整数剩余环 Zn 上的 Falconer 距离逆定理 Z_n

Shalender Singh*[1], Vishnu Priya Singh[2]

摘要

我们为整数剩余环上的二次距离像确立了一个理想论刚性原理。具体而言，我们证明，在 Z_n^d 中，距离集近极值地坍缩会迫使其具有强代数结构，而这种结构由源自 n 算术性质的湮灭子子模支撑。

由此，我们得到关于合数模数下 Z_n 上 Falconer 距离问题的第一个逆定理。我们证明，若集合 $E \subset Z_n^d$ 的大小为 $|E| \asymp n^{(d+1)/2}$，且只能确定 $O(n)$ 个不同的平方距离，那么 E 必须由某个湮灭子子模的陪集支撑，并且距离型在该子模上代数退化。

证明引入了 Z_n 中固有的因子深度分解，以及一种提升机制，可将素数模数下的局部退化转化为全局理想论约束。由此，我们完整分类了环情形下 Falconer 距离问题的近极值集，揭示出一种在域上没有类似现象的刚性现象。

关键词：Falconer 距离问题、逆定理、整数剩余环、中国剩余定理、结构提升、多项式恒等式测试、算术刚性。

1. 引言

Falconer 距离问题探讨集合 E 需要多大，才能确保其距离集 $\Delta(E) = \{||x-y||^2 : x, y \in E\}$ 具有结构上的重要性（例如具有正测度或较大的基数）。该问题由 Falconer 在连续情形下提出[6], , 现已成为几何测度论的基石，并与傅里叶分析和限制理论建立了深刻联系；Mattila [7] 和 Wolff [8], 的工作以及近期对l^2 解耦猜想[4]的解决进一步推动了这一领域的发展。

在离散情形下，该问题转化为确定 $E \subset \mathbb{F}_q^d$ 需要多大，才能使 $\Delta(E)$ 包含域中一个正比例的元素。Iosevich 和 Rudnev [3] 建立了尖锐的正向界，Hart 等人 [9] 对其进行了改进。然而，逆问题——刻画那些无法生成预期数量距离的集合——仍远未得到充分理解。最近，Singh 和 Parmar [1, 2] 利用结构提升和多尺度能量分解的方法，针对有限域 $\mathbb{F}_q$ $(d \geq 3)$ 研究了这一问题，证明近极值集合必须集中在次数有界的代数簇上。

1.1. 环论上的差距

文献中仍存在一个关键空白。现代算术组合学和基于格的密码学大多并非在域上，而是在整数剩余环 Z_n 上进行，其中 n 是一个合数。Z_n^d 的几何性质与 $\mathbb{F}_q^d$ 截然不同，因为零因子的存在会破坏标准的几何直觉——直线会相交于多个点，球面也可能退化或可约 [10, 11]。因此，在域中发现的“代数簇”障碍不足以描述环中的困难性。

尽管关于环上距离集的正向结果已有所出现 [10], ，但目前尚无对 $\mathbb{Z}_n$ 中近极值集合的严格分类。现有的几何工具无法处理由 n 的因子所诱导的算术分层。

1.2. 主要结果

本文通过证明模 $\mathbb{Z}_n^d$ 上的第一个 Falconer 逆定理，弥合了这一差距。我们证明，在域中观察到的“代数刚性”可推广为环中的“理想论刚性”。

定理 1.1（$\mathbb{Z}_n$ 中的 Falconer 逆定理）

设 n 是一个合数，且 $E \subset \mathbb{Z}_n^d$ 是满足 $|E| \asymp n^{(d+1)/2}$ 的集合。假设 E 确定的平方距离数量近乎最小，即 $|\Delta(E)| \ll n$。

那么，E 表现出代数刚性：存在一个非平凡的湮灭子理想 $I \subset \mathbb{Z}_n$，以及一个由 I 个子模 M 生成的子模 $x + M \subset \mathbb{Z}_n^d$ 的陪集，使得 E 中有正比例的元素包含于 $x + M$ 中，并且平方距离型限制在 M 上时是退化的。

特别地，$\mathbb{Z}_n$ 上 Falconer 距离问题的近极值集，恰好是支撑在由 n 的素因数分解确定的湮灭子子模上的那些集合。定理 *5.1* 给出了完整的结构分类。

该结果证实了以下猜想，该猜想提出于 [1]: **猜想 1.2（内在误差理想猜想——环版本 [1]）**。

设 R 是有限交换环，且 $Q: \mathrm{R}^d \to \mathrm{R}$ 是一个二次型。若大小为 $|E| \approx |\mathrm{R}|^{(d+1)/2}$ 的集合 $E \subset \mathrm{R}^d$ 满足 $|Q(E)| \ll |\mathrm{R}|$，则 E 必须集中在子模 M 的某个陪集上，其中 Q 是退化的。此外，M 必须是 R 中某个元素的湮灭子理想，这反映了在含有零因子的环中区分结构与随机性的计算困难性。

定理 5.1 证明了当 $\mathrm{R} = \mathbb{Z}_n$ 且 Q 为平方距离型时，这一猜想成立。

1.3. 方法论：结构提升与多项式恒等式刚性

我们的证明融合了两种不同的方法。首先，我们改造了 [2], 中的多尺度能量分解，以“算术因子尺度”取代有限域中使用的“二进几何尺度”。在 $\mathbb{Z}_n$ 中，能量的自然分层依据并非空间邻近程度，而是代数深度——差向量 $x - y$ “被零整除”的程度。

