Mathematische Annalen
https://doi.org/10.1007/s00208-024-02879-9

Mathematische Annalen

Studying Hilbert's 10th problem via explicit elliptic curves

Debanjana Kundu[1] · **Antonio Lei**[2] · **Florian Sprung**[3]

Received: 20 July 2022 / Revised: 18 December 2023 / Accepted: 10 April 2024

Abstract
N. García-Fritz and H. Pasten showed that Hilbert's 10th problem is unsolvable in the ring of integers of number fields of the form $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$ for positive proportions of primes p and q. We improve their proportions and extend their results to the case of number fields of the form $\mathbb{Q}(\sqrt[3]{p}, \sqrt{Dq})$, where D belongs to an explicit family of positive square-free integers. We achieve this by using multiple elliptic curves, and replace their Iwasawa theory arguments by a more direct method.

Mathematics Subject Classification Primary 11G05 · 11U05

1 Introduction

1.1 Historical remarks

In 1900, D. Hilbert posed the following problem:
Hilbert's 10th problem "Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: to devise a process accord-

✉ Debanjana Kundu
dkundu@math.toronto.edu

Antonio Lei
antonio.lei@uottawa.ca

Florian Sprung
ian.sprung@gmail.com

[1] Department of Mathematical and Statistical Sciences, UTRGV, 1201 W University Dr., Edinburg, TX 78539, USA

[2] Department of Mathematics and Statistics, University of Ottawa, 150 Louis-Pasteur Pvt, Ottawa, ON K1N 6N5, Canada

[3] School of Mathematical and Statistical Sciences, Arizona State University, 901 S Palm Walk, Tempe, AZ 85287-1804, USA

Published online: 04 May 2024

ing to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.[1]"

This problem is now known to have a negative answer, i.e., such a general 'process' (algorithm) does not exist. In one sentence, the reason for this negative answer is that the *computably enumerable sets* (whose elements an algorithm can list) in $\mathbb{Z}$ are precisely the *Diophantine* sets over $\mathbb{Z}$ (roughly, 'coming from polynomials and integers', see Definition 2.1). For the convenience of the reader, we give a brief sketch of the argument described in [12, Chapter 5, Section 7].

The Diophantine sets of integers can be algorithmically enumerated—call them $D_1, D_2, \ldots, D_n, \ldots$ Cantor's diagonalization method shows that the set $V = \{n : n \notin D_n\}$ is not Diophantine, that is, it is not computationally enumerable. On the other hand, the set of ordered pairs (n, x) with n an integer and $x \in D_n$ is Diophantine (*Universality Theorem*), i.e., they are characterized as the solutions to $f(n, x, y_1, \ldots, y_m) = 0$ for some integers $y_1, \ldots, y_m$ and a fixed polynomial f. Now if a putative algorithm $\mathcal{A}$ could determine whether an arbitrary Diophantine equation has integral solutions, then $\mathcal{A}$ could do this for f and thus test whether $x \in D_n$. But then $\mathcal{A}$ could test whether $n \in D_n$ and list all those n with $n \notin D_n$, contradicting that V is *not* computably enumerable.

M. Davis, H. Putnam, and J. Robinson made significant progress towards answering Hilbert's 10th Problem in the 1950s and 1960s, showing that the computably enumerable sets are exponential Diophantine[2] [5]. The final piece of the puzzle, showing that the exponential function is Diophantine, was proved by Y. Matiyasevič in 1970 [10]. The proof involved showing that the Fibonacci numbers are Diophantine, and allowed for the conclusion that no algorithm as solicited by Hilbert exists:

MRDP Theorem *Hilbert's* 10th *Problem has a negative solution.*

J. Denef and L. Lipshitz [4] generalized the discussion surrounding Hilbert's 10th Problem as follows:

Denef–Lipshitz Conjecture $\mathbb{Z}$ *is a Diophantine subset of the ring of integers of any number field* L.

This conjecture would imply a negative answer to Hilbert's 10th problem for $\mathcal{O}_L$, see Claim 3.2 in the main body of the article. Here are the instances where this conjecture has been resolved.

