

第8章 方程 $c_1x_1^k + \cdots + c_sx_s^k = 0$

The equation $c_1x_1^k + \cdots + c_sx_s^k = 0$

我们现在研究上述方程在整数（正的或负的）范围内的解，其中 $c_1, \dots, c_s$ 是固定的整数，没有一个为 0。如果 k 是偶数，我们显然必须假设这些系数并非全部同号。如果 k 是奇数，则我们可以在必要时把 x_i 换成 $-x_i$ 来保证这一点。于是，稍微改变记号后，我们可以把方程写成

$$c_1x_1^k + \cdots + c_rx_r^k - c_{r+1}x_{r+1}^k - \cdots - c_sx_s^k = 0, \quad (8.1)$$

其中 $c_1, \dots, c_s$ 现在都是正整数，且 $1 \leq r \leq s-1$ 。我们研究 (8.1) 在正整数范围内的解。

与第7章所处理的方程相比，第一个不同之处在于：这里不存在一个对未知数大小施加限制的大数 N 。因此我们必须自行为变量规定取值范围，而最自然的做法是选取一个大数 P ，对每个 $1 \leq j \leq s$ 定义 $P_j = [P/c_j^{1/k}]$ ，并考虑 (8.1) 满足下述条件的解的个数：

$$1 \leq x_j \leq P_j, \quad (1 \leq j \leq s). \quad (8.2)$$

我们像之前在 (7.1) 中那样定义指数和 $T_j(\alpha)$ 。于是 (8.1) 在条件 (8.2) 下的解数 $\mathcal{N}(P)$ 由下式给出

$$\mathcal{N}(P) = \int_0^1 T_1(\alpha) \cdots T_r(\alpha) T_{r+1}(-\alpha) \cdots T_s(-\alpha) d\alpha.$$

我们再次沿用对华林问题的处理方式，作出与前一节相同的细微改动。唯一进一步的改动来自奇异级数与奇异积分中 N 的缺失。在 (4.10) 中，我们须把 $J(P^\delta)$ 替换为

$$(c_1 \cdots c_s)^{-1/k} \int_{|\gamma| < P^\delta} \left(\prod_{j=1}^s \int_0^1 e(\pm \gamma \xi_j^k) d\xi_j \right) d\gamma,$$

其中符号在 $j \leq r$ 时取 $+$ ，在 $j > r$ 时取 $-$ 。如同 (4.16) 那样，我们被引向对下述积分的求值

$$J = \int_{-\infty}^{\infty} k^{-s} \left(\prod_{j=1}^s \int_0^1 \zeta_j^{-1+1/k} e(\pm \gamma \zeta_j) d\zeta_j \right) d\gamma.$$

正如定理 4.1 的证明中那样，我们把变量从 ζ_s 换成 u ，其中

$$\zeta_1 + \cdots + \zeta_r - \zeta_{r+1} - \cdots - \zeta_s = u,$$

于是我们求得

$$J = k^{-s} \int_0^1 \cdots \int_0^1 \{\zeta_1 \cdots \zeta_s (\zeta_1 + \cdots \pm \zeta_{s-1})\}^{-1+1/k} d\zeta_1 \cdots d\zeta_{s-1},$$

其中 $0 < \zeta_1 + \cdots \pm \zeta_{s-1} < 1$ 。我们所需要知道的只是 $J > 0$ ，而这一点成立，是因为存在某个含于 $0 < \zeta_j < 1$ （对所有 j ）内的开集，在其上有

$$0 < \zeta_1 + \cdots \pm \zeta_{s-1} < 1.$$

这样，对 $s \geq 2^k + 1$ 已证明的 $\mathcal{N}(P)$ 的渐近公式取下述形式

$$\mathcal{N}(P) = \frac{C'_{k,s}}{(c_1 \cdots c_s)^{1/k}} P^{s-k} \mathfrak{S} + O(P^{s-k-\delta}), \quad (8.3)$$

其中

$$C'_{k,s} = k^{-s} \int_0^1 \cdots \int_0^1 \{\eta_1 \cdots \eta_s (\eta_1 + \cdots - \eta_{s-1})\}^{-1+1/k} d\eta_1 \cdots d\eta_{s-1}, \quad (8.4)$$

且

$$\mathfrak{S} = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^q q^{-s} S_{c_1 a, q} \cdots S_{-c_s a, q}. \quad (8.5)$$

