MAZUR'S WORK RELATING LOGIC AND ARITHMETIC GEOMETRY

BJORN POONEN

Barry Mazur has had a longstanding interest in questions of decidability in number theory, continuing a long tradition going back at least to Hilbert. This has guided him to interesting new questions and theorems in arithmetic geometry.

Hilbert's tenth problem, from the list of 23 problems he published after a famous lecture in 1900, asked for an algorithm to decide, given a multivariable polynomial equation with integer coefficients, whether it has a solution in integers. In 1970, Matiyasevich [Mat70], building on work of Davis, Putnam, and Robinson [DPR61], proved that no such algorithm exists; Mazur himself wrote a beautiful survey article on this [Maz94].

But if the question is changed by replacing $\mathbb{Z}$ by $\mathbb{Q}$, it is not known whether an algorithm exists. One possible approach: If $\mathbb{Z}$ is *diophantine* over $\mathbb{Q}$ (that is, there is a $\mathbb{Q}$-variety X with a morphism to $\mathbb{A}^1$ such that the image of $X(\mathbb{Q}) \to \mathbb{A}^1(\mathbb{Q}) = \mathbb{Q}$ is $\mathbb{Z}$), then the negative answer for $\mathbb{Z}$ implies a negative answer for $\mathbb{Q}$.

The suggestion that $\mathbb{Z}$ might be diophantine over $\mathbb{Q}$ led Mazur, in a contrarian mood, to pose a new type of question, about "topology of rational points": he asked whether, for every variety X over $\mathbb{Q}$, the closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ (with respect to the Euclidean topology) has at most finitely many connected components [Maz92, Conjecture 3]. Mazur observed that a positive answer to this question would imply that $\mathbb{Z}$ is *not* diophantine over $\mathbb{Q}$ and hence would rule out one approach to a negative answer to Hilbert's tenth problem over $\mathbb{Q}$. There has been little progress on Mazur's question beyond the special cases that Mazur himself proved in [Maz92]. But this is not for a lack of interest! Rather, it is a testament to the difficulty of understanding rational points on higher-dimensional varieties. Mazur also asked about stronger versions of his question: for example, he asked whether, for a smooth variety X in which $X(\mathbb{Q})$ is Zariski dense, the closure of $X(\mathbb{Q})$ must be a union

---

Date: July 11, 2025.

The writing of this article was supported in part by National Science Foundation grant DMS-2101040 and Simons Foundation grants #402472 and #550033.

of connected components of $X(\mathbb{R})$ [Maz92, Conjecture 1]. The answer to this turned out to be no [CTSSD97, Section 5].

In a different direction, Denef and Lipshitz conjectured in 1978 that for every number field K, Hilbert's tenth problem over the ring of integers $\mathcal{O}_K$ has a negative answer [DL78]. This was proved in the 1970s and 1980s for several classes of number fields, by using unit groups [Den75, DL78, Den80, Phe88, Shl89]; building on these methods, Mazur, Rubin, and Shlapentokh recently constructed a uniform definition of $\mathbb{Z}$ in the rings of integers of many *infinite* algebraic extensions of $\mathbb{Q}$, and answered a 1948 question of Tarski by proving that the first-order theory of the field of constructible numbers is undecidable [MRS24a]. On the other hand, various authors observed that elliptic curves could be used in place of unit groups [Poo02, CPZ05, Shl08]. In particular, for an extension of number fields L/K, if there exists an elliptic curve E over K with $0 < \operatorname{rank} E(K) = \operatorname{rank} E(L)$, then $\mathcal{O}_K$ is diophantine over $\mathcal{O}_L$, so a negative answer to Hilbert's tenth problem for $\mathcal{O}_K$ implies a negative answer for $\mathcal{O}_L$; one might hope to reach every number field inside a tower of such extensions.

Mazur and Rubin then began to investigate this phenomenon of "diophantine stability". In particular, using an approach inspired by [Kol90] and developed further in [MR04], Mazur and Rubin gave a conditional proof that for every prime-degree cyclic extension of number fields L/K, such an elliptic curve exists [MR10, Theorem 1.13]. This was enough to yield a *conditional* proof that for every number field K, Hilbert's tenth problem over $\mathcal{O}_K$ has a negative answer [MR10]. The results were conditional on the finiteness of Tate–Shafarevich groups, but this finiteness was widely believed to hold, so the Mazur–Rubin result was strong evidence for the Denef–Lipshitz conjecture. The strategy of Mazur and Rubin involved a delicate analysis of how Selmer groups change in a family of quadratic twists: for many elliptic curves over number fields, they showed that by twisting carefully, they could make the Selmer rank go up or down. By iterating this, they proved that over every number field K, there is an elliptic curve of rank 0, and they could also force rank 1 over K and L simultaneously, assuming finiteness of Tate–Shafarevich groups (used to ensure parity, to prevent the rank over K from dropping to 0). In later joint work with Klagsbrun, they also used these ideas towards results in arithmetic statistics, concerning the distribution of 2-Selmer ranks in a family of quadratic twists of an elliptic curve [KMR13, KMR14]. Mazur and Rubin returned to questions of diophantine stability in [MR18, MR20]; the former article produced new families of field extensions L/K and K-varieties V such that $V(K) = V(L)$, with applications to new unconditional cases of Hilbert's tenth problem over rings of integers, and applications to determining the possible field extensions generated by a varying algebraic point on a given variety.

Afterword: Koymans and Pagano found a way to use a theorem of additive combinatorics to construct rank-stable elliptic curves for enough extensions to prove a negative answer to Hilbert's tenth problem over $\mathcal{O}_K$ for *every* number field K [KP25]. About two months later, Alpöge, Bhargava, Ho, and Shnidman posted a second argument, using a less sophisticated input from additive combinatorics but constructing only an *abelian variety* exhibiting rank stability, not an elliptic curve [ABHS25]. Fortunately for them, Mazur, Rubin, and Shlapentokh had just proved what they needed, that a rank-stable abelian variety would do just as well as a rank-stable elliptic curve for proving the negative answer to Hilbert's tenth problem for rings of integers [MRS24b]!

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.

[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

[CTSSD97] J.-L. Colliot-Thélène, A. N. Skorobogatov, and Peter Swinnerton-Dyer, *Double fibres and double covers: paucity of rational points*, Acta Arith. **79** (1997), no. 2, 113–135. MR 1438597

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

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

[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

[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

[KMR13] Zev Klagsbrun, Barry Mazur, and Karl Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320, erratum in Ann. of Math. (2) **198** (2023), no. 2, 879–880. MR 3043582

[KMR14] ———, *A Markov model for Selmer ranks in families of twists*, Compos. Math. **150** (2014), no. 7, 1077–1106. MR 3230846

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR 1106906

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

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

[Maz92] Barry Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45. MR 1181085

[Maz94] B. Mazur, *Questions of decidability and undecidability in number theory*, J. Symbolic Logic **59** (1994), no. 2, 353–371. MR 1276620

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96. MR 2031496

[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

[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

[MR20] ———, *Big fields that are not large*, Proc. Amer. Math. Soc. Ser. B **7** (2020), 159–169. MR 4173816

[MRS24a] Barry Mazur, Karl Rubin, and Alexandra Shlapentokh, *Defining $\mathbb{Z}$ using unit groups*, Acta Arith. **214** (2024), 235–255. MR 4772285

[MRS24b] ———, *Existential definability and diophantine stability*, J. Number Theory **254** (2024), 1–64, corrigendum in J. Number Theory **262** (2024), 539–540. MR 4633727

[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

[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

[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

[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

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

Email address: `poonen@math.mit.edu`

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