arXiv:2602.04468v1 [math.NT] 4 Feb 2026

有限生成环上的希尔伯特第十问题

Peter Koymans * Carlo Pagano †

2026年2月5日

1 希尔伯特纲领

1900年，在朋友闵可夫斯基的鼓励下，希尔伯特在巴黎举行的国际数学家大会上提出了一份极具影响力的23个问题清单。清单中的第十个问题如下。

> **希尔伯特第十问题：**“给定一个含有任意多个未知量、且数值系数为有理整数的丢番图方程：设计一种程序，使其能够在有限次运算内判定该方程是否有有理整数解。”

这里，丢番图方程是指形如

$$f(x_1, \ldots, x_n) = 0,$$

其中 $f \in \mathbb{Z}[x_1, \ldots, x_n]$，并且要在集合 $\mathbb{Z}^n$ 中寻找一个解（x_1，…，x_n），具体如所引问题末尾所述。早在希尔伯特之前，欧拉、Fermat 和拉格朗日等数学家就已经设计出极具巧思的方法，用于处理某些特殊类型的丢番图方程。希尔伯特第十问题非正式地问道：在完全一般的情况下，求解丢番图方程这一任务是否可以归约为一种完全机械化的程序。

希尔伯特非常清楚丢番图方程理论的丰富性，而他对于存在这样一种过程的乐观态度，是他将整个数学加以机械化这一总体愿望的一个具体体现，这一愿望也被称为希尔伯特纲领。这个“过程”一词在直观意义上使用，旨在表达后来被形式化为算法的概念。这很快引发了一系列戏剧性的进展，揭示了希尔伯特纲领在理论上的局限性。



图 1：大卫·希尔伯特

希尔伯特纲领的这些局限性显现出来后，数学界的目标转向了对希尔伯特第十问题本身给出否定答案。1970年，马季亚谢维奇–罗宾逊–戴维斯–普特南的共同努力最终为希尔伯特第十问题给出了否定答案。

自1970年以来，数论学家一直试图证明：对于任何由有限元素集经加法和乘法构造而成的无限数系，希尔伯特第十问题的答案都是否定的。

*Peter Koymans 是乌得勒支大学的博士后。他的电子邮件地址是 p.h.koymans@uu.nl。

†Carlo Pagano 是康考迪亚大学的助理教授。他的电子邮件地址是 carlein90@gmail.com。

这一概念凝练为有限生成环 的概念（见第4节），并最终促成了近期对 $\mathbb{Z}$的MRDP结果的一项重大推广。

定理1.1 ([KP24])**.** 设 R 为一个有限生成的无限环。则希尔伯特第十问题在 R上是不可判定的。

本文回顾希尔伯特问题的历史，描述MRDP给出的否定性解答，阐释Poonen借助椭圆曲线理论提出的新方法，并最终概述定理1.1证明中的主要思想。特别地，我们说明定理1.1的证明如何将下降法——椭圆曲线算术中的一种古老方法——与更为现代的算术组合学领域结合起来。

2 理论局限性

我们回顾，希尔伯特纲领旨在使全部数学机械化。特别地，希尔伯特希望给出一种算法，用以判定任一数学陈述的真伪。

1931年，G¨odel对希尔伯特纲领造成了第一次重大打击，建立了他的不完备定理。在其第一不完备定理中，G¨odel证明：任何其定理可由算法列出的一致公理系统，都无法证明关于自然数算术的全部真理。

1937年，Turing 再次重创了希尔伯特纲领，证明不存在这样的算法：它以任意计算机程序及其输入为输入，并能判断该程序在给定输入下会停止还是永远运行。这就是所谓的停机问题。在这项工作中，Turing 为计算机程序这一概念奠定了坚实的基础，为数字时代的兴起铺平了道路。有了这些基础，我们便可以精确地表述希尔伯特第十问题。

