 若存在比 k 小的正周期, 则称为非原特征. 设 e 是最小的正周期, 则容易证明 $e|k$.

定理 11 $\chi(n,k)$ 是模 k 的原特征的充要条件是所有的 $\chi(n;p_j^{\alpha_j})$ $(1\leqslant j\leqslant s)$ 均为原特征.

证 由定理 8 的证明知

$$\chi(n;k)=\prod_{j=1}^{s}\chi(n_j;p_j^{\alpha_j}),\tag{21}$$

这里 $n=k_1^{-1}k_1n_1+\cdots+k_s^{-1}k_sn_s$.

先证充分性, 用反证法.

若 $\chi(n;k)$ 不是原特征, 则必有 $e|k, e<k$ 使对任意的

$$n\equiv n'\,(\mathrm{mod}\,e),\quad (n,k)=(n',k)=1\tag{22}$$

有

$$\chi(n;k)=\chi(n';k).\tag{23}$$

设 $e=p_1^{\beta_1}\cdots p_s^{\beta_s}$, 因为 $e|k, e<k$, 故至少有一个 j, 使得 $\beta_j<\alpha_j$, 这样对任意的

$$n_j\equiv n_j'\ (\mathrm{mod}\ p_j^{\beta_j}),\quad (n_j,p_j)=(n_j',p_j)=1$$

及 $n_i=n_i'=1, i\neq j$ 所对应的 n 及 n' 必满足条件 (22), 再由 (21) 及 (23) 得到

$$\chi(n_j;p_j^{\beta_j})=\chi(n;k)=\chi(n';k)=\chi(n_j';p_j^{\alpha_j}),$$

所以 $\chi(n;p_j^{\alpha_j})$ 不是原特征, 矛盾.

再证必要性, 若对某一个 $j,\chi(n;p_j^{\alpha_j})$ 不是原特征, 则必有一 $\beta_j<\alpha_j$ 存在, 使得对任意的

$$n_j\equiv n_j'\pmod{p_j^{\beta_j}},\quad (n_j,p_j)=(n_j',p_j)=1$$

有

$$\chi(n_j;p_j^{\alpha_j})=\chi(n_j';p_j^{\alpha_j}).$$

现在我们取 $n=k_1^{-1}k_1n_1+\cdots+k_s^{-1}k_sn_s, n'=k_1^{-1}k_1n_1'+\cdots+k_s^{-1}k_sn_s'$, 这里 $n_j\equiv n_j'\,(\mathrm{mod}\ p_j^{\beta_j}), n_i\equiv n_i'\,(\mathrm{mod}\ p_i^{\alpha_i})$, 当 $i\neq j, 1\leqslant i\leqslant s$, 因此我们有

$$n\equiv n'\,(\mathrm{mod}\,e),\quad (n,k)=(n',k)=1,$$

这里 $e=kp_j^{\beta_j-\alpha_j}<k$. 对满足上面条件的 n 和 n' 显然有

$$\chi(n;k)=\chi(n';k),$$

所以 $\chi(n;k)$ 不是原特征, 矛盾, 定理证毕. □

定理 12 *$\chi(n;k)$ 是模 k 的实原特征的充要条件是所有的 $\chi(n;p_j^{\alpha_j})$ $(1\leqslant j\leqslant s)$ 均为实原特征, 其模 k 必为 $2^\alpha p_1p_2\cdots p_s$ 形式, $\alpha=0,2,3$.*

证 可由定理 10, 定理 11 及定理 7 推出结论. □

由定理 11 及定理 5 可得到下面的定理.

定理 13 对模 k 的每一个非主特征 $\chi(n;k)$ 必存在唯一的一个模 $k^*, k^*|k$ 及唯一的一个模 k^* 的原特征 $\chi^*(n;k^*)$, 使对所有的 $n,(n,k)=1$ 成立

$$\chi(n;k)=\chi^*(n;k^*).$$

反过来, 对模 k^* 的一个原特征 $\chi^*(n;k^*)$, 对每一个模 $k, k^*|k$ 必存在唯一的一个模 k 的非主特征 $\chi(n;k)$, 使对所有的 $n,(n,k)=1$ 成立

$$\chi^*(n;k^*)=\chi(n;k).$$

我们把上述性质所刻画的一一对应关系, 称为 χ^* 是 χ 所对应的原特征, 而 χ 是由 χ^* 导出的特征, 记作

$$\chi \Longleftrightarrow \chi^* \quad 或 \quad \chi(n;k) \Longleftrightarrow \chi^*(n;k^*).$$

由原特征的定义知模 $k\,(k\geqslant 2)$ 主特征是非原特征. 有时为了方便起见, 我们把模 $k=1$ 的特征定义为 $\chi(n;1)\equiv 1$, 它是主特征, 但显然满足原特征的定义, 所以亦是一个原特征. 这时就把它看作所有模 k 的主特征所对应的原特征. 反过来, 任意模 k 的主特征是 $\chi(n;1)$ 导出的特征.