其次，我们采用结构提升算子，将来自素域 $\mathbb{F}_p$ 的局部障碍“提升”出来。根据中国剩余定理，集合 $E \subset \mathbb{Z}_n$ 投影为集合 $E_p \subset \mathbb{F}_p$。我们证明，如果全局能量较高，那么局部投影 E_p 必须在 $\mathbb{F}_p$ 中近极值，从而通过有限域逆定理 [2] 将它们限制在低次数簇 V_p 中。随后，提升算子将这些局部约束重构为 $\mathbb{Z}_n$ 中的一个全局理想。

最后，为了刻画这些全局理想，我们借鉴算术多项式恒等式测试的原理。我们将距离函数视为多项式映射，并证明要使其像集较小，其定义域必须位于某种代数结构中，使得该多项式实际上恒等于零。

1.4 组织结构

第2节构造了适用于 $\mathbb{Z}_n$ 的算术能量泛函和因子尺度分解。第3节介绍结构提升算子，并证明较高的全局能量会迫使素域中出现局部刚性，进而提升为子模集中。第 4 节通过多项式恒等式测试和计算复杂性给出另一种刻画。第5节将这些结果结合起来，得到主要分类定理。第6节总结全文，并介绍应用和开放问题。

记号：

本文中，我们使用以下渐近记号：• $f \ll g$ （等价地，$f = O(g)$）表示，对于某个绝对常数 C，有 $|f| \le C \cdot g$。• $f \approx g$ 表示对于常数 $0 < c \le C$，有 $c \cdot g \le f \le C \cdot g$。• $f \gg g$ 表示，对于某个绝对常数 $c > 0$，有 $f \ge c \cdot g$。• 涉及参数时，我们写作 $f = O_d(g)$，表示隐含常数可能依赖于维数 d。

具体而言：
• $|E| \approx n^{(d+1)/2}$表示$c_d \cdot n^{(d+1)/2} \le |E| \le C_d \cdot n^{(d+1)/2}$。• $|\Delta(E)| \ll n$ 表示对于一个较小的绝对常数 C（例如 $C \le 1/10$），有 $|\Delta(E)| \le C \cdot n$。• $\mathrm{E}_n(E) \gg |E|^4/n$ 表示对于近极值常数 $K \ge 2$，有 $\mathrm{E}_n(E) \ge K \cdot |E|^4/n$。

2. 算术能量泛函与因子尺度

本节将 [2] 中为有限域建立的关联能量形式推广到环情形 $\mathbb{Z}_n$。环中的主要障碍是零因子的存在，它们会使非平凡向量的范数为零，或使其坍缩到低维子模中。

2.1. 算术关联能量

设 n 为一个合数。定义距离映射 $\Delta: \mathbb{Z}_n^d \times \mathbb{Z}_n^d \to \mathbb{Z}_n$ by$\Delta(x, y)$
$= \| x - y \|^2 = \sum_{i=1}^{d} (x_i - y_i)^2$(模 n)。

定义 2.1（算术关联能量）。

对于有限集合 $E \subset \mathbb{Z}_n^d$，E 的算术关联能量 $\mathrm{E}_n(E)$是保持模 n 的平方距离的四元组 $(x, y, z, w) \in E^4$ 的数量：

$$\mathcal{E}_n(E) := |\{(x, y, z, w) \in E^4 : \|x - y\|^2 \equiv \|z - w\|^2 \pmod{n}\}|$$

注意：这包括 $x = y$and $z = w$ 时的对角贡献，该贡献等于 $|E|^2$。“非平凡”能量为 $\mathrm{E}_n(E) - |E|^2$。
等价地，令 $\nu_E(t)$ 表示距离 $t \in \mathbb{Z}_n$ 的重数：

$$\nu_E(t) := |\{(x, y) \in E^2 : \|x - y\|^2 \equiv t \pmod{n}\}|$$

于是由标准的L^2 恒等式：

$$\mathcal{E}_n(E) = \sum_{t\in\mathbb{Z}_n} \nu_E\,(t)^2 = \| \nu_E \|_2^2$$

在距离集大小$|\Delta(E)|$较小（具体为$|\Delta(E)| \ll n$）的“近极值”情形下，柯西-施瓦茨不等式表明$\mathrm{E}_n(E)$必定很大：

$$\mathcal{E}_n(E) \geq \frac{|E|^4}{|\Delta(E)|} \gg \frac{|E|^4}{n}$$

2.2. 多尺度因子分解

在有限域中，重叠能量按共享关联数分层。在环中，自然的分层方式是代数性的：差向量落入 Z_n 的理想结构的“深度”如何。

定义 2.2（因子尺度分解）。

设 $D(n)$ 为 n 的因子集合。对于任意一对 $(x,y) \in E^2$，我们将其尺度 $k(x,y)$ 定义为满足向量差 $x-y$ 模 k 为零的最大因子 $k \mid n$：

$$k(x,y) := \max\{k \in D(n) : x \equiv y \pmod{k}\}$$

（注意：这检查的是逐坐标同余。）

我们将总能量 $\mathrm{E}_n(E)$ 分解为因子能量层 $\{\mathrm{E}^{(k)}\}_{k|n}$：

$$\mathrm{E}^{(k)}(E) := \#\{(x,y,z,w) \in E^4 : \|x-y\|^2 \equiv \|z-w\|^2 \pmod{n}, \text{ and } k(x,y) = k(z,w) = k\}$$

