RANK STABILITY MAKES RINGS OF INTEGERS DIOPHANTINE

BJORN POONEN

Abstract. The recent negative answer to Hilbert's tenth problem over rings of integers relies on a theorem that for every extension of number fields L/K, if there is an abelian variety A over K such that $0 < \operatorname{rank} A(K) = \operatorname{rank} A(L)$, then $\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine. We present an alternative proof of this theorem and review how it is used.

1. Introduction

1.1. **History.** Hilbert's tenth problem asked for an algorithm to decide, given a multivariable polynomial equation with integer coefficients, whether it has a solution in integers. By [DPR61, Mat70], there is no such algorithm.

For each number field K, replacing $\mathbb{Z}$ with the ring of integers $\mathcal{O}_K$ yields a new question. The negative answer for $\mathbb{Z}$ implies a negative answer for $\mathcal{O}_K$ *if* $\mathbb{Z}$ *is* $\mathcal{O}_K$*-diophantine*; see Section 2 for the definition. This led Denef and Lipshitz [DL78] to conjecture that $\mathbb{Z}$ is $\mathcal{O}_K$-diophantine for *every* number field K. Their conjecture was proved for many classes of number fields by using the structure of integer points on algebraic tori, specifically, Pell equations [Den75, DL78, Den80, Phe88, Shl89].

Starting with Denef, various authors [Den80, Poo02, CPZ05, Shl08, MRS24] showed that one could use elliptic curves or abelian varieties in place of algebraic tori, if certain rank conditions could be proven. The strongest of these results states, for an extension L/K of number fields, that if the condition

$\mathcal{A}_{K,L}$: There exists an abelian variety A over K such that $0 < \operatorname{rank} A(K) = \operatorname{rank} A(L)$.

holds, then $\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine [MRS24, Theorem 1.1] (in fact, this result applies to some *infinite* algebraic extensions as well). Via such results, [MR10, MR18, MP18, GFP20, Pas23, SW23, KLS24, RW24] proved that $\mathbb{Z}$ is $\mathcal{O}_F$-diophantine for many new number fields F.

Recently, [KP25], using an input from additive combinatorics, constructed elliptic curves proving $\mathcal{A}_{K,L}$ for enough degree 2 extensions L/K to prove the full Denef–Lipshitz conjecture. Soon thereafter, [ABHS25, Theorem 1.1] gave a simpler proof, yielding $\mathcal{A}_{K,L}$ for all degree 2 extensions L/K, though they constructed abelian varieties that were not necessarily elliptic curves. In contrast with [KP25], [ABHS25] requires no additive combinatorics beyond a number field analogue of Vinogradov's method from the 1930s. Later, [Zyw25, Theorem 1.2]

Date: November 16, 2025.

2020 *Mathematics Subject Classification.* Primary 11G10; Secondary 11R04, 11U05, 14K15.

Key words and phrases. Hilbert's tenth problem, diophantine set, ring of integers, abelian variety, rank stability.

This research was supported in part by National Science Foundation grant DMS-2101040 and Simons Foundation grants #402472 and #550033. It was done partly while the author was visiting the 2025 program "Definability, decidability, and computability" at the Hausdorff Research Institute in Bonn.

proved the stronger theorem that for every degree 2 extension L/K, there exist infinitely many elliptic curves E over K with $\operatorname{rank} E(K) = \operatorname{rank} E(L) = 1$.

1.2. **Outline.** The proof that $\mathbb{Z}$ is $\mathcal{O}_F$-diophantine for all number fields F can be broken into four independent steps:

(i) If E is a totally real number field, then $\mathbb{Z}$ is $\mathcal{O}_E$-diophantine [Den80].
(ii) $\mathcal{A}_{K,L}$ holds for all degree 2 extensions L/K [KP25, ABHS25, Zyw25].
(iii) $\mathcal{A}_{K,L}$ implies that $\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine [MRS24, Theorem 1.1].
(iv) If $\mathbb{Z}$ is $\mathcal{O}_E$-diophantine for all totally real E, and $\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine for all degree 2 extensions L/K, then $\mathbb{Z}$ is $\mathcal{O}_F$-diophantine for all number fields F. This reduction is due to Shlapentokh [MRS24, Theorem 4.8].

Remark 1.1. What is proved towards (ii) determines how strong a version of (iii) is needed. Specifically, [KP25] constructs elliptic curves and hence needs only [Shl08], whereas [ABHS25] needs the full abelian variety statement of [MRS24], and [Zyw25] needs only [Poo02].

