

三次型：奇异级数

Cubic forms: the singular series

把引理 15.1、15.4 与 16.1 的结果合在一起，我们现在已经证明：若 $n \geq 17$ ，且排除引理 13.4 的备选 A，又若盒子 $\mathfrak{B}$ 选取得当，则盒子 $P\mathfrak{B}$ 中满足 $C(\mathbf{x}) = 0$ 的整点个数 $\mathcal{N}(P)$ 满足

$$\mathcal{N}(P) = P^{n-3} \mathfrak{S}(P^\Delta) \{J_0 + o(1)\} + O(P^{n-3-\delta}),$$

其中 $\delta > 0$ 。引理 15.4 中给出的级数 $\mathfrak{S}(P^\Delta)$ ，若延拓到无穷，则绝对收敛（前提是 $n \geq 17$ 且排除备选 A），因为此时由引理 15.3 有

$$q^{-n} |S_{a,q}| \ll q^{-\frac{1}{8}n + \varepsilon - 2 - \delta}.$$

由第 14 章的工作，备选 A 蕴含 $C(\mathbf{x}) = 0$ 有非平凡的整数解。这样我们就证明了：

定理 17.1. 若 $n \geq 17$ 且 $\mathfrak{S} > 0$ ，则方程 $C(\mathbf{x}) = 0$ 有非平凡的整数解。

因为若不存在非平凡解，我们便得到

$$\mathcal{N}(P) \sim P^{n-3} \mathfrak{S} J_0 \quad \text{当 } P \rightarrow \infty,$$

从而 $\mathcal{N}(P) \rightarrow \infty$ ，产生矛盾。

这里当然 $\mathfrak{S}$ 表示延拓到无穷的奇异级数，即

$$\mathfrak{S} = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^q q^{-n} S_{a,q}.$$

剩下需要证明的是：对每一个变元个数不少于 17 的三次型，都有 $\mathfrak{S} > 0$ 。引理 5.1 的证明适用于一般的指数和（如当时所指出的），它表明若令

$$A(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^q q^{-n} S_{a,q},$$

则 $A(q)$ 是 q 的乘性函数（对互素的 q 值而言）。在 $n \geq 17$ 且 $C(\mathbf{x})$ 不表示零的前提下，由引理 15.3 我们有

$$|A(q)| \ll q^{1-\frac{1}{8}n+\varepsilon} \ll q^{-1-\delta}.$$

因此 $\mathfrak{S} = \sum_q A(q)$ 绝对收敛，从而可知

$$\mathfrak{S} = \prod_p \chi(p),$$

其中

$$\chi(p) = 1 + \sum_{\nu=1}^{\infty} A(p^{\nu}).$$

在上述条件下我们还有

$$|\chi(p) - 1| \ll p^{-1-\delta},$$

所以存在 p_0 ，使得

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

正如引理 5.2 的推论所示。引理 5.3 的论证表明

$$\chi(p) = \lim_{\nu \rightarrow \infty} \frac{M(p^\nu)}{p^{\nu(n-1)}},$$

其中 $M(p^\nu)$ 表示同余式

$$C(x_1, \dots, x_n) \equiv 0 \pmod{p^\nu}, \quad 0 \leq x_j < p^\nu$$

的解的个数。

因此，为了证明 $\mathfrak{S} > 0$ （在当前条件下），只需证明：对每一个素数 p ，都有

$$M(p^\nu) \geq C_p p^{\nu(n-1)}, \quad C_p > 0, \quad (17.1)$$

对一切充分大的 ν 成立。

在处理加性型的型时，我们曾发现：同余式

$$a_1 x_1^k + \dots + a_n x_n^k \equiv 0 \pmod{p^{\gamma_1}}$$

只要存在一个解，其中 $x_1, \dots, x_n$ 并非全都被 p 整除，就足以蕴含 (17.1) 对一切充分大的 ν 成立——这里 γ_1 是一个适当的指数，依赖于 p 和 k ，以及整除各系数 a_j 的 p 的方幂。对一般的型，情形并不那么简单。看来人们需要的不仅仅是一个 $(\text{mod } p^{\gamma_1})$ 的解；人们需要这样一个解：其偏导数 $\partial C / \partial x_1, \dots, \partial C / \partial x_n$ 并非全都能被 p 的过高方幂整除。对于加性型，存在一个明显的限制，因为关于 x_j 的导数是 $a_j k x_j^{k-1}$ ，而总有某个 j 使 x_j 不被 p 整除。