例 2.3。

考虑 $n = 6 = 2\cdot 3$ 和 $d = 2$。

令 $E = \{(0,0), (2,0), (3,0), (0,2)\} \subset \mathrm{Z}_6^2$。距离集为 $\Delta(E) = \{0,4,3\}$（模 6）。

注意 $|\Delta(E)| = 3 \ll 6$。根据中国剩余定理，$\mathrm{Z}_6 \cong \mathrm{Z}_2 \times \mathrm{Z}_3$，，因此 E 的投影为：
- $E_2 =$ 0,0 1,0 $\subset$ $\frac{2}{2}$ {( ), ( )} Z {( ), ( ),( )} $\subset \mathrm{Z}_3^2$
- $E_3 =$ 0,0 2,0 0,2

我们有 $|\Delta(E_2)| = \{0,1\}$以及 $|\Delta(E_3)| = \{0,1,1\} = \{0,1\}$。两个投影都集中在坐标子空间（仿射子空间）上，体现了坍缩机制。

引理 2.1（能量分层）。

$$\mathcal{E}_n(E) = \sum_{k|n} \mathcal{E}^{(k)}(E) + \mathcal{E}_{mixed}$$

其中，E_{mixed} 包含不同尺度之间的交叉项。

2.3. 通过中国剩余定理传递能量

设 $n = p_1 p_2 \ldots\ldots p_r$ 为一个无平方因子整数。根据中国剩余定理（CRT），存在一个环同构 Φ: $\mathrm{Z}_n \to \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_r}$。设 $\pi_i \colon \mathrm{Z}_n \to \mathbb{F}_{p_i}$ 为典范投影。对于集合 $E \subset \mathrm{Z}_n^d$，令 $E_i = \pi_i(E) \subset \mathbb{F}_{p_i}^d$。

引理 2.2（中国剩余定理能量乘积）。

设 $E \subset \mathrm{Z}_n^d$ where $n = p_1 \ldots p_r$。若 E 是笛卡尔积集合 $E = A_1 \times \cdots \times A_r$，且同构由中国剩余定理给出（其中 $A_i \subset \mathbb{F}_{p_i}^d$），则算术能量可完美分解为：

$$\mathcal{E}_n(E) = \prod_{i=1}^{r} \mathcal{E}_{p_i}(A_i)$$

其中 $\mathrm{E}p_i$ 是有限域 $\mathbb{F}_{p_i}$ 上的标准关联能量。

证明。

设 $\mathbf{x}, \mathbf{y} \in E$。根据中国剩余定理，我们将 $\mathbf{x} \leftrightarrow$ 识别为 $(x^{(1)}, \ldots, x^{(r)})$，其中 $x^{(i)} \in A_i$。同余条件成立当且仅当它在各分量上分别成立：

$$\| \mathbf{x} - \mathbf{y} \|^2 \equiv \| \mathbf{z} - \mathbf{w} \|^2 \pmod{n} \iff \forall i, \| x^{(i)} - y^{(i)} \|^2 \equiv \| z^{(i)} - w^{(i)} \|^2 \pmod{p_i}$$

定义 $\mathbb{F}_{p_i}$ 中距离约束的示性函数：
$\mathbb{I}_i(a, b, c, d) = 1$ 若距离相等则取该值，否则为 0。

$$\mathcal{E}_n(E) = \sum_{\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{w} \in E} \prod_{i=1}^{r} \mathbb{I}_i\left(x^{(i)}, y^{(i)}, z^{(i)}, w^{(i)}\right) = \prod_{i=1}^{r} \mathcal{E}_{p_i}(A_i)$$

□

推论 2.2.1（提升原理）。

如果 E 不是乘积集，那么较高的全局能量 $\mathrm{E}n(E)$ 仍意味着投影到 $\mathbb{F}_{p_i}$ 上的加权投影必须具有较高能量。具体而言，如果 $\mathrm{E}n(E) \gg \frac{|E|^4}{n}$，则至少存在一个素因子 $p \mid n$，使得投影 E_p 在 $\mathbb{F}_p$ 中是近极值的。这种局部刚性为我们在第3节中的结构提升提供了基例。

3. 结构提升与理想刚性

在此 本节中，我们将 [1] 中引入的结构提升算子应用于环情形 .

