

DAVENPORT · 圆法 · 高中详解版

华林问题：数 $G(k)$

Waring's problem: the number $G(k)$

本页是面向中国普通高中生的逐段精讲。彩色框（目标 / 符号 / 分步推演 / 配图）是为你准备的详解；我们把原书里所有"显然""容易看出""不难"的地方，统统拆成一步一步的完整推导，并把每一个超出高中范围的符号都从零讲清。读起来会很长——但读完，你能真正看懂 Vinogradov 这条著名定理的每一处细节。

本章要解决什么

每个正整数都能写成若干个完全 k 次幂（如 $1, 2^k, 3^k, \dots$ ）之和——这是 18 世纪 Waring 的猜想。本章关心的是"对所有充分大的整数，最少需要几个 k 次幂"，这个最少个数记作 $G(k)$ 。

读完你将掌握：

- $G(k)$ 的精确定义，以及它的简单下界 $G(k) \geq k + 1$ 、上界 $G(k) \leq 2^k + 1$ 从何而来；
- 圆法 (the circle method) 怎样把"有多少种表示法"变成一个定积分 $\int_0^1$ ；主弧、次弧如何划分区间 $[0, 1]$ ；
- van der Corput 的"求和换积分"引理、Vinogradov 的"双线性和"估计这两件核心工具，以及它们各自的完整证明；
- 怎样把这些零件拼起来，证出 Vinogradov 1934 年的著名上界

$$G(k) < (6 + \delta) k \log k.$$

预备：先把记号从零讲清

本章用到大量分析数论的"行话"。它们其实都能用高中知识理解，只是写法陌生。下面这一组卡片请先扫一遍，遇到不懂的符号随时回来查。

求和号 $\sum$ 与连乘 $\prod$ $\sum_{x=1}^P f(x)$ 读作"对 x 从 1 到 P 求和"，就是

$f(1) + f(2) + \cdots + f(P)$ 。下标写条件（如 $\sum_{(a,q)=1}$ ）表示"只对满足该条件的项求和"。这和高中数列求和完全是一回事，只是项可以是复数。

复指数 $e(\alpha) = e^{2\pi i \alpha}$

这是全章的主角，务必弄懂。这里 i 是虚数单位（ $i^2 = -1$ ）， π 是圆周率。由欧拉公式

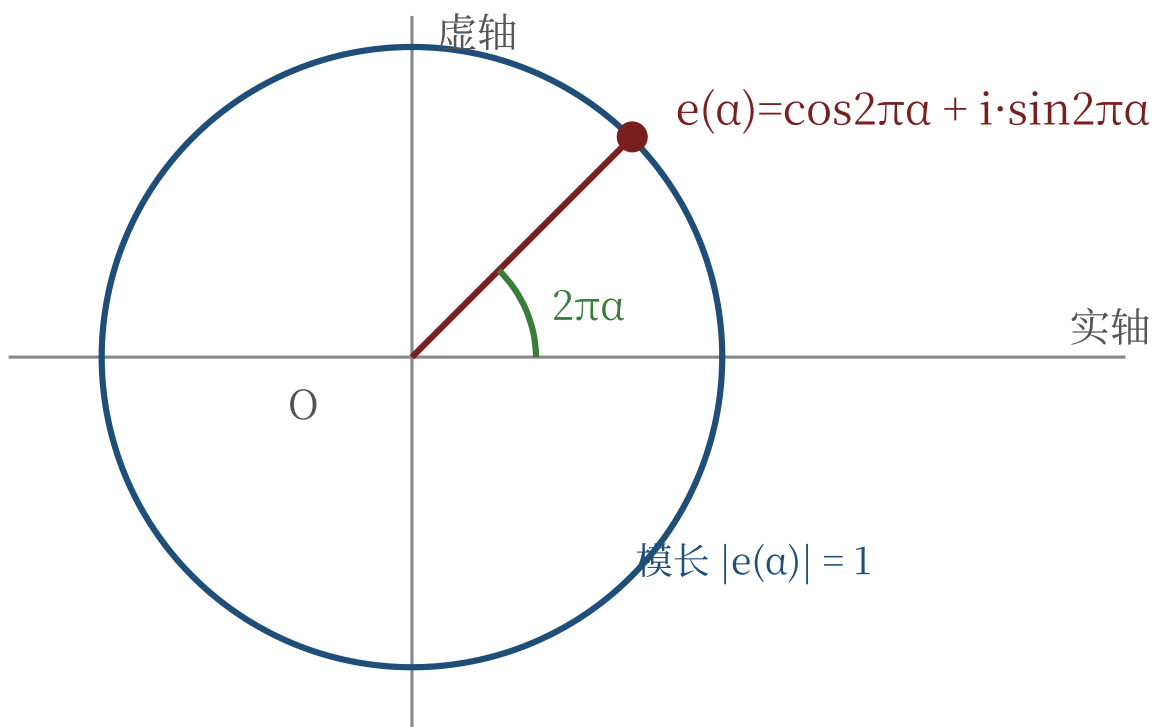
$$e^{i\theta} = \cos \theta + i \sin \theta,$$

所以

$$e(\alpha) = e^{2\pi i \alpha} = \cos(2\pi \alpha) + i \sin(2\pi \alpha).$$

它是一个模长为 1 的复数，落在复平面的单位圆上。当 α 增加 1，角度 $2\pi \alpha$ 增加 2π ，转回原处——所以 $e(\alpha)$ 只看 α 的小数部分，是个周期为 1 的函数。两条最常用的性质：

- $e(\alpha) e(\beta) = e(\alpha + \beta)$ （指数相加，对应角度相加）；
- $|e(\alpha)| = 1$ （模长恒为 1）。



$e(\alpha)$ 是单位圆上一个点： α 增大就沿圆逆时针匀速转，转满一圈对应 α 增加 1。整个圆法的“圆”指的就是这个单位圆。

定积分 $\int_0^1$ 与正交关系

$\int_0^1 g(\alpha) d\alpha$ 就是高中学的定积分（函数图象与横轴之间的“带符号面积”），这里被积函数取复值，把实部虚部分别积分即可。本章反复用到一条**正交关系**：对任意整数 m ,

$$\int_0^1 e(m\alpha) d\alpha = \begin{cases} 1, & m = 0, \\ 0, & m \neq 0. \end{cases}$$

为什么？当 $m = 0$ 时被积函数恒为 1，积分得 1；当 $m \neq 0$ 时 $e(m\alpha)$ 在 $[0, 1]$ 上正好转 $|m|$ 整圈，正负抵消，面积为 0。直接算：
 $\int_0^1 e^{2\pi i m \alpha} d\alpha = \left[\frac{e^{2\pi i m \alpha}}{2\pi i m} \right]_0^1 = \frac{e^{2\pi i m} - 1}{2\pi i m} = 0$ ，因为 $e^{2\pi i m} = 1$ 。这条关系是圆法的总开关：它能从一大堆 $e(\cdot)$ 之和里，精确“挑出”指数为 0 的那一项。

大 O 与 $\ll, \gg$ 记号

这是“略去常数、只看增长速度”的速记。

- $f = O(g)$ (读作" f 是大 O 的 g ") 意思是: 存在一个与变量无关的常数 $C > 0$, 使 $|f| \leq Cg$ 恒成立。即 f 的大小被 g 的某个倍数压住。
- $f \ll g$ 与 $f = O(g)$ 完全同义 (Vinogradov 记号)。
- $f \gg g$ 表示 $g \ll f$, 即 $f \geq cg$ (f 至少是 g 的某个正倍数)。
- 同时 $f \ll g$ 且 $f \gg g$, 就说 f 与 g 同阶。

例: $3n^2 + 5n = O(n^2)$, 因为 $3n^2 + 5n \leq 8n^2$ 。本章里这些常数 C 允许依赖 k (但不依赖 P, N 这些"趋于无穷"的量), 这一点很关键。符号 ε 表示"任意小的正数", P^ε 用来吸收像 $\log P$ 这样增长极慢的因子。

渐近 $\sim$ 、到最近整数的距离 $\|x\|$ 、整数部分 $[x]$

- $f \sim g$ (当 $X \rightarrow \infty$) 表示 $f/g \rightarrow 1$, 即两者比值趋于 1, "几乎相等"。
- $\|x\|$ 表示 x 到离它最近的整数的距离, 例如 $\|2.3\| = 0.3$, $\|2.8\| = 0.2$, 总有 $0 \leq \|x\| \leq \frac{1}{2}$ 。它度量" x 离整数有多近"。
- $[x]$ 是下取整 (不超过 x 的最大整数), 如 $[3.7] = 3$ 。

同余、互素 $(a, q) = 1$ 、欧拉函数 φ

- $a \equiv b \pmod{q}$ 表示 $a - b$ 能被 q 整除 (" a, b 除以 q 余数相同")。这是初中"被几整除"的精确写法。
- (a, q) 表示 a, q 的最大公约数; $(a, q) = 1$ 即两者互素 (没有大于 1 的公因子)。
- 欧拉函数 $\varphi(q)$ 表示 $1, 2, \dots, q$ 中与 q 互素的数的个数 (本章在"奇异级数"里间接用到)。

几个一会儿要登场的"角色"

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

生成函数 (指数和): 把 $1^k, 2^k, \dots, P^k$ 都"挂"到单位圆上。它的 s 次幂展开后, 指数恰好是各种 k 次幂之和, 这正是华林问题需要的。

$$S_{a,q} = \sum_{z=1}^q e(az^k/q)$$

一个**完整指数和**（高斯和的推广），只跟模 q 的算术有关，反映" k 次幂模 q 的分布"。

$$I(\beta) = \int_0^P e(\beta \xi^k) d\xi$$

奇异积分的雏形，是把 T 里的求和换成积分得到的连续版本。

$$\mathfrak{S}(M)$$

奇异级数：把所有 q 的 $S_{a,q}$ 贡献加起来，是一个反映"模任意数都无障碍"的正因子。

$$\mathfrak{M} \text{ (主弧)} / \mathfrak{m} \text{ (次弧)}$$

把区间 $[0, 1]$ 切成两部分：靠近"分母小的分数 a/q "的一小段段叫主弧，其余叫次弧。

先看圆法的总思路（务必理解）

设我们想数： N 写成 s 个 k 次幂之和 $x_1^k + \cdots + x_s^k = N$ （每个 $1 \leq x_j \leq P$ ）共有几种方法。把

$$T(\alpha)^s = \left(\sum_{x=1}^P e(\alpha x^k) \right)^s = \sum_{x_1} \cdots \sum_{x_s} e(\alpha(x_1^k + \cdots + x_s^k))$$