(a) L is totally real or a quadratic extension of a totally real field; see [3, 4].
(b) $[L : \mathbb{Q}] = 4$, L is not totally real, and $L/\mathbb{Q}$ has a proper intermediate field; see [4].
(c) L has exactly one complex place; see [20, 25, 30].
(d) L is a subfield of one of the extensions mentioned above; see [28]. In particular, it follows from the Kronecker–Weber Theorem that the analogue of Hilbert's 10th Problem is unsolvable when $L/\mathbb{Q}$ is abelian.

[1] Gegeben eine diophantische Gleichung mit beliebig vielen Unbekannten und mit rationalen ganzzahligen numerischen Koeffizienten: Ein Verfahren entwickeln, nach dem in endlich vielen Operationen bestimmt werden kann, ob die Gleichung in rationalen ganzen Zahlen lösbar ist.

[2] A set S of ordered n-tuples is called *exponential Diophantine* if there exists a polynomial $f(x_1, \ldots, x_n, u_1, \ldots, u_m, v_1, \ldots, v_m, w_1, \ldots, w_m)$ such that $(x_1, \ldots, x_n) \in S$ if and only if there exists u_i, v_i, w_i with $f = 0$ and $u_i = v_i^{w_i}$ for each i.

(e) If the conjecture holds for a number field F, then it holds for certain infinite families of degree ℓ^n-extensions L of F. More precisely, once F has been chosen, then for all but finitely many primes ℓ and all $n \geq 1$, the conjecture holds for infinitely many cyclic ℓ^n-extensions L of F; see [16, 17].[3] See also [23] for a recent result on cyclotomic $\mathbb{Z}_\ell$-extensions.
(f) L belongs to an explicit family of number fields of the form $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$; see [6].
(g) In [2], G. Cornelissen, T. Pheidas and K. Zahidi studied the case where L is a number field satisfying two specific arithmetic conditions.
(h) In the recent preprint of B. Mazur, K. Rubin and A. Shlapentokh [18], related questions for a large family of Galois extensions of $\mathbb{Q}$ have been studied.

Results in (e)–(g) make use of a link initiated by B. Poonen between the Denef-Lipshitz Conjecture and the theory of elliptic curves. Poonen showed in [21] that extensions of number fields are *integrally Diophantine* (Definition 2.3) if there is an elliptic curve whose rational points in those number fields have rank 1. A. Shlapentokh in [25] vastly generalized this to arbitrary non-zero rank (Shlapentokh's Theorem). B. Mazur and K. Rubin showed in [16] that if the 2-torsion part of the Shafarevich–Tate groups of elliptic curves is a square for every number field, then the Denef-Lipshitz Conjecture holds. In [14], R. Murty and H. Pasten considered this problem from the point of view of analytic aspects of L-functions instead, showing that the automorphy conjecture and the rank part of the Birch and Swinnerton-Dyer conjecture would imply it.

The precise version of the most recent result (f) above of N. García-Fritz and H. Pasten is:

Theorem 1.1 (García-Fritz–Pasten) *There are explicit Chebotarev sets (see Definition 3.4) 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 $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$.*

1.2 Our results

We give a more direct proof of Theorem 1.1 without using results from Iwasawa theory and improve the density of both $\mathscr{P}$ and $\mathscr{Q}$, as well as proving similar results for new families of extensions. The key result for this more direct proof is a vanishing theorem of certain Selmer groups, see Theorem 3.6, which allows us to form the set $\mathscr{P}$. Similar to the method utilized in [6], the set $\mathscr{Q}$ is obtained by seeking rank-one quadratic twists of our auxiliary elliptic curve, which relies crucially on the work of Kriz and Li [7]. By carefully refining the techniques developed in [6], we prove the following improvement of Theorem 1.1.

Theorem A (Theorem 4.3) *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 $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$.*

[3] We thank Karl Rubin for patiently clarifying this point. The main ingredient for deriving this from [17, Theorem 1.2] is that the simple abelian variety can be chosen to be a non-CM elliptic curve.

The key ingredient of the proofs of both Theorems 1.1 and A is the exhibition of an explicit auxiliary elliptic curve E (of Mordell–Weil rank 0) such that the Mordell–Weil ranks of E over $\mathbb{Q}(\sqrt[3]{p})$ and $\mathbb{Q}(\sqrt{-q})$ are 0 and 1, respectively (see Sect. 3 where we review the general strategy employed). By working with a new auxiliary elliptic curve, we are able to prove a similar result for the following new families of number fields:

Theorem B (Theorem 5.3) *Let*

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

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 $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{Dq})$.