3.1. Z_n中的提升算子

设 $n = p_1 \dots p_k$ 无平方因子。中国剩余定理诱导出自然投影 π_p: $\mathrm{Z}_n^d \to \mathbb{F}_p^d$。

定义 3.1（一致性包）。

一致性包是一个局部代数约束元组 $\mathcal{V} = (V_{p_1}, \dots, V_{p_k})$，其中每个 $V_{p_i} \subset \mathbb{F}_{p_i}^d$ 都是次数为 $\leq \delta$的代数簇。提升结构 $\mathrm{L}(\mathcal{V})$ 是 Z_n^d 中同时满足每个局部约束的点的集合：

$$\mathcal{L}(\mathcal{V}) := \{x \in \mathbb{Z}_n^d : \pi_{p_i}(x) \in V_{p_i} \text{ for all } i = 1, \dots, k\}$$

从几何角度看，$\mathrm{L}(\mathcal{V})$ 对应于由局部定义多项式的提升所生成的理想的零点集。

3.2. 由局部极值性导出的全局刚性

定理 3.1（通过局部近极值性实现的全局刚性）。

设 $n = p_1 \dots p_k$ 是一个无平方因子合数。假设 $E \subset \mathrm{Z}_n^d$ 满足高能量条件：

$$\mathcal{E}_n(E) \geq K \cdot \frac{|E|^4}{n}$$

其中$K \gg 1$ 是近极值参数。于是存在素因子的一个非空子集$\mathcal{P} \subseteq \{p_1, \dots, p_k\}$，使得对每个$p \in \mathcal{P}$，投影$E_p = \pi_p(E)$都是$\mathbb{F}_p^d$中的近极值集合，满足$\mathrm{E}p(E_p) \geq K^{1/k} \cdot \frac{|E_p|^4}{p}$。因此，由有限域逆定理[2], ，对每个$p \in \mathcal{P}$，存在一个有界次数的非平凡代数簇$V_p \subset \mathbb{F}_p^d$，使得$E_p$ 集中于V_p。

证明。

步骤 1：通过中国剩余定理分解。

条件$\| \mathbf{x} - \mathbf{y} \|^2 \equiv \| \mathbf{z} - \mathbf{w} \|^2 \pmod{n}$等价于模每个$p_i$的条件组。

步骤 2：乘积情形。

若$E = \prod A_i$，则$\mathrm{E}n(E) = \prod \mathrm{E}p_i(A_i)$。假设$\mathrm{E}n(E) \geq K \frac{|E|^4}{n}$ 蕴含$\prod (\mathcal{E}_{p_i}(A_i) |A_i|^4/p_i) \geq K$。由抽屉原理，至少有一个因子必须超过$K^{1/k}$。

步骤 3：通过纤维分解处理一般情形。

我们定义有效最大纤维重数 $M = \max_{\mathbf{v}} |\{x \in E : \pi(x) = \mathbf{v}\}|$。（注意：根据抽屉原理，我们将 E 限制在一个子集 $E' \subseteq E$ 中，其中 $|E'| \geq c|E|$，使得纤维大小在相差不超过 2 倍的范围内保持一致。我们滥用记号，将这个子集称为 E。）

我们通过纤维分析建立能量界。对于投影的乘积中的每个元组 $(\mathbf{v},\mathbf{v}',\mathbf{u},\mathbf{u}')$，令 $F_{\mathbf{v}} = \{x \in E\colon \pi(x) = \mathbf{v}\}$ 表示其纤维。于是：

$$\mathcal{E}_n(E) = \sum_{\mathbf{v},\mathbf{v}',\mathbf{u},\mathbf{u}'} |F_{\mathbf{v}}| \cdot |F_{\mathbf{v}'}| \cdot |F_{\mathbf{u}}| \cdot |F_{\mathbf{u}'}| \cdot \mathbb{I}(\mathbf{v},\mathbf{v}',\mathbf{u},\mathbf{u}')$$

对纤维权重应用 Holder 不等式：

$$\leq (\max_{\mathbf{v}} |F_{\mathbf{v}}|)^4 \cdot \sum \mathbb{I}(\dots) = M^4 \prod_{i=1}^{k} \mathcal{E}_{p_i}(E_i)$$

代入 $\mathrm{E}n(E) \geq K\frac{|E|^4}{n}$ 并消去 M^4 （因为 $|E| \approx M\prod |E_i|$），得到与步骤 2 相同的乘积不等式。因此，局部能量必须很大。

步骤 4：运用有限域刚性。
我们应用 [2] 中的定理 3.4。输入：一个能量较高的集合 E_p。输出：一个次数为 O（$(K')^C$）的簇 V_p。

□

3.3. 从簇到子模

引理 3.2（子模集中）。

设 $n = p_1 \dots p_k$。假设 $E \subset \mathrm{Z}_n^d$ 是一个集合，其投影 E_{p_i} 集中在簇 V_{p_i}上。若全局距离集 $|\Delta(E)|$ 较小（具体而言，$|\Delta(E)| \ll n$），则每个局部簇 V_{p_i} 都必须是仿射子空间或各向同性锥。因此，E 集中在子模 $M \subset \mathrm{Z}_n^d$的一个陪集上。

证明。

我们首先证明，全局距离集的大小控制着局部距离集。

断言： 若 $|\Delta(E)| \ll n$，则对于至少 $\lfloor k/2 \rfloor$ 个素因子，有 $|\Delta(E_{p_i})| \ll p_i$。

