Canad. Math. Bull. Vol. **68** (3), 2025, pp. 939–949
http://dx.doi.org/10.4153/S0008439525000219
© The Author(s), 2025. Published by Cambridge University Press on behalf of Canadian Mathematical Society

Hilbert's 10th problem via Mordell curves

Somnath Jha, Debanjana Kundu, and Dipramit Majumdar

Abstract. We show that for 5/6-th of all primes p, Hilbert's 10th problem is unsolvable for the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$. We also show that there is an infinite set S of square-free integers such that Hilbert's 10th problem is unsolvable over the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt{D}, \sqrt[3]{p})$ for every $D \in S$ and for every prime $p \equiv 2, 5 \pmod 9$. We use the CM elliptic curves $y^2 = x^3 - 432D^2$ associated with the cube-sum problem, with D varying in suitable congruence class, in our proof.

1 Introduction

In 1900, D. Hilbert posed the following question (which was the tenth in his list of twenty-three questions): does there exist an algorithm (Turing machine) that takes as input polynomial equations over $\mathbb{Z}$ and decides whether they have integer solutions. Building on the work of M. Davis, H. Putnam, and J. Robinson in [6, 5, 19], Y. Matiyasevich proved that computably enumerable sets over $\mathbb{Z}$ are exactly the same as the Diophantine sets over $\mathbb{Z}$; see [15]. In other words, he proved that Hilbert's 10th problem is unsolvable.

Soon after in 1978, J. Denef and L. Lipshitz [7] asked whether there exists an algorithm (Turing machine) that takes as input polynomial equations over $\mathcal{O}_F$ (the ring of integers of a number field F) and decides whether they have integer solutions. A straight-forward argument shows that if $\mathbb{Z}$ is Diophantine in $\mathcal{O}_F$, then the analog of Hilbert's 10th problem for $\mathcal{O}_F$ has a negative solution.

At the start of the 21st century, it was first observed by B. Poonen that there is a connection between rank stabilization of elliptic curve in extensions of number fields and Hilbert's 10th problem, [18]. The result was further strengthened by A. Shlapentokh (which is recorded in Theorem 2.2) and has been one of the key tools in proving new cases of the conjecture of Denef–Lipshitz. For several classes of number fields, Denef–Lipshitz conjecture has been established. For example, (i) if a number field is totally real, (ii) if it a quadratic extension of a totally real number field, (iii) if the number field is abelian or (iv) if it has precisely one (pair of) complex places. There are also important related works of B. Mazur–K. Rubin [16]. For degree 6 number fields of the form $\mathbb{Q}(\sqrt{-q}, \sqrt[3]{p})$ as p and q vary over certain explicit set of primes of positive density, Denef–Lipshitz conjecture was established in [8, 13].

Received by the editors December 6, 2024; revised February 18, 2025; accepted February 18, 2025.
Published online on Cambridge Core February 26, 2025.
AMS subject classification: **11G05**, 11U05, 11D25.
Keywords: Hilbert's 10th Problem, cube-sum problem, elliptic curves, cubic twists.

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

On the other hand, [21] proves that for a positive proportion of integers a, Hilbert's 10th problem is unsolvable for $\mathcal{O}_F$ where F is of the form $\mathbb{Q}(\sqrt[6]{a})$.

We consider Hilbert's 10th problem for the ring of integers of certain S_3 extensions and degree 12 extensions of $\mathbb{Q}$. The Kummer extension $\mathbb{Q}(\zeta_3, \sqrt[3]{m})$, $m \in \mathbb{Z}$ is the first layer of the so called "false Tate curve" extension for $p = 3$ and is widely studied in (non-commutative) Iwasawa theory. Using Mordell curves $\mathsf{E}_a : y^2 = x^3 + a$, $a \in \mathbb{Z}$ and its cubic twists, we apply results on the cube-sum problem to prove new cases of the Hilbert's 10th problem. In particular, we prove the following results.

Theorem A *For $\frac{5}{6}$-th of all primes p, Hilbert's 10th problem has a negative solution over the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$.*

Proposition A *Hilbert's 10th problem is unsolvable over the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt{D}, \sqrt[3]{p})$, where D varies over an infinite set S consisting of square-free integers and p is a prime such that $p \equiv 2, 5 \pmod 9$. Further, $\#(S \cap [-X, X]) \gg X^{1-\varepsilon}$ where $X \gg 0$ and for any $\varepsilon > 0$.*

We emphasize that this result complements the results proven in [13] and indeed provides (infinitely many) new examples of number fields where Hilbert's 10th problem is unsolvable.