The families of number fields studied in Theorem B are disjoint from the ones studied in Theorem 1.1 and Theorem A. Furthermore, these number fields are not Galois over $\mathbb{Q}$ and have exactly two complex places. In particular, they are not covered in the list of previous known results.

We also prove a modified version of Theorem B by working with a pair of auxiliary elliptic curves, where we 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 C (Theorem 6.7) *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 $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{Dq})$.*

If one were to work with a large number of auxiliary elliptic curves, one should get higher density sets $\mathscr{P}$ that get arbitrarily close to 1 with the number of curves, at the expense of lower density sets $\mathscr{Q}$ and $\mathscr{Q}_D$—see Remark 6.8 for a brief discussion and Table 1 for the densities of $\mathscr{P}$. It would be very interesting to find such curves, for which significantly more computing power is certainly needed. It would be interesting to solve the following problem.

Problem 1.2 *Find a method that generates infinitely many such auxiliary elliptic curves.*

An affirmative answer to this problem would imply that the analogue of $\mathscr{P}$ would have density 1, while our current method of building $\mathscr{Q}$ could potentially give a set of density 0.

Problem 1.3 *If the answer to Problem 1.2 is affirmative, would it be possible to ensure that the resulting $\mathscr{Q}$ is non-empty? Or even have positive density?*

See Remark 6.8 for further discussion related to Problems 1.2 and 1.3.

Finally, we fix a congruent number elliptic curve as our choice of auxiliary elliptic curve and adapt the techniques developed in [6] to prove the following result.

Table 1 Densities of $\mathscr{P}_n$ for $1 \leq n \leq 7$

n	Density for $\mathscr{P}_n$		
1	$\frac{9}{16}$	=	0.5625
2	$\frac{103}{128}$	=	0.8046875
3	$\frac{933}{1024}$	=	0.9111328…
4	$\frac{7855}{8192}$	=	0.9588623…
5	$\frac{64269}{65536}$	=	0.9806671…
6	$\frac{519463}{524288}$	=	0.9907970…
7	$\frac{4175733}{4194304}$	=	0.9955723…

Theorem D (Theorem 7.5) *There is an explicit Chebotarev set of primes $\mathscr{P}_{\text{cong}}$ 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.*

The congruent number problem and Goldfeld's conjecture predict that the set of primes q in the statement of Theorem D should be $\frac{1}{2}$. Progress on these problems have been announced by Kriz [9] and Smith [27].

Organization

Including the introduction, there are seven sections and three appendices. In the preliminary Sect. 2, we record facts about Hilbert's 10th Problem and Selmer groups. In Sect. 3 we outline the strategy of using elliptic curves for proving that Hilbert's 10th Problem is unsolvable in rings of integers of certain number fields. In Sect. 4 we consider the setting of García-Fritz–Pasten's Theorem 1.1 and provide improvements on the proportions.

In Sects. 5 and 6, we deviate from the setting of [6]. We work with auxiliary elliptic curves with negative minimal discriminant, allowing us to prove the insolubility in rings of integers of number fields disjoint from those considered in [6]. In the final Sect. 7, we approach the problem with congruent number elliptic curves. This curve was not covered by the methods of [6] because of difficult behaviour at the prime 3. More precisely, it has *supersingular* reduction at the prime 3 with non-surjective image of the mod 3 residual representation.

The appendices contain a MAGMA code provided to us by Harris B. Daniels and the SAGE codes that were used to verify various hypotheses in this article.

2 Preliminaries

2.1 Facts related to Hilbert's 10th problem

We record definitions and properties required for our purposes. For further details we refer the reader to [12, Chapters 5 and 7].