断言的证明： 反设对于一组素数 L（其中 L / ），

| Δ E_{p_i} | |≥ ( ) |≥ $c \cdot p_i$。定义映射

$\lfloor k \ 2 \rfloor + 1$

$$\phi\colon \Delta(E) \to \prod_{i=1}^{k} \Delta(E_{p_i})$$

通过自然的中国剩余定理投影 $t \mapsto (t \bmod p_1, \dots, t \bmod p_k)$。由于子集的中国剩余定理提升并不唯一，$\phi$ 不一定是单射；不过，像的基数受到“较大”坐标的约束。积环中的标准和集增长估计表明，如果投影既大又稠密，那么全局和集的规模就会增长为显著因子的乘积（但会因结构而有所损失）。由此得到一个下界

$$|\Delta(E)| \gtrsim \prod_{i \in \mathcal{L}} |\Delta(E_{p_i})|^{1/2}.$$

由于 $| \quad | \approx k \ 2, \quad n^{1/2+\epsilon} \quad | \Delta \ E \ | \mathrm{L} /$ 这一乘积的尺度为，这 $\ll n \quad | \Delta \ E \ | \quad n$ 与近极小假设（）相矛盾（尤其是在（）接近平凡界，或较大时）。因此，大多数局部距离集都很大的假设必定不成立。△

回到主要证明：对于满足 $|\Delta(E_{p_i})| \ll p_i$ 的“重”素数，集合 $E_{p_i} \subset \mathbb{F}_{p_i}^d$ 生成的距离数相对于域的大小而言很少。在有限域几何中，生成退化距离集（基数为 $O(1)$ 或 $\ll p$）的簇不可能是一般超曲面（如标准球面）。它必须是仿射子空间或各向同性锥（二次型在其上消失的簇）。

根据中国剩余定理，这些线性／各向同性结构的笛卡尔积可提升为环 $\mathbb{Z}_n^d$ 中的一个子模（一个理想生成的格）。

□

4. 多项式恒等式测试与算术刚性

本节将运用算术多项式恒等式测试原理，给出一种互补的刻画。这证实了这些几何障碍根植于该环的代数复杂性。

4.1. 距离多项式

令 $P(\mathbf{x}, \mathbf{y}) = ||\mathbf{x} - \mathbf{y}||^2$。由于 $|\Delta(E)|$ 很小，这些值落在一个小集合 $S \subset \mathbb{Z}_n$ 中。构造湮灭多项式 $Q(T) = \prod (T - s)_{s \in S}$。那么复合多项式 $\Psi(\mathbf{x}, \mathbf{y}) = Q(P(\mathbf{x}, \mathbf{y}))$ 满足：对所有 $\mathbf{x}, \mathbf{y} \in E$，都有 $\Psi(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod{n}$。

4.2. 多项式恒等式刚性

在算术电路和恒等式测试理论中，在环 $\mathbb{Z}[5, 12]$, 上验证多项式恒等式$_n$ 通常是对结构刚性的测试。

定理 4.1（环中的多项式刚性）。

设 $\Psi \in \mathbb{Z}_n[x_1, \ldots, x_{2d}]$ 是一个次数为 D的多项式。设 $E \subset \mathbb{Z}_n^d$ 是一个集合，使得对于所有 $\mathbf{x}, \mathbf{y} \in E$，都有 $\Psi(\mathbf{x}, \mathbf{y}) \equiv 0$(模 n)。如果 $|E| > D^d$ 且 n 是合数，则 E 必包含于某个非平凡理想 J的零点集中。具体而言，如果 Ψ 是距离湮灭多项式，则 E 必包含于形如 $\mathbf{v} + \mathrm{Ann}(k)$ 的各向同性陪集的并集中。

证明。

1. **投影：**对所有 $p \mid n$，$\Psi \equiv 0$（模 n）$\implies$ $\Psi \equiv 0$（模 p）。2. **域刚性：**我们分别将该结果应用于每个素因子。在 $\mathbb{F}_p$ 中，Schwartz-Zippel引理指出，如果一个次数为 D 的非零多项式 Ψ_p 在随机集上取值为零，那么

概率为 $\leq D/p$。因此，如果 $|E_p|^2 > D \cdot p$，则该集合必定包含在簇 Z（Ψ_p）中。3. **距离多项式的非平凡性：**由于 Ψ 是从欧几里得距离形式推导得出的

，

其首项系数都是单位。因此，Ψ 不是 $\mathrm{Z}_n[X]$ 中的零多项式。4. **各向同性：**如引理 3.2 所示，若距离多项式在某个簇上恒为零，则该簇必须是各向同性的。5. **提升：**这意味着近似间隙由某个各向同性子模的理想生成，与 [1] 的框架一致。

□

4.3. 与计算复杂性的联系

“E 是否生成较少的距离？”这一问题等价于“距离多项式是否在 $E \times E$ 上近似为零？”在域的情形下，这是一个多项式恒等式测试问题，并且存在高效算法。在环的情形下，零因子的存在使该问题在标准密码学假设 [12] 下成为 NP 困难问题。我们的结构定理可作为一份“困难性证书”：距离较少的集合必定具有代数刚性，从而为计算困难性提供了确定性的解释。

5. 主要定理与分类

定理 5.1（Z_n 中的 Falconer 逆分类）。

设 $n = p_1 p_2 \dots p_k$ 是一个无平方因子合数。设 $E \subset \mathrm{Z}_n^d$ 是一个大小为 $|E| \geq C_d n^{(d+1)/2}$ 的集合，其中 C_d 是仅依赖于维数 d 的充分大常数。假设 E 是一个 Δ $|E| \ll n$ 近极值集（0）。那么它不是伪随机的。相反，E 它必然在结构上集中于一个结构性障碍 S 上，其定义如下：