乘上 $e(-N\alpha)$ 再沿 $[0, 1]$ 积分。由上面的正交关系，只有 $x_1^k + \cdots + x_s^k = N$ 的那些项积出 1，其余积出 0。于是

$$\int_0^1 T(\alpha)^s e(-N\alpha) d\alpha = \#\{(x_1, \dots, x_s) : x_1^k + \cdots + x_s^k = N\}.$$

这就把"数解的个数"变成了"算一个积分"。剩下的全部工作，就是估这个积分——把 $[0, 1]$ 切成主弧（贡献主项，给出正的下界）和次弧（贡献误差，要证明它小）。本章就是这条路线的一次精彩演出。

第1段： $G(k)$ 的定义与最朴素的上下界

译文：数 $G(k)$ 被（Hardy 和 Littlewood）定义为具有如下性质的最小的 s 值：每个充分大的整数 N 都可以表示为 s 个正整数 k 次幂之和。由定理 4.1 和定理 5.1，我们已经知道 $G(k) \leq 2^k + 1$ 。从相反的方向看，由密度方面的考虑容易推出 $G(k) \geq k + 1$ ；事实上，满足 $[x_1^k + \dots + x_k^k \leq X, \quad 0$

这一段在讲什么：先把研究对象 $G(k)$ 定义清楚，再说它现成已知的两道"夹板"——上界 $2^k + 1$ 和下界 $k + 1$ （以及更精细的 $\Gamma(k)$ ）。

$G(k)$ 到底是什么

" s 个正整数 k 次幂之和"指的是形如 $x_1^k + x_2^k + \dots + x_s^k$ ($x_j \geq 1$) 的数。 $G(k)$ 定义为：使得所有足够大的 N 都能这样表示的最小个数 s 。注意两个关键词：

- "充分大的"——允许有限个小的例外数不能表示，只要求大的都行。这正是 $G(k)$ 与另一个量 $g(k)$ （要求所有正整数都能表示）的区别。 $g(k)$ 常被几个特殊小数"绑架"而偏大； $G(k)$ 才真正反映问题的本质难度。
- "最小的 s "——少于这个数就一定有大整数表示不出来。

上界 $G(k) \leq 2^k + 1$ 从哪来：这是前几章（定理 4.1、5.1）已经证过的结论，用的正是上面说的圆法：取 $s = 2^k + 1$ 个变量，能保证次弧误差被华的不等式压住、主弧给出正的主项，于是大整数都有表示。本章的目标，是当 k 很大时把这个上界从指数级的 2^k 大幅降到 $k \log k$ 级别。

下界 $G(k) \geq k + 1$ 的"密度"论证——把省略补全：原文说"容易看出"个数渐近于 γX 且 $\gamma < 1$ 。我们把它说透。

1 数有序组的个数。考虑所有满足 $x_1^k + \dots + x_k^k \leq X$ 且 $(0$

2 用体积（重积分）估格点数。当 X 很大时，格点个数近似等于区域 $\{(t_1, \dots, t_k) : t_1^k + \dots + t_k^k \leq X, \quad 0$

3 体积正比于 X 。作伸缩 $t_j = X^{1/k} u_j$ ，则约束变成 $u_1^k + \cdots + u_k^k \leq 1$ ，每个 t_j 提供一个 $X^{1/k}$ 因子， k 个变量共提供 $(X^{1/k})^k = X$ 。所以体积 $= \gamma X$ ，其中 γ 是单位区域 $\{u_1^k + \cdots \leq 1, u_1 \leq \cdots \leq u_k\}$ 的体积，一个只依赖 k 的固定正常数，且 $\gamma < 1$ 。

4 对比"目标数"的个数得出结论。于是不超过 X 、能写成 $\leq k$ 个 k 次幂之和的数，至多约 γX 个 ($\gamma < 1$)。但 $\leq X$ 的正整数有 X 个。既然 γX 必有正比例 (约 $(1 - \gamma)X$ 个) 的整数表示不成 k 个 k 次幂之和，而且这种数要多少有多少 (X 越大越多)。所以 $s = k$ 不够， $G(k) \geq k + 1$ 。

$\Gamma(k)$ 与"同余障碍"

有时候问题"卡"在模某个数上：比如模 8 时，任何完全平方数只能是 0, 1, 4，于是 7 个奇平方相加也凑不出某些余数，这就给出比"密度"更强的下界。 $\Gamma(k)$ (第 4 章定义) 正是把所有这类同余障碍综合起来得到的下界，故 $G(k) \geq \Gamma(k)$ 。直观上：哪怕"实数层面"能凑出，只要"模某个数"凑不出，整数表示就不存在。

第 2 段：Vinogradov 定理与它的历史地位

译文：当 k 较大时，对 $G(k)$ 存在更好的上界。1934 年 Vinogradov 证明了当 $k > k_0(\delta)$ 时 $G(k) < (6 + \delta)k \log k$ ，其中 δ 是任意小的正数。我们现在给出该证明的一个阐述 (主要依据 Heilbronn)。系数 6 后来被 Vinogradov 于 1947 年改进为 3，但证明较难。

这一段在讲什么：交代本章主定理的出处、数值以及在历史上的分量。

历史脉络 (为什么这是里程碑)

- 问题起点 (1770)：Edward Waring 猜测每个 k 都有一个固定的 $g(k)$ ，使所有正整数是 $g(k)$ 个 k 次幂之和 (如 $g(2) = 4$ ：四平方和定理)。Hilbert 在 1909 年证明了 $g(k)$ 的存在性，但给出的界极其粗糙。

- **圆法登场 (1920s)**: Hardy 与 Littlewood 发明圆法，引入了我们正在用的 $G(k)$ ，并得到 $G(k) \leq (k-2)2^{k-1} + 5$ 一类**指数级**上界——当 k 大时这非常弱。
- **Vinogradov 的突破 (1934)**: 他把上界从指数级 2^k 一举降到**多项式对数级** $k \log k$ ，即本章的 $G(k) < (6 + \delta)k \log k$ 。这是 20 世纪解析数论的标志性成果：指数和的"光滑化"与双线性方法从此成为主流武器。
- **后续**: 1947 年他自己把 6 改进到 3；如今已知 $G(k) \leq k(\log k + \log \log k + O(1))$ (Wooley 等)。本章选讲 6 的版本，因为它最能清晰展示方法的骨架。

读懂 $(6 + \delta)k \log k$ 与 $k > k_0(\delta)$

这里 $\log$ 是**自然对数** (以 e 为底)。式子说：系数可以无限逼近 6，代价是 k 要足够大—— $k_0(\delta)$ 是一个只依赖 δ 的门槛， δ 越小门槛越高。这是分析里典型的" ε - N 式"说法：结论对大 k 成立，把开头有限个小 k 排除在外。Heilbronn 是把 Vinogradov 较难读的原证整理清楚的人，本章正文沿用他的叙述。

第 3 段：为什么旧的主弧不够用，需要新工具

译文: 读者记得第 4 章把 α 的积分区间分为主弧和次弧，主弧由那些容许有理逼近 a/q ($q \leq P^\delta, |\alpha - a/q|$

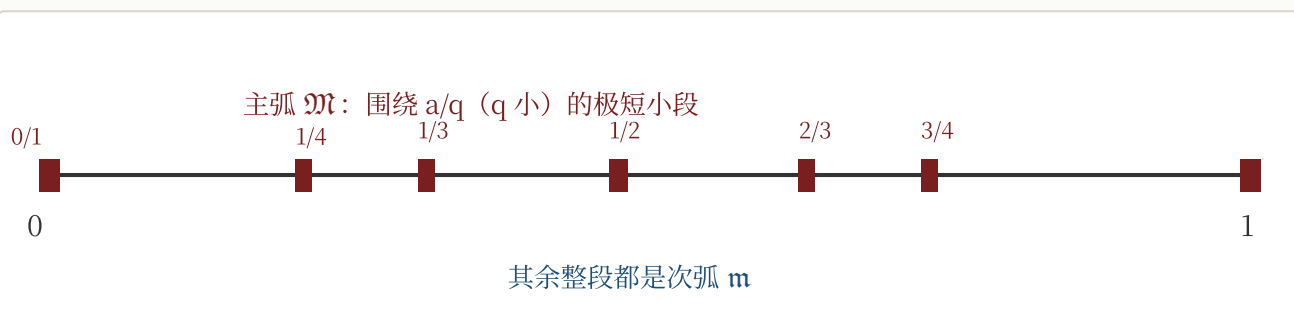
这一段在讲什么: 这是全章的"战略说明"。作者解释：以前用 $s = 2^k$ 个变量时，华的不等式很猛，主弧可以取得又少又短；但现在我们想用**少得多**的变量（只有 $4k$ 个 T ），次弧上没那么多"本钱"了，所以必须把主弧上对 $T(\alpha)$ 的逼近做得更精细。这就引出第一件新工具。

"节省 P^k "是什么意思

$T(\alpha)$ 有 P 项，每项模长 1，所以平凡上界 $|T(\alpha)| \leq P$ ，于是 $|T|^{2^k} \leq P^{2^k}$ ，积分平凡估计 $\leq P^{2^k}$ 。但华的不等式（引理 3.2）给出

$$\int_0^1 |T(\alpha)|^{2^k} d\alpha \ll P^{2^k - k + \varepsilon},$$

比平凡估计小了一个 P^k 因子——这就是"节省了几乎 P^k "。本质原因： $T(\alpha)$ 在大部分 α 上远小于 P ，只有在主弧附近才接近 P 。变量越多，这种节省越能压住次弧；变量少了，就得另想办法在主弧上把 T 算得更准。



主弧是围绕分母小的分数 a/q 的一些极窄区间（红条），合起来很短；剩下的几乎整个 $[0, 1]$ 都是次弧。主弧给主项，次弧给误差。

"用积分代替求和"——核心动机

$T(\alpha) = \sum_x e(\alpha x^k)$ 是离散求和，难算；而积分 $\int e(\alpha \xi^k) d\xi$ 是连续的，可以用换元、特殊函数算出干净的封闭形式。当 α 靠近 a/q 时，相邻项 $e(\alpha x^k)$ 变化很"平缓"，求和与积分几乎相等。**van der Corput 引理**就是把这个"几乎相等"精确化：在导数受控的条件下，求和等于积分加一个 $O(1)$ 的小误差。这正是我们需要的、比第 4 章粗糙办法精细得多的逼近。