We have nothing new to say about (i) and (ii). The main purpose of this note is to give an alternative proof of (iii); see Theorem 4.2(d). The key ideas are present in the earlier works, but we introduce several simplifications. In Section 5, we reproduce Shlapentokh's reduction argument (iv) since it is short.

1.3. **Notation.** Let K be a number field. Let $\mathcal{O}_K$ be its ring of integers. Given $a \in K^\times$, there exist unique coprime ideals $I, J \subset \mathcal{O}_K$ such that $(a) = I/J$; define $\operatorname{num}(a) := I$ and $\operatorname{den}(a) := J$. Let I be an ideal of $\mathcal{O}_K$. If $a, b \in \mathcal{O}_K$, the notation $a \equiv b \pmod{I}$ means $a - b \in I$. If $a, b \in K$, the notation $a \equiv' b \pmod{I}$ means $I \mid \operatorname{num}(a-b)$.

2. Diophantine sets

Let $R = \mathcal{O}_K$ for some K. For a finite-type R-scheme X, a subset $S \subset X(R)$ is R-diophantine if it is $f(Y(R))$ for some finite-type morphism $Y \to X$. A subset $S \subset R = \mathbb{A}^1(R)$ is R-diophantine if and only if $S = \{a \in R : (\exists x \in R^n)\ g(a,x) = 0\}$ for some $g \in R[t, x_1, \ldots, x_n]$ [BP25, Corollary 1.5]. Finite unions of R-diophantine subsets are R-diophantine. Any morphism of finite-type R-schemes $X \to X'$ maps R-diophantine subsets of $X(R)$ to R-diophantine subsets of $X'(R)$. Applying this to $\mathbb{A}^1 \times \mathbb{A}^1 \xrightarrow{\text{sum}} \mathbb{A}^1$ shows that if $S, T \subset R = \mathbb{A}^1(R)$ are R-diophantine, then so is $S + T := \{s + t : s \in S,\ t \in T\}$.

Lemma 2.1 ([DL78, Proposition 1(b)])**.** *The set $\mathcal{O}_K - \{0\}$ is $\mathcal{O}_K$-diophantine.*

Proof. For any *nonzero* ideal $I \subset \mathcal{O}_K$, there exists $x \in \mathcal{O}_K$ with $(2x-1)(3x-1) \equiv 0 \pmod{I}$ (use the Chinese remainder theorem to reduce to the case where I is a power of a prime ideal). For $a \in \mathcal{O}_K$, taking $I = (a)$ shows that

$$a \neq 0 \quad \iff \quad (\exists x, y \in \mathcal{O}_K)\ (2x-1)(3x-1) = ya. \qquad \square$$

Elements of K can be represented in the usual way as equivalence classes a/b of pairs (a,b) with $a, b \in \mathcal{O}_K$ and $b \neq 0$. Subsets of K can then be identified with certain subsets of $\mathcal{O}_K^2$. Lemma 2.1 lets us

- use polynomial equations involving K-valued variables in diophantine definitions and
- extend the $\mathcal{O}_K$-diophantine notion to subsets of $X(K)$ for finite-type K-schemes X.

For a finite extension L/K,

- choosing a finite presentation of $\mathcal{O}_L$ as an $\mathcal{O}_K$-module lets us use polynomial equations involving $\mathcal{O}_L$-valued variables in constructing $\mathcal{O}_K$-diophantine sets, and
- if $\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine, then any $\mathcal{O}_K$-diophantine set is $\mathcal{O}_L$-diophantine.

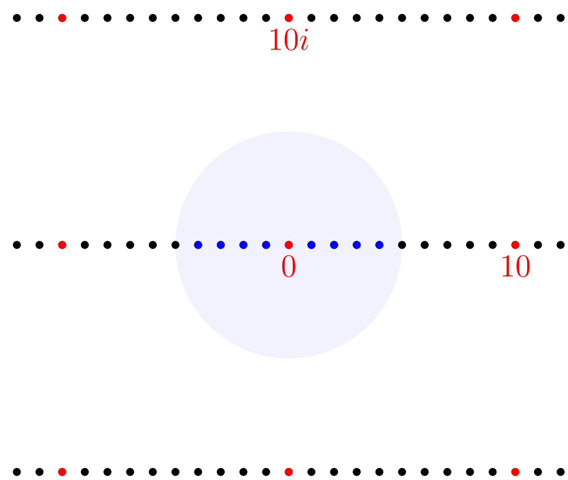
Each ideal $I \subset \mathcal{O}_K$ can be represented as (i_1, i_2) for some $i_1, i_2 \in \mathcal{O}_K$. Conditions involving ideals can be expressed in diophantine terms in terms of the generators. For example:

- $a \in I \iff (\exists x, y \in \mathcal{O}_K)\ \ a = xi_1 + yi_2$;
- $J|I \iff i_1, i_2 \in J$;
- $I = J \iff I|J$ and $J|I$;
- I, J are coprime $\iff (\exists i \in I)(\exists j \in J)\ \ i + j = 1$;
- for $s = a/b \in K$, we have $(s) = I/J \iff aJ = bI$;
- $I = \operatorname{num}(s) \iff (\exists J)\ \ (s) = I/J$ and I, J are coprime;
- $a \equiv b \pmod{I} \iff a - b \in I$; and
- $a \equiv' b \pmod{I} \iff I \,|\, \operatorname{num}(a - b)$.

3. Using congruences

Here is an example of how to use a congruence to force an algebraic integer to belong to a smaller ring of integers:

Example 3.1. If $\alpha \in \mathbb{Z}[i]$ is such that $|\alpha| < 5$ and $\alpha \equiv k \pmod{10\mathbb{Z}[i]}$ for some $k \in \mathbb{Z}$, then $\alpha \in \mathbb{Z}$. One proof: $\bar{\alpha} - \alpha \in 10\mathbb{Z}[i]$, but $|\bar{\alpha} - \alpha| < 5 + 5$, so $\bar{\alpha} = \alpha$; that is, $\alpha \in \mathbb{Z}$. (The dots below are the $\alpha \in \mathbb{Z}[i]$ congruent to an integer modulo $10\mathbb{Z}[i]$.)



To generalize to $\mathcal{O}_L \supset \mathcal{O}_K$ in place of $\mathbb{Z}[i] \supset \mathbb{Z}$, and an $\mathcal{O}_K$-ideal I in place of 10, we use a condition $(\alpha - 1) \cdots (\alpha - n) \mid I\mathcal{O}_L$ to express that "I is much bigger than α":

Lemma 3.2. *Fix number fields $L \supset K$. There exists $n \geq 1$ such that for all $\alpha \in \mathcal{O}_L$, all nonzero ideals $I \subset \mathcal{O}_K$, and all $k \in K$,*

$$(\alpha - 1) \cdots (\alpha - n) \mid I\mathcal{O}_L \quad \text{and} \quad \alpha \equiv' k \pmod{I\mathcal{O}_L} \qquad \Longrightarrow \qquad \alpha \in \mathcal{O}_K.$$

Proof. Enlarge L to assume that $L/\mathbb{Q}$ is Galois. Let $\ell = [L : \mathbb{Q}]$. Choose n such that $n > 23\ell$ and $10^{n-20\ell} > (4n)^\ell$. Below, j ranges over integers in $[1, n]$, and τ ranges over elements of $\operatorname{Gal}(L/\mathbb{Q})$. Given $\alpha \in \mathcal{O}_L$, embed L in $\mathbb{C}$ so that $|\alpha| \geq |{}^\tau\alpha|$ for all τ. Let $M = |\alpha|$.

Suppose that $(\alpha - 1) \cdots (\alpha - n) \mid I\mathcal{O}_L$ and $\alpha \equiv' k \pmod{I\mathcal{O}_L}$, but $\alpha \notin \mathcal{O}_K$. Choose $\sigma \in \operatorname{Gal}(L/K)$ with ${}^\sigma\alpha \neq \alpha$. Applying σ to $\alpha \equiv' k \pmod{I\mathcal{O}_L}$ and subtracting gives

$I\mathcal{O}_L \mid ({}^\sigma\alpha - \alpha)$, so $(\alpha-1)\cdots(\alpha-n) \mid ({}^\sigma\alpha - \alpha)$. Apply the norm $\mathrm{N}\colon L \to \mathbb{Q}$ and then $|\ |$:

$$\prod_{j,\tau} |{}^\tau\alpha - j| \le \prod_{\tau} |{}^{\tau\sigma}\alpha - {}^\tau\alpha| \le (2M)^\ell \quad \text{(since } |{}^\tau\alpha| \le |\alpha| = M \text{ for all } \tau).$$

We will contradict the last line by proving that many terms on the left are large. For each τ, let $J_\tau = \{j : |{}^\tau\alpha - j| < 10\}$, so $\#J_\tau \le 20$. Let $J_0 := \bigcup_\tau J_\tau$, so $\#J_0 \le 20\ell$. Let $J_1 := \{1,\ldots,n\} - J_0$, so $\#J_1 \ge n - 20\ell$.

