

DAVENPORT · 圆法 · 高中详解版

三次型

Cubic forms

本章要解决什么 我们想证明一件大事：一个整系数的齐次三次方程

$C(x_1, \dots, x_n) = 0$ ，只要变量个数 n 足够大（本书最终做到 $n \geq 17$ ），就一定有不全为 0 的整数解。本章是这条定理证明的第一步，目标很具体：研究与三次型挂钩的一个"指数和" $S(\alpha)$ ，并证明——

当 $|S(\alpha)|$ 大到某个程度时，**要么**这个三次型本身有大量"双线性零点"（选项 A），**要么**这个 α 必定非常靠近一个分母不大的分数 a/q （选项 B）。

读完你将掌握：复指数 $e(\alpha)$ 与圆法的基本框架、Weyl 差分法（把三次降成线性）、几何数论缩放引理的用法，以及"主弧/次弧"二分思想的来源。本章只搭舞台、磨刀，真正的估值在第 14、15 章。

阅读方式：灰色竖线框是原书译文（忠实翻译），其余彩色框与正文是面向高中生的逐句详解，把每个符号、每一步跳步都补全。

0. 先备齐工具：几个超出高中课本的记号

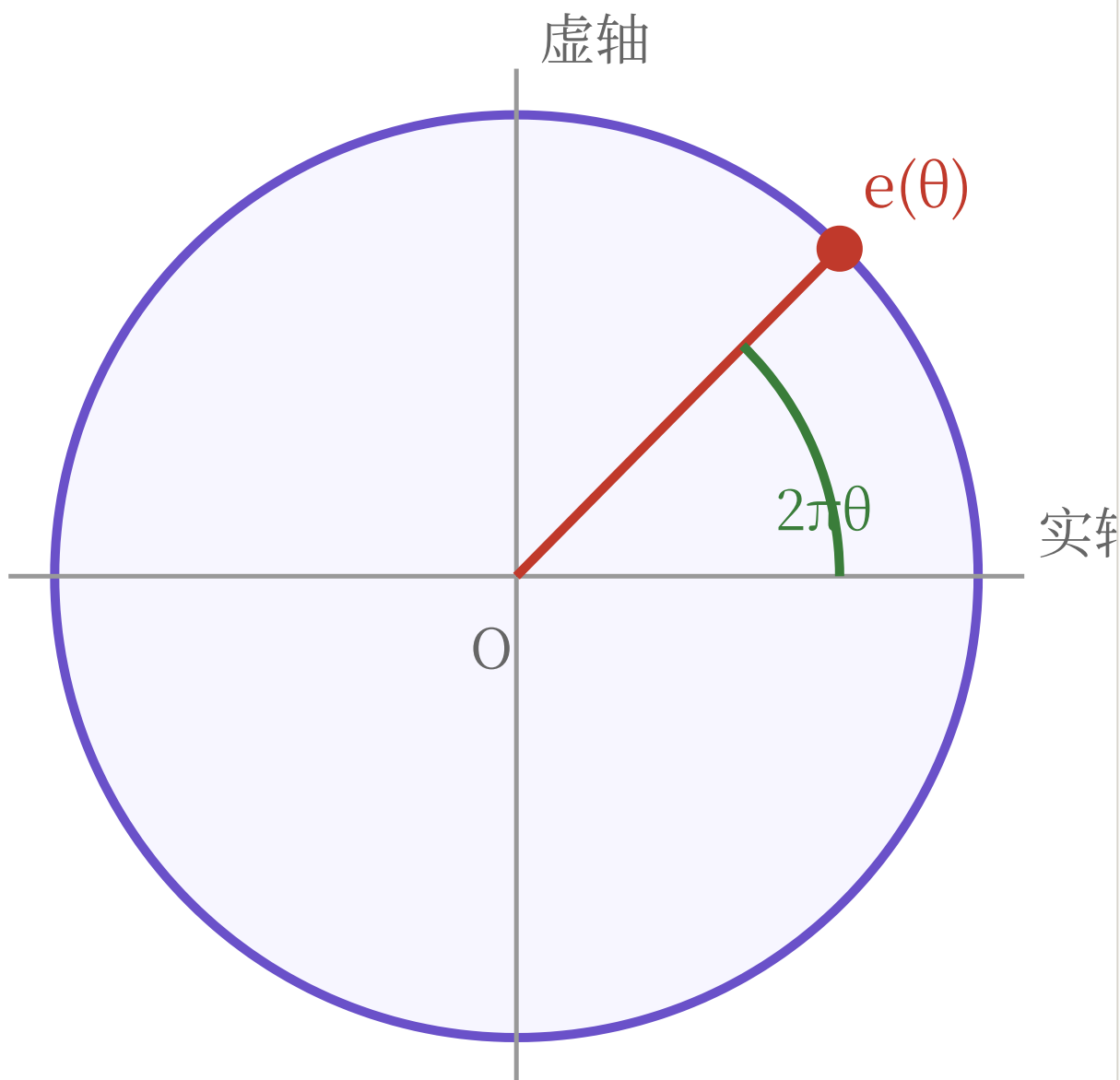
本章会反复用到几样高中没正式学过的东西。先一次性讲清，后面就不再打断。

记号 1 复指数 $e(\theta) = e^{2\pi i \theta}$ ，读作"e 的 $2\pi i \theta$ 次方"。这里 i 是虚数单位（ $i^2 = -1$ ）。由欧拉公式 $e^{i\varphi} = \cos \varphi + i \sin \varphi$ ，所以

$$e(\theta) = \cos(2\pi\theta) + i \sin(2\pi\theta).$$

它是一个模长恒为 1 的复数：把 θ 想成"转了几圈"， $\theta = 1$ 正好转回原点。关键性质：

- ① $|e(\theta)| = 1$ (永远在单位圆上)；
- ② $e(\theta_1)e(\theta_2) = e(\theta_1 + \theta_2)$ (指数相加)；
- ③ 只跟 θ 的小数部分有关： $e(\theta + m) = e(\theta)$ 对任意整数 m 成立 (转整圈等于没转)。



$e(\theta)$ 是单位圆上的点，幅角为 $2\pi\theta$ 。 θ 走一圈 (加 1)，点回到原处——这正是圆法把变量 α 限制在 $[0, 1]$ 的原因。

记号 2 求和号 $\sum$ 与积分号 $\int$ 。 $\sum_x f(x)$ 就是"把所有满足条件的 x 对应的 $f(x)$ 加起来"。本章求和往往跑遍一个盒子里的所有**整点**（坐标全是整数的点）。

$\int_0^1 g(\alpha) d\alpha$ 是定积分，可理解为"把 α 从 0 到 1 切成无数小片，每片宽 $d\alpha$ 、高 $g(\alpha)$ ，面积加起来"。后面有一条核心恒等式 $\int_0^1 e(m\alpha) d\alpha = \begin{cases} 1, & m = 0 \\ 0, & m \neq 0 \end{cases}$ (m 为整数)，它是圆法把"解的个数"写成积分的关键，下面会用到。

记号 3 到最近整数的距离 $\|\theta\|$ ，读作"theta 的范数"或"theta 到最近整数的距离"。定义

$$\|\theta\| = \min_{m \in \mathbb{Z}} |\theta - m|.$$

例如 $\|3.2\| = 0.2$, $\|3.8\| = 0.2$, $\|5\| = 0$ 。它永远落在 $[0, \frac{1}{2}]$ 。与之配套的还有**小数部分** $\{\theta\} = \theta - \lfloor \theta \rfloor$ （去掉整数部分，落在 $[0, 1)$ ）。例如 $\{3.8\} = 0.8$ 。 $\|\theta\|$ 越小，表示 θ 越接近某个整数。

记号 4 数量级记号 $O(\cdot)$ 、 $\ll$ 、 $\gg$ 。写 $A \ll B$ （等价于 $A = O(B)$ ）意思是"存在一个与 P 无关的常数 c ，使 $|A| \leq cB$ "——即" A 至多和 B 一个量级，最多差个固定倍数"。 $A \gg B$ 就是 $B \ll A$ 。这套记号让我们只关心随 P 增大时谁占主导，不纠缠具体常数。例如 $3n^2 + 5n \ll n^2$ 、 $n^2 \gg n$ 。本章满纸 $\ll, \gg$ ，因为我们要的从来不是精确值，而是"量级谁压过谁"。

记号 5 黑体向量 $\mathbf{x}$ 表示 n 个坐标 $(x_1, \dots, x_n)$ 打包成的点； $|\mathbf{x}|$ 在本章特指 $\max(|x_1|, \dots, |x_n|)$ （各坐标绝对值里最大的那个），这是脚注里特意声明的——与第 12 章用"到原点距离"不同，但只差固定倍数，量级上无所谓。

