

Waring 问题：奇异级数

Waring's problem: the singular series

我们现在来研究奇异级数 (singular series):

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^q (q^{-1}S_{a,q})^s e(-aN/q). \quad (5.1)$$

我们将会发现, $\mathfrak{S}(N)$ 的值与下列同余方程

$$x_1^k + \cdots + x_s^k \equiv N \pmod{q}$$

对一切正整数 q 的解数密切相关; 并且确实地, 若任何这样的同余方程无解, 则 $\mathfrak{S}(N) = 0$ 。这一点从渐近公式的形式上是可以预料到的, 因为此时 $r(N) = 0$ 。

我们记

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q), \quad A(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^q (q^{-1}S_{a,q})^s e(-aN/q). \quad (5.2)$$

引理 5.1. 若 $(q_1, q_2) = 1$, 则

$$A(q_1 q_2) = A(q_1) A(q_2). \quad (5.3)$$

证. 记

$$f(a, q) = (S_{a,q})^s e(-aN/q).$$

我们将证明: 若 $(a_1, q_1) = (a_2, q_2) = 1$ 且

$$\frac{a}{q} \equiv \frac{a_1}{q_1} + \frac{a_2}{q_2} \pmod{1}, \quad q = q_1 q_2, \quad (5.4)$$

则

$$f(a, q) = f(a_1, q_1) f(a_2, q_2). \quad (5.5)$$

这就足以给出所要的结果, 因为关系式 (5.4) 在既约剩余类 $a \pmod{q}$ 与既约剩余类对 $a_1 \pmod{q_1}$ 、 $a_2 \pmod{q_2}$ 之间建立了一一对应, 从而

$$\sum_{\substack{a=1 \\ (a,q)=1}}^q f(a, q) = \left(\sum_{\substack{a_1=1 \\ (a_1,q_1)=1}}^{q_1} f(a_1, q_1) \right) \left(\sum_{\substack{a_2=1 \\ (a_2,q_2)=1}}^{q_2} f(a_2, q_2) \right).$$

为了证明 (5.5), 我们使用一个相当类似的论证, 但这次用的是完全剩余系。令

$$\frac{z}{q} \equiv \frac{z_1}{q_1} + \frac{z_2}{q_2} \pmod{1},$$

则有

$$S_{a,q} = \sum_{z=1}^q e(az^k/q) = \sum_{z_1=1}^{q_1} \sum_{z_2=1}^{q_2} e\left(\frac{a}{q} q^k \left(\frac{z_1}{q_1} + \frac{z_2}{q_2}\right)^k\right),$$

并且由于

$$\frac{a}{q} q^k \left(\frac{z_1}{q_1} + \frac{z_2}{q_2}\right)^k \equiv \frac{a_1}{q_1} (q_2 z_1)^k + \frac{a_2}{q_2} (q_1 z_2)^k \pmod{1},$$

我们得到

$$\begin{aligned} S_{a,q} &= \sum_{z_1=1}^{q_1} e\left(\frac{a_1}{q_1} (q_2 z_1)^k\right) \sum_{z_2=1}^{q_2} e\left(\frac{a_2}{q_2} (q_1 z_2)^k\right) \\ &= S_{a_1,q_1} S_{a_2,q_2}. \end{aligned}$$

此外, 由于

$$e\left(-\frac{a}{q} N\right) = e\left(-\frac{a_1}{q_1} N\right) e\left(-\frac{a_2}{q_2} N\right),$$

我们便得到 (5.5)。

注. 这个引理的结果完全不依赖于 $S_{a,q}$ 是由特殊多项式 z^k 构成这一事实。我们可以把 z^k 换成任何具有整系数的多项式 $f(z)$ ，并且事实上可以把 $S_{a,q}$ 换成多重指数和