引理 9.1 (van der Corput): 把求和精确换成积分

引理 9.1. (van der Corput) 设 $f(x)$ 是实函数, 在 $A \leq x \leq B$ 上二次可微, 且在此区间内

$$0 \leq f'(x) \leq \frac{1}{2}, \quad f''(x) \geq 0.$$

那么

$$\sum_{A \leq n \leq B} e(f(n)) = \int_A^B e(f(x)) dx + O(1).$$

先读懂条件与结论

- $f'(x) \in [0, \frac{1}{2}]$: 相位 f 增长很慢, 相邻整点处 $e(f(n))$ 转过的角度不超过半圈, 不会剧烈震荡——这是"求和 $\approx$ 积分"的关键。
- $f''(x) \geq 0$: f' 单调不减 (f 是凸的), 保证后面用单调性论证。
- 结论里 $O(1)$ 表示误差被一个绝对常数压住 (与 A, B, f 无关, 下面会算出 $< 2/\pi$)。也就是说, 无论区间多长, "和"与"积分"只差一个有界的量。

证. 第一步：化简到方便的情形。 只需对 A, B 为整数、 f 实数。既然差是实数, 等式两边都可以只取实部, 即把 $e(f(x))$ 换成 $\cos(2\pi f(x))$ 。

为什么能"只取实部" 记 $D = \sum' - \int$ (复数)。乘以 $e(c)$ 后 D 变成 $e(c)D$, 适当选 c 可使 $e(c)D$ 为实数 (任何复数乘以一个合适的单位复数都能转到实轴上)。对实数而言, "它有界"等价于"它的实部有界", 而实部对应把 $e(\cdot) = \cos + i \sin$ 换成 $\cos$ 。于是问题简化为只处理 $\cos$ 。

第二步：欧拉-麦克劳林一格——单格分部积分。 令锯齿函数 $\Psi(x) = x - [x] - \frac{1}{2}$ 。对任意整数 m 与可微函数 F ,

$$\int_m^{m+1} \Psi(x) F'(x) dx = \frac{1}{2} \{F(m+1) + F(m)\} - \int_m^{m+1} F(x) dx. \quad (*)$$

逐步验证 (\$ast\$):

1 在区间 $(m, m+1)$ 上 $[x] = m$, 故 $\Psi(x) = x - m - \frac{1}{2}$ 。

2 对 $\int_m^{m+1} (x - m - \frac{1}{2})F'(x)dx$ 用分部积分 ($u = x - m - \frac{1}{2}, dv = F'dx$):

$$= \left[(x - m - \frac{1}{2})F(x) \right]_m^{m+1} - \int_m^{m+1} F(x) dx.$$

3 边界项: 上端 $x = m+1$ 时 $x - m - \frac{1}{2} = \frac{1}{2}$, 下端 $x = m$ 时 $= -\frac{1}{2}$ 。
代入得 $\frac{1}{2}F(m+1) - (-\frac{1}{2})F(m) = \frac{1}{2}\{F(m+1) + F(m)\}$, 正是 (\$ast\$)。

第三步: 拼成梯形求和公式。把 (\$ast\$) 对 $m = A, A+1, \dots, B-1$ 求和。右边第一项 $\sum_{m=A}^{B-1} \frac{1}{2}\{F(m+1)+F(m)\}$ 是经典的**梯形和**: 每个内部整点 $F(n)$ (A

第四步: 把锯齿展成傅里叶级数。对任意非整数 x , 锯齿波有展开

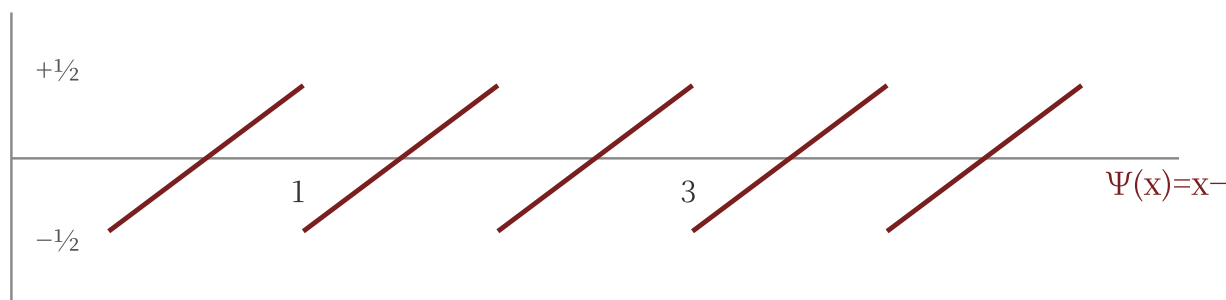
$$\Psi(x) = -\sum_{\nu=1}^{\infty} \frac{\sin 2\pi\nu x}{\pi\nu}.$$

这是 Ψ (周期 1 的奇函数) 的傅里叶正弦级数, 是标准结果。代入并交换求和与积分 (由级数**有界收敛**, 交换合法):

$$I = -\sum_{\nu=1}^{\infty} \frac{1}{\nu\pi} \int_A^B (\sin 2\pi\nu x) (\cos(2\pi f(x)))' dx.$$

锯齿函数 $\Psi(x) = x - [x] - \frac{1}{2}$ 是什么

$x - [x]$ 是 x 的小数部分，在 0 到 1 间锯齿状上升；减去 $\frac{1}{2}$ 把它居中得到 $[-\frac{1}{2}, \frac{1}{2})$ ，平均值为 0。它周期为 1，在每个整数处跳变。傅里叶级数把这种锯齿写成无穷个正弦波之和——这样就能把含 Ψ 的积分逐项处理。



锯齿波 Ψ ：周期 1，幅度 $\pm\frac{1}{2}$ ，整数处跳变；平均值为 0，故可展成纯正弦级数。

第五步：把积分整理成一个干净形状。注意 $(\cos(2\pi f))' = -2\pi f' \sin(2\pi f)$ ，代入上式，常数 -2π 与前面的 $-\frac{1}{\nu\pi}$ 合并出系数 $\frac{2}{\nu}$ ：

$$I = 2 \sum_{\nu=1}^{\infty} \frac{1}{\nu} \int_A^B (\sin 2\pi\nu x) (\sin 2\pi f(x)) f'(x) dx.$$

再用积化和差 $2 \sin A \sin B = \cos(A - B) - \cos(A + B)$ （这里 $A = 2\pi\nu x$, $B = 2\pi f$ ）：

$$I = \sum_{\nu=1}^{\infty} \frac{1}{\nu} \int_A^B f'(x) \left\{ \cos(2\pi(\nu x - f)) - \cos(2\pi(\nu x + f)) \right\} dx.$$

现在只要对每个 ν 、每个符号 $\pm$ ，证明单个积分小即可。

第六步：单个积分的估计——核心不等式。我们证

$$\left| \int_A^B f'(x) \cos(2\pi(\nu x \pm f)) dx \right| < \frac{1}{\pi(2\nu - 1)}. \quad (\dagger)$$

把被积函数改写：令 $\phi(x) = \sin(2\pi(\nu x \pm f))$ ，则 $\phi'(x) = 2\pi(\nu \pm f') \cos(2\pi(\nu x \pm f))$ 。于是

$$f' \cos(2\pi(\nu x \pm f)) = \frac{1}{2\pi} \cdot \frac{f'}{\nu \pm f'} \cdot \phi'(x),$$

积分变成 $\frac{1}{2\pi} \int_A^B \frac{f'}{\nu \pm f'} \phi' dx$ 。这是"单调函数 $\times$ 振荡导数"的标准形状，用**第二中值定理**处理。

1 振荡因子 ϕ' 的积分有界。 $\int_a^b \phi' dx = \phi(b) - \phi(a)$ ，而 $\phi = \sin(\cdots) \in [-1, 1]$ ，故任意上下限之间 $|\int \phi'| \leq 2$ 。

2 单调因子 $g = \frac{f'}{\nu \pm f'}$ 单调。求导： $g' = \frac{\nu f''}{(\nu \pm f')^2} \geq 0$ （因 $f'' \geq 0, \nu \geq 1$ ）。所以 g 关于 x 单调不减。

3 单调因子的最大值 $\leq \frac{1}{2\nu - 1}$ 。因为 $f' \in [0, \frac{1}{2}]$ ，把 g 看成 f' 的函数：
 $g = \frac{t}{\nu \pm t}$ ($t = f' \in [0, \frac{1}{2}]$) 关于 t 递增，最大在 $t = \frac{1}{2}$ 。取 +：
 $\frac{1/2}{\nu + 1/2} = \frac{1}{2\nu + 1}$ ；取 -： $\frac{1/2}{\nu - 1/2} = \frac{1}{2\nu - 1}$ 。两者都 $\leq \frac{1}{2\nu - 1}$ 。

4 合起来用**第二中值定理**。对单调的 g 与积分有界的 ϕ' ，有
 $|\int_A^B g \phi' dx| \leq \max |g| \cdot 2$ （第二中值定理把积分压到一个端点处的 g 值乘以一段 ϕ' 积分）。于是

$$\left| \frac{1}{2\pi} \int_A^B g \phi' dx \right| \leq \frac{1}{2\pi} \cdot \frac{1}{2\nu - 1} \cdot 2 = \frac{1}{\pi(2\nu - 1)},$$

即 ($\dagger$) 成立。

第七步：对 ν 求和收尾。 第 ν 项是两个 $\cos$ 积分之差 $\frac{1}{\nu} \int f' \{ \cos(2\pi(\nu x - f)) - \cos(2\pi(\nu x + f)) \} dx$ ，由 ($\dagger$) 每个积分的

绝对值都 $< \frac{1}{\pi(2\nu-1)}$ (其中 "+" 号那个由第六步还更小, $< \frac{1}{\pi(2\nu+1)}$)。按书中的写法逐项相加:

$$|I| < \frac{1}{\pi} \sum_{\nu=1}^{\infty} \frac{1}{\nu(2\nu-1)} < \frac{2}{\pi}.$$

为什么级数 < 2 : 首项 $\nu = 1$ 是 $\frac{1}{1 \cdot 1} = 1$, 其余 $\frac{1}{\nu(2\nu-1)} < \frac{1}{\nu(2\nu-2)} = \frac{1}{2\nu(\nu-1)}$ 可与收敛级数比较, 总和 $= 2 \ln 2 \approx 1.386 < 2$ 。于是 $|I| < \frac{2}{\pi}$, 是个绝对常数, 即 $I = O(1)$ 。引理 9.1 证毕。 ■

一句话总结引理 9.1 只要相位走得够慢 ($0 \leq f' \leq \frac{1}{2}$) 且凸 ($f'' \geq 0$), 离散的 $\sum e(f(n))$ 就等于连续的 $\int e(f(x))dx$, 误差不超过 $\frac{2}{\pi}$ 。这把"难算的和"变成"好算的积分"。