1. 定理与历史：为什么是 17，为什么 10 不能再少

我们现在着手证明：一个具有整系数的齐次三次方程 $C(x_1, \dots, x_n) = 0$ (13.1)，当 $n \geq 17$ 时，总能在整数 $x_1, \dots, x_n$ （不全为 0）中求解。第一个这样的结果，附带条件 $n \geq 32$ ，于 1957 年被证明；改进后的结果在 1962 年初被发现。1963 年我证明了条件 $n \geq 16$ 已经足够，但这需要一个性质上颇为特殊、超出 $n \geq 17$ 所需的更细致的论证。

这段在讲什么。开门见山地把全书这部分的主定理和它的历史进度条摆出来。先把名词拆开：

"齐次" (homogeneous)

方程里每一项的次数都相同。三次齐次就是每一项都是三个变量相乘（如 x_1^3 、 $x_1x_2x_3$ 、 $5x_2^2x_3$ ），没有二次项、一次项或常数项。齐次方程有个好处：若 $\mathbf{x}$ 是解，则 $t\mathbf{x}$ 对任意 t 也是解，所以我们只关心非平凡解（不全为零的解）。

"三次" (cubic)

最高次数是 3。

$$C(x_1, \dots, x_n) = 0$$

一个 n 元三次齐次多项式等于零。变量越多（ n 越大），自由度越高，越"容易"有解——这就是为什么定理形如" n 够大就一定有解"。

为什么"变量多就一定有解"是个难题？注意 $\mathbf{x} = \mathbf{0}$ 永远是解，但它平凡、没意义。要找非零整数解则毫不显然：方程只有一个，未知数有 n 个，看上去"方程少、未知数多"应该容易，但整数解的限制极强（不能取分数、不能取实数逼近），这正是丢番图问题之难。Davenport 这套圆法给出的，是一个能定量保证解存在的方法。

历史脉络 这是一条逐年被压低的"门槛"：

- 1 1957：首次证明 $n \geq 32$ 足够（文献 [21]）。即便条件还很宽，能证"够多变量必有解"已是突破。
- 2 1962 年初：改进结果（文献 [20]），门槛进一步降低。

3 1963: Davenport 本人证明 $n \geq 16$ 即可 (文献 [22]), 但用到一个"颇为特殊"的精细论证。

4 本书选择讲 $n \geq 17$ 的版本——因为它能用**统一、干净**的论证讲清楚, 而 $n \geq 16$ 那一步是为了抠掉最后一个变量额外耍的特殊技巧, 喧宾夺主。这正是"取舍": 教学上宁可门槛松一点 (17), 换来思路的清爽。

原文译文

Mordell 于 1937 年指出, 存在九个变量的三次型不表示零, 因而条件 $n \geq 10$ 对于 (13.1) 总可解而言是必不可少的。Mordell 的例子基于一个三次域的范数型的性质。如果 p 是一个在该域中不分解的素数, 那么范数型 $N(x, y, z)$ 永远不能被 p 整除, 除非 x, y, z 都能被 p 整除。由此容易推出, 方程

$$N(x_1, x_2, x_3) + pN(x_4, x_5, x_6) + p^2N(x_7, x_8, x_9) = 0$$

除平凡解外, 没有整数解 $x_1, \dots, x_9$ 。

这段在讲什么。上一段说"变量够多就有解", 这段从**反方向**立一根界桩: 变量太少时, 确实可能**无非零解**。所以门槛不能无限往下压—— $n \geq 10$ 是**必需的** (即存在 9 个变量的反例)。这保证了我们追求的 $n \geq 17$ 不是无的放矢。先解释名词。

"表示零"是什么意思 "三次型 C 表示零"指存在**非零**整点 $\mathbf{x}$ 使 $C(\mathbf{x}) = 0$ 。"不表示零"就是除 $\mathbf{x} = \mathbf{0}$ 外永远 $C(\mathbf{x}) \neq 0$ 。Mordell 找到了一个 9 元三次型, 它**不表示零**。

"范数型" $N(x, y, z)$ 是什么 这超出高中范围, 但可以这样理解。取一个特别的无理数 ω (本例是 $\omega = \sqrt[3]{2}$), 考虑形如 $x + y\omega + z\omega^2$ 的数 (x, y, z 为整数), 它们构成一个"三次域" $\mathbb{Q}(\omega)$ 。这个数的**范数** $N(x, y, z)$, 是把 ω 换成它的三个"共轭根" ($\omega, \omega\zeta, \omega\zeta^2$, ζ 是 1 的三次方根) 后三个值**相乘**得到的结果。神奇之处: 尽管中间出现复数, 乘起来恰好是一个**整系数三次齐次型**。对 $\omega = \sqrt[3]{2}$ 算出来就是下一段的

$N = x^3 + 2y^3 + 4z^3 - 6xyz$ 。范数最重要的性质是**可乘性**：两个数相乘，范数也相乘。

"不分解的素数"与整除性质。"素数 p 在域中不分解"是数论里的说法，对我们只需用它的一个**结论**：

关键事实（本段唯一要用的）：若 p 在该域不分解，则 $p \mid N(x, y, z)$ （即 N 能被 p 整除）当且仅当 x, y, z **全部**能被 p 整除。换句话说：只要 x, y, z 不全是 p 的倍数， $N(x, y, z)$ 就不被 p 整除。

这里"同余 / 整除"是高中数论的延伸： $p \mid a$ 读作" p 整除 a "，意思是 a 是 p 的倍数； $a \equiv 0 \pmod{p}$ 是同一件事的另一种写法。下面用这个关键事实，一步步证明那个 9 元方程只有平凡解。

补全推导：为什么 $N(x_1, x_2, x_3) + pN(x_4, x_5, x_6) + p^2N(x_7, x_8, x_9) = 0$ 只有平凡解

原文说"由此容易推出"，这里把"容易"摊开成完整的**无穷递降**论证。设 $\mathbf{x} = (x_1, \dots, x_9)$ 是整数解。记三块为

$$A = N(x_1, x_2, x_3), \quad B = N(x_4, x_5, x_6), \quad D = N(x_7, x_8, x_9),$$

方程即 $A + pB + p^2D = 0$ 。

1 先看 A 必被 p 整除。由 $A = -pB - p^2D = -p(B + pD)$ ，右边显然是 p 的倍数，故 $p \mid A$ ，即 $p \mid N(x_1, x_2, x_3)$ 。

2 用关键事实。 $p \mid N(x_1, x_2, x_3)$ 迫使 x_1, x_2, x_3 全是 p 的倍数。写 $x_1 = px'_1, x_2 = px'_2, x_3 = px'_3$ 。

3 范数随之被 p^3 整除。因为 N 是三次齐次，把每个变量放大 p 倍，整体放大 p^3 倍： $A = N(px'_1, px'_2, px'_3) = p^3N(x'_1, x'_2, x'_3)$ 。

- 4 代回方程并约去一个 p 。方程变成 $p^3 N(x'_1, x'_2, x'_3) + pB + p^2 D = 0$, 两边同除以 p :

$$p^2 N(x'_1, x'_2, x'_3) + B + pD = 0.$$

于是 $B = -p^2 N(x'_1, x'_2, x'_3) - pD = -p(\dots)$, 故 $p \mid B = N(x_4, x_5, x_6)$ 。

- 5 再次用关键事实: x_4, x_5, x_6 也全被 p 整除, 写 $x_4 = px'_4$ 等, 则

$B = p^3 N(x'_4, x'_5, x'_6)$ 。代回上式

$p^2 N(x'_1, x'_2, x'_3) + p^3 N(x'_4, x'_5, x'_6) + pD = 0$, 再除以 p :

$pN(x'_1, x'_2, x'_3) + p^2 N(x'_4, x'_5, x'_6) + D = 0$ 。于是

$p \mid D = N(x_7, x_8, x_9)$, 从而 x_7, x_8, x_9 全被 p 整除。

- 6 结论——无穷递降。至此 $x_1, \dots, x_9$ 全部都是 p 的倍数。设 $x_j = px'_j$, 由齐次性, $(x'_1, \dots, x'_9)$ 也是同一方程的解, 且每个坐标都缩小为原来的 $1/p$ 。若原解非零, 可一直这样除下去, 得到无穷多个越来越小的非零整数解——这不可能 (非零整数的绝对值不能无限缩小且仍是整数)。矛盾! 故唯一解是 $\mathbf{x} = \mathbf{0}$ 。 ■