精确表述：是否存在一台图灵机，它以任意 f *in*$\mathbb{Z}[x_1, \ldots, x_n]$ 作为输入，并输出：

- *YES if* $f = 0$ *has a solution in* $\mathbb{Z}^n$*,*
- 否则则为否。

哥德尔和 Turing 的证明的核心都在于存在自指语句，这一思想可以追溯到古希腊的说谎者悖论“这句话是假的”。时间上更近的一位先驱是 Cantor 的观察：给定$\{D_n : n \in \mathbb{Z}\}$， $\mathbb{Z}$的一个子集集合，该集合

$$\{n \in \mathbb{Z} : n \notin D_n\}$$

不可能具有 D_{n_0} 的形式，其中任意 n_0 都属于 $\mathbb{Z}$：若存在这样的 n_0，那么 n_0 属于 D_{n_0} 就会迫使 $n_0 \notin D_{n_0}$，而 n_0 不属于 D_{n_0} 则会迫使 $n_0 \in D_{n_0}$，两种情况都导致矛盾。

尽管存在这些理论上的局限，希尔伯特纲领的宏大目标仍然生机勃勃。将数学思维机械化并形式化的目标，至今仍是现代研究的重要驱动力，尤其是随着形式化验证器和人工智能的出现。

3 丢番图集

在 G¨odel 和 Turing 的研究之后，研究者们开始将注意力转向希尔伯特第十问题的否定答案。罗宾逊是这一思路中的关键人物之一。



图 2：朱莉娅·罗宾逊

戴维斯独立地开始寻找否定答案，后来戴维斯–普特南也加入了这一探索。最终，他们与罗宾逊携手合作，并于1960年对希尔伯特第十问题的一个变体给出了否定答案，该变体涉及指数丢番图方程，

也就是说，允许方程中的某些变量作为指数。

为概述其整体策略，我们先给出一个定义。

定义 3.1. 我们称子集 $S \subseteq \mathbb{Z}^n$ 是丢番图 的，如果存在某个多项式

$$P \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$$

使得对于所有元素$(a_1, \ldots, a_n) \in \mathbb{Z}^n$，都有$(a_1, \ldots, a_n) \in S$当且仅当存在$b_1, \ldots, b_m \in \mathbb{Z}$使得

$$P(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0.$$

简单来说，丢番图集是多项式方程的零点集在某个坐标上的投影。

例 3.2. 非负整数的集合 $\mathbb{Z}_{\geq 0}$ 是丢番图集。事实上，根据拉格朗日定理，每个 $n \in \mathbb{Z}_{\geq 0}$ 都可以写成四个整数的平方之和，

$$n = a^2 + b^2 + c^2 + d^2,$$

因此我们可以取 $P = x_1 - y_1^2 - y_2^2 - y_3^2 - y_4^2$。

例 3.3. 通常很难证明某个特定子集 $S \subseteq \mathbb{Z}^n$ 不是丢番图集。不过，由于 $\mathbb{Z}^n$ 有不可数多个子集，而多项式 $P \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ 只有可数多个（即使允许 m取任意值），因此必定存在非丢番图子集。

同样，我们将函数 $f\colon \mathbb{Z}^n \to \mathbb{Z}$ 称为丢番图函数，如果它的图像作为 $\mathbb{Z}^{n+1}$的子集是丢番图集。

他们方法中一个强有力的指导思想，源自人们熟悉的理论计算机科学：通过归约到一个更经典的不可判定问题（例如停机问题）来推进研究。为此，他们大胆地设想证明，丢番图函数类与可由图灵机计算的函数类完全相同；他们认为，丢番图方程理论足够丰富，实质上可以模拟任何计算。

这种方法可以具体表述如下：如果我们能够证明，每个可由图灵机计算的函数实际上都是丢番图函数，那么就有可能证明，$\mathbb{Z}$ 的所有丢番图子集都可以列为 $(D_n)_{n\in\mathbb{Z}}$，使得集合

$$U := \{n \in \mathbb{Z} : n \in D_n\} \subseteq \mathbb{Z}$$

是丢番图的。设 $G(x) \in \mathbb{Z}[x_1, \ldots, x_m]$ 是一个证明 U 为丢番图集的多项式。如果存在一种算法，能够检查下面这个特定多项式族是否有解

$$\{G(a, x_2, \ldots, x_m) : a \in \mathbb{Z}\} \subseteq \mathbb{Z}[x_2, \ldots, x_m], \quad (3.1)$$