主弧 $\mathfrak{M}_{a,q}$ 的定义与生成函数 $T(\alpha)$

译文: 我们为本章定义主弧 $\mathfrak{M}_{a,q}$, 由满足

$$(a, q) = 1, \quad 1 \leq a \leq q, \quad q \leq P^{1/2}, \quad |q\alpha - a| < \frac{1}{2kP^{k-1}} \quad (9.1)$$

的区间组成。如第 2 章, 定义 $T(\alpha) = \sum_{x=1}^P e(\alpha x^k)$ 。

这一段在讲什么: 正式划定"主弧"——即 $[0, 1]$ 里靠近某个分母 $q \leq P^{1/2}$ 的既约分数 a/q 的那些极窄区间; 同时重申主角生成函数 $T(\alpha)$ 。

逐条读 (9.1)

$$(a, q) = 1, \quad 1 \leq a \leq q$$

a/q 是既约分数, 分子在 1 到 q 之间。这样每个有理点 a/q 只数一次。

$$q \leq P^{1/2}$$

只取分母不太大的分数作主弧中心。分母越小的分数， $T(\alpha)$ 在其附近越接近峰值 P 。

$$|q\alpha - a| < \frac{1}{2kP^{k-1}}$$

等价于 $|\alpha - \frac{a}{q}| < \frac{1}{2kqP^{k-1}}$ ，即 α 离中心 a/q 的距离极小（ P 大时窄得可怕）。这就是主弧的"半径"。

所有这些小区间的并集记作 $\mathfrak{M}$ （主弧全体）； $[0, 1]$ 中剩下的部分记作 $\mathfrak{m}$ （次弧）。

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

把 $x = 1, 2, \dots, P$ 的 k 次幂 x^k 当相位挂到单位圆上求和。当 α 是整数时所有项都等于 1， $T = P$ （峰值）；当 α 一般时各项方向杂乱、互相抵消， $|T|$ 远小于 P 。主弧正是 T 接近峰值、贡献主项之处。这里取上限 P ，是因为我们要表示的 $N \sim P^k$ ，每个底数最大约 $N^{1/k} \approx P$ 。

引理 9.2：主弧上 $T(\alpha)$ 的精确逼近

引理 9.2. 对 $\mathfrak{M}_{a,q}$ 中的 α ，有

$$T(\alpha) = q^{-1} S_{a,q} I(\beta) + O(q), \quad (9.2)$$

记号同第 4 章（ $\beta = \alpha - a/q$ ）。

这一段在讲什么：把主弧上的 $T(\alpha)$ 拆成两部分相乘：一个算术因子 $q^{-1} S_{a,q}$ （只跟 q 的同余结构有关）乘上一个分析因子 $I(\beta)$ （连续积分），再加一个不大的误差 $O(q)$ 。这正是圆法主弧分析的标准形态。

证. 第一步：按模 q 的余数分类求和。 令 $x = qy + z$ （ z 是余数， $1 \leq z \leq q$ ； y 是商）。把 $\alpha = \frac{a}{q} + \beta$ 代入相位：

$$\alpha x^k = \left(\frac{a}{q} + \beta\right)(qy + z)^k.$$

关键观察： $(qy + z)^k \equiv z^k \pmod{q}$ （二项式展开后除首项 z^k 外每项都含 q 因子），故 $\frac{a}{q}(qy + z)^k = \frac{az^k}{q} + (\text{整数})$ 。由 $e(\text{整数}) = 1$,

$$e(\alpha x^k) = e\left(\frac{az^k}{q}\right) e(\beta(qy + z)^k).$$

于是

$$T(\alpha) = \sum_{z=1}^q e\left(\frac{az^k}{q}\right) \sum_y e(\beta(qy + z)^k),$$

内和对满足 $\backslash(0$

第二步：验证内和满足 van der Corput 条件。 令 $f(y) = \beta(qy + z)^k$ 。则（设 $\beta > 0$ ）

$$f'(y) = k\beta q(qy + z)^{k-1}.$$

因为 $qy + z \leq P$, $(qy + z)^{k-1} \leq P^{k-1}$; 又由 (9.1), $|\beta| < \frac{1}{2kqP^{k-1}}$ 。代入:

$\backslash [f'(y)]$ 恰好满足引理 9.1 的两个条件 $0 \leq f' \leq \frac{1}{2}$, $f'' \geq 0$ 。（若 $\beta < 0$, 对复共轭和同样适用, 因为 $\overline{e(f)} = e(-f)$, $-f$ 满足条件。）

第三步：用引理 9.1 把内和换成积分。

$$\sum_y e(\beta(qy + z)^k) = \int e(\beta(q\eta + z)^k) d\eta + O(1).$$

对 积 分 作 换 元 $\xi = q\eta + z$ ($d\xi = q d\eta$) :
 $\int e(\beta(q\eta + z)^k) d\eta = \frac{1}{q} \int e(\beta\xi^k) d\xi = \frac{1}{q} I(\beta)$, 其中 $I(\beta) = \int_0^P e(\beta\xi^k) d\xi$
 (积分上下限的小偏差并入误差)。

第四步：合并。代回外和：

$$T(\alpha) = \sum_{z=1}^q e\left(\frac{az^k}{q}\right) \left[\frac{1}{q} I(\beta) + O(1) \right] = \frac{1}{q} I(\beta) \underbrace{\sum_{z=1}^q e\left(\frac{az^k}{q}\right)}_{=S_{a,q}} + \underbrace{O(q)}_{q \uparrow O(1)}.$$

即 $T(\alpha) = q^{-1}S_{a,q}I(\beta) + O(q)$, 得 (9.2)。 ■

注. (9.1) 中条件 $q \leq P^{1/2}$ 在证明中并未用到——但当然, 若允许 q 接近 P 那么大, 结果就失去价值。

解读这条注: 证明里真正用到的只是 $|\beta|$ 的上界 (让 $f' \leq \frac{1}{2}$)。 $q \leq P^{1/2}$ 是为了让误差 $O(q)$ 相对主项足够小 (下条引理 9.3 会精确利用)。如果 q 大到接近 P , 误差 $O(q)$ 就可能淹没主项 $q^{-1}S_{a,q}I(\beta)$, 逼近失去意义。这是"为什么这样取参数"的典型例子。

译文 (补充逼近): 还有更有效的逼近: 若 $q \leq P^{1-\delta}$ 且 $\backslash(|q\backslash\alpha-a|$

解读: 这是一个更强但更难证的版本 (来自 Davenport 的论文), 本章主线不用它, 只是顺带提及。它把误差从 $O(q)$ 改进到 $O(q^{3/4+\varepsilon})$, 而且这个 $3/4$ 与 k 无关——这很反直觉, 因为 k 越大问题通常越难。作者点出它, 是想让读者知道"主弧逼近还能更精细", 但为保持证明简洁, 本章用引理 9.2 的较弱版本就够了。这体现了一种取舍: 够用即可, 不追求最优。

引理 9.3: 主弧积分的下界 (带 M 的范围)

引理 9.3. 设 $s \geq 4k$ 。那么, 对

$$\frac{1}{5}P^k \leq M \leq P^k, \quad (9.3)$$

有

$$\int_{\mathfrak{M}} T(\alpha)^s e(-M\alpha) d\alpha \gg P^{s-k}, \quad (9.4)$$

其中 $\mathfrak{M}$ 是主弧 $\mathfrak{M}_{a,q}$ 的全体。

注. 我们想对一个 M 值范围（而非单个数）得到该结果，理由稍后显现：它将省去我们在主弧上对一个相当复杂的指数和作逼近的麻烦。

这一段在讲什么：引理 9.3 说，只要变量个数 $s \geq 4k$ ，主弧上的核心积分就有一个正的下界 $\gg P^{s-k}$ ，而且对一整段 M 都成立。这个"主项确实是正的、且足够大"是整个圆法成功的命脉——它保证表示数最终为正。"对一个范围的 M "这个细节，是为了后面把 $u_1, u_2, y^k v$ 这些变动的量塞进 M 里（见主要思想 (9.5)）。

证. 第一步：把 (9.2) 升到 s 次幂，先备好两块零件的大小。由引理 6.4，算术因子满足

$$q^{-1}|S_{a,q}| \ll q^{-1/k};$$

分析因子满足

$$I(\beta) \ll \min(P, |\beta|^{-1/k}).$$

解释这两条：

1 $I(\beta) \ll P$ 是平凡的： $|I(\beta)| = \left| \int_0^P e(\beta \xi^k) d\xi \right| \leq \int_0^P 1 d\xi = P$ 。

2 $I(\beta) \ll |\beta|^{-1/k}$ ：作换元 $\eta = |\beta| \xi^k$ （则 $\xi = (\eta/|\beta|)^{1/k}$ ，
 $d\xi = \frac{1}{k} |\beta|^{-1/k} \eta^{-1+1/k} d\eta$ ），得

$$I(\beta) = \frac{1}{k} |\beta|^{-1/k} \int_0^{P^k |\beta|} e(\pm \eta) \eta^{-1+1/k} d\eta.$$

最后那个积分对一切上限都有界（被积函数在 0 附近可积，且振荡使大 η 部分收敛），故 $I(\beta) \ll |\beta|^{-1/k}$ 。两者取小者即 $\min(P, |\beta|^{-1/k})$ 。

所以 (9.2) 主项的模 $\ll q^{-1/k} \min(P, |\beta|^{-1/k})$ 。

第二步：误差 $O(q)$ 不超过主项。要证 $q \ll q^{-1/k} \min(P, |\beta|^{-1/k})$ ，即 $q^{1+1/k}$ 同时 $\backslash (q^{1+1/k})$

- $\backslash (q^{1+1/k})$

- $q^{1+1/k} < |\beta|^{-1/k}$: 由 (9.1), $|\beta| < \frac{1}{2kqP^{k-1}}$, 故

$$|\beta|^{-1/k} > (2kqP^{k-1})^{1/k} \geq q^{1/k} P^{(k-1)/k}. \text{ 又 } q \leq P^{1/2} \text{ 而 } (k-1)/k \geq 1/2,$$

可验 $\backslash (q^{1+1/k})$ 所以可写

$$T(\alpha)^s = (q^{-1} S_{a,q} I(\beta))^s + O\left\{q \cdot q^{-(s-1)/k} (\min(P, |\beta|^{-1/k}))^{s-1}\right\}.$$