$$\sum e\left(\frac{a}{q}f(z_1, \dots, z_n)\right),$$

其中每个 $z_1, \dots, z_n$ 各自跑遍一组完全剩余系 $(\bmod q)$ 。证明完全相同。

引理 5.2. 若 $s \geq 2^k + 1$ ，则

$$\mathfrak{S}(N) = \prod_p \chi(p), \quad (5.6)$$

其中

$$\chi(p) = 1 + \sum_{\nu=1}^{\infty} A(p^\nu). \quad (5.7)$$

又有

$$|\chi(p) - 1| \ll p^{-1-\delta} \quad (5.8)$$

对某个固定的 $\delta > 0$ 成立。

证. 由引理 5.1 可知，若 $q = p_1^{\nu_1} p_2^{\nu_2} \cdots$ ，则

$$A(q) = A(p_1^{\nu_1}) A(p_2^{\nu_2}) \cdots.$$

于是

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q) = \prod_p \left\{ \sum_{\nu=0}^{\infty} A(p^\nu) \right\} = \prod_p \chi(p),$$

这一点由 $\sum |A(q)|$ 的收敛性所保证，而后者已在前一章中证明。

我们已经有了估计

$$|A(q)| \ll q^{-1-1/K+\varepsilon} \ll q^{-1-\delta},$$

这蕴含

$$|\chi(p) - 1| \ll \sum_{\nu=1}^{\infty} p^{-\nu(1+\delta)} \ll p^{-1-\delta},$$

这就是 (5.8)。

推论. 若 $s \geq 2^k + 1$, 则存在 $p_0 = p_0(k)$ 使得

$$\frac{1}{2} \leq \prod_{p > p_0} \chi(p) \leq \frac{3}{2}.$$

这立即由 (5.8) 得出, 因为我们可以取 δ 仅依赖于 k 。同样地, 我们将会看到这个结果在 $s \geq 2k + 1$ 时也成立。

定义. 设 $M(q)$ 表示同余方程

$$x_1^k + \cdots + x_s^k \equiv N \pmod{q}$$

的解数, 其中 $0 < x_1, \dots, x_s \leq q$ 。

引理 5.3. 我们有

$$1 + \sum_{\nu=1}^n A(p^\nu) = M(p^n)/p^{n(s-1)}, \quad (5.9)$$

从而

$$\chi(p) = \lim_{n \rightarrow \infty} M(p^n)/p^{n(s-1)}. \quad (5.10)$$

证. 我们可以用一个程序把 $M(q)$ 表示为指数和, 这个程序是 (2.7) 中把 $r(N)$ 表示为积分那种方法的算术类比。我们有

$$M(q) = q^{-1} \sum_{t=1}^q \sum_{x_1=1}^q \cdots \sum_{x_s=1}^q e \left(\frac{t}{q} (x_1^k + \cdots + x_s^k - N) \right),$$

因为对 t 求和当同余方程成立时给出 q ，否则给出 0。我们把那些与 q 有相同最大公因子的 t 值汇集在一起。若这个最大公因子记为 q/q_1 ，则相应的 t 值为 uq/q_1 ，其中 $1 \leq u \leq q_1$ 且 $(u, q_1) = 1$ 。于是

$$M(q) = q^{-1} \sum_{q_1|q} \sum_{\substack{u=1 \\ (u, q_1)=1}}^{q_1} \sum_{x_1=1}^q \cdots \sum_{x_s=1}^q e \left(\frac{u}{q_1} (x_1^k + \cdots + x_s^k - N) \right).$$

现在

$$\sum_{x=1}^q e \left(\frac{u}{q_1} x^k \right) = \frac{q}{q_1} \sum_{x=1}^{q_1} e \left(\frac{u}{q_1} x^k \right) = \frac{q}{q_1} S_{u, q_1}.$$

因此

$$\begin{aligned} M(q) &= q^{-1} \sum_{q_1|q} \sum_{\substack{u=1 \\ (u, q_1)=1}}^{q_1} \left(\frac{q}{q_1} \right)^s (S_{u, q_1})^s e \left(-\frac{uN}{q_1} \right) \\ &= q^{s-1} \sum_{q_1|q} A(q_1). \end{aligned}$$

这个公式当 $q = p^n$ 时即成为 (5.9)，而 (5.10) 也由它得出。

注. 对每个特定的 N ，(5.9) 左边的级数都会终止，因此 (5.10) 在 n 充分大时无需取极限即成立。然而该级数终止的那一点不仅依赖于 k 和 p ，也依赖于 N 。