1. **局部簇结构：** 对每个素因子 $p \mid n$，投影 E_p 集中于一个有界次数代数簇 V_p 上（根据定理 3.1）。2. **全局理想结构：** 这些提升后构成子模 $M \subset \mathrm{Z}_n^d$的一个陪集。具体而言，E 包含于形如 $S = \mathbf{v} + \mathrm{Ann}(\mathcal{K})$ 的集合之并中，其中 $\mathrm{Ann}(\mathcal{K}) = \{x \in \mathrm{Z}_n^d : \mathcal{K}x = 0\}$ 是因子 $\mathcal{K} \mid n$的湮灭子理想。3. **各向同性：** 子模 M 是各向同性的：对于任意 $x, y \in S$, $\| x - y \|^2 \equiv 0$（模 k）对某个非平凡因子 $k \mid n$ 成立（即 $1 < k < n$）。

注 5.1.1（定量界）。

常数 C_d 可以取为 $C_d = 2^{2^{O(d)}}$。这个塔式界源于有限域逆定理中的次数界和多项式恒等式测试界。将这些界改进为多项式依赖关系仍是一个开放问题。

注 5.2（一般非无平方因子情形）。

当 $n = p_1^{a_1} \dots p_k^{a_k}$ 且存在某个 $a_i > 1$ 时，该环含有幂零元。若 $n = p^2$，元素 x 可写成 $x = a + pb$。在商环 $\mathrm{Z}_{p^2}/(p) \cong \mathbb{F}_p$ 中，距离结构是刚性的，而

在理想 (p) 中则不受约束。通过将投影 $\mathbb{Z}_{p^2} \to \mathbb{F}_p$ 的纤维视为理想 $p\mathbb{Z}_{p^2}$ 的陪集，我们的分类结果也适用于这种情形。

证明。

证明通过综合第2节中的能量估计、第3节中的结构提升以及第 4 节中的多项式刚性来进行。

步骤 1：能量下界
已知距离集较小：$|\Delta(E)| \ll n$。对重数函数 $\nu_E(t)$ 应用柯西–施瓦茨不等式，可得算术关联能量满足：

$$\mathcal{E}_n(E) = \sum_t \nu_E(t)^2 \geq \frac{(\sum \nu_E(t))^2}{|\operatorname{supp}(\nu_E)|} = \frac{|E|^4}{|\Delta(E)|}.$$

代入假设 $|\Delta(E)| \ll n$，得到下界：

$$\mathcal{E}_n(E) \gg \frac{|E|^4}{n}.$$

步骤 2：局部化到素因子
根据定理 3.1（全局刚性），这一全局能量下界意味着，对于相当一部分素因子而言，“能量比”必须很大。具体而言，存在一个素数集 $\mathcal{P}$，使得对每个 $p \in \mathcal{P}$，投影 $E_p = \pi_p(E) \subset \mathbb{F}_p^d$ 满足：

$$\mathcal{E}_p(E_p) \geq c \cdot \frac{|E_p|^4}{p}.$$

这使得局部集合 E_p 处于有限域 Falconer问题的近极值情形。

步骤 3：有限域逆定理
我们将有限域逆定理（[2]中的定理 3.4）应用于每个 E_p（其中 $p \in \mathcal{P}$）。这保证了 E_p 在低次数代数簇 $V_p \subset \mathbb{F}_p^d$上具有结构性集中性（包含一个大子集）。

步骤 4：提升到全局子模
现在我们确定 V_p 3 |的几何类型。根据引理 .2, ΔE | 全局距离集（ ）的较小规模对局部距离集（E_p）| Δ 施加了严格约束。具体而言，对于这些“重”素数，$|\Delta(E_p)| \ll p$。

在有限域中，能够生成退化距离集的唯一簇是点、仿射子空间或各向同性锥（其中二次型为零）。任意曲面（例如非退化球面）都会生成大小为 $\sim p/2$ 的距离集，从而违反该条件。

因此，每个 V_p 都必须是线性结构或各向同性结构。根据中国剩余定理，这些局部线性结构的笛卡尔积可提升为子模 $M \subset \mathbb{Z}_n^d$ 的一个陪集。

步骤 5：通过多项式恒等式实现各向同性
最后，我们刻画 M 的度量性质。根据定理 4.1（多项式刚性），距离只取少数几个值这一事实意味着距离多项式 $\Psi(\mathbf{x},\mathbf{y})$ 在 $E \times E$ 上实际上恒为零。若一个非平凡二次型在某个子模上为零，则该子模必定是各向同性的。

这意味着，对于任意位移向量 $\mathbf{v} \in M - M$，其范数满足 $|| \mathbf{v} ||^2 \equiv 0$ （模 k），其中某个非平凡因子 $k \mid n$ 对应于“重”素数。这证实了结构 $S = \mathbf{v} + \mathrm{Ann}(\mathcal{K})$。

□

6. 结论

这项工作表明，环中距离统计的“弥散式”违例只是表象。从结构提升的角度来看，它们归结为刚性的代数对象。我们证明了，Falconer 猜想在 $\mathbb{Z}_n$ 中的障碍受模数 n的算术复杂度支配。