- If $M \ge 2n$ (so in particular $M \ge 4$, so $(M/2)^3 \ge 2M$), then $\prod_{j \in J_1} |\alpha - j| \ge (M/2)^{\#J_1} \ge (M/2)^{n-20\ell} > (M/2)^{3\ell} \ge (2M)^\ell$. If $M < 2n$, then $\prod_{j\in J_1}|\alpha - j| \ge 10^{\#J_1} \ge 10^{n-20\ell} > (4n)^\ell > (2M)^\ell$.
- For $\tau \ne 1$, we have $\prod_{j \in J_1} |{}^\tau\alpha - j| \ge \prod_{j\in J_1} 10 \ge 1$.
- For $j \in J_0$, we use $\prod_\tau |{}^\tau\alpha - j| = |\mathrm{N}(\alpha - j)| \ge 1$.

Multiplying these inequalities gives $\prod_{j,\tau} |{}^\tau\alpha - j| > (2M)^\ell$, a contradiction. □

4. Weakly approximating $\mathbb{Z}$

Let K be a number field. For each prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, let $K_\mathfrak{p}$ be the completion. Let $S \subset K$. Say that S weakly approximates $\mathbb{Z}$ if any of the following equivalent conditions holds:

(i) $\mathbb{Z}$ is contained in the closure of S in $\prod_\mathfrak{p} K_\mathfrak{p}$.
(ii) for every $k \in \mathbb{Z}$ and primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ of $\mathcal{O}_K$, there is a sequence in S converging to k in $K_{\mathfrak{p}_i}$ simultaneously for every i;
(iii) for every $k \in \mathbb{Z}$ and nonzero ideal $I \subset \mathcal{O}_K$, the congruence $x \equiv' k \pmod{I}$ has a solution in S.

Lemma 4.1. *If $S \subset K$ weakly approximates $\mathbb{Z}$ and $0 \ne \beta \in \mathcal{O}_K$, then there exists $s \in S$ with $\beta \mid \operatorname{num}(s)$.*

Proof. The congruence $x \equiv' 0 \pmod{(\beta)}$ has a solution in S. □

Theorem 4.2. *For an extension of number fields L/K, if $\mathcal{A}_{K,L}$ holds, then*
(a) *there exists an infinite $\mathcal{O}_L$-diophantine subset $T \subset K$; and*
(b) *there exists an $\mathcal{O}_L$-diophantine subset $S \subset K$ that weakly approximates $\mathbb{Z}$;*
(c) *there exists an $\mathcal{O}_L$-diophantine subset U with $\mathbb{Z} \subset U \subset \mathcal{O}_K$;*
(d) *the subset $\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine.*

Proof. Fix A as in $\mathcal{A}_{K,L}$. Let $r = (A(L) : A(K))$. Then $A(K)$ is a finite union of cosets of $rA(L)$, so $A(K)$ is $\mathcal{O}_L$-diophantine.

(a) Choose a closed immersion $A \hookrightarrow \mathbb{P}^N_K$ for some N, and let T be the set of ratios of projective coordinates of the points in $A(K) \subset \mathbb{P}^N(K)$, excluding ratios with denominator 0. Since $A(K)$ is infinite, T is infinite. By definition, T is $\mathcal{O}_L$-diophantine.
(b) Let $y_1, \ldots, y_g \in K(A)$ be local parameters for A at 0. Define

$$S = \left\{ \frac{y(Q)}{y(P)} : P, Q \in A(K),\ y \in \sum_{i=1}^{g} T y_i \right\} \quad \subset K;$$

we exclude ratios $y(Q)/y(P)$ in which $y(P)$ or $y(Q)$ is undefined or in which $y(P) = 0$. By definition, S is $\mathcal{O}_L$-diophantine.