我们注意到，现在 $\mathfrak{S}$ 的值是一个仅依赖于系数 $c_1, \dots, -c_s$ 以及 k 的数。如前所述，定义 $\mathfrak{S}$ 的级数在 $s \geq 2k + 1$ 时绝对收敛，并可因子分解为 $\prod \chi(p)$ 。同样存在一个 p_0 使得

$$\prod_{p > p_0} \chi(p) \geq \frac{1}{2}.$$

为了确保 $\mathfrak{S} > 0$ (现在无需再写成 $\mathfrak{S} \geq C_1(k, s) > 0$, 因为不再有参数 N), 只需对每个单独的 p 证明 $\chi_p > 0$ 即可。如前所述, 只要满足下式即足够

$$M(p^\nu) \geq C_p p^{\nu(s-1)} \quad (8.6)$$

对所有充分大的 ν 成立, 这里 $M(p^\nu)$ 表示同余式

$$c_1 x_1^k + \cdots - c_s x_s^k \equiv 0 \pmod{p^\nu}, \quad 0 \leq x < p^\nu \quad (8.7)$$

的解的总数。

我们现在的目标是求出 k 的某个明确的函数 $s_1(k)$, 使得对每个 p , 只要 $s \geq s_1(k)$, (8.6) 即成立。于是渐近公式 (8.3) 将是有意义的, 因为其中主项的阶为 P^{s-k} , 从而当 $P \rightarrow \infty$ 时 $\mathcal{N}(P) \rightarrow \infty$ 。在证明这一结果时, (8.7) 中系数的符号不起任何作用, 因此我们回到原始记号, 即系数前不带负号的记号。

第一步是导出一个未知数个数较少、且其中没有任何系数能被 p 整除的同余式, 使得若 (8.6) 对这个新同余式成立, 则它对原同余式也成立。我们记

$$c_j = d_j p^{h_j k + l_j}, \quad (1 \leq j \leq s),$$

其中

$$p \nmid d_j, \quad 0 \leq l_j < k.$$

于是 (8.7) 变为

$$\sum_{j=1}^s d_j p^{l_j} (p^{h_j} x_j)^k \equiv 0 \pmod{p^\nu}.$$

令 $h = \max h_j$ 。我们将自己限于下述形式的解

$$x_j = p^{h-h_j} y_j.$$

这样, 对于大的 ν , 我们可以从同余式中消去 p^{hk} , 于是它变成

$$\sum_{j=1}^s d_j p^{l_j} y_j^k \equiv 0 \pmod{p^{\nu-hk}}, \quad (8.8)$$

受下述约束

$$0 \leq y < p^{\nu-h+h_j}.$$

如果我们用 $M'(p^{\nu-hk})$ 表示 (8.8) 满足

$$0 \leq y < p^{\nu-hk}$$

的解的个数, 那么 (因为 $h - h_j < hk$) 我们有

$$M(p^\nu) \geq M'(p^{\nu-hk}).$$

因此只需对 $M'(p^\nu)$ 证明 (8.6) 的类比即可。

令 $l = \max l_j$ 。在新的同余式 (8.8) 中 (但取模 p^ν)，我们按 l_j 的值把各项归并到一起。共有 k 组，其中至少有一组必含有 v 项，这里 $v \geq s/k$ 。我们在其余项中令 $y_j = py'_j$ ，并在除去一个因子 p^l 之后，得到下述形式的同余式

$$d_1 y_1^k + \cdots + d_v y_v^k + p(d_{v+1} y_{v+1}^k + \cdots) + \cdots \equiv 0 \pmod{p^{\nu-l}}. \quad (8.9)$$

我们仍可在右边把 $\nu - l$ 换成 ν ，因为这只是把 (8.6) 这类结果中的 C_p 改变一下。在这最后一个同余式中，我们有

$$d_1 d_2 \cdots d_v \not\equiv 0 \pmod{p}.$$

像通常那样定义 γ (见 (5.11))。利用引理 5.5 证明中所用的论证，所求结果 (8.6) 对同余式 (8.9) 将成立，只要下述同余式

$$d_1 y_1^k + \cdots + d_v y_v^k \equiv 0 \pmod{p^\gamma} \quad (8.10)$$

有一个解，其中 $y_1, \dots, y_v$ 并非全部能被 p 整除。

设 $p > 2$ 。我们像定理 7.2 证明中那样论证，把 (8.10) 中各项按系数 d_j 所属的 k 次幂剩余类或非剩余类归并成组。只要满足下式即足够

$$\frac{v}{p^{\gamma-1}\delta} > 2k - 1,$$

又因为 $p^{\gamma-1}\delta = p^\tau\delta \leq k$, 所以只要满足下式即足够

$$v > k(2k - 1).$$

因此只要满足下式即足够

$$s > k^2(2k - 1).$$

设 $p = 2$ 。再一次, 若 $\tau = 0$, 即 k 为奇数, 则不成问题。若 $\tau > 0$, 我们可以像定理 7.2 证明中那样论证, 但有一个更有效的论证相当简单。我们将证明

$$d_1y_1^k + \cdots + d_vy_v^k \equiv 0 \pmod{2^\gamma}$$

有一个解, 其中 $y_1, \dots, y_v$ 并非全为偶数, 只要 $v \geq 2^\gamma$ 。我们通过取 $y_j = 0$ 或 1 来找到这些解 (如同与引理 5.6 相关联时所指出的, 当 k 是 2 的幂时这不损失一般性)。