为什么是这个误差：设主项 $\sim M_0$ ，误差 $\sim q \leq |M_0|$ ，则

$$(M_0 + E)^s = M_0^s + O(E M_0^{s-1}), \text{ 代入}$$

$$E = q, M_0^{s-1} \sim (q^{-1/k} \min)^{s-1} = q^{-(s-1)/k} \min^{s-1}.$$

第三步：误差项积分并对 a, q 求和——确认它是低阶。对 β 积分（范围可放大到 $(-\infty, \infty)$ ），用 $\int (\min(P, |\beta|^{-1/k}))^{s-1} d\beta \ll P^{s-1-k}$ ，得每个 $\mathfrak{M}_{a,q}$ 上误差 $\ll q \cdot q^{-(s-1)/k} P^{s-1-k} = q^{1-(s-1)/k} P^{s-1-k}$ 。再对 a （至多 q 个）与 $q \leq P^{1/2}$ 求和：

$$\ll P^{s-1-k} \sum_q q \cdot q^{1-(s-1)/k} = P^{s-1-k} \sum_q q^{2-(s-1)/k} \ll P^{s-k-1},$$

级数收敛因为指数 $2 - \frac{s-1}{k} < -1$ ，即 $s-1 > 3k$ ，由 $s \geq 4k$ 成立。结论：误差是 P^{s-k-1} ，比目标 P^{s-k} 低一个 P 因子。

第四步：主项的贡献。主项对 (9.4) 的贡献为

$$\sum_q \sum_a (q^{-1} S_{a,q})^s e(-Ma/q) \int I^s(\beta) e(-M\beta) d\beta.$$

把 β 积分扩展到 $(-\infty, \infty)$ ，所添尾部用 $|I| \ll |\beta|^{-1/k}$ 估计：

$$\ll \sum_q q q^{-s/k} \int_{(2kq)^{-1} P^{1-k}}^{\infty} \beta^{-s/k} d\beta \ll \sum_q q^{1-s/k} q^{s/k-1} P^{(k-1)(s/k-1)} \ll P^{s-k-s}$$

(用了 $\int_c^\infty \beta^{-s/k} d\beta \sim c^{1-s/k}$, $c = (2kq)^{-1}P^{1-k}$, 并对 $P^{1/2}$ 个 q 求和; 指数 $-s/k + 3/2 \leq -4 + 1.5 < -1$ 。) 于是尾部也是低阶的。

第五步：算干净的核心积分 $\int I^s e(-M\beta) d\beta$ 。先作变量替换把 I 标准化：令 $I(\beta) = Pk^{-1}I_1(\beta P^k)$, 其中 $I_1(\gamma) = \int_0^1 e(\gamma\eta)\eta^{-1+1/k} d\eta$ 。验证：在 $I(\beta) = \int_0^P e(\beta\xi^k) d\xi$ 中令 $\eta = (\xi/P)^k$ (即 $\xi = P\eta^{1/k}$, $d\xi = \frac{P}{k}\eta^{-1+1/k} d\eta$), 则 $\beta\xi^k = \beta P^k \eta$,

$$I(\beta) = \frac{P}{k} \int_0^1 e(\beta P^k \eta) \eta^{-1+1/k} d\eta = Pk^{-1} I_1(\beta P^k).$$

再令 $\beta = P^{-k}\gamma$ ($d\beta = P^{-k}d\gamma$):

$$\int_{-\infty}^{\infty} I^s(\beta) e(-M\beta) d\beta = P^{s-k} k^{-s} \int_{-\infty}^{\infty} I_1^s(\gamma) e(-\theta\gamma) d\gamma, \quad \theta = \frac{M}{P^k} \in [\frac{1}{5}, 1]$$

第六步：用傅里叶积分定理算出封闭形式。如定理 4.1 的证明,

$$\int_{-\infty}^{\infty} I_1^s(\gamma) e(-\theta\gamma) d\gamma = \int_0^1 \cdots \int_0^1 \{\zeta_1 \cdots \zeta_{s-1} (\theta - \zeta_1 - \cdots - \zeta_{s-1})\}^{-1+1/k} d\zeta_1$$

积分区域是 $\zeta_1 + \cdots + \zeta_{s-1} < \theta$ 的单纯形。这是一个 Beta/Dirichlet 型积分, 算得

$$\int_{-\infty}^{\infty} I_1^s(\gamma) e(-\theta\gamma) d\gamma = \theta^{s/k-1} \frac{\Gamma(1/k)^s}{\Gamma(s/k)}.$$

因 $\theta \geq \frac{1}{5}$, 这是一个正的、与 P 无关的常数 (含 Γ 函数值), 故

$$\int_{-\infty}^{\infty} I^s(\beta) e(-M\beta) d\beta \gg P^{s-k}.$$

这里的 Γ 是伽马函数 (别和 $\Gamma(k)$ 同名混淆)

$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$ 是阶乘的连续推广 ($\Gamma(n) = (n-1)!$)。上式的 $\Gamma(1/k)^s / \Gamma(s/k)$ 就是那个"奇异积分"的精确值, 是个固定正数。它和第 1 段里"同余障碍"的 $\Gamma(k)$ 毫无关系, 只是恰好都用了希腊字母 Γ 。

第七步：奇异级数给出正的算术下界。剩下要给

$$\sum_{q \leq P^{1/2}} \sum_{\substack{a=1 \\ (a,q)=1}}^q (q^{-1} S_{a,q})^s e(-Ma/q)$$

一个正下界。把它延拓到 $q = \infty$ ，所添尾部由 P 的负幂界定（引理 6.4，因 $s \geq 4k > 2k + 1$ 保证级数收敛）。延拓后它就是奇异级数 $\mathfrak{S}(M)$ ，由定理 6.1 它有一个不依赖 M 的正下界。把第五、六、七步合起来，主项 $\gg P^{s-k}$ ；与第三、四步的误差 $\ll P^{s-k-1}$ 相比占绝对优势。故 (9.4) 成立。引理 9.3 证毕。 ■

为什么"对一个范围的 M "如此重要 后面 (9.5) 里 N 被拆成 " $4k$ 个 x_j^k " 加 " $u_1 + u_2 + y^k v$ "。对每一组 (u_1, u_2, y, v) ，前 $4k$ 个幂要凑的目标其实是 $M = N - u_1 - u_2 - y^k v$ ，它随这些变量变化。引理 9.3 对整段 $[\frac{1}{5}P^k, P^k]$ 的 M 一律给出 $\gg P^{s-k}$ ，于是我们不必为每个 M 单独估计，直接套用即可——这正是"省去对复杂指数和逐一逼近的麻烦"。

证明的主要思想：表示 (9.5)

译文：现在来到证明的主要思想：考虑大数 N 的如下表示

$$N = x_1^k + \cdots + x_{4k}^k + u_1 + u_2 + y^k v, \quad (9.5)$$

其中 (i) $1 \leq x_j \leq P$ ；(ii) u_1, u_2 遍历所有小于 $\frac{1}{4}P^k$ 且可表示为 ℓ 个正整数 k 次幂之和的不同的数；(iii) $1 \leq y \leq P^{1/2k}$ ；(iv) v 遍历小于 $\frac{1}{4}P^{k-1/2}$ 且可表示为 ℓ 个 k 次幂之和的不同的数。这样我们把 N 表示为 $4k + 3\ell$ 个 k 次幂之和。取 $P = [N^{1/k}] + 1$ ，则 $\lfloor \frac{1}{5}P^k \rfloor$

这一段在讲什么：这是全章的战略核心。直接用 s 个变量 $x_1^k + \cdots + x_s^k = N$ 需要 s 很大才能让圆法奏效。Vinogradov 的妙招是：只用 $4k$ 个"自由幂" x_j^k （由引理 9.3 掌控），其余的"凑数"任务交给三个"打包好的零件" $u_1, u_2, y^k v$ ——它们各自已经是 ℓ 个

k 次幂之和。这样总幂数是 $4k + 3\ell$ ，只要 ℓ 取成 $\sim 2k \log 3k$ ，就得到 $k \log k$ 量级的上界。

逐项理解 (9.5) 的四类零件

$x_1^k + \cdots + x_{4k}^k$ ($4k$ 个自由幂)

对应生成函数 $T(\alpha)^{4k}$ ，由引理 9.3 ($s = 4k$) 保证主弧贡献为正。这是"主力部队"。

u_1, u_2 (两个"打包数"，对应 $R(\alpha)$)

每个 u 本身是 ℓ 个 k 次幂之和，且 $< \frac{1}{4}P^k$ 。"遍历不同的数"意味着我们只关心能凑出多少不同的 u ，个数越多，表示就越容易出现。

$y^k v$ (一个"放大的打包数"，对应 $S(\alpha)$)

v 是 ℓ 个 k 次幂之和，乘以 y^k 后 $y^k v = \sum (y w_i)^k$ 仍是 ℓ 个 k 次幂之和。引入 y 这个额外乘子，是为了在次弧上获得一个额外的"双线性"和"节省" (见引理 9.5)。

总幂数： $4k$ (来自 x_j) + ℓ (u_1) + ℓ (u_2) + ℓ ($y^k v$) = $4k + 3\ell$ 。所以一旦证明这种表示对大 N 必存在，就得到 $G(k) \leq 4k + 3\ell$ 。

$$\boxed{\begin{array}{c} x_1^k + \cdots + x_{4k}^k \\ 4k \text{ 个自由幂} \rightarrow T(\alpha)^{4k} \end{array}} \quad \boxed{\begin{array}{c} u_1 + u_2 \\ \text{各 } \ell \text{ 个幂} \rightarrow R(\alpha)^2 \end{array}} \quad \boxed{\begin{array}{c} y^k \cdot v \\ \ell \text{ 个幂} \rightarrow S(\alpha) \end{array}} = N$$

总幂数 = $4k + \ell + \ell + \ell = 4k + 3\ell$ ，故 $G(k) \leq 4k + 3\ell$ 。

取 $\ell \approx 2k \cdot \log(3k)$ ，即得 $G(k) < 4k + 6k \cdot \log(3k) + 3$ 。

(9.5) 的分块结构：每块对应一个生成函数 (T, R, S) ，积分时三者相乘。把"凑数"任务外包给 u, v 这些预制零件，是把变量数从 2^k 降到 $O(k \log k)$ 的关键。

为什么取 $P = \lceil N^{1/k} \rceil + 1$ ，以及 (9.6) 的完整验证：

1 这样取保证 $P^k > N$ 。由 $[N^{1/k}] \leq N^{1/k} < [N^{1/k}] + 1 = P$ ，两边 k 次方得 $P^k > N$ ，即 $(N - u_1 - u_2 - y^k v)$

2 三个打包数的总和 $< \frac{3}{4}P^k$ 。由条件： $u_1 < \frac{1}{4}P^k$ ， $u_2 < \frac{1}{4}P^k$ ；而 $y \leq P^{1/2k} \Rightarrow y^k \leq P^{1/2}$ ， $v < \frac{1}{4}P^{k-1/2}$ ，故 $(y^k v)$