那么 U 的补集就是丢番图集，因为其特征函数可由图灵机计算。这意味着存在一个 $n_0 \in \mathbb{Z}$ 使得 $\mathbb{Z} - U = D_{n_0}$。由此我们可以得出结论:

$$D_{n_0} = \mathbb{Z} - U = \{n \in \mathbb{Z} : n \notin D_n\},$$

这根据第1节末尾所解释的论证是不可能的。在他们的工作中，戴维斯–普特南–罗宾逊 [DPR61] 证明，只要证明这个函数

$$n \mapsto 2^n$$

是丢番图函数。稍微更一般的版本被称为*J.R.*猜想（以朱莉娅·罗宾逊的名字命名），并且这个问题悬而未决达20年之久。尽管取得了巨大的进展，整个研究思路仍依赖于这类奇特丢番图集的存在，而数学界对此是否可能持怀疑态度。

1970年，年轻的 Matiyasevich [Mat70]找到了这样一个丢番图函数，局面因此发生了巨大变化。

凭借一个极其巧妙的论证，他证明了这个函数

$$n \mapsto F_n$$

是丢番图的，其中 F_n 是第 n个斐波那契数。他的证明后来经多位作者简化，并指出论证中的关键工具是

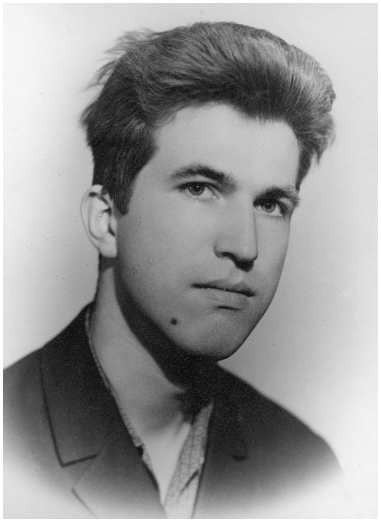


图 3：尤里·马季亚谢维奇

佩尔方程的算术。佩尔方程是一种形如以下形式的方程

$$x^2 - dy^2 = 1,$$

其中 d 是一个正整数。后续对马季亚谢维奇的论证的阐述利用了佩尔方程的参数族

$$x^2 - (a^2 - 1)y^2 = 1, \tag{3.2}$$

当 a 遍历大于 1 的整数时。对于正整数 n，记

$$x_n(a) + y_n(a) \cdot \sqrt{a^2 - 1} := (a + \sqrt{a^2 - 1})^n,$$

不难证明，方程 (3.2) 的所有解（其中x，y均为正整数）都具有形式 $(x_n(a)\ y_n(a))$。马季亚谢维奇在获得指数 n时发现的关键附加性质是

$$y_m(a)^2 \mid y_n(a) \iff y_m(a) \mid n.$$

注意到，关系 $y_m(a)^2 \mid y_n(a)$ 可以重新表述为方程 $y_m(a)^2 \cdot t = y_n(a)$，从而提供了获取指数 n 的丢番图途径。他以极其巧妙的方式运用这一方法，得以证明函数

$$(a, n) \mapsto y_n(a)$$

是丢番图的。

由此，我们可以证明指数函数是丢番图的，进而按照上文概述的方式得出结论：希尔伯特第十问题不可判定；不存在能够同时判定所有丢番图方程在 $\mathbb{Z}$上的可解性的算法。总而言之，这些作者的共同努力后来被称为 MRDP 定理。