下面的定理说明了定理 $1'$ 中刻画的特征的三个性质是它的最基本的特性.

定理 14 设 k 为自然数, $f(n)$ 是一不恒为零的数论函数, 满足下面三个条件:

(1) $f(n)=0,(n,k)>1$;

(2) $f(n+k)=f(n)$;

(3) $f(mn)=f(m)f(n)$,

则必有一个模 k 的特征 $\chi(n;k)$ 存在, 使得

$$\chi(n;k)=f(n).$$

证 设 $(a,k)=1$, χ 为模 k 的任一特征, 则

$$T=\sum_{n=1}^{k} f(n)\overline{\chi}(n)=\sum_{n=1}^{k} f(an)\overline{\chi}(an)=f(a)\overline{\chi}(a)T,$$

亦即有

$$T(1-f(a)\overline{\chi}(a))=0.$$

由上式推知, 要么存在一特征 χ, 使得 $T\neq 0$, 那么对这个特征 χ 就有

$$1-f(a)\overline{\chi}(a)=0,$$

即

$$f(a)=\overline{\chi}(a);$$

要么对所有的特征 χ 均有 $T=0$, 下面证明后面这种情形是不可能成立的.

假设 $T=0$, 则对任意的 $l,(l,k)=1$ 有

$$\sum_{\chi(\mathrm{mod}\,k)}\chi(l)\sum_{n=1}^{k} f(n)\overline{\chi}(n)=0,$$

但由 (17′) 知上式左边等于

$$\sum_{n=1}^{k} f(n)\sum_{\chi(\mathrm{mod}\,k)}\chi(l)\overline{\chi}(n)=f(l)\varphi(k).$$

因为 $f(n)$ 不恒为零, 所以一定存在一个 l, 使得 $f(l)\neq 0$, 至此定理证毕. □

由定理 14 可推出下面的定理.

定理 15 设 $\chi(n;k_1),\chi(n;k_2)$ 分别为模 k_1,k_2 的特征, 则

$$\chi(n;k_1)\ \chi(n;k_2)$$

为模 $[k_1,k_2]$ 的特征.

上面的定理当然亦可从特征的定义来直接证明.

§3 特征和

设 $k \geqslant 2, \chi(n)$ 为模 k 的特征, m 为整数, 我们称

$$G(m;\chi) = \sum_{l=1}^{k} \chi(l) e\left(\frac{ml}{k}\right) \tag{24}$$

为 Gauss 和. 当 $m = 1$ 时, 我们记

$$G(1;\chi) = \tau(\chi). \tag{25}$$

当 $\chi = \chi^0$ 时, 我们记

$$G(m;\chi^0) = C(m;k), \tag{26}$$

即

$$C(m;k) = \sum_{\substack{l=1 \\ (l,k)=1}}^{k} e\left(\frac{ml}{k}\right), \tag{27}$$

通常 $C(m;k)$ 称为 Ramanujan 和.

由 Gauss 和的定义不难得到下面的定理.

定理 16 (1) $G(m_1;\chi) = G(m_2;\chi),\ m_1 \equiv m_2 \pmod{k}$;

(2) $G(-m;\chi) = \overline{\chi}(-1)G(m;\chi)$;

(3) $G(m;\overline{\chi}) = \chi(-1)\overline{G(m;\chi)}$;

(4) $G(0;\chi^0) = \varphi(k), G(0;\chi) = 0, \chi \neq \chi^0$;

(5) $G(m;\chi) = \overline{\chi}(m)\tau(\chi),\ (m,k) = 1$.