We are interested in Hilbert's 10th problem for the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{m})$, $m \in \mathbb{Z}$ and it raised the following natural question which is of interdependent interest: given a Mordell elliptic curve $\mathsf{E}_a : y^2 = x^3 + a$, $a \in \mathbb{Z}$ does there exist a cube-free integer D co-prime to a such that precisely one of the elliptic curves $\mathsf{E}_a, \mathsf{E}_{aD^2}, \mathsf{E}_{aD^4}$ has positive Mordell–Weil rank over $\mathbb{Q}$? We did an extensive computation on this on SAGE/MAGMA which are mentioned in Section 3. This led us to apply results from the cube-sum problem.

As we were completing our preprint, C. Pagano–P. Koymans announced an unconditional proof of the unsolvability of Hilbert's 10th problem [12] over the ring of integers of any number field. Their result is accomplished by constructing elliptic curves E and studying their quadratic twists to guarantee that there is no rank growth of E in certain quadratic extensions. They use 2-descent argument and tools from additive combinatorics. On the other hand, our approach involves studying cubic twists instead of quadratic twists of elliptic curves. In fact, we specifically use Mordell curves. We use results from the cube-sum problem to study the cubic twists of the Mordell curves. Thus our method is different. Even more recently, L. Alpöge–M. Bhargava–W. Ho–A. Shnidman announced another proof; see [1].

Organization

Including this introduction, there are four sections in this short note. Section 2 is preliminary in nature, where we record crucial results that will be used in the main argument. In Section 3, we discuss the main motivation behind this note and also raise questions which we have not been able to answer completely. In Section 4, we state and prove the main result of our note.

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

2 Preliminaries

In this section, we record some results which will be used crucially in our argument(s).

2.1 Cube-sum problem

The classical Diophantine cube-sum problem asks the question: which integers D can be expressed as a sum of two rational cubes? An integer D is called a cube-sum (resp. not a cube-sum), if $x^3 + y^3 = D$ has (resp. does not have) a rational solution. The elliptic curve $X^3 + Y^3 = DZ^3$ can be expressed in the Weierstrass equation as $y^2 = x^3 - 432D^2$ and for a cube-free integer $D > 2$ it is known that torsion subgroup of $\mathsf{E}_{-432D^2}(\mathbb{Q})$ vanishes. Thus, a cube-free integer $D > 2$ satisfies $D = a^3 + b^3$ for $a, b \in \mathbb{Q}$ if and only if the Mordell-Weil group $E_{-432D^2}(\mathbb{Q})$ has a positive rank. The cube-sum problem has been studied in great detail with important contributions by J. Sylvester, F. Lucas, T. Pépin, E. Selmer, P. Satgé, D. Lieman, F. R. Villegas–D. Zagier etc. Some recent works include [2–4, 9]. We refer to [2, 4] for a literature review. We record the special cases below which will be used in the article.

Theorem 2.1

(a) *Suppose that* $p \equiv 2, 5 \pmod 9$ *is an odd prime. By [22, Section 2] the integers* $p, p^2, 9p,$ *and* $9p^2$ *are not cube-sum. In other words for all primes* $p \equiv 2, 5 \pmod 9$*, we have*

$$\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432p^2}(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432p^4}(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432(9p)^2}(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432(9p^2)^2}(\mathbb{Q}) = 0.$$

(b) *Suppose that* $p \equiv 4, 7 \pmod 9$ *is an odd prime.*
   (i) *By [4], if* $3 \notin \mathbb{F}_p^3$*, then* p *is a cube-sum. In other words* $\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432p^2}(\mathbb{Q}) > 0$.
   (ii) *Suppose that* $\ell \equiv 8 \pmod 9$ *is a prime such that* $\ell \notin \mathbb{F}_p^3$*. By [14] the integers* $\ell p, \ell p^2,$ *and* $p\ell^2$ *are not cube-sum. Equivalently,*

$$\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432(\ell p)^2}(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432(\ell p^2)^2}(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432(p\ell^2)^2}(\mathbb{Q}) = 0.$$