Let $k \in \mathbb{Z}$. Let p be a prime number. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ above p. If $R \to 0$ along a smooth analytic arc in the p-adic manifold $A(K_\mathfrak{p})$ and $y \in K(A)$ is a uniformizer at 0 along this arc, then $y(kR)/y(R) \to k$ in $K_\mathfrak{p}$ (l'Hôpital's rule). Let $a \in A(K)$ be a point of infinite order. Using formal group coordinates shows that $N!a \in A(K_\mathfrak{p})$ tends to 0 along such an arc as $N \to \infty$, and the function $y := \sum t_i y_i$ is a uniformizer at 0 along the arc for any $(t_1, \dots, t_g) \in K^g$ outside a hyperplane $H_\mathfrak{p} \subset \mathbb{A}^g_{K_\mathfrak{p}}$. Now, given *finitely many* primes $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ of $\mathcal{O}_K$, we can choose $(t_1, \dots, t_g) \in T^g$ outside all of $H_{\mathfrak{p}_1}, \dots, H_{\mathfrak{p}_m}$, since T is infinite; then $y(k(N!a))/y(N!a) \to k$ in $K_{\mathfrak{p}_i}$ for each $i \in \{1, \dots, m\}$. Thus S weakly approximates $\mathbb{Z}$.

(c) Let n be as in Lemma 3.2. Let U' be the set of $\alpha \in \mathcal{O}_L$ such that there exist $k \in S$ and $I = \operatorname{num}(s)$ for some $s \in S$ such that $(\alpha - 1) \cdots (\alpha - n) \mid I\mathcal{O}_L$ and $\alpha \equiv' k \pmod{I\mathcal{O}_L}$. The end of Section 2 implies that U' is $\mathcal{O}_L$-diophantine. By Lemma 3.2, $U' \subset \mathcal{O}_K$.

If $\alpha \in \mathbb{Z} - \{1, \dots, n\}$, Lemma 4.1 provides $s \in S$ such that $(\alpha - 1) \cdots (\alpha - n) \mid I\mathcal{O}_L$, where $I := \operatorname{num}(s)$. Since S weakly approximates $\mathbb{Z}$, there exists $k \in S$ such that $k \equiv' \alpha \pmod{I}$. Thus $\alpha \in U'$.

Take $U := U' \cup \{1, \dots, n\}$, which is $\mathcal{O}_L$-diophantine.

(d) Let $b_1, \dots, b_\kappa$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then $\mathcal{O}_K = \sum_{i=1}^{\kappa} U b_i$, which is $\mathcal{O}_L$-diophantine. □

Remark 4.3. In order to guarantee that some y was a uniformizer along the arc for each of $\mathfrak{p}_1, \dots, \mathfrak{p}_m$, we let y range over all linear combinations of $y_1, \dots, y_g$ with coefficients in an infinite set T. But in fact, if we assume (as we may) that A is simple, then already y_1 suffices, because the p-adic analogue of Wüstholz's analytic subspace theorem implies that for every $\mathfrak{p}$, the $\mathfrak{p}$-adic logarithm $\log_\mathfrak{p} a \in \operatorname{Lie} A_{K_\mathfrak{p}}$ does not lie in any hyperplane defined over K; see [Mat10, Theorem 1] or [FP15, Proposition 2.5].

5. Shlapentokh's reduction

Theorem 5.1 (Shlapentokh)**.** *Assume that*

- *$\mathbb{Z}$ is $\mathcal{O}_E$-diophantine for every totally real number field E, and*
- *$\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine for every degree 2 extension of number fields L/K.*

Then $\mathbb{Z}$ is $\mathcal{O}_F$-diophantine for every number field F.

Proof. If F'/F is a finite extension and $\mathbb{Z}$ is $\mathcal{O}_{F'}$-diophantine, then $\mathbb{Z}$ is also $\mathcal{O}_F$-diophantine. Thus we may enlarge F to assume that F is Galois over $\mathbb{Q}$.