定义. 设 p 为素数， ℓ 为正整数。我们称 $C(\mathbf{x})$ 具有性质 $\mathcal{A}(p^\ell)$ ，若存在

$$C(x_1, \dots, x_n) \equiv 0 \pmod{p^{2\ell-1}} \quad (17.2)$$

的一个解，使得

$$\partial C / \partial x_i \equiv 0 \pmod{p^{\ell-1}} \quad \text{对一切 } i \quad (17.3)$$

且

$$\partial C / \partial x_i \not\equiv 0 \pmod{p^\ell} \quad \text{对某个 } i. \quad (17.4)$$

引理 17.1. 设 $C(\mathbf{x})$ 具有性质 $\mathcal{A}(p^\ell)$ 。则

$$M(p^{2\ell-1+\nu}) \geq p^{(n-1)\nu},$$

从而 $\chi(p) > 0$ 。

证. 我们对 ν 作归纳, 证明同余式

$$C(x_1, \dots, x_n) \equiv 0 \pmod{p^{2\ell-1+\nu}} \quad (17.5)$$

至少有 $p^{(n-1)\nu}$ 个满足 (17.3) 与 (17.4) 的解, 且这些解关于模 $p^{\ell+\nu}$ 两两不同余 (从而对模 $p^{2\ell-1+\nu}$ 更是如此)。这将蕴含所要的结果。当 $\nu = 0$ 时, 断言就是假设本身。

对任意整数 $x_1, \dots, x_n, u_1, \dots, u_n$, 我们有

$$C(\mathbf{x} + p^{\ell+\nu}\mathbf{u}) \equiv C(\mathbf{x}) + p^{\ell+\nu}(u_1 \partial C / \partial x_1 + \dots) \pmod{p^{2\ell+2\nu}}.$$

我们假设上述结果对某个特定的 ν 成立, 并取 $x_1, \dots, x_n$ 为 (17.5) 的 $p^{(n-1)\nu}$ 个满足 (17.3) 与 (17.4) 的解之一, 这些解关于模 $p^{\ell+\nu}$ 两两不同余。我们可以令

$$C(\mathbf{x}) = ap^{2\ell-1+\nu}, \quad \partial C / \partial x_i = D_i p^{\ell-1},$$

其中 $a, D_1, \dots, D_n$ 为整数, 且对某个 i 有 $D_i \not\equiv 0 \pmod{p}$ 。同余式

$$C(\mathbf{x} + p^{\ell+\nu}\mathbf{u}) \equiv 0 \pmod{p^{2\ell+\nu}}$$

成立当且仅当

$$a + D_1 u_1 + \dots + D_n u_n \equiv 0 \pmod{p}.$$

这在 $\mathbf{u}$ 上有 p^{n-1} 个解, 关于模 p 两两不同余。

这样，对应于每一个 $\mathbf{x}$ ，我们得到 p^{n-1} 个值 $\mathbf{y} = \mathbf{x} + p^{\ell+\nu}\mathbf{u}$ 。这些值满足

$$C(\mathbf{y}) \equiv 0 \pmod{p^{2\ell+\nu}}, \quad \mathbf{y} \equiv \mathbf{x} \pmod{p^{\ell+\nu}}.$$

由后一式可知，每个 $\mathbf{y}$ 满足 (17.3) 与 (17.4)。我们总共得到 $p^{(n-1)(\nu+1)}$ 个 $\mathbf{y}$ 值，且它们关于模 $p^{\ell+\nu+1}$ 两两不同余。于是断言对 $\nu + 1$ （代替 ν ）成立，这就证明了结果。 ■

关于对每个 p 都存在某个 ℓ 使得 $C(\mathbf{x})$ 具有性质 $\mathcal{A}(p^\ell)$ 的证明，构成下一章的主题。