(c) *Let* d *be a positive integer and* $a \equiv 8 \pmod 9$ *be an integer co-prime to* d*. By [11, Theorem B], there are infinitely many primes* $p \equiv a \pmod{9d}$ *such that* p *is a cube-sum.*

2.2 Hilbert's 10th problem and elliptic curves

Theorem 2.2 (A. Shlapentokh [20]) *Let* L/F *be an extension of number fields. Suppose that there is an elliptic curve* E *defined over* F *such that*

$$\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}(L) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}(F) > 0.$$

Then $\mathcal{O}_F$ *is Diophantine in* $\mathcal{O}_L$.

If further, it is known that $\mathbb{Z}$ *is Diophantine in* $\mathcal{O}_F$ *(i.e., the analog of Hilbert's 10th problem for* $\mathcal{O}_F$ *has a negative solution) then (by transitivity)* $\mathbb{Z}$ *is Diophantine in* $\mathcal{O}_L$ *and the analog of Hilbert's 10th problem for* $\mathcal{O}_L$ *has a negative solution.*

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

A useful corollary of Shlapentokh's theorem was proved in [8, Proposition 3.3], which we record below.

Theorem 2.3 *Let $F/\mathbb{Q}$ and $K/\mathbb{Q}$ be extensions of number fields with $K/\mathbb{Q}$ quadratic. Let L be the compositum of F and K over $\mathbb{Q}$. Suppose that there is an elliptic curve $\mathsf{E}/\mathbb{Q}$ satisfying the conditions:*

(i) $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(F) = 0$ *and*
(ii) $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(K) > 0$.

Then $\mathcal{O}_L/\mathcal{O}_F$ is integrally Diophantine.

If further, it is known that the analog of Hilbert's 10th problem for $\mathcal{O}_F$ has a negative solution, then the analog of Hilbert's 10th problem for $\mathcal{O}_L$ has a negative solution.

3 Some computations

3.1 Sufficient conditions

Let a be a non-zero integer and consider the elliptic curve

$$\mathsf{E} = \mathsf{E}_a : y^2 = x^3 + a.$$

It is well known that E_a is an elliptic curve with complex multiplication by $\mathbb{Z}[\zeta_3]$ and there is a degree 3 rational isogeny $\phi_a : \mathsf{E}_a \to \mathsf{E}_{-27a}$. It follows that $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(K) = 2\,\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q})$, here K denotes the number field $K = \mathbb{Q}(\zeta_3)$. Fix a cube-free (rational) integer D and define the elliptic curves

$$\mathsf{E}_1 = \mathsf{E}_{aD^2} : y^2 = x^3 + D^2 a$$
$$\mathsf{E}_2 = \mathsf{E}_{aD^4} : y^2 = x^3 + D^4 a.$$

The curves E_1 and E_2 are the cubic twists of E, i.e., the three elliptic curves E, E_1, and E_2 are isomorphic over $F = \mathbb{Q}(\sqrt[3]{D})$. In particular, the three elliptic curves are isomorphic over the Galois closure of F, in other words over the extension $L = F \cdot K = \mathbb{Q}(\zeta_3, \sqrt[3]{D})$.

Recall that

$$\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(L) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_1(L) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_2(L) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(K) + \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_1(K) + \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_2(K). \tag{3.1}$$

Now, suppose that for a fixed cube-free integer D, there exists an elliptic curve

$$\mathsf{E} : y^2 = x^3 + a_D$$

such that *exactly one* of E, E_1, E_2 has positive Mordell–Weil rank r over $\mathbb{Q}$ and the other two have Mordell–Weil rank 0. Without loss of generality, suppose that $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = r > 0$. Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(K) = 2r$ and by the assumption in the previous paragraph, it follows that $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_1(K) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_2(K) = 0$. This implies

$$\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(L) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(K) = 2r + 0 + 0 = 2r > 0.$$

Since Hilbert's 10th problem is unsolvable in $K = \mathbb{Q}(\zeta_3)$, using Shlapentokh's result (Theorem 2.2) we deduce the following lemma.