原文译文

事实上, 我们还可以进一步断言: 相应的模 p^3 的同余式除了所有变量都 $\equiv 0 \pmod{p}$ 之外没有解。一个简单的例子可由取 $p = 7$ 并令

$$N(x, y, z) = x^3 + 2y^3 + 4z^3 - 6xyz$$

给出, 这正是由 $\sqrt[3]{2}$ 生成的域的范数型。一个与上述类似的构造, 给出了 k^2 个变量中 k 次齐次不可解方程的例子。

这段在讲什么。把上面的反例做得更"狠", 并给出一个具体可验证的例子。"更狠"体现在: 不只整数方程无非零解, 连模 p^3 的同余式都只有平凡解。

"模 p^3 同余式只有平凡解" 同余式 $F(\mathbf{x}) \equiv 0 \pmod{m}$ 是问 " $F(\mathbf{x})$ 能否被 m 整除", 比 "等于零" 宽松得多。这里断言: 即便把方程左边只要求被 p^3 整除 (而非严格为零), 仍然逼得所有变量 $\equiv 0 \pmod{p}$ 。把上面证明的第 1-5 步原样搬到 "模 p^3 " 下即可 (每一步的整除推理仍成立)。**为什么这点重要?** 因为圆法最后会出现一个叫 "奇异级数" 的量, 它由各个素数下的同余式解数堆叠而成; 若某个 p 下连同余式都只有平凡解, 奇异级数就会 "塌掉" 为零, 渐近主项消失——这正是 9 变量反例能成立的 **深层机制**。所以作者强调这个 "模 p^3 " 版本, 是在预告后面奇异级数那一章的关键。

动手验证这个范数型 取 $p = 7$, $N(x, y, z) = x^3 + 2y^3 + 4z^3 - 6xyz$ 。

- 1 它确实是 $\sqrt[3]{2}$ 的范数型。令 $\omega = \sqrt[3]{2}$ ($\omega^3 = 2$), 数 $\xi = x + y\omega + z\omega^2$ 。三个共轭是把 ω 换成 $\omega, \omega\zeta, \omega\zeta^2$ ($\zeta = e(1/3)$ 是 1 的复立方根)。三者相乘 $N = \prod (x + y\omega\zeta^k + z\omega^2\zeta^{2k})$, 展开 (利用 $1 + \zeta + \zeta^2 = 0, \omega^3 = 2$) 正好得到 $x^3 + 2y^3 + 4z^3 - 6xyz$ 。系数 2, 4 来自 $\omega^3 = 2, \omega^6 = 4$, -6 来自交叉项 $-3\omega^3 = -6$ 。
- 2 为什么取 $p = 7$? 因为 7 是一个在 $\mathbb{Q}(\sqrt[3]{2})$ 中 "不分解" 的素数 (即 2 不是模 7 的三次剩余: $1^3, 2^3, \dots \equiv 1, 1, 6, 1, 6, 6 \pmod{7}$ 取不到 2)。这保证了上面的 "关键事实" 成立。换个 p (如 $p = 31$, 那里 2 是模 31 的三次剩余, 故 31 在域中分解, "关键事实" 不再成立) 就不行——这就是 "为什么这样取参数"。

" k^2 个变量、 k 次" 的推广。 把上面 "三块、系数 $1, p, p^2$ " 的把戏推到 k 次: 用一个 k 次域的范数型 N (k 个变量), 堆 k 块、系数 $1, p, p^2, \dots, p^{k-1}$, 共用 $k \cdot k = k^2$ 个变量, 同样的无穷递降说明它 **不可解**。当 $k = 3$ 就回到 $9 = 3^2$ 个变量的三次情形。这说明: 对 k 次方程, 门槛至少得超过 k^2 。

2. 搭舞台：指数和 $S(\alpha)$ 与圆法的出发点

原文译文

关于三次方程的定理的证明分为若干章，每一章在很大程度上是自成一体的。我们从考虑与一个三次型相关联的指数和开始。写

$$C(\mathbf{x}) = C(x_1, \dots, x_n) = \sum_i \sum_j \sum_k c_{ijk} x_i x_j x_k,$$

其中各求和指标从 1 跑到 n ，系数 c_{ijk} 是整数，并且我们可以假设 c_{ijk} 是关于 i, j, k 的对称函数。

这段在讲什么。正式给三次型一个统一写法，并约定系数对称。这两点是后面所有计算的地基。

三重求和 $\sum_i \sum_j \sum_k$ i, j, k 各自独立地从 1 取到 n ，把所有组合 (i, j, k) 对应的 $c_{ijk} x_i x_j x_k$ 全加起来，共 n^3 项。每一项都是三个变量相乘，所以是三次、且每项次数都是 3，所以齐次。 c_{ijk} 是这一项的整数系数。

"对称函数"是什么、为什么可以这样假设 " c_{ijk} 对称"指交换三个下标的次序值不变： $c_{ijk} = c_{jik} = c_{ikj} = \dots$ ($3! = 6$ 种排列都相等)。

为什么"可以假设"? 因为 $x_i x_j x_k$ 这个乘积本身与下标次序无关 (乘法可交换)，所以同一个单项式 $x_1 x_2 x_3$ 会在 6 个不同下标组合里出现。我们总可以把这 6 个系数平均掉，换成对称的系数而不改变整个多项式的值。例如某项原本只在 c_{123} 写了 6、其余写 0，可改成 $c_{123} = c_{132} = \dots = 1$ (六个各 1)，总和 $6x_1 x_2 x_3$ 不变。对称化是纯粹为后面求导/差分时系数好看 (会反复出现 3、6 这样的整齐倍数)，属于"先把记号理顺"的预备动作。

原文译文

设 P 是一个大的正整数。设 $\mathfrak{B}$ 是 n 维空间中一个固定的盒子，即由 n 个区间构成的笛卡尔积 $x'_j < x_j \leq x''_j$ ($1 \leq j \leq n$)。仅为方便起见，我们假设 $x''_j - x'_j < 1$ 。令

$$S(\alpha) = \sum_{P\mathfrak{B}} e(\alpha C(x_1, \dots, x_n)),$$

其中求和遍历盒子 $P\mathfrak{B}$ 中的所有整点，盒子 $P\mathfrak{B}$ 由下式给出 $Px'_j < x_j \leq Px''_j$ ($1 \leq j \leq n$)。

这段在讲什么。定义本章的主角——**指数和** $S(\alpha)$ 。它把"我们关心的整点"全部塞进一个和式，是圆法的发动机。逐件解释。

P (大正整数)

"放大倍数"。我们让 $P \rightarrow \infty$ ，看解的个数如何随 P 增长。所有 $\ll, \gg$ 里的"常数与 P 无关"都是相对它而言。

固定盒子 $\mathfrak{B}$

n 维空间里一个长方体：第 j 个坐标被限制在小区间 $(x'_j, x''_j]$ 。"笛卡尔积"就是各坐标区间独立组合成的盒子。假设每条边长 $x''_j - x'_j < 1$ 只是技术性的"小盒子"约定，方便计数。

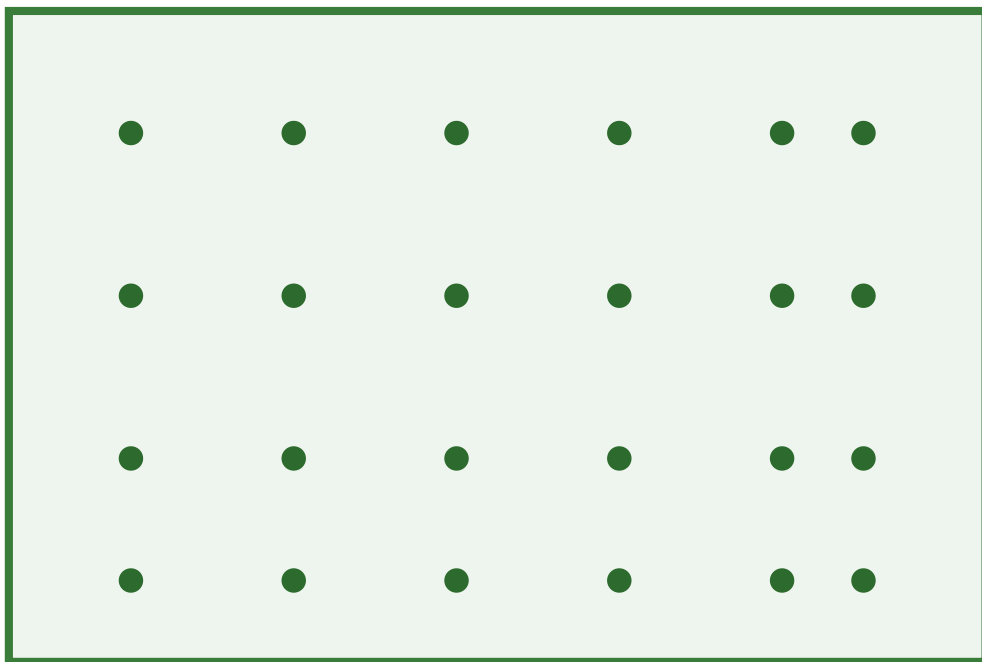
放大盒子 $P\mathfrak{B}$

把盒子整体放大 P 倍，得到 $Px'_j < x_j \leq Px''_j$ 。它的每条边长约 $P(x''_j - x'_j)$ ，所以里面大约有 $\prod_j P(x''_j - x'_j) \sim P^n$ 个整点。这就是"自变量 $\mathbf{x}$ 的取值范围"。

α (实数，取自 $[0, 1]$)

一个旋钮。 $S(\alpha)$ 把每个整点 $\mathbf{x}$ 贡献一个单位圆上的复数 $e(\alpha C(\mathbf{x}))$ ，再全部相加。改变 α 就改变所有相位。