定理 3.4 （“MRDP 定理”）。不存在这样一种算法：它以 f 中的任意方程为输入，并判定 $f = 0$ 在 $\mathbb{Z}^n$ 中是否有解。

利用用于定义集合 (3.1) 的多项式 G，我们可以看到，即使对所涉及的变量个数给出统一上界，不可判定性依然成立。

尽管 MRDP 定理对统一算法是否存在给出了明确的理论限制，希尔伯特第十问题在精神上依然生机勃勃。现代丢番图几何正在发展各种算法技术，以处理数论中自然出现的特殊方程类别。例如，人们普遍相信，如果将范围限制在两个变量的多项式 $F(x_1,\ x_2)$ 上，也就是相信存在一种算法，能够判定一条代数曲线是否有整点。

4 有限生成环

Matiyasevich 完成 MRDP 定理的证明后，提出了一个自然的后续问题：在希尔伯特第十问题中，如果将所有 $\mathbb{Z}$ 都替换为一个有限生成环 R，会发生什么？根据定义，有限生成环 R 同构于一个商

$$R \cong \mathbb{Z}[x_1, \ldots, x_n]/I$$

对于某个理想 $I \subseteq \mathbb{Z}[x_1, \ldots, x_n]$。这不仅是一类规模庞大且重要的环，也是一类适合研究判定问题的自然对象，因为此类环 R 中的每个元素都可以用有限的数据编码（例如复数则不然）。

例4.1。 通常的整数 $\mathbb{Z}$、高斯整数 $\mathbb{Z}[\sqrt{-1}]$：$= \{a + b\sqrt{-1} : \ a, b \in \mathbb{Z}\}$，以及多项式环 $\mathbb{Z}[x]$ 和 $\mathbb{Z}[x, y]$ 都是有限生成环。

例4.2。 不是有限生成环的例子包括有理数 $\mathbb{Q}$、实数 $\mathbb{R}$或复数 $\mathbb{C}$。

注意，对于有限环 R 上的多项式方程 $f(x_1, \ldots, x_n) = 0$，只需将多项式代入每个 $(a_1, \ldots, a_n) \in R^n$ 中计算，就能轻易求解。因此，以下我们将注意力限制在具有无限基数的有限生成环上。

有理由认为，对于这类环，希尔伯特第十问题的答案仍应是否定的。事实证明，归约策略再次发挥作用；现在，我们尝试将 R 上的希尔伯特第十问题归约为 $\mathbb{Z}$上的希尔伯特第十问题。确实，通过将一个环中系数为某些元素的丢番图方程编码到另一个环中系数为某些元素的丢番图方程里，我们有望将已知情形中的不可判定性推广到许多新的情形。这引出了对定义 3.1 的以下推广，其中环 $\mathbb{Z}$ 被环 R 取代。

定义4.3。 我们称子集 $S \subseteq R^n$ 是R-丢番图的，如果存在某个多项式

$$P \in R[x_1, \ldots, x_n, y_1, \ldots, y_m]$$

使得 $(a_1, \ldots, a_n) \in S$ 当且仅当存在$b_1, \ldots, b_m \in R$ 使得

$$P(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0.$$

换句话说， R-丢番图集是某个关于 R的多项式方程的解集在前 n 个坐标上的投影。这一概念是希尔伯特第十问题归约论证的核心。事实上，如果整数集 $\mathbb{Z}$ 可以表示为 R的一个R-丢番图子集，那么每个关于 $\mathbb{Z}$ 的丢番图方程都可以编码为关于 R的丢番图方程。因此，关于 R 的希尔伯特第十问题是不可判定的。

那么，我们如何证明 $\mathbb{Z}$ 在R上是丢番图的呢？事实证明这是一项艰巨的任务，而在1970年 MRDP 证明之后，文献中开始出现一系列复杂的归约步骤。Eisentr¨ager [Eis03] 在她的博士论文中证明，要解决所有有限生成环上的希尔伯特第十问题，只需证明 $\mathbb{Z}$ 在一个小得多、也更易处理的环类上是丢番图的，下面我们将对此作出说明。

