STUDYING HILBERT'S 10^{th} PROBLEM VIA EXPLICIT ELLIPTIC CURVES

DEBANJANA KUNDU, ANTONIO LEI, AND FLORIAN SPRUNG

During our four weeks at the IAS as part of the Summer Collaboration Program (2022), we made progress in the study of the analogue of Hilbert's 10^{th} Problem for rings of integers of number fields. The precise question is the following:

Is $\mathbb{Z}$ a Diophantine subset of the ring of integers of a number field L?

A positive answer to this question implies that the analogue of Hilbert's 10^{th} Problem is unsolvable for the ring of integers of L. Our strategy to prove such results is inspired by the work of N. Garcia-Fritz–H. Pasten, see [GFP20]. However, there are some important differences which will be explained after mentioning the key ingredients that go into the proof. The manuscript is available via arXiv, see [KLS22].

Theorem (García-Fritz–Pasten)**.** *There are explicit Chebotarev sets of primes $\mathscr{P}$ and $\mathscr{Q}$, of density $\frac{5}{16}$ and $\frac{1}{12}$, such that for all $p \in \mathscr{P}$ and $q \in \mathscr{Q}$, the analogue of Hilbert's 10th Problem is unsolvable for the ring of integers of $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$.*

Main ideas of the proof. The proof consists the following three main steps:

Step 1: The starting point is the following corollary of a result by A. Shlapentokh [Shl08]: Suppose that there exists a rank-zero elliptic curve over $\mathbb{Q}$ satisfying the following two conditions:

- in a quadratic extension $K/\mathbb{Q}$, the rank jumps *and*
- in an Integrally Diophantine extension $F/\mathbb{Q}$, the rank remains zero.

Then the analogue of the Hilbert's 10th problem has a *negative solution* for the ring of integers of the composite number field, $L = K \cdot F$.

Step 2: Find a rank-zero elliptic curve $E/\mathbb{Q}$ (with mild conditions) and two families of number fields satisfying the following two properties:

- a family of Integrally Diophantine cubic number fields such that rank does not jump.
- a family of quadratic extensions such that rank jumps.

Step 3: Determine 'how big' these families are.

In [GFP20], the authors used Iwasawa theory to study rank stabilization of elliptic curves in cubic extensions. On the other hand in [KLS22], we provide a direct argument which allows us to construct larger families where the rank does not jump.

To count the number of quadratic extensions with rank jump requires the work of D. Kriz–C. Li [KL19] (or the work of A. Smith [Smi16] when working with the congruent number curves).

Improving the results of Garcia-Fritz–Pasten. First, we refine the results of [GFP20, Theorem 1.2] and improve the densities of both $\mathscr{P}$ and $\mathscr{Q}$.

Theorem. *There are explicit Chebotarev sets of primes $\mathscr{P}$ and $\mathscr{Q}$, of density $\frac{9}{16}$ and $\frac{7}{48}$, such that for all $p \in \mathscr{P}$ and $q \in \mathscr{Q}$, the analogue of Hilbert's 10th Problem is unsolvable for the ring of integers of $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$.*

Complementary Results. Second, it was possible to provide a direct proof by proving the vanishing of certain 3-Selmer groups (rather than the finiteness of 3^∞-Selmer group). This allows significant weakening of the hypotheses and the possibility to find many auxiliary elliptic curves (not necessarily of positive minimal discriminant).

Theorem. *Let*

$$\mathfrak{D} = \{7, 39, 95, 127, 167, 255, 263, 271, 303, 359, 391, 447, 479, 527, 535, 615, 623, 655, 679, 695\}.$$

For all $D \in \mathfrak{D}$, there are explicit Chebotarev sets of primes $\mathscr{P}$ (independent of D) and $\mathscr{Q}_D$, of density $\frac{9}{16}$ and $\frac{1}{12}$ such that for all $p \in \mathscr{P}$ and $q \in \mathscr{Q}_D$, the analogue of Hilbert's 10th Problem is unsolvable for the ring of integers of $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{Dq})$.

By working with a pair of auxiliary elliptic curves, it is possible to improve significantly the density of $\mathscr{P}$, at the expense of a smaller set of $\mathfrak{D}$ and a lower density for the sets $\mathscr{Q}_D$.

Theorem. *Let $D \in \{7, 615\}$. There are explicit Chebotarev sets of primes $\mathscr{P}$ (independent of D) and $\mathscr{Q}_D$, of density $\frac{103}{128}$ and $\frac{1}{36}$, such that for all $p \in \mathscr{P}$ and $q \in \mathscr{Q}_D$, the analogue of Hilbert's 10th problem is unsolvable for the ring of integers of $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{Dq})$.*

Finally, the more direct approach permits working with elliptic curves with good supersingular reduction at 3. This provides the opportunity to work with congruent number elliptic curves, on which many important breakthroughs have been announced in recent years (see for example [Smi16, Kri20]).

Theorem. *There is an explicit Chebotarev set of primes $\mathscr{P}$ with density $\frac{11}{16}$ such that Hilbert's 10th Problem is unsolvable for the ring of integers of $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{q})$ whenever q is a congruent number.*

Outlook

As per the knowledge of the authors, this is the first time that the study of an analogue of Hilbert's 10^{th} Problem has been related to the Congruent Number Problem.

Our approach towards proving the aforementioned theorems required finding explicit curves satisfying certain properties. It would therefore be interesting to consider the following problem(s).

Problem.

(*a*) *Find a method that generates infinitely many such auxiliary curves.*
(*b*) *If such a method exists, is it be possible to ensure that the resulting $\mathscr{Q}$ is non-empty? Or even have positive density?*

Acknowledgements

We were fortunate to spend four weeks at the Institute. Our daily discussions gave rise to the results and the problem described above and much more, e.g. the discovery of a bug in SAGE. We heartily thank the Institute for the kind support, warm hospitality, and jovial lunch conversations.

References

[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.

[KL19] Daniel Kriz and Chao Li, *Goldfeld's conjecture and congruences between Heegner points*, Forum Math. Sigma **7** (2019), Paper No. e15, 80.

[KLS22] Debanjana Kundu, Antonio Lei, and Florian Sprung, *Studying Hilbert's 10th problem via explicit elliptic curves*, preprint, ArXiv:2207.07021.

[Kri20] Daniel Kriz, *Supersingular main conjectures, Sylvester's conjecture and Goldfeld's conjecture*, 2020, preprint, ArXiv:2002.04767.

[Shl08] Alexandra Shlapentokh, *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.

[Smi16] Alexander Smith, *The congruent numbers have positive natural density*, 2016, preprint, ArXiv:1603.08479.