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

Lemma 3.1 *If there exists an elliptic curve* $\mathsf{E} : y^2 = x^3 + a$ *such that upon twisting by a cube-free integer D exactly one of* $\mathsf{E}/\mathbb{Q}$, $\mathsf{E}_1/\mathbb{Q}$, $\mathsf{E}_2/\mathbb{Q}$ *has positive Mordell–Weil rank, then Hilbert's 10th problem is unsolvable for* $\mathcal{O}_L$ *where* $L = \mathbb{Q}(\zeta_3, \sqrt[3]{D})$.

3.2 Data

We now present the data for the following SAGE computations. We fixed an elliptic curve $\mathsf{E} : y^2 = x^3 + a_D$ and varied $1 < D \leq 100$ over cube-free integers to check in which cases exactly one of the cubic twists had positive rank over $\mathbb{Q}$. By the earlier discussion we know that Hilbert's 10th problem is unsolvable in $\mathcal{O}_L$.

Example 3.2 Let D be an integer in the set

$$\{3, 5, 7, 9, 10, 11, 13, 21, 23, 25, 26, 28, 29, 31, 33, 39, 41, 44, 45, 46, 47, 49, 51, 55, 59, 61, 65, 66, 67,$$
$$69, 75, 76, 77, 82, 87, 91, 93, 95, 97, 98, 99, 100\}.$$

Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 1.$$

Then $\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}(\mathbb{Q}) = 0$ but using the SAGE code given below one can check that exactly one of $\mathsf{E}_1/\mathbb{Q}$ or $\mathsf{E}_2/\mathbb{Q}$ has rank 0 and the other has positive rank r. We can conclude that the Hilbert's 10th problem is unsolvable for the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{D})$.

```
a = 1
for d in range(1,100):
#sometimes the code stopped running; changed range
            manually
    E=EllipticCurve([0,a])
    E1=EllipticCurve([0,d^2*a])
    E2=EllipticCurve([0,d^4*a])
    print(d, E.rank(), E1.rank(), E2.rank())
```

Note: In the following examples, we only explicitly write the set of new D's.

Example 3.3 Fix $D \in \{17, 35, 71\}$. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 2.$$

Then a SAGE/MAGMA check shows that $\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}(\mathbb{Q}) = 1$ whereas $\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_1(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_2(\mathbb{Q}) = 0$.

Example 3.4 Fix D to be an integer in the set

$$\{12, 18, 20, 34, 42, 50, 53, 63, 83, 84, 94\}.$$

Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 3.$$

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

Then a SAGE/MAGMA check shows that $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 1$ whereas $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_1(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_2(\mathbb{Q}) = 0$.

Example 3.5 Let $D \in \{15, 38, 43, 57, 60, 62, 74, 75, 79, 85\}$ be an integer. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 4.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 0$ and exactly one of $\mathsf{E}_1/\mathbb{Q}$ or $\mathsf{E}_2/\mathbb{Q}$ has rank 0 and the other has positive rank r.

Example 3.6 Fix $D \in \{5, 6, 30, 36\}$. Let

$$\mathsf{E} : y^2 = x^3 + 5.$$

Then a SAGE check shows that $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 1$ whereas $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_1(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_2(\mathbb{Q}) = 0$.

Example 3.7 Let $D \in \{2, 4, 19, 52, 73, 86\}$ be an integer. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 6.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 0$ while exactly one of $\mathsf{E}_1/\mathbb{Q}$ or $\mathsf{E}_2/\mathbb{Q}$ has rank 0 and the other has positive rank r.

Example 3.8 Let $D \in \{34, 78, 90\}$ be an integer. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 7.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 0$, exactly one of $\mathsf{E}_1/\mathbb{Q}$ or $\mathsf{E}_2/\mathbb{Q}$ has rank 0 and the other has $r > 0$.

Example 3.9 Let $D \in \{68, 70\}$ be an integer. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 13.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 0$ and exactly one of $\mathsf{E}_1/\mathbb{Q}$ or $\mathsf{E}_2/\mathbb{Q}$ has rank 0 and the other has positive rank r.

Example 3.10 Let $D = 22$. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 14.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 0$ and exactly one of $\mathsf{E}_1/\mathbb{Q}$ or $\mathsf{E}_2/\mathbb{Q}$ has rank 0 and the other has rank $r > 0$.

