

Waring 问题：历史

Waring's problem: history

Edward Waring 在他的《代数沉思录》（*Meditationes algebraicae*, 1770）中陈述道：每个数都可表示为 4 个平方数之和，或 9 个立方数之和，或 19 个四次方数之和，“依此类推”。由最后这句话可推知，他想要断言的是：对于每个 $k \geq 2$ ，都存在某个 s ，使得每个正整数 N 可表示为

$$N = x_1^k + x_2^k + \cdots + x_s^k, \quad (2.1)$$

其中 $x_i \geq 0$ 。这个断言首先由 Hilbert 于 1909 年证明。Hilbert 的证明是一项非常伟大的成就，尽管其中部分功劳也应归于 Hurwitz，他的工作提供了出发点。Hurwitz 此前已经证明：若该断言对某个指数 k 成立，则它对 $2k$ 也成立。通常用 $g(k)$ 表示使得每个 N 都可表示的最小 s 值。如今 $g(k)$ 的确切值对所有 k 值都已知晓。我在此不讨论 Hilbert 的证明方法；关于这一点，可参阅 Stridsberg [79]、Schmidt [72] 或 Rieger [71] 的论文。

Hardy 与 Littlewood 的工作出现在一系列题为“关于数的分拆”（“On Partitio Numerorum”，简记 P.N.）的若干篇论文中，该系列的其余论文主要关注 Goldbach 的三素数问题。在 P.N. I [37] 中，他们得到了关于 $r(N)$ （即 N 表示为形如 (2.1) 且 $x_i \geq 1$ 的表法数目）的一个渐近公式，只要 $s \geq s_0(k)$ （ k 的某个确切函数）即成立。该渐近公式具有如下形式：

$$r(N) = C_{k,s} N^{s/k-1} \mathfrak{S}(N) + O(N^{s/k-1-\delta}), \quad (2.2)$$

其中 $\delta > 0$ 且

$$C_{k,s} = \frac{\Gamma(1 + 1/k)^s}{\Gamma(s/k)} > 0.$$

在上述公式中， $\mathfrak{S}(N)$ 是一个纯算术性质的无穷级数，Hardy 与 Littlewood 称之为奇异级数 (singular series)。他们进一步证明了

$$\mathfrak{S}(N) \geq \gamma > 0, \quad (2.3)$$

其中 γ 与 N 无关，只要 $s \geq s_1(k)$ 。然而他们在该阶段并未给出 $s_1(k)$ 的任何确切值。于是该公式蕴含着

$$r(N) \sim C_{k,s} N^{s/k-1} \mathfrak{S}(N) \quad (2.4)$$

当 $N \rightarrow \infty$ ，只要 $s \geq \max(s_0(k), s_1(k))$ ，从而独立地给出了 Hilbert 定理的一个证明。

Hardy 与 Littlewood 引入记号 $G(k)$ 表示使得每个充分大的 N 都可表示为形如 (2.1) 的最小 s 值；这个函数实际上比 $g(k)$ 更具意义，因为后者受到表示某一两个特殊数 N 的难度的影响。在 P.N. II [38] 和 P.N. IV [39] 中，Hardy 与 Littlewood 证明了渐近公式以及 $\mathfrak{S}(N)$ 的下界两者都对 $s \geq (k-2)2^{k-1} + 5$ 成立，这蕴含着

$$G(k) \leq (k-2)2^{k-1} + 5.$$

在 P.N. VI [40] 中，他们对 $G(k)$ 找到了一个更好的上界（尽管对渐近公式的成立性并非如此），特别地，他们证明了 $G(4) \leq 19$ 。该系列的最后一篇论文 P.N. VIII [41] 则完全关注奇异级数以及由它引出的同余问题。

Hardy 与 Littlewood 以 $r(N)$ 的母函数（生成函数）作为他们的出发点，也就是幂级数

$$\sum_{N=0}^{\infty} r(N) z^N = \left(\sum_{n=0}^{\infty} z^{n^k} \right)^s.$$

他们借助 Cauchy 给出幂级数系数的公式，利用沿圆周 $|z| = \rho$ （其中 ρ 略小于 1）取的围道积分，把 $r(N)$ 用此函数表示出来。Vinogradov 在 1928 年作出了一项有益的技术简化；它在于用一个有限的指数和来代替幂级数，其效果是消除了 Hardy 与 Littlewood 原始论述中出现的若干不重要的复杂之处。

记 $e(t) = e^{2\pi it}$ 。对于实变量 α ，我们定义 $T(\alpha)$ 为

$$T(\alpha) = \sum_{x=1}^P e(\alpha x^k), \quad (2.5)$$

其中 P 是一个正整数。则

$$(T(\alpha))^s = \sum_m r'(m) e(m\alpha), \quad (2.6)$$

其中 $r'(m)$ 表示 m 表示为

$$x_1^k + \cdots + x_s^k, \quad (1 \leq x_i \leq P)$$

的表法数目。若 $P \geq [N^{1/k}]$ （其中 $[\lambda]$ 表示实数 λ 的整数部分），则 $r'(N)$ 就是 N 表示为形如 (2.1) 且 $x_i \geq 1$ 的表法总数。因此 $r'(N) = r(N)$ 。若我们将 (2.6) 的两边乘以 $e(-N\alpha)$ 并在单位区间 $[0, 1]$ 上（或任何长度为 1 的区间上）积分，便得到

$$r(N) = \int_0^1 (T(\alpha))^s e(-N\alpha) d\alpha. \quad (2.7)$$

这就是我们研究 Waring 问题工作的出发点。它对应于 Hardy 与 Littlewood 所用的 $r(N)$ 的围道积分，只是把 z 替换成了 $e^{2\pi i\alpha}$ 。

我们的首要目标是建立渐近公式 (2.2) 对 $r(N)$ 当 $N \rightarrow \infty$ 时的成立性，所受的条件为 $s \geq 2^k + 1$ 。借助华罗庚于 1938 年发现的一个不等式（下文引理 3.2），有可能以一种相对简单的方式做到这一点。值得注意的是：就渐近公式本身而言，迄今尚未对小 k 值的条件 $s \geq 2^k + 1$ 作出任何改进。对于大的 k ，Vinogradov 已经证明形如 $s > Ck^2 \log k$ 的条件即足够。

若我们对某个特定的 s 值（比如 $s = s_1$ ）证明了渐近公式成立，那么就可推出每个大数都可表示为 s_1 个 k 次方之和，从而 $G(k) \leq s_1$ 。但为了证明这一点，并不必证明关于表法总数的渐近公式；只需对某种特殊类型的表法证明它即可，即作为 s_1 个 k 次方之和。这使得有可能得到比由渐近公式的成立性所能得到的更好的 $G(k)$ 估计。1934 年 Vinogradov 证明了对大的 k 有 $G(k) < Ck \log k$ ，我们将在第 9 章给出一个证明。对小 k 已知的最佳结果由 Davenport 于 1939–41 年间找到 [19]。

关于 Hilbert 定理的一个新的“初等”证明由 Linnik 于 1943 年给出 [58]，并被 Khintchine 选入他的“三颗明珠” [53] 之中。这个证明的根本思想无疑是受到了 Hardy–Littlewood 方法某些特征的启发，特别是受到了华罗庚不等式的启发。