Definition 2.1 Let R be a commutative unitary ring and let n be a given positive integer. We say a set $S \subseteq R^n$ is *Diophantine over* R if there exists a positive integer m and a polynomial $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$ with coefficients in R such that $(a_1, \ldots, a_n)$ is in S if and only if there exist elements $b_1, \ldots, b_m$ of R for which $P(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0$. That is,

$$(a_1, \ldots, a_n) \in S \Longleftrightarrow (\exists\, b_1, \ldots, b_m)(P(a_1, \ldots, a_n, b_1, \ldots, b_m)) = 0$$

When $n = 1$, the set S is said to be *Diophantine in* R.

Example 2.2 (1) The set of non-negative integers $a \in \mathbb{Z}_{\geq 0}$ is Diophantine in $\mathbb{Z}$:

$$a \in \mathbb{Z}_{\geq 0} \Longleftrightarrow (\exists\, b_1, b_2, b_3, b_4)(a - b_1^2 - b_2^2 - b_3^2 - b_4^2 = 0).$$

(2) Any finite set $S = \{a_1, \ldots, a_r\}$ is Diophantine in any integral domain:

$$a \in S \Longleftrightarrow (a - a_1) \ldots (a - a_r) = 0.$$

(3) The set of composite numbers is Diophantine in $\mathbb{Z}$:

$$a \text{ is a composite number } \Longleftrightarrow (\exists\, b_1, \ldots, b_8) \left(a = \left(\sum_{i=1}^{4} b_i^2 + 2 \right) \left(\sum_{i=5}^{8} b_i^2 + 2 \right) \right).$$

(4) If S_1 and S_2 are Diophantine, then $S_1 \cup S_2$ and $S_1 \cap S_2$ are also Diophantine.

Definition 2.3 Let L_2/L_1 be an extension of number fields. If $\mathcal{O}_{L_1}$ is Diophantine in $\mathcal{O}_{L_2}$, then L_2/L_1 is said to be *integrally Diophantine*.

The following result tells us about the Diophantine relationships between algebraic number fields.

Transitive Property If $L_3/L_2/L_1$ is a tower of number fields and both L_2/L_1 and L_3/L_2 are integrally Diophantine, then so is L_3/L_1.

Proof See [28, Theorem 2.1]. □

Shlapentokh's Theorem Let L_2/L_1 be an extension of number fields. Suppose that there is an elliptic curve E/L_1 such that rank $E(L_2) =$ rank $E(L_1) > 0$. Then L_2/L_1 is integrally Diophantine.

Proof See [25]. □

2.2 Facts about Selmer groups of elliptic curves

Throughout this article, ℓ is an odd prime number and E is an elliptic curve defined over $\mathbb{Q}$ with good reduction at ℓ.

Given a module A over the absolute Galois group G_L of a number field L, and $i \geq 0$, the cohomology group $H^i(L, A)$ is defined to be the discrete cohomology group $H^i(G_L, A)$.

The ℓ-*Selmer group* of E over L is defined as the kernel of the following restriction map

$$\mathrm{Sel}_\ell(E/L) := \ker\left(H^1(L, E[\ell]) \longrightarrow \prod_w H^1\left(L_w, E(\overline{L_w})\right)[\ell]\right).$$

An equivalent definition of the ℓ-Selmer group given in [13, § 1 Corollary 6.6] is the following: let S be a finite set of primes L containing all the archimedean primes, the primes above ℓ, and the primes where E has bad reduction. Then

$$\mathrm{Sel}_\ell(E/L) := \ker\left(H^1(L_S/L, E[\ell]) \longrightarrow \prod_{w\in S} H^1\left(L_w, E(\overline{L_w})\right)[\ell]\right).$$

Here, L_S/L is the maximal extension of L unramified outside the set S.

Now we record a result of J. Brau crucial for our results. Let r be a prime of semi-stable reduction and choose an integer a so that $r^s \parallel a$, i.e., $a = r^s d$ such that $\gcd(d, r) = 1$ for an integer d. Since r is semi-stable, we can write $j = r^{-n}\frac{e}{f}$ (where e, f are coprime to r). Define