Example 3.11 Let $D = 37$. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 15.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 2$ and we check using SAGE that $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_1(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_2(\mathbb{Q}) = 0$.

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

Table 1: Values of cube-free $1 \le D \le 100$ for which unsolvability of Hilbert's 10th problem is obtained using the method outlined above.

1	2	3	4	5	6	7	**8**	9	10
11	12	13	14	15	**16**	17	18	19	20
21	22	23	**24**	25	26	**27**	28	29	30
31	**32**	33	34	35	36	37	38	39	**40**
41	42	43	44	45	46	47	**48**	49	50
51	52	53	**54**	55	**56**	57	58	59	60
61	62	63	**64**	65	66	67	68	69	70
71	**72**	73	74	75	76	77	78	79	**80**
81	82	83	84	85	86	87	**88**	89	90
91	92	93	94	95	**96**	97	98	99	100

Example 3.12 Let $D = 58$. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 23.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 0$ and exactly one of $\mathsf{E}_1/\mathbb{Q}$ or $\mathsf{E}_2/\mathbb{Q}$ has rank 0 and the other has rank $r > 0$.

Example 3.13 Let $D \in \{14, 92\}$ be an integer. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 25.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 0$ and exactly one of $\mathsf{E}_1/\mathbb{Q}$ or $\mathsf{E}_2/\mathbb{Q}$ has rank 0 and the other has positive rank r.

Example 3.14 Let $D = 89$. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 + 89.$$

Then $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}) = 2$ and we check that $\mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_1(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}_2(\mathbb{Q}) = 0$.

Remark 3.15 We thank the referee for pointing out to us that using MAGMA one can check that the pairs $(a, D) = (2, 71)$ and $(a, D) = (3, 83)$ have the desired property.

3.3 Follow-up questions

These observations raise the following two obvious questions:

Question 1 *For every cube-free integer D does there always exist an elliptic curve of the type $\mathsf{E} : y^2 = x^3 + a$ such that on twisting by D exactly one of E, E_1, E_2 has positive rank (over $\mathbb{Q}$) and the other two have rank 0 (over $\mathbb{Q}$)?*

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

Even though this question has implications for Hilbert's 10th problem, in particular it proves that Hilbert's 10th problem is unsolvable in the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{D})$ for every (cube-free integer) D, the question is interesting in its own right.

Question 2 *Fix an elliptic curve $\mathsf{E} : y^2 = x^3 + a$. For what proportion of cube-free integers D, does exactly one of E, E_1, E_2 have positive rank r (over $\mathbb{Q}$) and the other two have rank 0 (over $\mathbb{Q}$)?*

4 Main result and proof

4.1 Hilbert's 10th problem for $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$

We begin this section by proving some lemmas which will be required for the main theorem.

Lemma 4.1 *Let p be a prime such that $p \equiv 2, 4, 5, 7 \pmod 9$. Then Hilbert's 10th problem is unsolvable for the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$.*

Proof In each of these cases, we prove the unsolvability of Hilbert's 10th Problem in $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$ by applying Lemma 3.1 on an appropriately chosen elliptic curve E_a.

(a) **When** $p \equiv 2, 5 \pmod 9$. The elliptic curve E_{-432*9^2} has rank 1 over $\mathbb{Q}$. As noted in Theorem 2.1(a), both $9p$ and $9p^2$ are not cube-sums i.e., both the elliptic curves $\mathsf{E}_{-432*9^2*p^2}$ and $\mathsf{E}_{-432*9^2*p^4}$ have rank 0 over $\mathbb{Q}$. Now the result follows from Lemma 3.1.

(b) **When** $p \equiv 4, 7 \pmod 9$. Fix an integer B such that $B \notin \mathbb{F}_p^3$. By Chinese Remainder Theorem, there exists an integer A such that $A \equiv 8 \pmod 9$ and $A \equiv B \pmod p$. Now by Theorem 2.1(c), there exists a prime ℓ such that $\ell \equiv A \pmod{9p}$ which is a cube-sum and hence $\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432\ell^2}(\mathbb{Q}) > 0$. On the other hand, as mentioned in Theorem 2.1(b)(ii), both ℓp and ℓp^2 are not cube-sums and the result follows from Lemma 3.1. ∎

Lemma 4.2 *For 100% of the primes p (with respect to the natural density) of the form $p \equiv 8 \pmod 9$, Hilbert's 10th problem is unsolvable for the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$.*

Proof Consider the infinite set consisting of primes $S = \{\ell \mid \ell \equiv 4, 7 \pmod 9 \text{ and } 3 \notin \mathbb{F}_\ell^3\}$. Enumerate the primes of S as $\ell_1 = 7, \ell_2 = 13, \ell_3 = 31, \ldots$. Further note that for every $\ell \in S$, the prime ℓ is a cube-sum by Theorem 2.1(b)(i).