3 下界： $N - u_1 - u_2 - y^k v > N - \frac{3}{4}P^k$ 。又由取法 $N \geq (P - 1)^k$ （因 $[N^{1/k}] = P - 1 \leq N^{1/k}$ ）。当 N （从而 P ）很大时，
 $(P - 1)^k = P^k(1 - \frac{1}{P})^k \rightarrow P^k$ ，故 $(P - 1)^k > 0.95P^k$ 。于是

$$N - u_1 - u_2 - y^k v > 0.95P^k - \frac{3}{4}P^k = 0.2P^k = \frac{1}{5}P^k.$$

(9.6) 下界成立。

4 结论。 $\frac{1}{5}P^k$

"以后必须用 k 来选取 ℓ "的含义： ℓ 是每个打包数里用的幂数，是我们手里的自由参数。 ℓ 越大，打包数能凑出的不同值越多（表示越容易存在），但总幂数 $4k + 3\ell$ 也越大（上界越差）。后面会精确地把 ℓ 取到刚好够用的最小值 $\sim 2k \log 3k$ ，这是一次典型的"取舍优化"。

引理 9.4 (Hardy–Littlewood)：打包数能凑出多少个

引理 9.4. (Hardy 和 Littlewood) 设 $U_\ell(X)$ 表示直到 X 为止、可表示为 ℓ 个正整数 k 次幂之和的不同的数的个数。那么，只要 $X > X_0(k, \ell)$ ，就有

$$U_\ell(X) \gg X^{1-\lambda^\ell}, \quad \lambda = 1 - \frac{1}{k}. \quad (9.7)$$

这一段在讲什么：这条引理量化了"打包数到底有多丰富"——不超过 X 的、能写成 ℓ 个 k 次幂之和的不同数，至少有 $X^{1-\lambda^\ell}$ 个。注意 $\lambda = 1 - \frac{1}{k} \in (0, 1)$ ，故 λ^ℓ 随 ℓ 增大迅速趋于 0，指数 $1 - \lambda^\ell$ 趋于 1——意思是"用足够多的幂，几乎每个数都能凑出"。

$\lambda = 1 - \frac{1}{k}$ 与 λ^ℓ 的直觉

每加一个 k 次幂，能凑出的数的"维度"就以因子 $\lambda = 1 - \frac{1}{k}$ 的方式逼近满额。 $\ell = 1$ 时只有完全 k 次幂，稀疏得很（指数 $1 - \lambda = \frac{1}{k}$ 很小）； ℓ 一大， $\lambda^\ell = (1 - \frac{1}{k})^\ell$ 指数式衰减，指数 $1 - \lambda^\ell$ 飞快逼近 1。例如要让 $\lambda^\ell \approx \frac{1}{Ck^2}$ ，取 $\ell \approx Ck \log k$ 即可（后面正是这么选）。

证. 对 ℓ 用数学归纳法。

奠基 $\ell = 1$ ：能写成"一个 k 次幂"且 $\leq X$ 的数就是 $1^k, 2^k, \dots$ ，共 $[X^{1/k}]$ 个， $\gg X^{1/k} = X^{1-\lambda}$ （因 $1 - \lambda = \frac{1}{k}$ ）。成立。

归纳步：设结论对 $\ell - 1$ 成立，证它对 ℓ 成立。构造形如 $x^k + z$ 的数，其中 $x \leq (\frac{1}{4}X)^{1/k}$

1 这些数两两不同。反设 $x_1^k + z_1 = x_2^k + z_2$ 且 $x_1 > x_2$ 。则一方面，因 $x_1 \geq x_2 + 1$ ，

$$x_1^k - x_2^k \geq (x_2 + 1)^k - x_2^k > kx_2^{k-1} > k\left(\frac{1}{4}X\right)^{(k-1)/k} = k\left(\frac{1}{4}X\right)^{1-1/k} ;$$

（最后一步： $k\left(\frac{1}{4}\right)^{1-1/k} = \frac{k}{4} \cdot 4^{1/k} \geq \frac{1}{2}$ 对 $k \geq 2$ 成立，例如 $k = 2$ 时 $= 1$ 。）

2 另一方面 $z_2 - z_1$ 矛盾。故所有 $x^k + z$ 互不相同。

3 计数。 x 的取值个数 $\gg X^{1/k}$ （区间 $(\left(\frac{1}{4}X\right)^{1/k}, \left(\frac{1}{2}X\right)^{1/k})$ 长度正比于 $X^{1/k}$ ）；对每个 x ， z 的取值个数为 $U_{\ell-1}\left(\frac{1}{2}X^{1-1/k}\right)$ 。因各 $x^k + z$ 互不相同，乘起来：

$$U_\ell(X) \gg X^{1/k} U_{\ell-1}\left(\frac{1}{2}X^{1-1/k}\right).$$

4 代入归纳假设。 $U_{\ell-1}(Y) \gg Y^{1-\lambda^{\ell-1}}$ ，取 $Y = \frac{1}{2}X^{1-1/k}$ ：

$$U_\ell(X) \gg X^{1/k} \cdot X^{(1-1/k)(1-\lambda^{\ell-1})} = X^{\frac{1}{k} + \lambda(1-\lambda^{\ell-1})} = X^{\frac{1}{k} + \lambda - \lambda^\ell}.$$

而 $\frac{1}{k} + \lambda = \frac{1}{k} + (1 - \frac{1}{k}) = 1$ ，故指数 $= 1 - \lambda^\ell$ ，得 $U_\ell(X) \gg X^{1-\lambda^\ell}$ 。
归纳完成。 ■

大间隔 x^k (相邻差 $> \frac{1}{2}X^{1-1/k}$)



小宽度 $z < \frac{1}{2}X^{1-1/k}$ ($\ell-1$ 个幂之和)



$x^k + z$ 落在各自小段里，互不重叠

0

X

归纳构造的几何图景：不同的 x^k 相隔很远 ($> \frac{1}{2}X^{1-1/k}$)，而 z 的"摆动幅度"很小 ($< \frac{1}{2}X^{1-1/k}$)，所以不同 (x, z) 给出的 $x^k + z$ 不会撞车。个数相乘即得递推。

注. 对一般 k ，没有比 (9.7) 实质更好的结果，任何真正改进都有意义。对小 k 有更好结果 (见 Davenport 的论文)。

解读：(9.7) 是这套方法里相对"粗"的一环，至今仍是瓶颈之一。改进它就能改进 $G(k)$ 的上界——这也解释了为什么后来人们能把系数从 6 降到 3 再继续降：很大程度靠把这类计数与指数和估计做得更精细。

引理 9.4 的推论：把计数翻译成积分估计 $R(\alpha)$

推论. 设

$$R(\alpha) = \sum_{u < \frac{1}{4}P^k} e(\alpha u), \quad (9.8)$$

其中 u 遍历可表示为 ℓ 个 k 次幂之和的不同的数。那么

$$\int_0^1 |R(\alpha)|^2 d\alpha = R(0) \ll P^{-k(1-\lambda^\ell)} R^2(0). \quad (9.9)$$

这一段在讲什么：把"打包数有多少个"这个计数事实，翻译成圆法需要的积分语言。 $R(\alpha)$ 是打包数 u 的生成函数； $\int_0^1 |R|^2$ 恰好等于打包数的个数 $R(0)$ ，而引理 9.4 又告诉我们这个个数很大，于是 $\int |R|^2$ 相对 $R(0)^2$ 很小——这正是次弧估计要用的"节省"。

证.

1 $\int_0^1 |R|^2 d\alpha = R(0)$ 。展开
 $|R(\alpha)|^2 = R(\alpha)\overline{R(\alpha)} = \sum_u \sum_{u'} e(\alpha(u - u'))$ 。逐项积分，用正交关系 $\int_0^1 e(\alpha(u - u')) d\alpha = [u = u']$ ：只有 $u = u'$ 的对角项存活，每项积出 1，共有" u 的个数"项。故积分 = $\#\{u\} = R(0)$ （因 $R(0) = \sum_u e(0) = \sum_u 1$ 就是项数）。这对任意一组不同整数的指数和都成立。

2 $R(0) \gg P^{k(1-\lambda^\ell)}$ 。 $R(0) = U_\ell(\frac{1}{4}P^k)$ ，由引理 9.4，
 $\gg (\frac{1}{4}P^k)^{1-\lambda^\ell} \gg P^{k(1-\lambda^\ell)}$ 。

3 合并。把 $\int |R|^2 = R(0)$ 写成 $\frac{R(0)^2}{R(0)}$ ，再用第 2 步的
 $\frac{1}{R(0)} \ll P^{-k(1-\lambda^\ell)}$ ：

$$\int_0^1 |R|^2 d\alpha = R(0) = \frac{R^2(0)}{R(0)} \ll P^{-k(1-\lambda^\ell)} R^2(0).$$

得 (9.9)。

■

注. 用 $R(0)$ 表示项数很方便。平凡估计是 $R^2(0)$ ，与之相比我们在 P 的指数上节省了 $k(1 - \lambda^\ell)$ 。我们最终选 ℓ 使 λ^ℓ (即 $(1 - 1/k)^\ell$) 约为 $1/Ck^2$ ，节省约为 $k - 1/Ck$ 。当 α 在次弧 $\mathfrak{m}$ 时，还需多节省一些 (比 $1/Ck$ 更多)，这由对应于 $y^k v$ 的指数和的估计来实现。该估计依赖下面这条非常一般的引理。

把这条关键的"注"讲透：

1 平凡估计是什么。对任意 $R(\alpha)$ ， $|R(\alpha)| \leq R(0)$ (项数)，故 $\int_0^1 |R|^2 \leq R(0)^2$ 。这是"什么都不用就有"的上界。

2 我们实际省了多少。(9.9) 给出 $\int |R|^2 \ll P^{-k(1-\lambda^\ell)} R^2(0)$ ，比平凡估计小了 $P^{k(1-\lambda^\ell)}$ 倍，即在 P 的指数上省了 $k(1 - \lambda^\ell)$ 。这来自"打包数很多、很密"，所以 $R(\alpha)$ 在大部分 α 上不大。

3 为什么把 λ^ℓ 调到约 $1/Ck^2$ 。此时节省量 $k(1 - \lambda^\ell) \approx k(1 - \frac{1}{Ck^2}) = k - \frac{1}{Ck}$ ，即"几乎省满 k ，只差一点点 $\frac{1}{Ck}$ "。把 $(1 - \frac{1}{k})^\ell \approx \frac{1}{Ck^2}$ 取对数解出 $\ell \approx Ck \log k$ 量级——这正是 $\ell \sim 2k \log 3k$ 的来历。