$$u_{r,a} = d^n\left(\frac{e}{f}\right)^s.$$

Theorem 2.4 (Brau) *Let ℓ be an odd prime and $E/\mathbb{Q}$ be an elliptic curve with good reduction at ℓ. Let $k = \mathbb{Q}(\mu_\ell)$ and suppose that $\mathrm{Sel}_\ell(E/k)$ is trivial. Consider the family of ℓ-extensions $k_a = k(\sqrt[\ell]{a})$. Write S to denote the set of primes containing the primes above ℓ, the primes of bad reduction of E, the primes which ramify in k_a/k, and the archimedean primes. Denote by G_v the Galois group $\mathrm{Gal}(k_{a,w}/k_v)$ (where w is a prime of k_a lying above v) and set $\delta_v = \dim_{\mathbb{F}_\ell} H^1\left(G_v, E(k_{a,w})\right)$. Denote by c_v is the Tamagawa number of E/k_v and by q_v the size of the residue field of k_v. Then*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell\left(E/k_a\right)^{\mathrm{Gal}(k_a/k)} = \sum_{v\in S} \delta_v.$$

The values of δ_v (when v is not a prime of additive reduction) are given in the following table:

Reduction type of E at v	*v ramified in k_a/k*	*v inert in k_a/k*	*v split in k_a/k*
good ordinary, $v \mid \ell$	$\delta_v = \begin{cases} 1 \text{ or } 2 & \text{if } \tilde{E}(\kappa_v)[\ell] \neq 0 \\ 0 & \text{otherwise} \end{cases}$	$\delta_v = 0$	
good supersingular, $v \mid \ell$	$\delta_v = \begin{cases} \ell - 2 & \text{if } \ell \mid a \\ 0 & \text{otherwise} \end{cases}$	$\delta_v = 0$	
good, $v \nmid \ell$	$\delta_v = \dim_{\mathbb{F}_\ell} \tilde{E}(\kappa_v)[\ell]$	$\delta_v = 0$	
split multiplicative	$\delta_v = \begin{cases} 1 & \text{if } u_{r_v,a}^{\frac{q_v-1}{\ell}} \equiv 1 \mod r_v \\ 0 & \text{otherwise} \end{cases}$	$\delta_v = \begin{cases} 1 & \text{if } \ell \mid c_v \\ 0 & \text{otherwise} \end{cases}$	$\delta_v = 0$
non-split multiplicative	$\delta_v = 0$		

Here, r_v is the rational prime below v.

Proof The first assertion of the theorem is [1, Proposition 5.2], which is deduced from results of Mazur and Rubin proven in [15], and relates the left-hand side of the formula with the $\mathbb{F}_\ell$-dimensions of local cohomology groups (see also [1, Remark 5.3] where an alternative proof of the assertion is outlined). We note that the description of the set S is not clearly mentioned in *op. cit.*: a partial description of the set S is included in Proposition 2.1 of *op. cit.* We further need to include the primes which ramify in k_a/k to ensure that k_a is a finite extension of k contained in k_S. The values of δ_v at non-additive primes are given in the statement of Theorem 1.1 of *op. cit.*

We now give a brief sketch of the proof of the formulae for the values of δ_v given in the statement of the theorem. The local cohomology groups of interest are denoted by W_{v,k_a} and are isomorphic to $H^1\left(G_v, E(k_{a,w})\right)$ with $G_v = \mathrm{Gal}(k_{a,w}/k_v)$; their $\mathbb{F}_\ell$ dimensions are denoted by δ_v. As one would expect, the value of δ_v depends on the reduction type of E at v and on the splitting behaviour of v in k_a. Note that when v is an archimedean prime or is totally split in k_a, then we have trivially $H^1\left(G_v, E(k_{a,w})\right) = 0$. Hence, one is only required to consider the cases of non-archimedean primes v that are inert or ramified in k_a.

When $v \nmid \ell$, and v is a prime of good reduction or or a prime of non-split multiplicative reduction, the dimension calculations follow from the standard short exact sequence [26, Chapter VII, Proposition 2.1]

$$0 \longrightarrow \widehat{E}(k_{a,w}) \longrightarrow E_0(k_{a,w}) \longrightarrow \widetilde{E}_{\mathrm{ns}}(\kappa_w) \longrightarrow 0,$$