定义4.4。 称整环 R 为一个序，如果其底层加法群同构于某个 $n \geq 1$的 $\mathbb{Z}^n$ 。

例4.5. 每个序都是有限生成环。然而，反过来并不成立。多项式环 $\mathbb{Z}[x]$作为环是有限生成的，但它不是序，因为其底层加法群同构于可数多个 $\mathbb{Z}$ 的直和。序的例子包括 $\mathbb{Z}$ 本身、高斯整数环 $\mathbb{Z}[\sqrt{-1}]$，以及由下式定义的高斯整数环的有限指数子环

$$\left\{a + 2b\sqrt{-1} : a, b \in \mathbb{Z}\right\}.$$

尤其是，Eisentr¨ager 的工作表明，只需将注意力限制在极大序 R上；也就是说，考虑不存在严格更大的序 S 满足

$$R \subsetneq S \quad \text{and} \quad [S : R] < \infty.$$

极大序具有特别良好的代数性质，在数论中发挥着核心作用。在许多方面，它们是代数几何中非奇异曲线的算术类比物。极大序通常称为整数环，这反映了它们与通常的整数 $\mathbb{Z}$ 十分相似。

更早之前，Denef [Den80]，在 Matiyasevich 的思想基础上，利用佩尔方程的算术性质，证明了许多这类极大序上的希尔伯特第十问题具有不可判定性。然而，Denef 的方法仅适用于极大序 R 是全实的情形，这意味着 R 到 $\mathbb{C}$的每个嵌入实际上都有像包含于 $\mathbb{R}$ 中。尽管这些成果代表了重大进展，但仍有一大类极大序超出了佩尔型方法的适用范围。对于这些剩余情形，则需要一个从根本上全新的思路。

5 椭圆曲线

定义上， E 上的椭圆曲线 $\mathbb{Q}$是形如以下形式的方程

$$E : y^2 = x^3 + ax + b \tag{5.1}$$

其中 a， $b \in \mathbb{Q}$ 为固定值，且右侧的三次多项式没有重根。

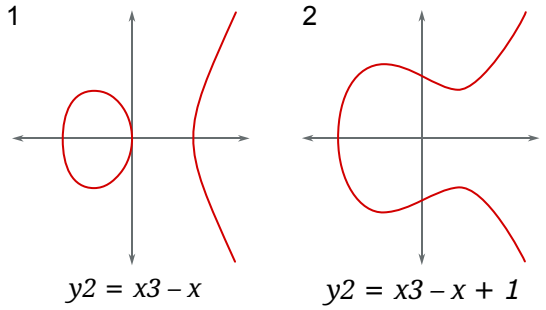


图4：实数域上的两条椭圆曲线

椭圆曲线在数论中占据着重要地位。最著名的例子是，它们是 Wiles 证明费马大定理的关键组成部分。尽管经过数十年的深入研究，椭圆曲线的许多方面仍然深不可测。

早在古希腊，人们就已认识到，方程 (5.1) 的解可以用来构造新的解；用现代术语来说，这意味着椭圆曲线具有自然的群结构。要定义这一结构，我们先取曲线的射影闭包，这相当于添加一个额外的点，称为无穷远点，记作 O。这个点充当群的单位元。

群运算可以用简单的几何方式来描述。如果三个点 P、Q 和 R 位于椭圆曲线上且共线，那么我们规定

$$P + Q + R = O.$$

关于加法定律的示意图，请参见图5。

给定一条椭圆曲线 E，我们将其有理点集合定义为

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + ax + b\} \cup \{O\}.$$

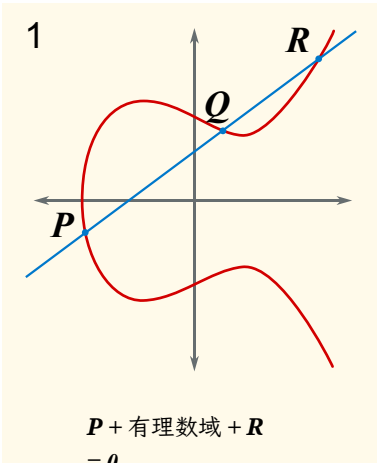


图5：加法定律

更一般地，对于任意域 K，我们都可以定义 $E(K)$。

20世纪初，Mordell 证明了以下基本结果：

定理 5.1。我们有

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times (\text{finite group}).$$