定理 17 设 $k = k_1k_2, (k_1,k_2) = 1, \chi_1, \chi_2$ 分别是模 k_1, k_2 的特征, 令 $\chi = \chi_1\chi_2$, 则有

$$G(m;\chi) = \chi_1(k_2)\chi_2(k_1)G(m;\chi_1)G(m;\chi_2). \tag{28}$$

证 由定理 15 知 χ 为模 k 的特征, 令 $l=k_2l_1+k_1l_2$, 则当 l_1,l_2 通过模 k_1,k_2 的完全系时, l 通过模 k 的完全系, 所以

$$\begin{aligned}G(m;\chi)&=\sum_{l=1}^{k}\chi(l)e\left(\frac{ml}{k}\right)=\sum_{l_1=1}^{k_1}\sum_{l_2=1}^{k_2}\chi(k_2l_1+k_1l_2)e\left(\frac{m(l_1k_2+l_2k_1)}{k}\right)\\&=\sum_{l_1=1}^{k_1}\chi_1(k_2l_1)e\left(\frac{ml_1}{k_1}\right)\sum_{l_2=1}^{k_2}\chi_2(k_1l_2)e\left(\frac{ml_2}{k_2}\right)\\&=\chi_1(k_2)\chi_2(k_1)G(m;\chi_1)G(m;\chi_2).\end{aligned}$$

□

推论 设 $k=k_1k_2,(k_1,k_2)=1$, 则有

$$C(m;k)=C(m;k_1)C(m;k_2),\tag{29}$$

即 $C(m;k)$ 为 k 的可乘函数.

定理 18

$$C(m;k)=\mu\left(\frac{k}{(m,k)}\right)\varphi(k)\varphi^{-1}\left(\frac{k}{(m,k)}\right),\tag{30}$$

特别地, 当 $(m,k)=1$ 时, 有

$$C(m;k)=C(1;k)=\mu(k).\tag{31}$$

证 因为 $C(m;k)$ 为 k 的可乘函数, 所以只要对 $k=p^\alpha$ 的情形来证明 (30) 即可.

$$\begin{aligned}C(m;p^\alpha)&=\sum_{\substack{l=1\\(l,p)=1}}^{p^\alpha}e\left(\frac{ml}{p^\alpha}\right)=\sum_{l=1}^{p^\alpha}e\left(\frac{ml}{p^\alpha}\right)-\sum_{l=1}^{p^{\alpha-1}}e\left(\frac{ml}{p^{\alpha-1}}\right)\\&=\begin{cases}p^\alpha-p^{\alpha-1}, & p^\alpha\big|m,\\-p^{\alpha-1}, & p^{\alpha-1}\big\|m,\\0, & p^{\alpha-1}\nmid m,\end{cases}\end{aligned}$$

所以

$$C(m;p^\alpha)=\mu\left(\frac{p^\alpha}{(p^\alpha,m)}\right)\varphi(p^\alpha)\varphi^{-1}\left(\frac{p^\alpha}{(p^\alpha,m)}\right).$$

定理得证. □

定理 17 说明了对一般 Gauss 和的讨论可以归结为对模为素数幂的特征的 Gauss 和的讨论. 而定理 16 的 (5) 表明当 $(m,k)=1$ 时, $G(m;\chi)$ 可以归结为较简单的 $\tau(\chi)$. 下面我们要证明, 当 χ 为原特征时, 定理 16 的 (5) 当 $(m,k)>1$ 时亦是成立的, 这是 Gauss 和的一个极为重要的性质.

定理 19 设 χ 为模 k 的原特征, 则有

$$G(m;\chi)=0,\quad (m,k)>1.$$

证 我们只要对模 $k=p^\alpha,\ p\geqslant 2$ 的情形来证明即可. 当 $k=2$ 时无原特征; 当 $k=2^2$ 时, 原特征为

$$\chi(n)=(-1)^{\frac{n-1}{2}},\quad (n,2)=1.$$

设 $m=2m'$, 则

$$G(m;\chi)=\chi(1)e\left(\frac{2m'}{4}\right)+\chi(3)e\left(\frac{2m'\cdot 3}{4}\right)=e\left(\frac{m'}{2}\right)(\chi(1)+\chi(3))=0.$$

现设 $k=2^\alpha,\ \alpha\geqslant 3,\ m=2m',\ \chi$ 为模 2^α 的原特征. 由定理 4 证明知

$$\chi(l)=(-1)^{m_{-1}r_{-1}}e\left(\frac{m_0r_0}{2^{\alpha-2}}\right),\quad (m_0,2)=1,\quad (l,k)=1,$$

这里 r_{-1},r_0 为 l 的指标组.

$$G(m;\chi)=\sum_{l=1}^{2^\alpha}\chi(l)e\left(\frac{lm}{2^\alpha}\right)=\sum_{l=1}^{2^\alpha}\chi(l)e\left(\frac{lm'}{2^{\alpha-1}}\right),$$