and the theory of formal groups. If the reduction type is good then

$$H^i\left(G_v, \widehat{E}(k_{a,w})\right) = 0 \text{ for } i = 1, 2,$$

which implies that

$$W_{v,k_a} \cong H^1(G_v, \widetilde{E}(\kappa_w)).$$

If v is ramified, the action of G_v on $\widetilde{E}(\kappa_w) = \widetilde{E}(\kappa_v)$ is trivial and the cohomology group on the right-hand side becomes $\mathrm{Hom}\left(\mathbb{Z}/\ell\mathbb{Z}, \widetilde{E}(\kappa_v)\right)$. Thus, the formula of δ_v follows. In the inert case, the result follows from Lang's theorem in [11, p. 204]; see [1, Proposition 5.6]. In the case of non-split multiplicative reduction, the group W_{v,k_a} is always trivial: in the ramified case, this follows from our assumption that $\ell \geq 3$ and

in the inert case this is a consequence of Lang's theorem (see Proposition 5.8 of *op. cit.*).

When $v \nmid \ell$ is a prime of split multiplicative reduction, it follows from the theory of Tate curves that there exists a unique $q \in k_v$ such that E over k_v is isomorphic to $E_q(\overline{k}_v)$. Moreover, $\delta_v = 1$ if and only if q is the norm of a unit. If the prime v is (tamely) ramified in the cyclic extension then one uses the properties of tame Hilbert symbol (see [24, Chapter XIV]). On the other hand, when v is unramified, the norm map is surjective on the units and the condition on the q being a norm element can be translated to a condition on the local Tamagawa number. For details, the reader may refer to Propositions 5.7 and 6.1 in [1].

Finally, when $v \mid \ell$, the case when E has good ordinary reduction was studied in [15] (see also [1, Proposition 5.9]). On the other hand, the case of supersingular reduction involves studying the image of the norm map of a formal groups of height > 1; see Proposition 5.10 and 6.2 of *op. cit.* for details. □

Remark 2.5 Attentive readers will have noticed that we have left out the description of δ_v at additive primes, which were not studied in [1]. For our purposes, it is enough to consider elliptic curves whose additive primes satisfy very specific conditions, which is why they are left out in the statement of Theorem 2.4. The treatment of the particular additive primes we are interested in will be carried out in the proof of Theorem 3.6 below.

3 Strategy

In this section, we outline the strategy of the proofs of Theorems A–D. Our approach is inspired by the techniques developed in [6] but is more direct and free of Iwasawa theoretic arguments. The following consequence of Shlapentokh's Theorem plays a key role.

Proposition 3.1 *Let $F/\mathbb{Q}$ be any number field and $K/\mathbb{Q}$ be a quadratic extension. Consider the compositum $L = F \cdot K$. If there is an elliptic curve $E/\mathbb{Q}$ satisfying*

(i) rank $E(F) = 0$ *and*
(ii) rank $E(K) > 0$,

then L/F is integrally Diophantine, i.e., $\mathcal{O}_F$ is Diophantine in $\mathcal{O}_L$.

Proof See [6, Proposition 3.3]. □

If we further know that $F/\mathbb{Q}$ is integrally Diophantine (i.e., $\mathbb{Z}$ is Diophantine in $\mathcal{O}_F$), then by the Transitive Property, $L/\mathbb{Q}$ is also integrally Diophantine. The following argument is standard, but we repeat it for the reader's convenience.

Claim 3.2 *If $\mathbb{Z}$ is Diophantine in $\mathcal{O}_L$ (Definition 2.1), then the analogue of Hilbert's 10th Problem for $\mathcal{O}_L$ has a negative solution.*

Justification: Let P be the polynomial in $\mathcal{O}_L[X_i, Y_{j,j'}]_{1 \le i,j \le n, 1 \le j' \le l}$ that shows that $\mathbb{Z}$ is Diophantine in $\mathcal{O}_L$ and let $f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_n]$. By Definition 2.1, the

collection of polynomials

$$f_1, \ldots, f_m, P(X_1, Y_{1,1}, \ldots, Y_{1,k}), \ldots, P(X_n, Y_{n,1}, \ldots, Y_{n,k})$$

is solvable in $\mathcal{O}_L$ precisely if the polynomials $f_1, \ldots, f_m$ are solvable in $\mathbb{Z}$. In other words, if we are able to decide the solubility of polynomials over $\mathcal{O}_L$, then we would be able to decide the solubility of $f_1, \ldots, f_m$ over $\mathbb{Z}$. This is a contradiction to MRDP Theorem, which completes the justification.