6.1. 未来方向与开放问题

1. **定量界：**定理 5.1 中的 C_d 能否改进为关于 d 的多项式？ 2. **算法应用：**这一刻画能否用于设计高效算法，以找出包含近极值集合的最小子模？ 3. **密码学影响：**这些刚性结果对基于 $\mathbb{Z}_n$ 运作的格密码系统的安全性有何影响？

参考文献

[1] Singh, S. & Parmar, V. P. S. (2024). 通过结构提升确定性认证近似间隙。Zenodo. https://zenodo.org/records/18503287[2] Singh, S. & Parmar, V. P. S. (2024). 有限域上点与球关联的逆定理。Zenodo. https://doi.org/10.5281/zenodo.18393143[3] Iosevich, A., & Rudnev, M. (2007). 有限域上向量空间中的 Erdős 距离问题。美国数学会会刊, 359(12), 6127-6142.[4] Bourgain, J., & Demeter, C. (2015). l^2解耦猜想的证明。数学年刊, 182(1), 351-389.[5] Agrawal, M., Kayal, N., & Saxena, N. (2004). PRIMES 属于 P. 数学年刊, 160(2), 781-793.[6] Falconer, K. J. (1985). 距离集的豪斯多夫维数。Mathematika, 32(2), 206-212.[7] Mattila, P. (1987). 傅里叶变换的球面平均……Mathematika, 34(2), 207-228.[8] Wolff, T. (1999). 圆平均的衰减……《国际数学研究通知》, 1999(10), 547-567.[9] Hart, A., et al. (2011). 超平面上的平均……美国数学会会刊, 363(6), 3255-3275.[10] Covert, D., Iosevich, A., & Pakianathan, J. (2012). 模 p^l 整数环上的几何构型。《印第安纳大学数学杂志》, 61(5), 1949-1969.[11] Hickman, J., & Wright, J. (2018). 傅里叶限制……《离散分析》, 2018:11.[12] Kabanets, V., & Impagliazzo, R. (2004). 多项式恒等式测试去随机化……计算复杂性, 13(1-2), 1-46.

附录 A

引入的结构引理与分歧点

本附录为方便审稿人，记录了所采用的配套预印本中的精确结构性输入，并明确指出本文在哪些方面偏离了这些预印本。此处陈述的所有结果仅用作黑箱结构工具；本文的主要定理和障碍均为新的，且专属于环情形。

A.1 有限域上的能量—结构二分法（引入）

以下　　引理是有限域上大距离关联能量所导致的结构性结论　　s.

引理 A.1（有限域能量刚性，引入）

设 $E \subset \mathbb{F}_q^d$、 $d \geq 3$，并假设距离集 $\Delta(E)$ 满足 $|\Delta(E)| \leq Kq$，其中某个 $K \geq 1$。那么存在一个子集 $E' \subset E$，满足 $|E'| \gtrsim K^{-O(1)} q^{(d+1)/2}$，以及一个次数为 $\deg F \leq K^{O(1)}$ 的非零多项式 $F \in \mathbb{F}_q[x_1, \ldots, x_d]$，使得 $E' \subset Z(F)$。

备注。

1. 该引理通过有限域逆关联框架，结合多尺度能量分解和多项式方法得以证明。2. 结论本质上属于代数几何范畴：近极值构型集中在低次数簇上。

在 $\mathbb{Z}_n$ 上的失效。

对于合数 n，引理 A.1 在环情形 $\mathbb{Z}_n^d$ 中失效，这是由于零因子的存在。较大的距离能量并不必然意味着点集中在任何低次数多项式的零点集上。本文第 2.2 节给出了明确的反例。

本文中的替代

引理 A.1 的作用由定理 3.1 取代；该定理通过将近极值集合包含在由 $\mathbb{Z}_n$ 的中国剩余分解产生的结构化子模和湮灭子理想中，对其进行分类。

A.2 跨算术尺度的结构提升（引入）

第二个引入的要素是提升原理，它允许将全局能量局部化到算术因子上。

引理 A.2（结构局部化，引入）。

设 $E \subset \mathbb{F}_q^d$ 满足全局距离能量下界 $\mathrm{E}(E) \geq Kq^{2d-1}$。那么存在一个尺度（或在合数情形下的一个素因子），使得相当比例的能量集中于此，从而得到一个结构化子构型。

备注。

- 在有限域情形下，这个引理通过对频率壳层取平均并运用组合抽屉原理来证明。• 该引理本身并非几何性的，而是一种纯粹的算术分解原理。

本文中的改动。
在环情形中，由于不同素数幂分量之间的相互作用，引理 A.2 的类似结果并非平凡。第 4 节引入了一种**除子深度过滤**，细化了针对中国剩余定理纤维的提升论证

$$\mathbb{Z}_n^d \cong \prod_{p^k \| n} \mathbb{Z}_{p^k}^d,$$

并追踪湮灭子层之间的能量，而非频率。

这一细化是新的，对于隔离理想论障碍至关重要。

A.3 引入内容与新内容概述

为明确起见，我们总结如下依赖关系：

- **已引入（仅限有限域）：**
  - 能量–结构二分（引理 A.1），仅作为动机使用。◦ 结构局部化原理（引理 A.2），经过改编，但未逐字复用。
- **本文新增：**
  - 在 Z_n 上代数簇刚性的失效。◦ 除子深度多尺度分解。◦ 通过子模和湮灭子理想对近极值构型进行分类。◦ 逆 Falconer 障碍的中国剩余定理提升。◦ 定理 1.1、3.1 和 4.2（核心结果）。