令 $l=v+u2^{\alpha-1}$, 得

$$G(m;\chi)=\sum_{v=1}^{2^{\alpha-1}}e\left(\frac{vm'}{2^{\alpha-1}}\right)\sum_{u=0}^{1}\chi(u2^{\alpha-1}+v).\tag{32}$$

我们要证明对任意的 $(v,2)=1$, 成立

$$\sum_{u=0}^{1}\chi(u2^{\alpha-1}+v)=0.\tag{33}$$

因为 $(v,2)=1$, 所以可设 $vv^{-1}\equiv 1 \pmod{2^\alpha}$, 必有 $(v^{-1},2)=1$, 因此

$$\chi(v^{-1})\sum_{u=0}^{1}\chi(u2^{\alpha-1}+v)=\sum_{u=0}^{1}\chi(u2^{\alpha-1}+1)=\chi(1)+\chi(1+2^{\alpha-1}). \tag{34}$$

我们只要证明 $\chi(1+2^{\alpha-1})=-1$ 即可, 设 r_{-1},r_0 为 $1+2^{\alpha-1}$ 对模 2^α $(\alpha\geqslant 3)$ 的指标组, 则有 $r_{-1}=0, r_0=2^{\alpha-3}$, 因为 $(m_0,2)=1$, 所以

$$\chi(1+2^{\alpha-1})=e\left(\frac{m_0 2^{\alpha-3}}{2^{\alpha-2}}\right)=(-1)^{m_0}=-1,$$

因此 (33) 式成立.

下面来讨论 $k=p^\alpha,\ p>2$ 的情形. 首先当 $\alpha=1$ 时, 由 $p|m$ 及 $\chi\neq\chi^0$ 立即推出

$$G(m;\chi)=\sum_{l=1}^{k}\chi(l)=0,$$

所以剩下的只要证明 $\alpha\geqslant 2$ 的情形, 为此令 $l=v+up^{\alpha-1}$, 则有

$$\begin{aligned}G(m;\chi)&=\sum_{v=1}^{p^{\alpha-1}}{}'\sum_{u=0}^{p-1}\chi(up^{\alpha-1}+v)e\left(\frac{mup^{\alpha-1}}{p^\alpha}\right)e\left(\frac{mv}{p^\alpha}\right)\\&=\sum_{v=1}^{p^{\alpha-1}}{}'e\left(\frac{m'v}{p^{\alpha-1}}\right)\sum_{u=0}^{p-1}\chi(up^{\alpha-1}+v),\end{aligned}\tag{35}$$

这里 $m=m'p$, 因为 $(v,p)=1$, 所以由 (35) 式得到

$$G(m;\chi)=\sum_{v=1}^{p^{\alpha-1}}{}'e\left(\frac{m'v}{p^{\alpha-1}}\right)\chi(v)\sum_{u=0}^{p-1}\chi(up^{\alpha-1}+1). \tag{36}$$

现在我们来证明

$$\sum_{u=0}^{p-1}\chi(up^{\alpha-1}+1)=0. \tag{37}$$

设 g 为所有模 p^β $(\beta\geqslant 1)$ 的原根, 以 $r=r(u),\ r'=r(v)$ 分别表示 $up^{\alpha-1}+1$ 对模 $p^\alpha,\ p^{\alpha-1}$ 的指标, 则由指标性质知必有

$$r'=0,\quad r\equiv r' \pmod{\varphi(p^{\alpha-1})}.$$

由上式得到

$$r = r(u) = b(u)p^{\alpha-2}(p-1), \quad 0 \leqslant b(u) < p,$$

由于当 $0 \leqslant u \leqslant p-1$ 时, $up^{\alpha-1}+1$ 对模 p^α 两两不同余, 所以它们的指标对模 $\varphi(p^\alpha)$ 亦两两不同余, 因此 $b(u)$ 对模 p 两两不同余, 所以当 u 遍历模 p 的完全系时, $b = b(u)$ 亦遍历模 p 的完全系, 得

$$\begin{aligned}\sum_{u=0}^{p-1}\chi(up^{\alpha-1}+1) &= \sum_{u=0}^{p-1} e\left(\frac{mr(u)}{\varphi(p^\alpha)}\right) = \sum_{u=0}^{p-1} e\left(\frac{mb(u)p^{\alpha-2}(p-1)}{\varphi(p^\alpha)}\right)\\ &= \sum_{u=0}^{p-1} e\left(\frac{mb(u)}{p}\right) = \sum_{b=0}^{p-1} e\left(\frac{mb}{p}\right) = 0,\end{aligned}$$

这里 $(m,p)=1$. 至此定理全部证毕. □

由定理 19 及定理 16 (5) 得到下面的定理.