整数 r 称为椭圆曲线的秩 。

这使得 E 成为替代佩尔方程在 Denef的论证中所起作用的一个自然候选对象。请注意，当 E 的秩等于 1 时，它与佩尔方程的类比尤其密切；在这种情况下，这两个方程的解集都具有秩相同的自然群结构。然而，椭圆曲线有一个相当严重的缺点。尽管阿贝尔群 $E(\mathbb{Q})$的形式很简单，目前仍没有已知的（可证明正确的）算法能够计算秩 r。相应地，定理 5.1 的证明是非构造性的。

坏消息就说到这里。首先传来的一条好消息是，Poonen [Poo02] 能够用椭圆曲线取代佩尔方程在 Denef 的论证中所起的作用。这由此导出了以下定理。

定理 5.2 ([Poo02])**.** 设 R 是一个极大阶。设 K 是 R 的分式域。假设存在一条椭圆曲线 E： $y^2 = x^3 + ax + b$

满足 a、$b \in \mathbb{Q}$，使得

$$\operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} E(K) = 1. \tag{5.2}$$

那么 $\mathbb{Z}$ 是 R-丢番图的。

在 Poonen 的研究时期，即使是找到秩为 $E(K) = 1$ 的椭圆曲线，也还是一个未解决的问题。尽管如此，定理 5.2 仍然是一次重大的概念性突破。它为证明 $\mathbb{Z}$ 是 R-丢番图的提供了清晰的路线图，从而也为证明希尔伯特第十问题对于所有具有无限基数的有限生成环 R 都没有算法解提供了路线图。

如前所述，目前还没有已知算法可以计算秩。然而，如果我们愿意假设 Birch–Swinnerton-Dyer 猜想，情况就会发生巨大变化。这个猜想是千年难题之一，目前仍悬而未决。BSD猜想的一个惊人推论是，椭圆曲线的秩应当等于某个复解析函数的消失阶；特别是，这提供了一种计算秩的具体方法。在这一假设下，Mazur 和 Rubin [MR10], 在 Shlapentokh [Shl08], 对 Poonen 结果的推广基础上，证明了以下结论：

定理 5.3 ([MR10])。假设 *BSD* 猜想成立。设 R 是一个极大阶。那么 $\mathbb{Z}$ 是 R-丢番图的。特别地，希尔伯特第十问题在 R上不可判定。

结合 Eisentr¨ager 的结果，我们推断，假设 *BSD* 猜想成立，希尔伯特第十问题对每个具有无限基数的有限生成环 R 都不可判定。

6 近期进展

在 Mazur 和 Rubin 的工作之后，数学家们开始寻求无条件解决希尔伯特第十问题在有限生成环上的情形。首先，让我们暂且搁置方程 (5.2) 引入的额外复杂性，专注于核心挑战：证明在 K上存在一条秩为 1 的椭圆曲线。

Mazur 和 Rubin 已经使用过的一项关键工具是下降法。下降法是数论中的一种经典方法，其渊源可追溯到古希腊。Fermat 本人精通下降法，并曾以此著名地解决了 $n = 4$ 费马大定理中的情形。如今，下降法仍是一种强有力的方法，尽管其现代形式抽象得多。

下面概述下降法的原理。假设我们要证明某个方程$f(x, y) = 0$ 在正整数中无解。我们要做的是证明，如果有人给出一个解 (x_1, y_1)，我们就能利用这个解构造出一个新的“更小”的解 (x_2, y_2)，使其满足

$$x_2 < x_1.$$

注意这里是不等式。重复这一过程，我们会发现，即使只有一个解，也能用它构造出一列解，其 x坐标都是正数且严格递减。这显然矛盾，说明方程无解！你可能会问，我们如何利用给定的解构造出一个更小的新解？答案因问题而异，从毕达哥拉斯学派用来证明 $\sqrt{2}$ 是无理数的相对简单的论证，到用于证明定理 5.1 的深奥方法，不一而足。