放大盒子 $P \cdot B$ (边长 $\sim P$)



约 P^n 个整点 $\mathbf{x}$, 每个贡献 $e(\alpha C(\mathbf{x}))$

$S(\alpha)$ 就是把盒子里约 P^n 个整点的单位向量 $e(\alpha C(\mathbf{x}))$ 首尾相加。它们指向越乱, 相消越多, $|S(\alpha)|$ 越小。

原文译文

设 $\mathcal{N}(P)$ 表示 $P\mathfrak{B}$ 中满足 (13.1) 的整点 $\mathbf{x}$ 的个数。则

$$\mathcal{N}(P) = \int_0^1 S(\alpha) d\alpha. \quad (13.2)$$

这段在讲什么。圆法的命门：把"解的个数" $\mathcal{N}(P)$ 写成一个积分。这一步把组合问题（数解）变成分析问题（算积分），是整套方法的灵魂。原文直接给结论，下面补全为什么成立。

补全推导：(13.2) 为什么成立

1 核心恒等式。对任意整数 m :

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

理由：若 $m = 0$ ，被积函数 $e(0) = 1$ ，积分 $\int_0^1 1 d\alpha = 1$ 。若 $m \neq 0$ ， $\int_0^1 e(m\alpha) d\alpha = \frac{e(m\alpha)}{2\pi im} \Big|_0^1 = \frac{e(m) - e(0)}{2\pi im} = \frac{1 - 1}{2\pi im} = 0$ （因为 $e(m) = 1$ ，整数转整圈回原点）。这是一个"探测器"：它只在 $m = 0$ 时亮 1，其余全灭。

2 把 $S(\alpha)$ 代入积分。

$$\int_0^1 S(\alpha) d\alpha = \int_0^1 \sum_{\mathbf{x} \in P\mathfrak{B}} e(\alpha C(\mathbf{x})) d\alpha.$$

3 交换求和与积分（有限和，可逐项积分）：

$$= \sum_{\mathbf{x} \in P\mathfrak{B}} \int_0^1 e(\alpha C(\mathbf{x})) d\alpha.$$

4 用探测器。这里 $m = C(\mathbf{x})$ 是整数。由第 1 步，每一项的积分在 $C(\mathbf{x}) = 0$ 时为 1，否则为 0。于是

$$\int_0^1 S(\alpha) d\alpha = \sum_{\mathbf{x} \in P\mathfrak{B}} [C(\mathbf{x}) = 0] = \#\{\mathbf{x} \in P\mathfrak{B} : C(\mathbf{x}) = 0\} = \mathcal{N}(P)$$

积分把"满足方程的点记 1、不满足记 0"自动加总，得到的正是解的个数。

为什么叫"圆法"。变量 α 跑遍 $[0, 1]$ ，而 $e(\alpha \cdot)$ 在 α 加 1 时不变，所以 $[0, 1]$ 首尾相接其实是一个圆（Hardy-Littlewood 当年正是在单位圆上做积分）。本章不直接算这个积分，而是先研究被积函数 $S(\alpha)$ 在不同 α 处有多大——这决定了哪些 α 是"主力"、哪些可丢弃。

3. 目标与那个"自相矛盾"的策略

原文译文

我们的目标（原则上）是证明：通过适当选取盒子 $\mathfrak{B}$ ，当 $P \rightarrow \infty$ 时 $\mathcal{N}(P)$ 有一个渐近公式，其中主项的阶为 P^{n-3} 。实际上这并不总是成立。我们将要得到的，是一个看似自相矛盾的结果：该渐近公式在 (13.1) 不可解（从而 $\mathcal{N}(P) = 0$ ）的假设下成立！这对我们的目的而言已经足够，因为它将证明 (13.1) 是可解的。

这段在讲什么。说明整套证明的逻辑诡计，这是全章最妙、也最容易看晕的一句话。慢慢拆。

"渐近公式，主项阶 P^{n-3} "

"渐近公式"指当 P 很大时 $\mathcal{N}(P) \approx cP^{n-3}$ （再加更低阶的误差）。为什么是 P^{n-3} ？直觉：盒子里约 P^n 个点，方程 $C(\mathbf{x}) = 0$ 是"一个三次方程"的约束， $C(\mathbf{x})$ 的取值范围约 P^3 ，命中 0 的"概率"约 P^{-3} ，于是解数约 $P^n \cdot P^{-3} = P^{n-3}$ 。只要 $c > 0$ 且 $n > 3$ ，这就是正且趋于无穷的——意味着有解，而且解很多。

"自相矛盾"的策略（反证法的变体）。直接证 $\mathcal{N}(P) \sim cP^{n-3} > 0$ 很难、且"并不总成立"。于是改用一招：假设方程无解（ $\mathcal{N}(P) = 0$ ），在这个假设下去推导渐近公式 $\mathcal{N}(P) = cP^{n-3} + (\text{更小误差})$ 。

一旦推出来，矛盾就来了：左边 = 0，右边 $\geq cP^{n-3} - (\text{误差}) > 0$ （ P 大时主项压过误差）。 $0 > 0$ 不可能！所以"无解"的假设错误，方程必有解。

妙处在于："无解"这个假设反而让某些捣乱项消失，使渐近公式更容易证出来。我们不需要真的算出解的个数，只要逼出一个矛盾。这就是"看似自相矛盾却足够用"的含义。

4. 平凡估计与"大 S 假设"(13.3)

原文译文

$|S(\alpha)|$ 的平凡估计是 P^n 。我们首先研究：若对于某个特定的 α ，有 $|S(\alpha)| \geq P^{n-K}$ (13.3)，会发生什么，其中 K 是某个正数。最终，正如前几章那样，我们的目标是能够从 α 的集合中去掉任何对积分贡献的量低于 P^{n-3} 阶的子集。

这段在讲什么。给 $S(\alpha)$ 立一个"上限标杆"，并提出本章真正要攻的问题。

为什么平凡估计是 P^n $S(\alpha) = \sum_{\mathbf{x}} e(\alpha C(\mathbf{x}))$ 是约 P^n 个复数之和，每个复数模长 = 1。由三角不等式 $|\sum a_k| \leq \sum |a_k|$,

$$|S(\alpha)| \leq \sum_{\mathbf{x} \in P\mathfrak{B}} |e(\alpha C(\mathbf{x}))| = \sum_{\mathbf{x}} 1 = \#(P\mathfrak{B} \cap \mathbb{Z}^n) \ll P^n.$$

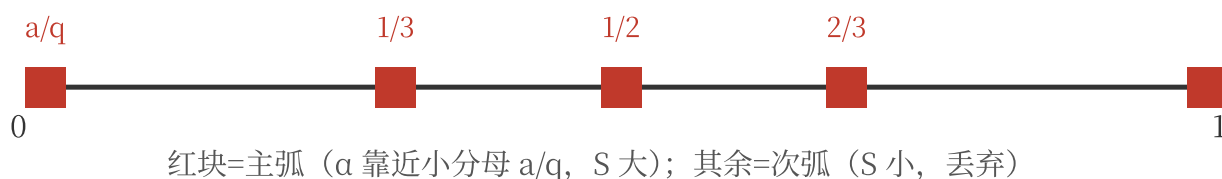
"平凡"是说这一步啥技巧没用、只把模长全加起来。它在 $\alpha = 0$ 时确实达到（那时每个 $e(0) = 1$ 同向，毫不相消， $S(0) \sim P^n$ ）。一般的 α 会让相位错乱、彼此相消， $|S(\alpha)|$ 远小于 P^n 。

假设 (13.3): $|S(\alpha)| \geq P^{n-K}$ K 是一个正的损失指数。 $P^{n-K} = P^n / P^K$ ，所以这条假设是说" $S(\alpha)$ 还没小太多，至多比满额 P^n 小了 P^K 倍"。我们研究哪些 α 能让 S 这么大。直觉上， S 大意味着那约 P^n 个单位向量没怎么相消、相位高度一致，这是很强的约束，会反过来逼出 α 的特殊结构（靠近某个 a/q ）。 K 越小，假设越苛刻（要求 S 越大），能满足的 α 越少。

本章的战略目标 ("去掉小贡献的 α ")。积分 $\int_0^1 S(\alpha) d\alpha$ 的主项要是 P^{n-3} 阶。任何一片 α 区间，如果它对积分的贡献低于 P^{n-3} 阶，就可以安心丢掉（归入误差）。这正是圆法的主弧 / 次弧二分：

- **次弧 (minor arcs):** $S(\alpha)$ 普遍偏小的那些 α ，贡献小，丢掉；
- **主弧 (major arcs):** $S(\alpha)$ 可能很大的那些 α （靠近 a/q ），它们贡献主项 P^{n-3} ，要精算。