4 还差的那一点由谁补。次弧上仅靠 R 还差一口气 (差 $\frac{1}{Ck}$)，这缺口由第三个零件 $y^k v$ 的生成函数 $S(\alpha)$ 的额外节省补上。 S 的估计就是下面 Vinogradov 引理 9.5 的用武之地。

引理 9.5 (Vinogradov): 双线性 and 的威力

引理 9.5. (Vinogradov) 设 x 遍历含于长度 X 区间内的 X_0 个不同整数, y 遍历含于长度 Y 区间内的 Y_0 个不同整数。设 $\alpha = a/q + O(q^{-2})$, 其中 $(a, q) = 1, q > 1$ 。那么

$$\left| \sum_x \sum_y e(\alpha xy) \right|^2 \ll X_0 Y_0 \frac{\log q}{q} (q + X)(q + Y). \quad (9.10)$$

这一段在讲什么: 这是 Vinogradov 方法的"心脏"。它处理的是**双线性**和 $\sum_x \sum_y e(\alpha xy)$ ——相位 αxy 是两个变量的**乘积**。关键在于: 只要 α 能被一个**中等大小**的分母 q 逼近, 这个和就比平凡估计 $X_0 Y_0$ 小很多。这种"乘积型相位"在 $y^k v$ (y^k 与 v 相乘) 里天然出现, 正好能用。

为什么"双线性"是好事

单变量指数和 $\sum_x e(\alpha x^k)$ 难估计, 因为相位是高次的。但 $\sum_x \sum_y e(\alpha xy)$ 的相位对每个变量都是一次的——固定 x 后对 y 求和是等比级数, 能直接算! Vinogradov 的洞见是: 很多高次和可以拆成或比较成这种双线性形状, 从而借用等比级数的好性质。这一原理"在 Vinogradov 的大部分工作中起重要作用"。

证. 记该和为 S 。

1 柯西-施瓦茨不等式登场。 把 x 求和看成 $\sum_x 1 \cdot (\text{内和})$, 用柯西-施瓦茨 $|\sum a_x b_x|^2 \leq (\sum |a_x|^2)(\sum |b_x|^2)$:

$$|S|^2 \leq \left(\sum_x 1 \right) \left(\sum_x \left| \sum_y e(\alpha xy) \right|^2 \right) = X_0 \sum_x \left| \sum_y e(\alpha xy) \right|^2.$$

这一步的**目的**: 把"对 x 求和"的复杂性转移成一个平方, 从而能展开内和。

- 2 展开内和并放大 x 的范围。 $|\sum_y e(\alpha xy)|^2 = \sum_y \sum_{y'} e(\alpha x(y - y'))$ 。
把外层 x 的范围从"原来那 X_0 个数"放大到"包含它们的整个长度 X 区间内的所有整数" (项非负, 放大只会变大):

$$|S|^2 \leq X_0 \sum_{x=x_1}^{x_1+X} \sum_y \sum_{y'} e(\alpha x(y - y')).$$

- 3 先对 x 求和 (等比级数)。固定 $y - y' = t$, $\sum_x e(\alpha xt)$ 是公比 $e(\alpha t)$ 的等比级数, 其模 $\ll \min(X, \|\alpha t\|^{-1})$ (项数至多 X ; 若 αt 离整数远, 则求和因相消而 $\ll \|\alpha t\|^{-1}$)。故

$$|S|^2 \ll X_0 \sum_y \sum_{y'} \min(X, \|\alpha(y - y')\|^{-1}).$$

- 4 按差值 $t = y - y'$ 归并。 $|y - y'| \leq Y$, 且每个 t 值至多来自 Y_0 对 (y, y') 。所以

$$|S|^2 \ll X_0 Y_0 \sum_{|t| \leq Y} \min(X, \|\alpha t\|^{-1}).$$

- 5 分块估计 $\sum_t$ (与引理 3.1 同理)。把 t 按每 q 个连续值分块, 块数 $\ll Y/q + 1$ 。在一块里, $\alpha t = \frac{at}{q} + \tau + O(\frac{1}{q})$, 当 t 跑遍 q 个连续整数时 $\frac{at}{q} \bmod 1$ 取遍 $0, \frac{1}{q}, \dots, \frac{q-1}{q}$ 的一个排列 (因 $(a, q) = 1$)。于是

$$\sum_{t=t_1+1}^{t_1+q} \min\left(X, \left\|\frac{at}{q} + \tau + O\left(\frac{1}{q}\right)\right\|^{-1}\right) \ll X + \sum_{1 \leq u \leq \frac{1}{2}q} \frac{q}{u} \ll X + q \log q$$

(其中 X 来自最靠近整数的那一项, $\sum q/u \sim q \log q$ 是调和级数。)

- 6 合并。

$$|S|^2 \ll X_0 Y_0 (Y/q + 1)(X + q \log q).$$

注意 $Y/q + 1 = \frac{Y+q}{q}$, $X + q \log q \ll (X+q) \log q$, 即得
 $|S|^2 \ll X_0 Y_0 \frac{\log q}{q} (q+X)(q+Y)$, 这就是 (9.10)。 ■

柯西-施瓦茨不等式（高中版回顾）

对实数 $(\sum a_x b_x)^2 \leq (\sum a_x^2)(\sum b_x^2)$ ——这就是高中的 " $(\vec{u} \cdot \vec{v})^2 \leq |\vec{u}|^2 |\vec{v}|^2$ "。复数版把平方换成模平方。本证明取 $a_x = 1$, 把"和的平方"换成 " X_0 乘以各项平方和", 从而打开了对 x, y, y' 三重求和的展开之路。这是分析数论里最常用的一招。

引理 9.5 的推论：估计 $S(\alpha)$

推论. 设

$$S(\alpha) = \sum_y \sum_v e(\alpha y^k v), \quad (9.11)$$

求和条件即前面 (iii)、(iv)。那么, 若 $\alpha = a/q + O(q^{-2})$ 且 $\backslash [P^{1/2}]$

这一段在讲什么：把刚证的一般引理 9.5 套到我们具体的 $S(\alpha)$ （第三个零件 $y^k v$ 的生成函数）上。结论是：在次弧 ($q > P^{1/2}$) 上, $|S(\alpha)|$ 比它的平凡上界 $S(0)$ 小一个约 $P^{1/4k}$ 的因子。这就是前面"注"里说的、用来补足缺口的**额外节省**。

证. 第一步：把 $S(\alpha)$ 认成引理 9.5 的双线性和。相位是 $\alpha \cdot (y^k) \cdot v$, 两个"变量"分别是 y^k 和 v :

v 这一边

区间长度 $X = \frac{1}{4} P^{k-1/2}$, 不同值个数 $X_0 = U_\ell(\frac{1}{4} P^{k-1/2})$ 。

y^k 这一边

y 从 1 到 $P^{1/2k}$, 故 y^k 落在长度 $Y = (P^{1/2k})^k = P^{1/2}$ 的区间内, 不同值个数 $Y_0 = P^{1/2k}$ 。

第二步: 代入 (9.10) 并化简。

$$|S(\alpha)|^2 \ll X_0 P^{\frac{1}{2k}} \frac{\log q}{q} \left(q + \frac{1}{4} P^{k-\frac{1}{2}} \right) (q + P^{1/2}).$$

现在用条件 $\backslash(P^{\wedge\{1/2\}}$

- $q + \frac{1}{4} P^{k-1/2}$: 由 $q \leq 2kP^{k-1}$ 而 $\frac{1}{4} P^{k-1/2} = \frac{1}{4} P^{k-1} \cdot P^{1/2}$ 量级更大 (比值 $\sim P^{1/2} \rightarrow \infty$), 故 $\ll P^{k-1/2}$ 。
 - $q + P^{1/2}$: 由 $q > P^{1/2}$, 故 $\ll q$ 。
 - 于是
- $$\frac{\log q}{q} (q + X)(q + Y) \ll \frac{\log q}{q} \cdot P^{k-1/2} \cdot q = (\log q) P^{k-1/2} \ll (\log P) P^{k-1/2}$$
- 。

得 $|S(\alpha)|^2 \ll X_0 P^{\frac{1}{2k}} (\log P) P^{k-\frac{1}{2}}$ 。

第三步: 除以 $S(0)^2$ 。平凡值 $S(0) = \sum_y \sum_v 1 = P^{\frac{1}{2k}} X_0 \gg P^{\frac{1}{2k}} X_0$ 。所以

$$\left| \frac{S(\alpha)}{S(0)} \right|^2 \ll \frac{X_0 P^{\frac{1}{2k}} (\log P) P^{k-\frac{1}{2}}}{(P^{\frac{1}{2k}} X_0)^2} = \frac{(\log P) P^{k-\frac{1}{2}}}{P^{\frac{1}{2k}} X_0} \ll P^{-\frac{1}{2k} + (k-\frac{1}{2}) + \varepsilon} X_0^{-1}$$

($\log P$ 被 P^ε 吸收。)

第四步: 用引理 9.4 估 X_0 。 $X_0 = U_\ell(\frac{1}{4} P^{k-1/2}) \gg P^{(k-\frac{1}{2})(1-\lambda^\ell)}$, 故 $X_0^{-1} \ll P^{-(k-\frac{1}{2})(1-\lambda^\ell)}$ 。代入:

$$\left| \frac{S(\alpha)}{S(0)} \right|^2 \ll P^{-\frac{1}{2k} + (k-\frac{1}{2}) + \varepsilon - (k-\frac{1}{2})(1-\lambda^\ell)} = P^{-\frac{1}{2k} + (k-\frac{1}{2})\lambda^\ell + \varepsilon}.$$

开平方 (指数减半, ε 可略):

$$\left| \frac{S(\alpha)}{S(0)} \right| \ll P^{-\frac{1}{4k} + \frac{1}{2}(k-\frac{1}{2})\lambda^\ell},$$

即 (9.12)。

注. 只要 λ^ℓ 较小, (9.12) 就在 P 的指数中比平凡估计节省了几乎 $1/4k$ 。

解读: 当 λ^ℓ 很小 (我们会让它 $\approx \frac{1}{Ck^2}$) 时, 指数里 $\frac{1}{2}(k - \frac{1}{2})\lambda^\ell$ 那一项可忽略, 于是 $|S(\alpha)| \ll S(0)P^{-1/4k}$ ——次弧上额外省了 $\frac{1}{4k}$ 。这恰好就是前面"注"里说"还需多省一点 (比 $\frac{1}{Ck}$ 更多)"的那一点。三块拼图 (T 的平凡 P 、 R 的 $k(1 - \lambda^\ell)$ 、 S 的 $\frac{1}{4k}$) 合起来, 才够把次弧压下去。