Thus, the tasks at hand are the following:

(1) Find a rank 0 elliptic curve $E/\mathbb{Q}$ and two families of number fields:
   - one family such that rank of $E/\mathbb{Q}$ does not jump in the number fields.
   - another family of (quadratic) extensions such that rank does jump.

(2) Determine how large these families are.

3.1 Step 1: rank stabilization in cubic extensions

Throughout this section, $E/\mathbb{Q}$ is an elliptic curve with good reduction at a fixed prime ℓ. Consider the Galois group $G_{E,\ell} := \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$, and note that $G_{E,\ell}$ may be viewed as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ via the residual representation

$$\bar{\rho}_{E,\ell} : G_{E,\ell} \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Assume that $p \neq \ell$ is a prime coprime to the conductor of E, i.e., p is unramified in $\mathbb{Q}(E[\ell])$. Let $\sigma_p \in G_{E,\ell}$ be the Frobenius at p. The trace and determinant of $\bar{\rho}(\sigma_p)$ are as follows

$$\begin{aligned} \mathrm{trace}\ \bar{\rho}_{E,\ell}(\sigma_p) &= a_p(E) = p + 1 - \#\widetilde{E}(\mathbb{F}_p), \\ \det \bar{\rho}_{E,\ell}(\sigma_p) &= p. \end{aligned}$$

For a prime $v \mid p$ of $\mathbb{Q}(\mu_\ell)$, let f be the integer such that the residue field of $\mathbb{Q}(\mu_\ell)$ at v is given by $\kappa_v = \mathbb{F}_{p^f}$ (note that f is independent of the choice of v). According to a formula of A. Weil (see [26, Theorem V.2.3.1]),

$$\#E(\kappa_v) = p^f + 1 - \alpha^f - \beta^f \equiv 2 - \alpha^f - \beta^f \mod \ell,$$

where α and β are the eigenvalues of $\bar{\rho}_{E,\ell}(\sigma_p)$.

Definition 3.3 For $g \in G_{E,\ell}$, denote by $f(g)$ the smallest positive integer f satisfying

$$\det \bar{\rho}_{E,\ell}(g)^f = 1. \tag{1}$$

Define the set $H_{E,\ell}$ to consist of all $g \in G_{E,\ell}$ such that the eigenvalues $\alpha, \beta \in \overline{\mathbb{F}}_\ell$ of $\bar{\rho}(g)$ satisfy

$$\alpha^{f(g)} + \beta^{f(g)} \neq 2. \tag{2}$$

Note that (1) implies that $(\alpha\beta)^{f(g)} = 1$. Therefore, the condition (2) is equivalent to $\alpha^{f(g)} \neq 1$.

Definition 3.4 A set of primes $\mathcal{S}$ is called a *Chebotarev set* if there is a Galois extension $K/\mathbb{Q}$ and a conjugacy-stable set $\mathcal{C} \subseteq \mathrm{Gal}(K/\mathbb{Q})$ such that up to a finite set, $\mathcal{S}$ agrees with the set $\{p\colon \mathrm{Frob}_p \in \mathcal{C}\}$.

Finite unions, finite intersections, and complements of Chebotarev sets are again Chebotarev.

The Chebotarev density theorem states that if $\mathcal{S}$ arises from K and $\mathcal{C}$ as above, then the *density of* $\mathcal{S}$ defined as the limit

$$\lim_{x\to\infty} \frac{\#\mathcal{S} \cap [1, x]}{\pi(x)}$$

exists and is equal to $\#\mathcal{C}/[K : \mathbb{Q}]$. Here, we have used the standard notation $\pi(x)$ to denote the number of prime numbers $\leq x$.