设 R 是一个序，K 是它的分式域，E 是由一个系数属于 K 的方程定义的椭圆曲线。将下降法工具应用于椭圆曲线 E 时，会得到一列塞尔默群 $S(E, K, n)$，每个 $n \geq 2$ 对应一个。群 $S(E, K, n)$ 具有以下性质：

- $S(E, K, n)$ 可以有效计算。
- $S(E, K, n)$ 大致上是一些阶为 n 的循环群的乘积。我们将其秩（生成元的个数）记为 $s(E, K, n)$。
- 商群 $E(K)/nE(K)$ 是 $S(E, K, n)$ 的一个子群。特别地，对所有 $n \geq 2$,

$$\text{rank of } E(K) \leq s(E, K, n),$$

这里强调，对于任意给定的 n，塞尔默秩 $s(E, K, n)$ 都可以有效计算。

假设 BSD猜想成立，则对所有 k，$s(E,\ K,\ p^k)$ 的最小值等于 $E(K)$ 的秩。此外，在温和的假设下，$s(E,\ K,\ p^k)$ 与 $E(K)$ 的秩奇偶性相同。实际上，即使是$s(E,\ K,\ 2)$，也常常等于 E 的秩。

在若干值得注意的情形中，我们可以掌握 $s(E,\ K,\ 2)$ 随着E 遍历一族椭圆曲线时的统计行为。事实上，Mazur–Rubin [MR10] 证明，对于每个极大阶 R，都存在一条椭圆曲线 E，定义在 R 上，使得 $s(E,K,\ 2)\ =\ 1$。由于 $s(E,K,\ 2)$ 是 E 秩的上界，而且在假设 BSD 猜想成立时具有相同的奇偶性，因此 E 的秩也必定为 1。这一观察是他们论证的核心。若要使这一论证无条件成立，我们必须同时确保两个彼此独立的要素：

(i) 找到一族 $\mathcal{F}$ 椭圆曲线，使得其中每条$E \in \mathcal{F}$ 的秩至少为 1，

(ii) 存在一条椭圆曲线 $E\ \in\ \mathcal{F}$，使得$s(E,K,\ 2)\ \leq 1$。

条件（i）提供了秩的统一下界，而条件（ii）则给出了相应的上界。二者结合，意味着存在一条秩恰好为 1 的椭圆曲线。

单独来看，条件（i）和（ii）都不难实现。例如，对于（i），我们巧妙地选择系数 a and b，以确保存在一个无限阶的有理点。另一方面，条件（ii）正是 Mazur 和 Rubin 针对某些精心选取的族所证明的。直到最近，人们一直缺少一种方法，来控制满足以下性质的族中 $s(E,\ K,\ 2)$：其中每个成员 $E \in \mathcal{F}$ 都已先验地确定其秩至少为 1。

首个成功结合 (i) 和 (ii) 的工作出自作者 [KP24]。他们从构造一个合适的椭圆曲线族入手。固定元素 $a_1, a_2, a_3 \in R$，并考虑椭圆曲线

$$\widetilde{E} : y^2 = (x - a_1)(x - a_2)(x - a_3) =: f(x),$$

其定义三次多项式[1] $f(x)$ 完全分解为线性因子。

据此，他们定义了一个二参数族 $\mathcal{F} =(E_{m,\ n})_{m,\ n}$，其定义如下：

$$y^2 = \big(x - a_1 f(m/n)\big)\big(x - a_2 f(m/n)\big)\big(x - a_3 f(m/n)\big).$$

该族中的每条曲线 $E_{m,\ n}$ 都配有一个典范有理点，其表达式为：

$$x = f(m/n) \cdot m/n, \qquad y = f(m/n),$$

因此，条件（i）自动满足。剩下的挑战是建立条件（ii）：在从一开始就内置有理点的族中，我们该如何控制 2-塞尔默秩 $s(E_{m,\ n},\ K,\ 2)$?