本章的引理 13.1–13.4 就是要刻画" S 大"的 α 长什么样，为第 15 章的二分做准备。



圆法把 $[0, 1]$ 切成"主弧" (围绕小分母分数的短区间) 与"次弧" (其余)。本章的任务是证明：
 S 大的 α 只能落在主弧里。

5. Weyl 不等式的推广：双线性型 B_j

原文译文

第一步是证明 Weyl 不等式的一个推广。对于任意两点 $\mathbf{x}, \mathbf{y}$ ，我们定义一组 n 个双线性型：

$$B_j(\mathbf{x} | \mathbf{y}) = \sum_i \sum_k c_{ijk} x_i y_k, \quad (1 \leq j \leq n).$$

这段在讲什么。引入本章第二位主角——**双线性型 B_j** 。它是把三次型"求两次差分、降两次次数"后剩下的线性骨架，后面所有引理都围着它转。

什么是"双线性型"，为什么要引入它 $B_j(\mathbf{x} | \mathbf{y}) = \sum_i \sum_k c_{ijk} x_i y_k$ 对每个 j 是一个数。"双线性"指它对 $\mathbf{x}$ 是线性的 (固定 $\mathbf{y}$ ，关于 x_i 一次)、对 $\mathbf{y}$ 也是线性的 (固定 $\mathbf{x}$ ，关于 y_k 一次)。

动机：原三次型 C 是三次的，直接处理太难。Weyl 的思想是"差分降次"：三次型差一次降成二次、再差一次降成一次 (线性)。差两次后，跟求和变量 $\mathbf{z}$ 线性相关的系数恰好就是 $6\alpha B_j(\mathbf{x} | \mathbf{y})$ (见下一节推导)。所以 B_j 是"三次型经两次差分后留下的线性核心"，把对三次和的估计**转化**成对线性和的估计——这是整个 Weyl 方法的关键转译。

对称性提示：因 c_{ijk} 对称，交换 $\mathbf{x}, \mathbf{y}$ 的角色相当于交换下标 i, k ，所以 $B_j(\mathbf{x} | \mathbf{y})$ 关于 $\mathbf{x}, \mathbf{y}$ 也有良好对称性，后面会用到。

引理 13.1: Weyl 不等式的推广

引理 13.1. 假设 (13.3) 蕴含

$$\sum_{|\mathbf{x}| < P} \sum_{|\mathbf{y}| < P} \prod_{j=1}^n \min(P, \|6\alpha B_j(\mathbf{x} | \mathbf{y})\|^{-1}) \gg P^{3n-4K}.$$

这条引理在说什么。"如果 $S(\alpha)$ 大 (假设 13.3)，那么左边这个又长又怪的和必定也大 ($\gg P^{3n-4K}$)。"左边是对所有点对 $(\mathbf{x}, \mathbf{y})$ 求和，每项是 n 个 $\min(\dots)$ 的乘积。先读懂这个 $\min$ 。

$\min(P, \|6\alpha B_j\|^{-1})$ 是什么 它在两个数里取较小者：固定上限 P ，与 $\|6\alpha B_j\|^{-1} = 1/\|6\alpha B_j\|$ 。

- 当 $6\alpha B_j$ 很接近整数 ($\|6\alpha B_j\|$ 很小)， $1/\|\dots\|$ 很大，被 P 截住，取 P ；
- 当 $6\alpha B_j$ 离整数较远， $\|\dots\|$ 不小， $1/\|\dots\|$ 较小，取这个倒数。

这个量正是下一节那条"几何级数求和"估计的输出：一段长 $\leq P$ 的等差相位求和 $\sum_z e(\beta z)$ 的大小 $\ll \min(P, \|\beta\|^{-1})$ 。 $\min$ 越大，说明相位越"齐"、相消越少。所以引理左边大 = "存在很多点对让所有 B_j 都使相位齐整"。

证 (逐步补全 Weyl 两次差分)

1 第一次平方 (差分一次)。

$$|S(\alpha)|^2 = S(\alpha) \overline{S(\alpha)} = \sum_{\mathbf{z} \in P\mathfrak{B}} \sum_{\mathbf{z}' \in P\mathfrak{B}} e(\alpha C(\mathbf{z}') - \alpha C(\mathbf{z})).$$

这里用了 $\overline{e(\theta)} = e(-\theta)$ (共轭等于相位取负)，把 S 与其共轭相乘展成双重和。

2 换元 $\mathbf{z}' = \mathbf{y} + \mathbf{z}$ 。令 $\mathbf{y} = \mathbf{z}' - \mathbf{z}$ ，则

$$|S(\alpha)|^2 = \sum_{\mathbf{z} \in P\mathfrak{B}} \sum_{\mathbf{y} + \mathbf{z} \in P\mathfrak{B}} e(\alpha C(\mathbf{y} + \mathbf{z}) - \alpha C(\mathbf{z})).$$

"差分"二字就在这：被积相位从 C 本身变成了差 $C(\mathbf{y} + \mathbf{z}) - C(\mathbf{z})$ ，这是一个关于 $\mathbf{z}$ 的二次多项式（三次差一次降为二次），最高次降了一级。

- 3 把 $\mathbf{y}$ 提到外层、对内层取模长。对每个固定的 $\mathbf{z}$ ，"盒子 $P\mathcal{B}$ 平移 $-\mathbf{z}$ " 含于 $|\mathbf{y}| < P$ 之内（因为盒子边长 $\leq P$ ）。把 $\mathbf{y}$ 的范围放宽到 $|\mathbf{y}| < P$ 的公共部分（保证 $\mathbf{z}$ 和 $\mathbf{z} + \mathbf{y}$ 都在原盒子里）。

- 4 Cauchy 不等式再平方一次。Cauchy（柯西）不等式：

$\left| \sum_{k=1}^N a_k \right|^2 \leq N \sum_{k=1}^N |a_k|^2$ 。这里 $\mathbf{y}$ 的取值个数 $\ll P^n$ ，把它当作 N ：
 $|S(\alpha)|^4 = \left(\sum_{\mathbf{y}} e(\alpha C(\mathbf{y})) \right)^2 \leq N \sum_{\mathbf{y}} e(2\alpha C(\mathbf{y}))$ 线性。平方正好制造出"第二次差分"的机会。

- 5 第二次差分（对内层重复步骤 1-2）。内层 $\left| \sum_{\mathbf{z}} e(\dots) \right|^2$ 再展成关于新增变量 $\mathbf{x}$ 的双重和（ $\mathbf{z}$ 与 $\mathbf{z} + \mathbf{x}$ ）。结果其平方不超过

$$\sum_{|\mathbf{x}| < P} \left| \sum_{\mathbf{z} \in \mathcal{S}(\mathbf{x}, \mathbf{y})} e\left(\alpha(C(\mathbf{z} + \mathbf{x} + \mathbf{y}) - C(\mathbf{z} + \mathbf{x}) - C(\mathbf{z} + \mathbf{y}) + C(\mathbf{z}))\right) \right|^2$$

其中 $\mathcal{S}(\mathbf{x}, \mathbf{y})$ 是依赖 $\mathbf{x}, \mathbf{y}$ 的 $\mathbf{z}$ 盒子，各棱长 $\sim P$ （二阶混合差分）。

- 6 关键代数：二阶差分关于 $\mathbf{z}$ 是线性的。断言

$$C(\mathbf{z} + \mathbf{x} + \mathbf{y}) - C(\mathbf{z} + \mathbf{x}) - C(\mathbf{z} + \mathbf{y}) + C(\mathbf{z}) = 6 \sum_{i,j,k} c_{ijk} x_i y_j z_k + \dots$$

其中 ψ 不含 $\mathbf{z}$ 。为什么是这样、系数为何是 6：对一个三次型，做关于 $\mathbf{y}$ 的一阶差分 $C(\mathbf{z} + \mathbf{y}) - C(\mathbf{z})$ ，其含 $\mathbf{z}$ 二次的部分是 $3 \sum c_{ijk} y_i z_j z_k$ ；再做关于 $\mathbf{x}$ 的差分，把 $z_j z_k$ 换成

$(z_j + x_j)(z_k + x_k) - z_j z_k = x_j z_k + z_j x_k + x_j x_k$ ，其中含 $\mathbf{z}$ 一次的是 $x_j z_k + x_k z_j$ 。于是 $\mathbf{z}$ -线性项为 $3 \sum c_{ijk} y_i (x_j z_k + x_k z_j)$ ；利用 c_{ijk} 的对称性把两块都整理成 z_j 出头，合并得 $6 \sum c_{ijk} x_i y_k z_j$ 。系数 $6 = 2 \times 3$

正来自"两次差分各放出一个因子、再加对称排列"。其余项 ψ 全是 $\mathbf{x}, \mathbf{y}$ 的函数，不含 $\mathbf{z}$ 。最后按 j 归并 $\sum_{i,k} c_{ijk} x_i y_k = B_j(\mathbf{x} | \mathbf{y})$ 。