We have $\ell_1 = 7$, now take a prime $p \equiv 8 \pmod 9$ such that $p \not\equiv \pm 1 \pmod{\ell_1}$, i.e., choose a prime $p \equiv 8 \pmod 9$ such that $p \notin \mathbb{F}_{\ell_1}^3$. By Theorem 2.1(b)(ii), both $\ell_1 p$ and $\ell_1 p^2$ are not cube-sum. By Lemma 3.1, Hilbert's 10th problem is unsolvable for the ring of integers of $L = \mathbb{Q}(\zeta_3, \sqrt[3]{p})$. Thus among all the primes p of the form $p \equiv 8 \pmod 9$, for two-thirds of them (corresponds to those which are not of the form $\pm 1 \pmod 7$) Hilbert's 10th problem is unsolvable for $\mathcal{O}_L$.

Next we work with the prime $\ell_2 = 13$. We choose a prime p such that $p \equiv 8 \pmod 9$, $p \equiv \pm 1 \pmod 7$, and $p \not\equiv \pm 1, \pm 8 \pmod{13}$, that is $p \equiv 8 \pmod 9$, $p \in \mathbb{F}_{\ell_1}^3$ and $p \notin \mathbb{F}_{\ell_2}^3$. Again by Theorem 2.1(b)(ii) both $\ell_2 p$ and $\ell_2 p^2$ are not cube-sum and hence, we can

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

conclude by Lemma 3.1 Hilbert's 10th problem is unsolvable for $\mathcal{O}_L$. Consequently, we can now conclude that among all the of primes p of the form $p \equiv 8 \pmod 9$ and $p \equiv \pm 1 \pmod 7$, for 2/3-rd of them Hilbert's 10th problem is unsolvable for $\mathcal{O}_L$.

Combining the two cases, for $\frac{2}{3} + \left(\frac{1}{3} \times \frac{2}{3}\right) = \frac{8}{9}$-th of the primes p of the form $p \equiv 8 \pmod 9$, Hilbert's 10th problem is unsolvable for $\mathcal{O}_L$.

Proceeding in this way, we see that at the k-step, for a prime p with $p \equiv 8 \pmod 9$, $p \in \mathbb{F}^3_{\ell_i}$ for $1 \leq i \leq k$ and $p \notin \mathbb{F}^3_{\ell_{k+1}}$, Hilbert's 10th problem is unsolvable for $\mathcal{O}_L$. Consequently, we conclude that for $\left(1 - \frac{1}{3^{k+1}}\right)$ of primes p of the form $p \equiv 8 \pmod 9$, Hilbert's 10th problem is unsolvable for $\mathcal{O}_L$. The set S is infinite; by induction it follows that for 100% of primes p of the form $p \equiv 8 \pmod 9$, Hilbert's 10th problem is unsolvable for $\mathcal{O}_L$. ∎

Theorem 4.3 *For $\frac{5}{6}$-th (with respect to the natural density) of all primes p, Hilbert's 10th problem is unsolvable for the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$.*

Proof The result follows immediately from Lemmas 4.1 and 4.2. ∎

4.2 Hilbert's 10th problem for $\mathbb{Q}(\zeta_3, \sqrt{D}, \sqrt[3]{p})$

Once we have established that Hilbert's 10th Problem is unsolvable in the degree 6 extension $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$, we can extend it to certain degree 12 extensions by using the corollary of Shlapentokh's theorem.