经典结果表明，族 $\mathcal{F}$ 中的塞尔默秩$s(E,\ K,\ 2)$ 可以根据定义该椭圆曲线的三次多项式的判别式的素因子显式计算，即

$$(x - a_1 f(m/n))(x - a_2 f(m/n))(x - a_3 f(m/n)).$$

由于这个三次多项式可以分解为三个一次因子，且系数 $a_1,\ a_2,\ a_3$ 固定，该判别式的主要贡献来自以下量

$$n(m - a_1 n)(m - a_2 n)(m - a_3 n). \tag{6.1}$$

族 $\mathcal{F}$ 经过精心设计，使得表达式（6.1）是四个一次形式的乘积。因此，根据格林–陶定理，这四个因子可以同时取为素数；该定理最近由 Kai [Kai23] 推广到了极大序。利用这一结果，作者证明：

定理 6.1 ([KP24])。设 R 为一个极大阶。那么，$\mathbb{Z}$是 R-丢番图的。特别地，希尔伯特第十问题在 R上不可判定。

由此可立即得出，希尔伯特第十问题在每个无限基数的有限生成环上都是不可判定的。

[1]这种特殊形式在下降法论证中起着至关重要的作用。

在 [KP24], 发布几个月后，另外两组作者 [ABHS25,Zyw25]独立地解决了有限生成环上的希尔伯特第十问题。尽管这些论文中的具体族和下降法论证在技术细节上大不相同，但这三种方法都采用了共同的基本策略：将一项算术组合学结果与下降法相结合。值得一提的是， [ABHS25,Zyw25]只需要素数中的三项等差数列，而 [KP24] 则需要一个更高级的结果。

尽管最近取得了进展，该域仍有一个重大的未决问题，作者希望予以强调。如例4.2中已经指出的，域 $\mathbb{Q}$不是有限生成的，因此定理 6.1并不适用。事实上，$\mathbb{Q}$ 上的希尔伯特第十问题仍然完全未解决：

问题6.2. 判定是否存在一种算法，在输入多项式 $f \in \mathbb{Q}[x_1, \ldots, x_n]$时输出：

- 是 如果 f有零点$(a_1, \ldots, a_n) \in \mathbb{Q}^n$，并且
- 否否则。

人们普遍认为，问题6.2的答案应当是否定的。

与有限生成的情形形成鲜明对比的是，我们目前既不知道足以对问题6.2给出否定回答的充分条件，甚至也没有清晰的策略。找出一条能够回答问题 6.2的合理途径，似乎是一项艰巨的挑战！

参考文献

[ABHS25] L. Alp¨oge、M. Bhargava、W. Ho 和 A. Shnidman, *Rank stability in quadratic extensions and hilbert's tenth problem for the ring of integers of a number field* 2025 2501.18774 （），可见于 。[Den80] J. Denef, *Diophantine sets over algebraic integer rings. II* **257** 1980 ，《美国数学会汇刊》（），第 1 期，227–236。MR549163[DPR61] M. Davis、H. Putnam 和 J. Robinson, *The decision problem for exponential diophantine equations* 2 **74** 1961 425 436 ，《数学年刊》（）（），–。MR133227

[Eis03]A. K. Eisentr¨ager, *Hilbert's tenth problem and arithmetic geometry*，ProQuest LLC，密歇根州安娜堡，2003 年。博士论文——加州大学伯克利分校。MR2705180[Kai23] W. Kai, *Linear patterns of prime elements in number fields* 2023 2306.16983 （），可见于 。[KP24] P. Koymans 和 C. Pagano, *Hilbert's tenth problem via additive combinatorics* （2024），可见于 2412.01768。[Mat70] Ju. V. Matijasevič, *The Diophantineness of enumerable sets* **191** 1970 ，《苏联科学院学报》（），279–282。MR258744[MR10] B. Mazur 和 K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem* ，《数学发明》**181** （2010），第 3 期，541–575。MR2660452[Poo02] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*，《算法数论》（悉尼，2002），2002 年，第 33–42 页。MR2041072[Shl08] A. Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers* ，《美国数学会汇刊》**360**（2008），第 7 期，3541–3555。MR2386235[Zyw25] D. Zywina, *Rank one elliptic curves and rank stability* 2025 2505.16960 （），可见于 。