- 7 提出不含 $\mathbf{z}$ 的相位。 $e(\alpha\psi)$ 与 $\mathbf{z}$ 无关，模长为 1，可直接提到 $\mathbf{z}$ 求和外，不影响绝对值。于是内层关于 $\mathbf{z}$ 的和化为

$$\left| \sum_{\mathbf{z} \in \mathcal{S}(\mathbf{x}, \mathbf{y})} e\left(6\alpha \sum_j B_j(\mathbf{x} | \mathbf{y}) z_j\right) \right|.$$

相位对 $\mathbf{z}$ 已是线性——目标达成。

- 8 几何级数估计 ("现已熟悉的估计")。因为相位

$6\alpha \sum_j B_j z_j = \sum_j (6\alpha B_j) z_j$ 在各坐标 z_j 上分离，指数乘积拆成各坐标独立的几何级数之积：

$$\sum_{\mathbf{z}} e\left(\sum_j (6\alpha B_j) z_j\right) = \prod_j \left(\sum_{z_j} e((6\alpha B_j) z_j) \right).$$

单个几何级数 $\sum_{z_j} e(\beta z_j)$ (z_j 跑一段长 $\leq P$ 的连续整数, $\beta = 6\alpha B_j$) 的标准上界是 $\ll \min(P, \|\beta\|^{-1})$ (证明见下方小框)。于是

$$\left| \sum_{\mathbf{z} \in \mathcal{S}} e(6\alpha \sum_j B_j z_j) \right| \ll \prod_{j=1}^n \min(P, \|6\alpha B_j(\mathbf{x} | \mathbf{y})\|^{-1}).$$

- 9 回代汇总。把第 9 步代进第 5 步、再代进第 4 步 (全程只对 $|S|$ 平方两次：先 $|S|^2$ ，再经 Cauchy 得 $|S|^4$)，最终得到 $\ll \sum_{\mathbf{x}} |\mathbf{x}|^4$ ■

补证：几何级数 $\left| \sum_{z=0}^{N-1} e(\beta z) \right| \ll \min(N, \|\beta\|^{-1})$

- 1 若把它当 N 个模长 1 的数相加，三角不等式给上界 N 。这是 $\min$ 里的第一个候选。

2 当 β 不是整数时用等比数列求和: $\sum_{z=0}^{N-1} e(\beta z) = \frac{e(\beta N) - 1}{e(\beta) - 1}$ 。取模长, 分子 $|e(\beta N) - 1| \leq 2$, 分母 $|e(\beta) - 1| = 2|\sin \pi \beta|$ 。又有不等式 $|\sin \pi \beta| \geq 2\|\beta\|$ (正弦在到最近整数距离上的线性下界)。故

$$\left| \sum_z e(\beta z) \right| \leq \frac{2}{2|\sin \pi \beta|} \leq \frac{1}{2\|\beta\|} \ll \|\beta\|^{-1}.$$

这是第二个候选。

3 两个上界同时成立, 取较小者, 得 $\ll \min(N, \|\beta\|^{-1})$ 。直观: β 越接近整数, 相位转得越慢、相消越少、和越大 (趋于 N); β 离整数越远, 转得越快、相消越多、和越小 (趋于 $\|\beta\|^{-1}$)。■

原文译文

注. 在估计一个指数和时, 看一看平凡估计给出什么, 以判断 (如果有的话) 损失了多少 (永远地损失了), 是一种有用的预防措施。在当前情形中, 对乘积中始终取 P 作为最小值, 则 $|S(\alpha)|^4$ 的平凡估计将是 P^{4n} , 这是令人满意的。

这条注在提醒什么。 做估计前先"对账": 把不等式里每个 $\min$ 都取上限 P (最宽松情形), 看看会得到什么。这里乘积变成 P^n , 再对 P^n 个点对 $\mathbf{x}, \mathbf{y}$ 求和得 $P^n \cdot P^n \cdot P^n = P^{3n}$; 这对应 $|S(\alpha)|^4 \ll P^{4n}$, 即 $|S| \ll P^n$, 正是平凡估计, 没有出现荒谬 (比如 $|S|$ 被估得比 P^n 还大)。这说明引理 13.1 的不等式方向、量级都自洽, 没有"凭空多估"或"永远丢掉了不该丢的东西"。这是做解析数论的好习惯: 随时用平凡情形当"体检"。

6. 引理 13.2: 从"min 之和"到"小余项点对多"

原文译文

引理 13.2. 假设 (13.3) 蕴含：满足

$$|\mathbf{x}| < P, \quad |\mathbf{y}| < P, \quad \|6\alpha B_j(\mathbf{x} | \mathbf{y})\| < P^{-1}, \quad (1 \leq j \leq n) \quad (13.4)$$

的整点对 $\mathbf{x}, \mathbf{y}$ 的个数 $\gg P^{2n-4K}(\log P)^{-n}$ 。

这条引理在说什么、为什么要它。引理 13.1 的结论是个"加权和大"，但权重（那些 $\min$ ）是连续的、不好直接用。引理 13.2 把它翻译成一句更朴素的话：满足"所有 $\|6\alpha B_j(\mathbf{x} | \mathbf{y})\| < P^{-1}$ 点对个数很多 ($\gg P^{2n-4K}(\log P)^{-n}$)。从"加权和"过渡到"计数"，是为了后面能把它当成可数的几何对象处理。

$(\log P)^{-n}$ 是什么、为什么冒出来 $\log P$ 是自然对数，随 P 增长极慢（比任何 P^ε 都慢）。 $(\log P)^{-n} = 1/(\log P)^n$ 是一个"轻微的折损因子"。它来自下面证明里把连续权重 $\min(P, \cdot)$ 用"调和级数" $1 + \frac{1}{2} + \frac{1}{3} + \cdots \approx \log P$ 去打包时付出的代价。原文后面会说"这点损失不重要"——因为 $(\log P)^n$ 远小于任何 P^ε ，在量级比拼里可以忽略。

证（补全计数论证）

1 设 $Y(\mathbf{x}) =$ 对给定 $\mathbf{x}$ 满足 (13.4) 的 $\mathbf{y}$ 个数。目标是把引理 13.1 左边的和用 $Y(\mathbf{x})$ 控制住。

2 "鸽笼式"上界。把每个 $6\alpha B_j(\mathbf{x} | \mathbf{y})$ 的小数部分 $\{6\alpha B_j\} \in [0, 1)$ 按 $\frac{r_j}{P} \leq \{6\alpha B_j\} < \frac{r_j+1}{P}$ 分成 P 个等宽小格 ($r_j = 0, 1, \dots, P-1$)，并把 $\mathbf{y}$ 的每个坐标限制在一段长 P 的区间内。断言：落在某一组固定 $(r_1, \dots, r_n)$ 小格里的 $\mathbf{y}$ 个数 $\leq Y(\mathbf{x})$ 。

3 为什么 $\leq Y(\mathbf{x})$ (差分消格)。设 $\mathbf{y}'$ 是这组小格里某个固定点， $\mathbf{y}$ 是同组里任意点。两点在同一小格 $\Rightarrow$ 它们的 $\{6\alpha B_j\}$ 相差 $< 1/P$ ，于是 $\|6\alpha B_j(\mathbf{x} | \mathbf{y}) - 6\alpha B_j(\mathbf{x} | \mathbf{y}')\| < 1/P$ ，于是 $\|6\alpha B_j(\mathbf{x} | \mathbf{y})\| < \|6\alpha B_j(\mathbf{x} | \mathbf{y}')\| + 1/P < P^{-1} + 1/P < P^{-1}$ ，于是 $\mathbf{y}$ 满足 (13.4)。

$B_j(\mathbf{x}, \mathbf{y})$ 把绝对位置问题平移成相对位置问题的标准技巧。

4 把立方体切块、用 $Y(\mathbf{x})$ 控制加权和。把 $|\mathbf{y}|$

5 调和级数求和。单个坐标 $\sum_{r=0}^{P-1} \min(P, \frac{P}{r}, \frac{P}{r-1})$: $r = 0, 1$ 附近取 P , 其余取 P/r , 于是 $\approx P + P \sum_{r=1}^{P-1} \frac{1}{r} \approx P(1 + \log P) \ll P \log P$ 。 n 个坐标相乘得 $(P \log P)^n$ 。故 $|\sum \mathbf{y}|$

6 对 $\mathbf{x}$ 求和、代入引理 13.1。两边对 $|\mathbf{x}|$

7 解出计数。 $\sum_{\mathbf{x}} Y(\mathbf{x})$ 恰是满足 (13.4) 的点对 $(\mathbf{x}, \mathbf{y})$ 总数。于是

$$\#\{(\mathbf{x}, \mathbf{y}) \text{ 满足 (13.4)}\} = \sum_{\mathbf{x}} Y(\mathbf{x}) \gg \frac{P^{3n-4K}}{(P \log P)^n} = P^{2n-4K} (\log P)^n$$

得证。 ■

原文译文

注. 由于满足 (13.4) 的点对 $\mathbf{x}, \mathbf{y}$ 个数的平凡估计是 P^{2n} , 我们放弃了一个因子 $(\log P)^n$ 。但这并不重要。