定理 20 *设 χ 为模 k 的原特征, 则有*

$$G(m;\chi) = \overline{\chi}(m)\tau(\chi). \tag{38}$$

定理 21 *设 χ 为模 k 的原特征, 则有*

$$|\tau(\chi)| = \sqrt{k}. \tag{39}$$

证 由 (38) 得到

$$\sum_{m=1}^{k}|G(m;\chi)|^2 = \sum_{m=1}^{k}|\chi(m)|^2|\tau(x)|^2 = \varphi(k)|\tau(\chi)|^2, \tag{40}$$

但另一方面由 $G(m;\chi)$ 的定义得到

$$\begin{aligned}\sum_{m=1}^{k}|G(m;\chi)|^2 &= \sum_{m=1}^{k}\sum_{l_1=1}^{k}\chi(l_1)e\left(\frac{ml_1}{k}\right)\sum_{l_2=1}^{k}\overline{\chi}(l_2)e\left(\frac{-ml_2}{k}\right)\\ &= \sum_{l_1=1}^{k}\sum_{l_2=1}^{k}\chi(l_1)\overline{\chi}(l_2)\sum_{m=1}^{k}e\left(\frac{m(l_1-l_2)}{k}\right)\\ &= k\sum_{l=1}^{k}\chi(l)\overline{\chi}(l) = k\varphi(k).\end{aligned} \tag{41}$$

由 (40), (41) 即得 (39). □

最后我们指出特征和的一个重要性质, 设 χ 是模 k 的非特征, 则由 (18) 式知, 对任意的 M, N 有

$$\left|\sum_{n=N+1}^{N+M}\chi(n)\right| < \frac{1}{2}\varphi(k). \tag{42}$$

但这个估计是较粗糙的, 我们有下面的定理.

定理 22 设 χ 是模 k 的原特征, 则对任意的 M, N 有

$$\left|\sum_{n=N+1}^{N+M}\chi(n)\right| < \sqrt{k}\log k. \tag{43}$$

证 不失一般性, 可设 $M < k$, 由 (38) 式知

$$\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{l=1}^{k}\overline{\chi}(l)e\left(\frac{nl}{k}\right),$$

所以

$$\sum_{n=N+1}^{N+M}\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{l=1}^{k}\overline{\chi}(l)\sum_{n=N+1}^{N+M}e\left(\frac{nl}{k}\right).$$

若以 S 记作上式右边的和式, 则由上式得到

$$|S| \leqslant \frac{1}{\sqrt{k}}\sum_{l=1}^{k-1}\left|\sum_{n=0}^{M-1}e\left(\frac{nl}{k}\right)\right|. \tag{44}$$

由于当 $1 \leqslant l \leqslant k-1$ 时有

$$\left|\sum_{n=0}^{M-1}e\left(\frac{nl}{k}\right)\right| \leqslant \frac{2}{\left|1-e\left(\frac{l}{k}\right)\right|} = \left(\sin\frac{\pi l}{k}\right)^{-1},$$

所以

$$|S| \leqslant \frac{1}{\sqrt{k}}\sum_{l=1}^{k-1}\left(\sin\frac{\pi l}{k}\right)^{-1}. \tag{45}$$

但当 $0 \leqslant x \leqslant \frac{\pi}{2}$ 时, 有 $\sin x \geqslant \frac{2}{\pi}x$, 所以当 k 为奇数时, 由上式得到

$$|S| \leqslant \frac{2}{\sqrt{k}}\sum_{l=1}^{\frac{1}{2}(k-1)}\left(\sin\frac{\pi l}{k}\right)^{-1} < \sqrt{k}\sum_{l=1}^{\frac{1}{2}(k-1)}\frac{1}{l}; \tag{46}$$

当 k 是偶数时得到

$$|S| < \frac{2}{\sqrt{k}} \sum_{l=1}^{\frac{1}{2}(k-1)} \left(\sin \frac{\pi l}{k}\right)^{-1} + \frac{1}{\sqrt{k}} \leqslant \sqrt{k} \sum_{l=1}^{\frac{k}{2}-1} \frac{1}{l} + \frac{1}{\sqrt{k}}. \tag{47}$$