定义. 对每个素数 p ，设 p^τ 为整除 k 的 p 的最高幂，并令 $k = p^\tau k_0$ 。定义 γ 为

$$\gamma = \begin{cases} \tau + 1 & \text{若 } p > 2, \\ \tau + 2 & \text{若 } p = 2. \end{cases} \quad (5.11)$$

当然， γ 同时依赖于 p 和 k 。

引理 5.4. 若同余方程 $y^k \equiv m \pmod{p^\gamma}$ 有解, 其中 $m \not\equiv 0 \pmod{p}$, 则同余方程 $x^k \equiv m \pmod{p^\nu}$ 对每个 $\nu > \gamma$ 都有解。

证. 设 $p > 2$. 模 p^ν 的互素既约剩余类组成一个阶为 $\phi(p^\nu) = p^{\nu-1}(p-1)$ 的循环群, 可用模 p^ν 的原根 g 的各次幂来表示. 若 $\nu > \gamma$, 则 g 必然也是模 p^γ 的原根。

记

$$m \equiv g^\mu, \quad y \equiv g^\eta, \quad x \equiv g^\xi \pmod{p^\nu}.$$

那么假设 $y^k \equiv m \pmod{p^\gamma}$ 等价于

$$k\eta \equiv \mu \pmod{p^{\gamma-1}(p-1)}.$$

由于 $k = p^\tau k_0$ 且 $\tau = \gamma - 1$, 可知 μ 能被 $p^{\gamma-1}$ 整除, 也能被 $(k_0, p-1)$ 整除. 但现在我们可以找到 ξ 满足

$$k\xi \equiv \mu \pmod{p^{\nu-1}(p-1)},$$

因为 μ 能被 k 与 $p^{\nu-1}(p-1)$ 的最大公因子整除. 最后一个同余方程等价于 $x^k \equiv m \pmod{p^\nu}$.

设 $p = 2$. 首先, 若 $\tau = 0$, 即 k 为奇数, 则不成问题. 因为当 x 跑遍模 2^ν 的一组既约剩余系时 x^k 也跑遍这组既约剩余系, 从而同余方程 $x^k \equiv m \pmod{2^\nu}$ 对任何奇数 m 都无需任何假设即可解。

现在设 $k = 2^\tau k_0$ 为偶数. 我们有 $x^k \equiv 1 \pmod{4}$ 对一切 x 成立. 那些模 2^ν 且 $\equiv 1 \pmod{4}$ 的剩余类组成一个阶为 $2^{\nu-2}$ 的循环群, 而众所周知 5 是一个生成元, 即一个原根. 如前一样, 记

$$m \equiv 5^\mu, \quad y \equiv 5^\eta, \quad x \equiv 5^\xi \pmod{2^\nu}.$$

那么假设等价于

$$k\eta \equiv \mu \pmod{2^{\gamma-2}}.$$

由于 $k = 2^\tau k_0$ 且 $\tau = \gamma - 2$, 可知 μ 能被 2^τ 整除. 因此存在 ξ 使得

$$k\xi \equiv \mu \pmod{2^{\nu-2}},$$

这蕴含 $x^k \equiv m \pmod{2^\nu}$ 。这就完成了引理 5.4 的证明。

引理 5.5. 若同余方程

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma}$$

有解 $x_1, \dots, x_s$ 满足它们不全被 p 整除, 则

$$\chi(p) > 0.$$

证. 设 $a_1^k + \cdots + a_s^k \equiv N \pmod{p^\gamma}$ 且 $a_1 \not\equiv 0 \pmod{p}$ 。我们可以用如下构造对 $\nu > \gamma$ 得到 $x_1^k + \cdots + x_s^k \equiv N \pmod{p^\nu}$ 的许多解。我们任意地选取 $x_2, \dots, x_s$, 只须满足