这条注在说什么。又一次"对账"。点对 $(\mathbf{x}, \mathbf{y})$ 各自约 P^n 种, 总数平凡上界 P^{2n} 。我们的下界是 $P^{2n-4K} (\log P)^{-n}$ ——指数部分 $2n - 4K$ 比 $2n$ 小 (损失来自 K , 是真问题里不可避免的), 而 $(\log P)^{-n}$ 是额外多丢的一点点。作者明确说这 $(\log P)^n$ "不重要", 因为它比 P^ϵ 还小, 后面取 K 时留点余量就能吸收掉。

7. 引理 13.3: 把范围从 P 缩到 P^θ (两用几何数论)

原文译文

引理 13.3. 设 θ 与 P 无关且满足 $0 < \theta < 1$ 。假设 (13.3) 蕴含：满足

$$|\mathbf{x}| < P^\theta, \quad |\mathbf{y}| < P^\theta, \quad \|6\alpha B_j(\mathbf{x} | \mathbf{y})\| < P^{-3+2\theta} \quad (13.5)$$

的整点对 $\mathbf{x}, \mathbf{y}$ 的个数 $\gg P^{2n\theta-4K}(\log P)^{-n}$ 。

这条引理在说什么、为什么要它。引理 13.2 给出的是 "大盒子" $|\mathbf{x}|, |\mathbf{y}|$ 松余项 $\|6\alpha B_j\|$ 小盒子 (紧余项) (收缩"步骤, 靠两次调用第 12 章的几何数论缩放引理 (引理 12.6) 完成。

θ 是什么、为什么 $0 < \theta < 1$ θ 是一个固定的收缩指数 (与 P 无关)。 P^θ 比 P 小 (因 $\theta < 1$) 但仍趋于无穷 (因 $\theta > 0$)。它是一个可调旋钮：后面引理 13.4 会通过选 θ 来平衡"选项 A 的点对数"与"选项 B 的逼近质量"。

引理 12.6 (几何数论缩放引理) —— 本节的核心工具 我们不重证第 12 章, 只说清它说什么、怎么用。考虑一组满足对称性条件的线性型 L_j ("对称"指 L_j 中 y_k 的系数等于 L_k 中 y_j 的系数)。对一个缩放参数 Z , 定义不等式组 $|y_j| \leq Z$ 。引理 12.6 的结论：当把 Z 从大值 Z_2 缩小到小值 Z_1 ($Z_1 \leq Z_2$) 时,

$$N(Z_1) \gg \left(\frac{Z_1}{Z_2}\right)^n N(Z_2).$$

直观：盒子和余项同比例收缩 Z_1/Z_2 倍, 解数最多按"体积比" $(Z_1/Z_2)^n$ 下降——不会掉得更狠。这正是几何数论 (关于对称凸体里格点数的连续性) 保证的"缩放不吃大亏"。对称性条件不可少, 它保证了盒子与余项配成"自对偶"结构, 缩放才有这个干净的下界。

证 (两次应用引理 12.6, 逐步追指数)

第一次：固定 $\mathbf{x}$, 缩 $\mathbf{y}$ 。

- 1 认出线性型。固定 $\mathbf{x}$, 记 $L_j(\mathbf{y}) = 6\alpha B_j(\mathbf{x} | \mathbf{y})$ 。它关于 $\mathbf{y}$ 线性, 且满足对称性： L_j 中 y_k 的系数是 $6\alpha \sum_i c_{ijk} x_i$, 交换 j, k 时 (因 c_{ijk} 对称) 不

变。这正是引理 12.6 的前提。

2 把 (13.4) 摆成 12.6 的形状 ($Z_2 = 1$)。取

$a = P, Z_2 = 1, Z_1 = P^{-1+\theta}$ 。当 $Z = Z_2 = 1$: 盒子 $\set(|y_j|$ (此处用到 b 使 $bZ_2 = P^{-1}$ 。)

3 缩到 $Z_1 = P^{-1+\theta}$ 。盒子变 $\set(|y_j|$

4 对 $\mathbf{x}$ 求和。于是满足 $\set(|\mathbf{x}|$

第二次：固定 $\mathbf{y}$ ，缩 $\mathbf{x}$ 。现在 $\mathbf{y}$ 已缩到 $\set(|y_j|$

1 换角色认线性型。对每个 $\mathbf{y}$ ，把 (13.7) 看成关于 $\mathbf{x}$ 的系统，记 $M_j(\mathbf{x}) = B_j(\mathbf{y} | \mathbf{x})$ (即把 $\mathbf{x}, \mathbf{y}$ 角色对调，利用 B_j 的双线性对称)。(13.7) 即 $\set(|x_j|$

2 选缩放参数。这次取

$$a = P^{\frac{3}{2}-\frac{1}{2}\theta}, \quad Z = Z_2 = P^{-\frac{1}{2}+\frac{1}{2}\theta}, \quad Z_1 = P^{-\frac{3}{2}+\frac{3}{2}\theta}.$$

核对 Z_2 : 盒子 $\set(|x_j|$ 为什么这样取 a, Z_2 而不照搬上一次? 因为这一次的余项上界已经是 $P^{-2+\theta}$ (比第一次的 P^{-1} 紧), 要让"盒子边 $= aZ_2 = P$ 、余项 $= bZ_2 = P^{-2+\theta}$ "同时成立, a 与 Z_2 必须重新配比, 于是出现了 $\frac{3}{2}, \frac{1}{2}$ 这种半整数指数。参数是被"两端边界条件"逼出来的, 不是随手取的。

3 缩到 Z_1 。盒子 $\set(|x_j|$

4 对 $\mathbf{y}$ 求和收官。满足 (13.5) (即 $\set(|\mathbf{x}|, |\mathbf{y}|$ ■

回看这两步在干什么。从"大盒子松余项" (13.4) 到"小盒子紧余项" (13.5)，每缩一次都按几何数论付出 $P^{-n(1-\theta)}$ 的代价，但同时把范围收紧到 P^θ 、把余项收紧到 $P^{-3+2\theta}$ 。这就为引理 13.4 备好了弹药：在这么小、这么紧的系统里，要么 B_j 真的等于 0 (A)，要么逼出极好的有理逼近 (B)。

8. 引理 13.4：本章的总结论——非此即彼

原文译文

引理 13.4. 设 θ 与 P 无关且满足 $0 < \theta < 1$ 。设 ε 是任意小的固定正数。那么，或者

(A) 存在多于 $P^{n\theta+\varepsilon}$ 个满足

$$|\mathbf{x}| < P^\theta, \quad |\mathbf{y}| < P^\theta, \quad B_j(\mathbf{x}|\mathbf{y}) = 0, \quad (1 \leq j \leq n) \quad (13.8)$$

的整点对 $\mathbf{x}, \mathbf{y}$;

或者 (B) 对每个 α ，假设

$$|S(\alpha)| \geq P^{n-\frac{1}{4}n\theta+\varepsilon} \quad (13.9)$$

蕴含 α 有一个有理逼近 a/q 使得

$$(a, q) = 1, \quad 1 \leq q \ll P^{2\theta}, \quad |q\alpha - a| < P^{-3+2\theta}. \quad (13.10)$$

这条引理在说什么。本章的主结果，一个"二选一"（不是说有时 A 有时 B，而是说：对给定的三次型 C ，至少有一个分支永远成立）。

选项 (A)

三次型 C 自身的性质：双线性型 B_j 有"异常多"的公共零点对 $(\mathbf{x}, \mathbf{y})$ （多于 $P^{n\theta+\varepsilon}$ 个，比"正常的 $P^{n\theta}$ 量级"还多一个 P^ε 因子）。注意 (A) 完全不含 α ——它

是几何/代数性质。

选项 (B)

关于指数和的结论：只要 $S(\alpha)$ 还算大 (13.9)， α 就必定非常靠近一个分母 $q \ll P^{2\theta}$ 的最简分数 a/q ，逼近误差 $\backslash(|q\alpha - a| \cdot (a, q) = 1: a, q$ 互素（最简分数，没有可约的公因子）。

· $1 \leq q \ll P^{2\theta}$ ：分母 q 不超过 $P^{2\theta}$ 量级——"小分母"。分母越小，分数 a/q 越"特殊"、越稀疏。

· $\backslash(|q\alpha - a|$

证 (如何从引理 13.3 逼出二选一)

1 把 K 取成与 (13.9) 匹配。在 (13.3) 里取 $K = \frac{1}{4}n\theta - \varepsilon$ ，则 $P^{n-K} = P^{n-\frac{1}{4}n\theta+\varepsilon}$ ，于是 (13.3) 与 (13.9) 是同一条假设。这一步是把可调参数 K 钉死，让前面引理的输出对接到本引理要的形式。

2 引理 13.3 给出大量满足 (13.5) 的点对。代 $K = \frac{1}{4}n\theta - \varepsilon$ ：

$$\#(13.5) \gg P^{2n\theta-4K}(\log P)^{-n} = P^{2n\theta-(n\theta-4\varepsilon)}(\log P)^{-n} = P^{n\theta+4\varepsilon}$$