引理 9.6: 次弧贡献是低阶的

引理 9.6. 设 m 是次弧 ((9.1) 中区间 $\mathfrak{M}_{a,q}$ 的补集)。那么只要 $\ell \geq 2k \log 3k$, 就有

$$\int_m |T(\alpha)|^{4k} |R(\alpha)|^2 |S(\alpha)| d\alpha \ll P^{3k} R^2(0) S(0) P^{-\delta}$$

对某个固定 $\delta > 0$ 成立。

这一段在讲什么: 这是圆法的"清扫战"——证明次弧对总积分的贡献, 比主弧的主项 $P^{3k} R^2(0) S(0)$ 小一个 $P^{-\delta}$ 因子, 从而可以忽略。三块生成函数各出一份力, 合起来刚好把次弧压成低阶。

证. 第一步: 次弧上必有中等大小的分母。 由狄利克雷逼近定理, 对每个 α 存在 a, q 使

$$(a, q) = 1, \quad 1 \leq q \leq 2kP^{k-1}, \quad \left| \alpha - \frac{a}{q} \right| < \frac{1}{2kqP^{k-1}}.$$

若 α 不在任何主弧 $\mathfrak{M}_{a,q}$ 中 (即在次弧 m 上), 则必有 $q > P^{1/2}$ (否则它就落进某个主弧了)。这恰好满足推论 (9.12) 的条件 $\backslash(P^{1/2})$

第二步：搬来三块估计。

1 由引理 9.5 的推论： $|S(\alpha)| \ll S(0)P^{-\frac{1}{4k} + \frac{1}{2}(k-\frac{1}{2})\lambda^\ell}$ （次弧上点点成立）。

2 由引理 9.4 的推论： $\int_0^1 |R(\alpha)|^2 d\alpha \ll R^2(0)P^{-k+k\lambda^\ell}$ （全区间，更别说次弧子集）。

3 平凡估计： $|T(\alpha)| \leq P$ ，故 $|T(\alpha)|^{4k} \leq P^{4k}$ 。

第三步：把三块乘起来。在被积式里， $|T|^{4k}$ 用 P^{4k} 顶掉， $|S(\alpha)|$ 用其次弧上界顶掉（与 α 无关的常数因子可提出积分），剩下 $\int_{\mathfrak{m}} |R|^2 \leq \int_0^1 |R|^2$ ：

$$\int_{\mathfrak{m}} |T|^{4k} |R|^2 |S| d\alpha \ll P^{4k} \cdot S(0)P^{-\frac{1}{4k} + \frac{1}{2}(k-\frac{1}{2})\lambda^\ell} \cdot R^2(0)P^{-k+k\lambda^\ell}.$$

合并 P 的指数： $4k - k = 3k$ ；剩下 $-\frac{1}{4k} + [\frac{1}{2}(k - \frac{1}{2}) + k]\lambda^\ell$ 。注意 $\frac{1}{2}(k - \frac{1}{2}) + k = \frac{3}{2}k - \frac{1}{4} < \frac{3}{2}k$ ，故

$$\ll P^{3k} R^2(0) S(0) P^{-\frac{1}{4k} + \frac{3}{2}k\lambda^\ell}.$$

第四步：用 $\ell \geq 2k \log 3k$ 压住 λ^ℓ 。

$$\log \lambda^\ell = \ell \log \left(1 - \frac{1}{k}\right) < \ell \cdot \left(-\frac{1}{k}\right) = -\frac{\ell}{k} \leq -2 \log 3k,$$

（用了不等式 $\log(1-t) < -t$ ，对 $0 < t < 1$ ）

第五步：净得负幂。于是指数 $-\frac{1}{4k} + \frac{3}{2}k\lambda^\ell < -\frac{1}{4k} + \frac{1}{6k} = -\frac{1}{12k}$ 。取 $\delta = \frac{1}{12k} > 0$ （一个固定正数），即得

$$\int_{\mathfrak{m}} |T|^{4k} |R|^2 |S| d\alpha \ll P^{3k} R^2(0) S(0) P^{-\delta}.$$

三块节省如何"恰好够" 平凡估计下次弧贡献是 $P^{4k} \cdot R^2(0) \cdot S(0)$ 。三块各让出一点： R 让出 $P^{-k(1-\lambda^\ell)}$ (几乎 P^{-k})， S 让出 $P^{-1/4k}$ ， T 的指数从 $4k$ 降到记账上的 $3k$ 。最终净赚 $P^{-1/12k}$ 。 $\ell \geq 2k \log 3k$ 这个门槛，正是为了让 λ^ℓ 小到使 R 的让步逼近满额 P^{-k} ，从而 S 的 $\frac{1}{4k}$ 能盖过残留。这就是参数 ℓ 取这么大的原因。

定理 9.1: Vinogradov 的上界

定理 9.1. $G(k) < 4k + 6k \log 3k + 3$ 。

这一段在讲什么：收官。把前面所有引理像齿轮一样咬合：主弧给正主项（引理 9.3），次弧可忽略（引理 9.6），于是表示数 $r_1(N) \rightarrow \infty$ ，表示必存在，读出 $G(k)$ 的上界。

证. 第一步：把表示数写成积分。 设 $r_1(N)$ 为 N 在特殊形式 (9.5) 下的表示个数。由圆法（生成函数相乘 + 正交关系挑出"和 = N "的项）：

$$r_1(N) = \int_0^1 T^{4k}(\alpha) R^2(\alpha) S(\alpha) e(-N\alpha) d\alpha.$$

为什么是这个被积式： T^{4k} 对应 $4k$ 个 x_j^k ， R^2 对应 u_1, u_2 两个打包数， S 对应 $y^k v$ ，乘起来展开后指数恰是 $x_1^k + \cdots + x_{4k}^k + u_1 + u_2 + y^k v$ ；再乘 $e(-N\alpha)$ 积分，只留下该和 = N 的项，即表示数。

第二步：拆成主弧 + 次弧。 $\int_0^1 = \int_{\mathfrak{M}} + \int_{\mathfrak{m}}$ 。由引理 9.6，只要 $\ell \geq 2k \log 3k$ ，次弧部分

$$\left| \int_{\mathfrak{m}} \right| \ll P^{3k} R^2(0) S(0) P^{-\delta},$$

比主项低 P^δ 阶，可忽略。

第三步：主弧部分。把 $R^2(\alpha)S(\alpha)$ 按定义展开成对 u_1, u_2, y, v 的求和（每个 $e(\alpha \cdot)$ 提出来），主弧贡献为

$$\sum_{u_1} \sum_{u_2} \sum_y \sum_v \int_{\mathfrak{M}} T^{4k}(\alpha) e(\alpha(-N + u_1 + u_2 + y^k v)) d\alpha.$$

外层求和的项数 $= R(0) \cdot R(0) \cdot S(0) = R^2(0)S(0)$ (u_1, u_2 各 $R(0)$ 种, (y, v) 共 $S(0)$ 种)。

第四步：对每一项套引理 9.3。令 $M = N - u_1 - u_2 - y^k v$ 。第三步里的积分正是 $\int_{\mathfrak{M}} T^{4k}(\alpha) e(-M\alpha) d\alpha$ 。由 (9.6)，无论怎么选 u_1, u_2, y, v ，都有 $\frac{1}{P^k}$ 注意每一项都是正的（下界为正），所以求和不会相消。

第五步：合计并读出结论。主弧贡献 $\gg R^2(0)S(0) \cdot P^{3k}$ ，主导次弧的 $P^{3k} R^2(0)S(0)P^{-\delta}$ 。故

$$r_1(N) \gg P^{3k} R^2(0)S(0).$$

当 $N \rightarrow \infty$ 时 $P \rightarrow \infty$ ，且 $R(0), S(0) \rightarrow \infty$ ，所以 $r_1(N) \rightarrow \infty$ 。表示数趋于无穷，特别地大于 0，于是 (9.5) 形式的表示对所有充分大的 N 必存在。因为这种表示用了 $4k + 3\ell$ 个 k 次幂，故

$$G(k) \leq 4k + 3\ell.$$

取允许的最小 $\ell = \lceil 2k \log 3k \rceil \leq 2k \log 3k + 1$ ：

$$G(k) \leq 4k + 3(2k \log 3k + 1) = 4k + 6k \log 3k + 3.$$

定理 9.1 证毕。 ■

回看：这条 $4k + 6k \log 3k + 3$ 怎么对应 $(6 + \delta)k \log k$ ”

当 $k \rightarrow \infty$ 时， $\log 3k = \log k + \log 3$ ，于是

$$4k + 6k \log 3k + 3 = 6k \log k + (6 \log 3)k + 4k + 3 = 6k \log k \left(1 + \frac{6 \log 3 + 2}{6 \log k} + \frac{3}{6k \log k}\right)$$

括号里的修正项随 k 增大趋于 0，所以对任意 $\delta > 0$ ，当 $k > k_0(\delta)$ 时 $G(k) < (6 + \delta)k \log k$ ——正是第 2 段宣告的 Vinogradov 定理。低阶的 $4k, 3$ 等项在 k 大时全被 $k \log k$ 吞掉。

全章逻辑一图流

- 1 工具 A (引理 9.1): 求和换积分 $\Rightarrow$ 引理 9.2 主弧上 $T \approx q^{-1} S_{a,q} I(\beta)$ 。
- 2 引理 9.3: $4k$ 个 T 在主弧上给正主项 $\gg P^{3k}$ (对整段 M)。
- 3 引理 9.4 + 推论: 打包数 u 很多 $\Rightarrow R$ 在 L^2 上节省 $\approx P^{-k}$ 。
- 4 工具 B (引理 9.5) + 推论: 双线性和 $\Rightarrow S$ 在次弧额外节省 $P^{-1/4k}$ 。
- 5 引理 9.6: 三块节省合力 $\Rightarrow$ 次弧可忽略 ($P^{-\delta}$)。
- 6 定理 9.1: 主弧正 + 次弧小 $\Rightarrow r_1(N) \rightarrow \infty \Rightarrow G(k) \leq 4k + 3\ell < (6 + \delta)k \log k$ 。

1. 关于"主要依据 Heilbronn 的叙述 [44]": Vinogradov 1934 年的原始证明技术性极强、不易读。Heilbronn (一位以清晰著称的数论学家) 把它重新组织成更易跟随的形式，本章正文沿用他的安排。
2. 关于更精确逼近 $O(q^{3/4+\epsilon})$ (见 [18, 引理 8 和 9]): 这是 Davenport 等人后来的精细结果，误差指数 $3/4$ 与 k 无关，颇为惊人。本章主线不需要它，故仅作提及，以

示方法尚有改进空间。

返回 [全书目录](#)