$$x_j \equiv a_j \pmod{p^\gamma}, \quad 0 < x_j \leq p^\nu.$$

这些选择可以有 $p^{(\nu-\gamma)(s-1)}$ 种方式。然后选取 x_1 满足

$$x_1^k \equiv N - x_2^k - \cdots - x_s^k \pmod{p^\nu};$$

由引理 5.4 这是可能的, 因为右边

$$\equiv a_1^k \pmod{p^\gamma} \quad \text{且} \quad a_1 \not\equiv 0 \pmod{p}.$$

于是, 按照前面引入的记号, 我们有

$$M(p^\nu) \geq p^{(\nu-\gamma)(s-1)} = C_p p^{\nu(s-1)},$$

其中 $C_p = p^{-\gamma(s-1)} > 0$ 。由引理 5.3 的 (5.10), 这蕴含 $\chi(p) > 0$ 。 ■

引理 5.6. 若 $s \geq 2k$ (k 为奇数) 或 $s \geq 4k$ (k 为偶数), 则对一切素数 p 和一切 N 都有 $\chi(p) > 0$ 。

证. 由引理 5.5, 只须证明同余方程

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma} \tag{5.12}$$

有解 $x_1, \dots, x_s$ 不全被 p 整除。若 $N \not\equiv 0 \pmod{p}$, 则后一要求自动满足。若 $N \equiv 0 \pmod{p}$, 则只须解同余方程

$$x_1^k + \dots + x_{s-1}^k + 1^k \equiv N \pmod{p^\gamma}.$$

因此 (把 $s-1$ 换成 s) 我们看到, 只须证明当 $N \not\equiv 0 \pmod{p}$ 时 (5.12) 在 $s \geq 2k-1$ (k 奇) 或 $s \geq 4k-1$ (k 偶) 下可解。

设 $p > 2$ 。我们考虑一切满足

$$0 < N < p^\gamma, \quad N \not\equiv 0 \pmod{p}$$

的 N , 它们的个数为 $\phi(p^\gamma) = p^{\gamma-1}(p-1)$ 。设 $s(N)$ 表示使 (5.12) 可解的最小的 s 。若 $N \equiv z^k N' \pmod{p^\gamma}$, 则显然 $s(N) = s(N')$ 。因此, 如果我们按 $s(N)$ 的值把数 N 分成若干类, 每一类中的个数至少等于当 $z \not\equiv 0 \pmod{p}$ 时 z^k 所取的不同值的个数。令 $z \equiv g^\zeta \pmod{p^\gamma}$, 其中 g 是模 p^γ 的原根, 并令 $a \equiv g^\alpha \pmod{p^\gamma}$, 则容易看出, 同余方程 $z^k \equiv a \pmod{p^\gamma}$ 可解当且仅当 α 能被 $p^{\gamma-1}\delta$ 整除, 其中 $\delta = (k, p-1)$ 。由于 $\tau = \gamma-1$, α (模 $p^{\gamma-1}(p-1)$) 的不同值的个数 (这也是 a (模 p^γ) 的不同值的个数) 为

$$\frac{p^{\gamma-1}(p-1)}{p^{\gamma-1}\delta} = \frac{p-1}{\delta} = r,$$

记之为 r 。因此 N 的每个取值类都至少包含 r 个元素。

我们先枚举一切使 $s(N) = 1$ 的 N :

$$N_1^{(1)} < N_2^{(1)} < \dots < N_{r_1}^{(1)}, \quad \text{其中 } r_1 \geq r.$$

然后我们枚举一切使 $s(N) = 2$ 的 N :

$$N_1^{(2)} < N_2^{(2)} < \dots < N_{r_2}^{(2)}, \quad \text{其中 } r_2 \geq r,$$

依此类推。这些集合中有些可能为空, 但我们将证明任意两个相邻的集合不能都为空。

考虑不在前 $j-1$ 个集合中的最小的 $N' \not\equiv 0 \pmod{p}$ 。那么 $N'-1$ 或 $N'-2$ 之一 $\not\equiv 0 \pmod{p}$, 并且由于它小于 N' , 必定在前 $j-1$ 个集合之中。把 N' 表示成