These are new examples of rings of integers of number fields where Hilbert's 10th problem is being shown to be unsolvable. For the argument in [13], the authors found $\mathsf{E}/\mathbb{Q}$ with rank 0 over $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$ and positive rank over $\mathbb{Q}(\sqrt{D})$; this *did not* provide examples of degree 12 number fields $L_{D,p} = \mathbb{Q}(\zeta_3, \sqrt{D}, \sqrt[3]{p})$ where Hilbert's 10th problem is unsolvable for $\mathcal{O}_{L_{D,p}}$ because the unsolvability of Hilbert's 10th problem for the ring of integers of $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$ was not verified.

Proposition 4.4 *Let S be the set of square-free integers such that for every $D \in S$, the rank of the elliptic curve E_{-432D^3} is positive and T be the set of primes p of the form $p \equiv 2, 5 \pmod 9$. Hilbert's 10th problem is unsolvable for the ring of integers of $L_{D,p}$ for every $D \in S$ and every $p \in T$.*

Further, the set S is infinite and moreover for $X \gg 0$, we have

$$\#(S \cap [-X, X]) \gg X^{1-\varepsilon} \text{ for any } \varepsilon > 0.$$

Proof Consider the elliptic curve E_{-432}. By our assumption on S, we know that

$$\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432}(\mathbb{Q}(\sqrt{D})) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432}(\mathbb{Q}) + \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432D^3}(\mathbb{Q}) > 0.$$

Recall that for $p \in T$, by Theorem 2.1(a), both p and p^2 are not cube-sums, i.e., $\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432p^2}(\mathbb{Q}) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432p^4}(\mathbb{Q})$. Further recall that $\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_k(\mathbb{Q}(\zeta_3)) = 2\,\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_k(\mathbb{Q})$. Then it follows from (3.1) that

$$\mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432}(\mathbb{Q}(\zeta_3, \sqrt[3]{p})) = \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432}(\mathbb{Q}(\zeta_3)) + \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432p^2}(\mathbb{Q}(\zeta_3)) + \mathrm{rk}_{\mathbb{Z}}\, \mathsf{E}_{-432p^4}(\mathbb{Q}(\zeta_3)) = 0.$$

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

In Lemma 4.1, we have shown that Hilbert's 10th problem is unsolvable over $\mathbb{Q}(\zeta_3, \sqrt[3]{p})$. Hence using Theorem 2.3, we can guarantee that Hilbert's 10th problem is unsolvable over $\mathcal{O}_{L_{D,p}}$.

To prove the second assertion, we argue as follows: let E be an elliptic curve over $\mathbb{Q}$ and D be a square-free integer co-prime to the conductor of E. Let $\mathsf{E}^{(D)}$ denote the quadratic twist of E by D and let $L(\mathsf{E}, s)$ represent the complex L-function of $\mathsf{E}/\mathbb{Q}$. Put

$$N_1(\mathsf{E}, X) := \{|D| < X \mid \mathrm{ord}_{s=1}\ L(\mathsf{E}^{(D)}, s) = 1\}.$$

Then by [17], for $X \gg 0$, we have $N_1(\mathsf{E}, X) \gg_\varepsilon X^{1-\varepsilon}$, for any $\varepsilon > 0$. By the work of B. Gross–D. Zagier and V. Kolyvagin, it is known that for an elliptic curve $\mathsf{A}/\mathbb{Q}$, $\mathrm{rk}_{\mathbb{Z}}\, \mathsf{A}(\mathbb{Q}) = 1$ whenever $\mathrm{ord}_{s=1}\ L(\mathsf{A}, s) = 1$. By applying this argument to $\mathsf{E} = \mathsf{E}_{-432}$ and $\mathsf{A} = \mathsf{E}^{(D)}$, the assertion follows. ∎

Remark 4.5 Note that for the square-free integers of the form (i) $\pm(3k + 2)$ with $k > 0$ and (ii) $\pm 3(3k + 1)$ with $k > 0$, the root number computations due to B. Birch–N. Stephens implies that the global root number of $\mathsf{E}_{-432D^3}/\mathbb{Q}$, denoted by $\omega(\mathsf{E}_{-432D^3})$ is -1. Thus if we make an additional hypothesis that $\dim_{\mathbb{F}_3} Ш(\mathsf{E}_{-432D^3}/\mathbb{Q})[3]$ is even (see [10, Section 5]) for all square-free integers D, then the natural density of S is at least $\frac{1}{2}$. Note that for an elliptic curve E over a number field K, the hypothesis $\dim_{\mathbb{F}_2} Ш(\mathsf{E}/K)[2]$ being even is discussed in [16].