首先, 若 $\gamma = 1$, 我们可以求解

$$d_1t_1 + d_2t_2 \equiv 0 \pmod{2}$$

方法是取 $t_1 = t_2 = 1$ (因为 d_1, d_2 为奇数)。其次, 我们可以求解

$$d_1t_1 + d_2t_2 + d_3t_3 + d_4t_4 \equiv 0 \pmod{4}$$

方法是取 $t_1 = t_2 = 1, t_3 = t_4 = 0$ (若 $d_1 + d_2 \equiv 0 \pmod{4}$), 或者取 $t_1 = t_2 = 0, t_3 = t_4 = 1$ (若 $d_3 + d_4 \equiv 0 \pmod{4}$), 或者取 $t_1 = t_2 = t_3 = t_4 = 1$ 。这个过程继续下去, 证明可以容易地通过对 γ 作归纳来完成。

条件 $v \geq 2^\gamma$ 在 $v \geq 4k$ 时即满足, 因此当 $s > k(4k - 1)$ 时即满足。由于这个数小于 $k^2(2k - 1)$, 它对结果没有影响。

综合我们的结果, 我们已经证明:

定理 8.1. 设 $c_1, \dots, c_s$ 是给定的整数, 没有一个为 0, 且当 k 为偶数时不全同号。那么, 只要 $s \geq 2^k + 1$, 且

$$s \geq k^2(2k - 1) + 1, \tag{8.11}$$

方程

$$c_1 x_1^k + \cdots + c_s x_s^k = 0$$

就有无穷多组整数解 $x_1, \dots, x_s$, 其中没有一个为 0。

条件 (8.11) 来自我们对奇异级数的研究, 它并非最佳可能。在 [27] 中, Davenport 与 Lewis 证明了: 为确保 $\mathfrak{S} > 0$, 只要

$$s \geq k^2 + 1$$

即足够。当 $k+1$ 是素数 p 时这个条件是最佳可能的。因为这时 $x^k \equiv 1 \pmod{p}$ (若 $x \not\equiv 0 \pmod{p}$), 于是容易推出: 含 k^2 个变量的同余式

$$p^k \mid ((x_1^k + \cdots + x_k^k) + p(x_{k+1}^k + \cdots + x_{2k}^k) + \cdots + p^{k-1}(x_{k^2-k+1}^k + \cdots + x_{k^2}^k))$$

除非所有变量都能被 p 整除, 否则无解。然而, 对 k 的大多数值, 较小的值 $k^2 + 1$ 即足够。

在前面对方程

$$c_1 x_1^k + \cdots + c_s x_s^k = 0$$

的处理中, 我们已得到了: 当 $P \rightarrow \infty$ 时, 在 s 维盒子 $0 < x_j \leq P_j$ 中整数解个数的渐近公式。但这个盒子与方程之间并无任何独特方式的联系, 结果之所以有意义, 主要在于它确立了无穷多解的存在性。然而, 为证明这一点, 并不必须得到这样一个盒子中所有解的渐近公式; 只需考虑某个特殊子集就足够了。这样, 我们就可以使用类似于为估计华林问题中 $G(k)$ 所发展出来的方法。在第9章中, 我们将研究维诺格拉多夫 (Vinogradov) 的方法, 它对于大的 k 非常有效; 在随后的一章中, 我们将把这个方法应用于我们一直在研究的方程。

不过, 不应忽视的是: 我们一直在使用的方法特别适合于研究方程之解的分布。设 $\lambda_1, \dots, \lambda_s$ 是任意实数, 没有一个为 0, 并满足方程

$$c_1 \lambda_1^k + \cdots + c_s \lambda_s^k = 0.$$

那么本节的方法使人能够求得: 当 $P \rightarrow \infty$ 时, 我们的方程在盒子

$$1 - \delta < \frac{x_j}{\lambda_j P} < 1 + \delta$$

中整数解的渐近公式，这里 δ 是任意小的固定正数。用几何语言表述，这一结果意味着：从原点到锥面

$$c_1x_1^k + \cdots + c_sx_s^k = 0$$

上整点的那些"射线"，若把该锥面视为 s 维空间中的实轨迹，则它们在此锥面上处处稠密。因此，尽管现在要阐述的方法在确立无穷多解方面更为有效，但它并不能完全取代前一种方法。