$$(N'-1) + 1^k \quad \text{或} \quad (N'-2) + 1^k + 1^k,$$

我们推出 $s(N') \leq j + 1$ 。因此使 $s(N) = j$ 、 $s(N) = j + 1$ 的两个集合不能都为空。

设枚举中最后一个非空集合是使 $s(N) = m$ 的那个。那么前 $m - 1$ 个集合中至少有 $\frac{1}{2}(m - 1)$ 个非空，而第 m 个集合也非空，从而至少有 $\frac{1}{2}(m + 1)$ 个非空集合。由于每个集合至少含 r 个数，我们有

$$\frac{1}{2}(m + 1)r \leq \phi(p^\gamma) = p^{\gamma-1}(p - 1),$$

由此

$$\begin{aligned} (m + 1) &\leq \frac{2p^{\gamma-1}(p - 1)}{r} = 2p^{\gamma-1}\delta \\ &= 2p^\tau(k_0, p - 1) \leq 2k. \end{aligned}$$

因此 $m \leq 2k - 1$ ，从而对一切 N 有 $s(N) \leq 2k - 1$ 。这样，对 $p > 2$ ，当 $s \geq 2k - 1$ 时同余方程 (5.12) 可解。

设 $p = 2$ 。若 $\tau = 0$ ，即 k 为奇数，则正如引理 5.4 证明中所指出的，当 $N \not\equiv 0 \pmod{p}$ 时同余方程 (5.12) 在 $s = 1$ 时即可解。这就证明了引理 5.6 的结论，因为此时对来自素数 $p > 2$ 的 s 唯一有意义的限制就是这一条。

现在设 $\tau \geq 1$ ，即 k 为偶数。我们不妨设 $0 < N < 2^\gamma$ ，因为现在 N 是奇数。在 (5.12) 中取所有 x_j 为 0 或 1，我们当然可以在 $s \geq 2^\gamma - 1$ 时解出同余方程。现在

$$2^\gamma - 1 = 2^{\tau+2} - 1 \leq 4k - 1.$$

因此当 $s \geq 4k - 1$ 时即足够，这就在 k 为偶数的情形下证明了引理 5.6 的结论。

注. 尽管最后这个论证乍看起来可能显得粗糙，但当 $k = 2^\tau$ 且 $\tau \geq 2$ 时我们实际上毫无损失。因为此时若 x 为奇数则 $x^{2^\tau} \equiv 1 \pmod{2^{\tau+2}}$ ，若 x 为偶数则 $x^{2^\tau} \equiv 0 \pmod{2^{\tau+2}}$ ，所以 x^k 的值在此情形下就只是 0 和 1。

Hardy 与 Littlewood 定义 $\Gamma(k)$ 为使下述成立的最小的 s 值：同余方程 (5.12) 对一切 p 和一切 N 都有解 $x_1, \dots, x_s$ 不全被 p 整除。在此记号下，引理 5.6 表明当 k 为奇数时 $\Gamma(k) \leq 2k$ ，当 k 为偶数时 $\Gamma(k) \leq 4k$ 。Hardy 与 Littlewood 在

P.N.VIII [41] 中对 $\Gamma(k)$ 作了更为详细的研究。¹ 特别地，他们确定了所有满足 $\Gamma(k) > k$ 的 k 的类型。 $\Gamma(k)$ 的前几个值为：

k	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\Gamma(k)$	4	16	5	9	4	32	13	12	11	16	6	14	15	64

定理 5.1. 若 $s \geq 2^k + 1$ ，则

$$\mathfrak{S}(N) \geq C_1(k, s) > 0$$

对一切 N 成立。

证. 这个结果由引理 5.6 和引理 5.2 的推论得出，因为 $2^k + 1 \geq 2k$ (k 为奇数) 以及 $2^k + 1 \geq 4k$ (k 为偶数, $k > 2$)。 ■

定理 5.1 是对定理 4.1 的一个必要补充，它表明渐近公式中的主项是 $\gg N^{s/k-1}$ ，从而当 $N \rightarrow \infty$ 时 $r(N) \rightarrow \infty$ 。

在本章中我大体上遵循了 Vinogradov 的论述 [93，第 2 章]。² 这比 Hardy 与 Littlewood 原来的论述稍微简单一些。

1. 另见 Chowla [14]。↵
2. 我们的引理 5.4 中 $p = 2$ 的情形被 Vinogradov 无意中遗漏了。↵