再利用不等式

$$\log \frac{2m+1}{2m-1} = \int_{2m-1}^{2m+1} \frac{dt}{t} > \frac{1}{m}, \quad m \geqslant 1$$

可得, 当 k 为奇数时

$$\sum_{l=1}^{\frac{1}{2}(k-1)} \frac{1}{l} < \log k; \tag{48}$$

当 k 为偶数时

$$\sum_{l=1}^{\frac{k}{2}-1} \frac{1}{l} < \log(k-1) \leqslant \log k - \frac{1}{\sqrt{k}}. \tag{49}$$

由 (45)–(49) 即得 (43). □

校 后 记

本书是由潘承洞院士生前所写的《数论基础》讲义校对整理而成的. 整理过程中我们完全保持了讲义的原貌, 只是对文字做了仔细校对.

作为山东大学数学系七九级的一名学生, 我有幸在 1982 年旁听了潘承洞先生给数学系七八级本科生讲授 “数论基础” 这门选修课. 在我的印象里那时还没有印制好的讲义, 潘先生在讲台上讲, 我们边听边记. 虽然是选修课, 但是教室里坐得很满, 我只能在角落里找到一个位置. 现在想来, 或许那次系统的讲授正是本书最初形成的过程. 大学毕业后我成为潘先生的研究生, 我们这些学生们随后每人拿到了一本油印的《数论基础》讲义. 讲义是先生的 “手书版”, 也就是本书的原稿. 再后来, 这本油印讲义有了打印版, 它也从此成为潘先生所有学生以及学生的学生们的数论入门书籍. 遗憾的是, 先生手书的油印版书稿一本也没有保存下来.

不知何故这本书稿一直没有正式出版. 或许是因为先生忙碌疏忽了, 或许是他觉得已经有太多的数论入门书籍. 但是这本书却是我们

的最爱. 不论是在先生自己学术工作最具影响力的解析数论领域, 还是他在上世纪 80 年代就开始培养学生的现代密码学领域, 我们这些学生都觉得这本书由浅入深, 循序渐进, 内容既精选紧凑, 又全面深刻, 还附有大量的习题, 让我们在认真研读之中忘却了许多对数论的神秘和畏惧. 它的内容布局独具一格, 能够引导你迅速进入数论核心的领域, 了解数论最基本的思想和方法. 它对很多定理和结论的证明简洁明快, 既注重数论的技巧之美, 又清晰地勾勒出数论方法的系统性, 让你在 "不知不觉" 之中已经深入到那些最初看来 "深奥莫测" 的知识里. 所以, 我们觉得先生留下的这样一笔财富不能仅仅由他的学生们独享, 而应该让更多对数学特别是数论有兴趣的学生和学者来共同分享.

我和刘建亚教授的这一想法首先得到师母李淑英老师和潘先生的胞弟潘承彪教授的鼓励与支持, 而潘先生的学生们以及我们的学生们则一直期待这本书能够尽快出版. 这一愿望能够得以实现要感谢高等教育出版社的查卫平副总编, 他把这本书稿推荐给出版社的赵天夫编辑. 天夫严谨高效的工作使得本书的出版立项和编辑在最短时间内就完成了.

这本讲义的原稿中没有列出参考文献. 我们在学习数论时按照先生的指导常看的书籍有:《数论基础》, 维诺格拉陀夫著, 裘光明译, 高等教育出版社, 1956;《数论导引》, 华罗庚著, 科学出版社, 1975; *An Introduction to the Theory of Numbers*, G. H. Hardy 和 E. M. Wright 著, 牛津大学出版社, 2008 年出版了第六版;《阶的估计》, 潘承洞和于秀源编著, 山东科学技术出版社, 1983. 这些书籍亦可作为读者阅读本书的参考书目.

我们之所以希望赶在今年年底之前完成这本书的出版, 还有一个原因, 就是今年潘承洞先生离开我们已经整整 15 年了. 这位以 Goldbach 猜想研究闻名于世, 为解析数论研究作出卓越贡献的数论大家, 曾和华罗庚、陈景润、王元先生一起被国外同行誉为解析数论的中国学派 (Chinese School) 的代表. 他一生为培养年轻人才倾注了大量的心

血, 三十年前他为本科生讲授这门课程的情景今天依然历历在目. 以出版这本他生前完成的书稿来纪念他, 来激励我们后人学习他的学术精神, 传承他的学术思想, 是再合适不过的一种方式了.

展涛, 2012 年秋于北京