Acknowledgements We thank Alvaro Lozano-Robledo, Sudhanshu Shekhar, and Ari Shnidman for helpful discussions. We thank Antonio Lei for his interest in our paper. We thank the referee for their timely reading of the paper and for helpful comments; in particular, we thank them for suggesting using MAGMA to complete our list of examples.

References

[1] L. Alpöge, M. Bhargava, W. Ho, and A. Shnidman, *Rank stability in quadratic extensions and Hilbert's tenth problem for the ring of integers of a number field*. Preprint, 2025. https://arxiv.org/abs/2501.18774

[2] L. Alpöge, M. Bhargava, and A. Shnidman (with an appendix by A. Burungale and C. Skinner), *Integers expressible as the sum of two rational cubes*. Preprint, 2022. https://arxiv.org/abs/2210.10730

[3] L. Cai, J. Shu, and Y. Tian, *Cube sum problem and an explicit Gross-Zagier formula*. Amer. J. Math. **139**(2017), no. 3, 785–816.

[4] S. Dasgupta and J. Voight, *Problem and mock Heegner points*. Proc. Amer. Math. Soc. **146** (2018), no. 8, 3257–3273.

[5] M. Davis and H. Putnam, *Diophantine sets over polynomial rings*. Illinois J. Math. 7(1963), 251–256.

[6] M. Davis, H. Putnam, and J. Robinson, *The decision problem for exponential Diophantine equations*. Ann. Math. **74**(1961), no. 3, 425–436.

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

[8] N. Garcia-Fritz and H. Pasten, *Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points*. Math. Ann. 377(2020), no. 3, 989–1013.

[9] Y. Hu, J. Shu, and H. Yin, *An explicit Gross–Zagier formula related to the Sylvester conjecture*. Trans. Am. Math. Soc. 372(2019), no. 10, 6905–6925.

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press

[10] S. Jha, D. Majumdar, and P. Shingavekar, 3-*Selmer group, ideal class groups and cube sum problem*. Preprint, 2022. https://arxiv.org/abs/2207.12487
[11] S. Jha, D. Majumdar, and B. Sury, *Binary cubic forms and rational cube sum problem*. Preprint, 2023. https://arxiv.org/abs/2301.06970
[12] P. Koymans and C. Pagano, *Hilbert's tenth problem via additive combinatorics*. Preprint, 2024. https://arxiv.org/abs/2412.01768
[13] D. Kundu, A. Lei, and F. Sprung, *Studying Hilbert's 10th problem via explicit elliptic curves*. Math. Ann. **390**(2024), 5153–5183.
[14] D. Majumdar and P. Shingavekar, *Cube sum problem for integers having exactly two distinct prime factors*. Proc.-Math. Sci. **133**(2023), no. 2, 22 Pages.
[15] Y. Matijasevic, *Enumerable sets are diophantine*. Soviet Math. Dokl. **11**(1970), 354–358.
[16] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*. Invent. Math. **181**(2010), no. 3, 541–575.
[17] A. Perelli and J. Pomykała, *Averages of twisted elliptic L-functions*. Acta Arith. **80**(1997), no. 2, 149–163.
[18] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers*. In: International algorithmic number theory symposium, 2002, pp. 33–42.
[19] J. Robinson, *Unsolvable diophantine problems*. Proc. Amer. Math. Soc. **22**(1969), no. 2, 534–538.
[20] A. 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.
[21] A. Shnidman and A. Weiss, *Rank growth of elliptic curves over n-th root extensions*. Trans. Amer. Math. Soc. Ser. B **10** (2023), 482–506.
[22] J. Sylvester, *On certain ternary cubic-form equations*. Amer. J. Math. **2**(1879), no. 4, 357–393.

Department of Mathematical and Statistics, IIT Kanpur, Kanpur, India
e-mail: jhasom@iitk.ac.in

Department of Mathematical and Statistical Sciences, UTRGV, 1201 W University Dr., Edinburg, TX 78539, United States
e-mail: debanjana.kundu@utrgv.edu

Department of Mathematics, IIT Madras, Chennai, India
e-mail: dipramit@iitm.ac.in

https://doi.org/10.4153/S0008439525000219 Published online by Cambridge University Press