本文的主要定理均未出现在配套预印本中，且本稿件未在其他地方接受审稿。

附录 B

为什么代数簇在 $\mathbf{Z}_n$ 上是不充分的

本附录给出一个具体例子，表明在n 不是无平方因子的 Z_n 上，近极值距离行为并不意味着点集集中于低次代数超曲面。相反，阻碍来自理想论结构，源于与非平凡幂零理想相关的湮灭子结构。

在全文中，令 p 为一个**奇素数**，并令 $n = p^2$。

B.1 在$\mathrm{Z}_{p^2}^{d}$中的构造

固定一个维数 $d \geq 2$。令 $A \in M_d(\mathbb{F}_p)$ 为一个非零矩阵，该矩阵相对于**标准点积反对称**，即 $A^{\mathsf{T}} = -A$ in $M_d(\mathbb{F}_p)$。将 $\mathbb{F}_p$ 与典范代表元集 $\{0,1,\dots,p-1\} \subset \mathrm{Z}_{p^2}$ 视为相同。

定义 $E := \{\, x + pAx : x \in \mathbb{F}_p^d \,\} \subset \mathrm{Z}_{p^2}^{d}$。则 $|E| = p^d$，且自然投影 $\pi: \mathrm{Z}_{p^2}^{d} \longrightarrow (\mathrm{Z}_{p^2}/(p))^{d} \cong \mathbb{F}_p^d$ 限制为一个双射 $\pi(E) = \mathbb{F}_p^d$。

因此，E 在剩余域中最大程度地分散，同时在p-理想纤维中呈现非平凡结构 r.

B.2 距离集坍缩至剩余域

Let $x, y \in \mathbb{F}_p^d$, and write $X = x + pAx,\ Y = y + pAy$.

Then $X - Y = (x - y) + pA(x - y)$.

将平方范数模p^2展开,

$$\| X - Y \|^2 = \| x - y \|^2 + 2p\langle x - y, A(x - y)\rangle + p^2 \| A(x - y) \|^2$$

$$\equiv \| x - y \|^2 \quad (\text{模} p^2)$$

由于p 为奇数且A 在$\mathbb{F}_p$上反对称，因此对所有$v \in \mathbb{F}_p^d$，均有$v, Av = 0$，所以交叉项恒等于零。

因此 $\Delta(E) \subseteq \{0,1,\dots,p-1\} \subset \mathrm{Z}_{p^2}$，从而 $|\Delta(E)| \leq p = n^{1/2} \ll n$。

因此，尽管投影到整个剩余类空间 $\mathbb{F}_p^d$上，E 仍处于 $\mathrm{Z}_{p^2}^{d}$ 上的小距离范围内。

B.3 超曲面刚性的失效

We n现在证明，Z_{p^2} 上不存在任何非平凡的低次代数超曲面能够包含 E .

令 $F \in \mathrm{Z}_{p^2}[x_1, \dots, x_d]$ 为一个**总次数严格小于** p 的多项式，使得对所有 $z \in E$，$F(z) \equiv 0 \pmod{p^2}$ 成立。

模 p取模后，我们得到多项式 $F^{-}\in \mathbb{F}_p[x_1,\ldots,\ x_d]$ 满足对所有 $x \in \mathbb{F}_p^d$，$F^{-}(x) = 0$，因为 $z \equiv x$（模 p）且 $\pi(E) = \mathbb{F}_p^d$。

由于 $\deg(F^{-}) < p$，每个变量的次数都是 $<p$，而在 $\mathbb{F}_p^d$ 上处处为零的唯一此类多项式就是零多项式。

因此 $F^{-}\equiv 0$，所以 F 的每个系数都能被 p整除，我们可以写成 $F = pG$ ，其中 $G \in \mathrm{Z}_{p^2}[x_1,\ldots,\ x_d]$。

对 G应用相同的论证，我们得到 $G^{-}\equiv 0$，因此 G 也能被 p整除。所以 F 能被 p^2 整除，并且在 $\mathrm{Z}_{p^2}[x_1,\ldots,\ x_d]$ 中恒等为零。

因此，**不存在次数为** $<p$ 的非零多项式定义一个包含 E的超曲面。

B.4 理想论解释

前面的例子表明，在 $\mathrm{Z}p^2$上，小距离集可能源于湮灭子结构，而非代数几何。事实上，由于 $\Delta(E) \subseteq \{0,1,\ldots,p-1\}$，多项式

$$Q(T) = \prod_{a\in\mathbb{F}_p}(T-a) \in \mathbb{Z}_{p^2}[T]$$

对所有 $t \in \mathrm{Z}p^2$，满足 $Q(t) \equiv 0$ (模 p)，因此 $p\,Q(t) \equiv 0$ (模 p^2) 恒成立。

相应的距离湮灭子 $\Psi(X,Y) = p\,Q(\|X-Y\|^2)$ 模 p^2 恒等于零，这反映出刚性机制存在于非平凡理想 $(p) \subset \mathrm{Z}p^2$ 中，而非低次代数超曲面上。

这种现象在有限域中没有类比，也说明在 Z_n 上的逆 Falconer 刚性必须用理想论术语而非纯粹的代数几何术语来表述。