最后一步： $P^{4\varepsilon}(\log P)^{-n} \gg P^\varepsilon$ ，因为 $P^{3\varepsilon}$ 远大于 $(\log P)^n$ （多项式吃掉对数）。所以满足 (13.5) 的点对多于 $P^{n\theta+\varepsilon}$ 个。

3 二分。看这一大堆满足 (13.5) 的点对，问：是否所有点对都让所有 j 满足 $B_j(\mathbf{x} | \mathbf{y}) = 0$ ？

· 若是：那这些点对全都满足 (13.8)（注意 (13.8) 的盒子约束 $\backslash(|\mathbf{x}|, |\mathbf{y}| \leq P^{n\theta+\varepsilon})$ ），选项 (A) 成立。

4 · 若不是：则存在某个满足 (13.5) 的点对 $(\mathbf{x}, \mathbf{y})$ 和某个 j ，使 $B_j(\mathbf{x} | \mathbf{y}) \neq 0$ 且（由 (13.5) 第三条） $\backslash(|\mathbf{x}|, |\mathbf{y}| \leq P^{n\theta+\varepsilon})$

$$B_j(\mathbf{x}, \mathbf{y})$$

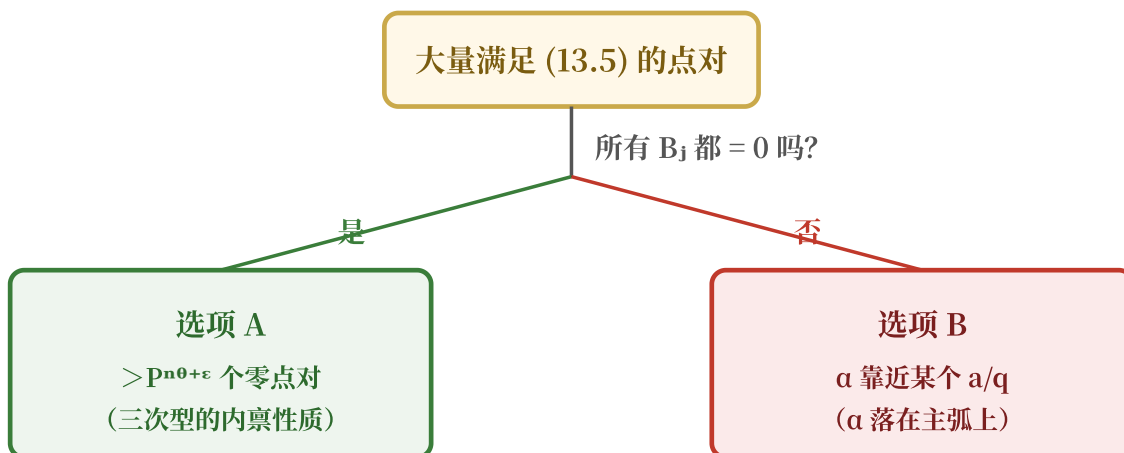
5 造 q 与 a 。取 $q = 6|B_j(\mathbf{x} | \mathbf{y})|$ (正整数, 因 $B_j \neq 0$ 、且 c_{ijk} 整数使 B_j 是整数), 取 a 为最接近 $q\alpha$ 的整数。则 $||q\alpha - a| = |6\alpha B_j|$

6 估 q 的大小。

$$q = 6|B_j(\mathbf{x} | \mathbf{y})| \ll \left| \sum_{i,k} c_{ijk} x_i y_k \right| \ll \sum_{i,k} |c_{ijk}| |x_i| |y_k| \ll |\mathbf{x}| |\mathbf{y}| \ll$$

其中 $|c_{ijk}|$ 是固定常数 (被 $\ll$ 吸收), $(|x_i| \leq |\mathbf{x}|)$

7 化简成最简分数。此时未必 $(a, q) = 1$, 但把 a, q 的公因子一并约掉, 得到的新 a/q 仍满足三条 (约分只会让 q 更小、 $|q\alpha - a|$ 更小)。于是选项 (B) 成立。 ■



引理 13.4 的逻辑: 一旦 $S(\alpha)$ 够大, 要么三次型本身有异常多双线性零点 (A), 要么 α 必在某个小分母分数附近 (B)。

9. 收尾的注: 两个选项各意味着什么

注. 可以看出选项 A 并不涉及 α 。它本质上也不涉及 θ ，因为若我们令 $R = P^\theta$ ，则其断言为：满足

$$|\mathbf{x}| < R, \quad |\mathbf{y}| < R, \quad B_j(\mathbf{x}|\mathbf{y}) = 0, \quad (1 \leq j \leq n) \quad (13.11)$$

的点对 $\mathbf{x}, \mathbf{y}$ 的个数大于 $R^{n+\varepsilon'}$ (对某个固定的 $\varepsilon' > 0$)。于是选项 A 关系到三次型的一个内禀性质。注意，如果我们愿意，可以从 (13.11) 中排除 $\mathbf{x} = \mathbf{0}$ 和 $\mathbf{y} = \mathbf{0}$ ，因为这类点对的个数 $\ll R^n$ 。

这条注在说什么。把选项 A "去掉伪装"，看清它的真实身份。

"不涉及 α "

(13.8) 里根本没有 α ，纯粹是问双线性型 B_j 有多少公共零点。所以 A 是三次型 C 自带的代数事实，与圆法的旋钮 α 无关。

"也不涉及 θ "

令 $R = P^\theta$ ，断言变成"在边长 R 的盒子里， B_j 的公共零点对多于 $R^{n+\varepsilon'}$ 个"。 θ 只是把 P 换了个名字成 R ，本质条件与 θ 无关——只跟"盒子大小 R "有关。这说明 A 是个纯几何计数命题。

"内禀性质"

"零点对多于 $R^{n+\varepsilon'}$ "是反常的：正常情况下， n 个方程 $B_j = 0$ 应把 $2n$ 维的 $(\mathbf{x}, \mathbf{y})$ 空间切到 n 维，零点对约 R^n 个；若多出 $R^{\varepsilon'}$ 倍，说明这些方程"退化"、三次型有特殊的几何结构。第 14 章正是要分析这种退化三次型。

"排除 $\mathbf{x} = \mathbf{0}$ 或 $\mathbf{y} = \mathbf{0}$ "

当 $\mathbf{x} = \mathbf{0}$ 时 $B_j(\mathbf{0}|\mathbf{y}) = 0$ 自动成立，这种"平凡零点对"有 $\ll R^n$ 个；同理 $\mathbf{y} = \mathbf{0}$ 。它们远少于 $R^{n+\varepsilon'}$ ，可以放心剔除而不影响 A 的断言——保证 A 里那些"异常多"的零点对是真有内容的非平凡零点。

原文译文

注 (续)。选项 B 给出了一个原则上与我们在前几章中已经熟悉的情形类似的局面。它将使我们能够在第 15 章中令人满意地估计由一大类 α 对

$\int_0^1 S(\alpha) d\alpha$ 所作的贡献，并留给我们相对较少的若干短区间，在其上我们可以逼近 $S(\alpha)$ 。

这条注在说什么、本章如何接到后面。选项 B 的形状 (" S 大 $\Rightarrow \alpha$ 靠近小分母 a/q ") 正是前面华林问题各章里 Weyl 不等式给出的同款结论——所以"原则上熟悉"。它的用处是实现主弧/次弧二分：

承上启下：

- 1 由 B，凡是 $S(\alpha)$ 大的 α ，都被关进"小分母分数 a/q 的窄邻域"里。这些窄邻域就是主弧，数量不多（小分母 q 的分数稀疏）、总长很短。
- 2 主弧之外的所有 α （次弧）， $S(\alpha)$ 必定小（否则就该被关进主弧）。于是次弧对积分 $\int_0^1 S(\alpha) d\alpha$ 的贡献低于 P^{n-3} 阶，可整体丢弃——这正是第 15 章要做的"令人满意地估计一大类 α 的贡献"。
- 3 剩下的只有"相对较少的若干短区间"（主弧），在其上 $S(\alpha)$ 可以被一个干净的近似公式代替，进而算出主项 cP^{n-3} （第 15–17 章）。
- 4 至于选项 A（三次型退化的情形），第 14 章专门处理：证明若 B_j 有异常多零点，三次型必含一个可解的子结构，照样能找出解。两条分支殊途同归，主定理得证。

10. 全章脉络一句话总结

本章把"三次方程有没有整数解"翻译成"指数和 $S(\alpha)$ 的积分"，再用两次 Weyl 差分把三次降为线性（引理 13.1），用鸽笼计数把加权和变成点对计数（引理 13.2），用两次几何数论缩放把范围收紧到 P^θ （引理 13.3），最终逼出

一个干净的二选一（引理 13.4）：要么三次型自身退化（选项 A，交给第 14 章），要么大 S 的 α 必在主弧上（选项 B，交给第 15 章）。这就为后续的主弧/次弧分析铺好了全部地基。

返回 [全书目录](#)