For each complex conjugation $\sigma \in \operatorname{Aut} F$ arising from a nonreal emebedding $F \hookrightarrow \mathbb{C}$, we have $[F : F^\sigma] = 2$, so $\mathcal{O}_{F^\sigma}$ is $\mathcal{O}_F$-diophantine. Let $E = \bigcap_\sigma F^\sigma$. Then the intersection $\mathcal{O}_E = \bigcap_\sigma \mathcal{O}_{F^\sigma}$ is $\mathcal{O}_F$-diophantine. On the other hand, E is totally real, so $\mathbb{Z}$ is $\mathcal{O}_E$-diophantine by assumption. By transitivity, $\mathbb{Z}$ is $\mathcal{O}_F$-diophantine. □

Remark 5.2. [KP25, Corollary 2.5] proved $\mathcal{A}_{K,L}$ (and hence that $\mathcal{O}_K$ is $\mathcal{O}_L$-diophantine) not for all degree 2 extensions L/K, but only those satisfying all of the following additional assumptions: $K \subset \mathbb{R}$, L is Galois over $\mathbb{Q}$, and $L \supset L_0 := \mathbb{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{19})$. But it is easy to adapt the proof of Theorem 5.1 to use its second hypothesis only for these extensions, by enlarging F to contain L_0.

Acknowledgments

I thank Laurent Moret-Bailly and Cong Wen for comments.

References

[ABHS25] Levent Alpöge, Manjul Bhargava, Wei Ho, and Ari Shnidman, *Rank stability in quadratic extensions and Hilbert's tenth problem for the ring of integers of a number field*, `https://arxiv.org/abs/2501.18774v1` [math.NT], 2025. 1, 2

[BP25] Bhargav Bhatt and Bjorn Poonen, *Diophantine sets*, `https://math.mit.edu/~poonen/papers/diophantine.pdf`, November 20, 2025. 2

[CPZ05] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735. MR 2212121 1

[Den75] J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220. MR 360513 1

[Den80] ———, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236. MR 549163 1, 2

[DL78] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391. MR 518221 1, 2

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR 133227 1

[FP15] C. Fuchs and D. H. Pham, *The p-adic analytic subgroup theorem revisited*, p-Adic Numbers Ultrametric Anal. Appl. **7** (2015), no. 2, 143–156. MR 3343453 5

[GFP20] Natalia Garcia-Fritz and Hector Pasten, *Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points*, Math. Ann. **377** (2020), no. 3-4, 989–1013. MR 4126887 1

[KLS24] Debanjana Kundu, Antonio Lei, and Florian Sprung, *Studying Hilbert's 10th problem via explicit elliptic curves*, Math. Ann. **390** (2024), no. 4, 5153–5183. MR 4816107 1

[KP25] Peter Koymans and Carlo Pagano, *Hilbert's tenth problem via additive combinatorics*, `https://arxiv.org/abs/2412.01768v2` [math.NT], 2025. 1, 2, 5

[Mat70] Yuri Matiyasevich, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282. MR 258744 1

[Mat10] Tzanko Matev, *The p-adic analytic subgroup theorem and applications*, `https://arxiv.org/abs/1010.3156v1` [math.NT], 2010. 5

[MP18] M. Ram Murty and Hector Pasten, *Elliptic curves, L-functions, and Hilbert's tenth problem*, J. Number Theory **182** (2018), 1–18. MR 3703929 1

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575. MR 2660452 1

[MR18] Barry Mazur and Karl Rubin, *Diophantine stability*, Amer. J. Math. **140** (2018), no. 3, 571–616, With an appendix by Michael Larsen. MR 3805014 1

[MRS24] Barry Mazur, Karl Rubin, and Alexandra Shlapentokh, *Existential definability and diophantine stability*, J. Number Theory **254** (2024), 1–64, corrigendum in J. Number Theory **262** (2024), 539–540. MR 4633727 1, 2

[Pas23] Héctor Pastén, *Elliptic surfaces and Hilbert's tenth problem*, Rev. Mat. Teor. Apl. **30** (2023), no. 1, 113–120. MR 4538034 1

[Phe88] Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. Amer. Math. Soc. **104** (1988), no. 2, 611–620. MR 962837 1

[Poo02] Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 33–42. MR 2041072 1, 2

[RW24] Anwesh Ray and Tom Weston, *Hilbert's tenth problem in anticyclotomic towers of number fields*, Trans. Amer. Math. Soc. **377** (2024), no. 5, 3577–3597. MR 4744788 1

[Shl89] Alexandra Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 7, 939–962. MR 1008797 1

[Shl08] ———, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555. MR 2386235 1, 2

[SW23] Ari Shnidman and Ariel Weiss, *Rank growth of elliptic curves over n-th root extensions*, Trans. Amer. Math. Soc. Ser. B **10** (2023), 482–506. MR 4575766 1

[Zyw25] David Zywina, *Rank one elliptic curves and rank stability*, https://arxiv.org/abs/2505.16960v1 [math.NT], 2025. 1, 2

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

Email address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/