Lemma 3.5 *For a prime $p \neq \ell$, let v be a prime of $\mathbb{Q}(\mu_\ell)$ above p, and κ_v be the residue field at v. The density of primes p coprime to the conductor of E so that $E(\kappa_v)[\ell] = 0$ is $\left(\frac{\#H_{E,\ell}}{\#G_{E,\ell}}\right)$.*

Proof This is [8, Lemma 8.9]—we repeat the brief proof for the convenience of the reader as we will be using it later. By definition, $\sigma_p \in H_{E,\ell}$ if and only if $E(\kappa_v)[\ell] = 0$. The result follows from the Chebotarev density theorem. □

We now work toward finding a set of primes $\mathscr{P}$ such that for all $p \in \mathscr{P}$ the Mordell–Weil rank of $E\left(\mathbb{Q}(\sqrt[3]{p})\right)$ is zero. We prove a modified version of [6, Theorem 4.1]. The major point in which our proof differs is that it does not rely on Iwasawa theory, but rather on Brau's Theorem 2.4.

Theorem 3.6 *Let $\ell > 2$ be a prime. Let $E/\mathbb{Q}$ be an elliptic curve with conductor N such that*

(1) *E has good reduction at ℓ;*
(2) $\mathrm{Sel}_\ell\,(E/\mathbb{Q}(\mu_\ell)) = 0$
(3) $\ell \nmid \mathit{Tam}\,(E/\mathbb{Q}(\mu_\ell)) \cdot \#\tilde{E}_\ell(\mathbb{F}_\ell)$.

Consider the set of prime numbers

$$\mathscr{P}(E, \ell) = \{p : p \nmid N, a_v(E) \not\equiv 2 \mod \ell\},$$

where v denotes any prime of $\mathbb{Q}(\mu_\ell)$ lying above p and $a_v(E) = 1 + \#\kappa_v - \#\tilde{E}_v(\kappa_v)$. Then for every ℓ-power free integer $a > 1$ supported in $\mathscr{P}(E, \ell)$, the Selmer group $\mathrm{Sel}_{\ell^\infty}\left(E/\mathbb{Q}(\mu_\ell, \sqrt[\ell]{a})\right)$ is trivial.

Proof We write $k = \mathbb{Q}(\mu_\ell)$ and $k_a = k(\sqrt[\ell]{a})$. Note that k_a/k is a Galois extension of number fields of degree ℓ. Let G denote its Galois group.

We make the following crucial observation: Suppose $v \nmid \ell$ is a prime in k that ramifies in k_a. Then we know that v divides a. But a is supported on $\mathscr{P}(E, \ell)$. This forces v to lie above a prime p for some $p \in \mathscr{P}(E, \ell)$, justifying our choice of letter v. We thus have by assumption that

$$a_v(E) \not\equiv 2 \mod \ell.$$

From the proof of Lemma 3.5, the primes of good reduction v satisfying the above condition are those which satisfy

$$\widetilde{E}_v(\kappa_v)[\ell] = (0).$$

Further, Lemma 3.5 itself tells us that $\mathscr{P}(E, \ell)$ is a Chebotarev set with density $\left(\frac{\#H_{E,\ell}}{\#G_{E,\ell}}\right)$.

In view of the assumption that $\mathrm{Sel}_\ell\,(E/\mathbb{Q}(\mu_\ell)) = 0$, we may apply Theorem 2.4. We shall consider two separate cases, namely when E is semi-stable and when E is not semi-stable.

Let us first consider the semi-stable case. The only primes that can ramify are the primes dividing ℓa. Since a lies in the support of $\mathscr{P}(E, \ell)$, it is clear that when $v \mid a$, we have $\delta_v = 0$, where δ_v is given as in the statement of Theorem 2.4 (we are in the row of $v \nmid \ell$, v good). Once again from Theorem 2.4 we see that the hypotheses on the Tamagawa number and the fact that ℓ is non-anomalous imply that $\mathrm{Sel}_\ell\,(E/k_a)^G = 0$ when $E/\mathbb{Q}$ has no prime of additive reduction. By [19, Proposition 1.6.12], we deduce that $\mathrm{Sel}_\ell\,(E/k_a)) = 0$.

Suppose now that E is not semi-stable. Again, by [19, Proposition 1.6.12], to show that $\mathrm{Sel}_\ell\,(E/k_a) = 0$, it suffices to show that $\mathrm{Sel}_\ell\,(E/k_a)^G = 0$.

As discussed in [1, Remark 5.3], there is an isomorphism of $\mathbb{F}_\ell$-vector spaces

$$\mathrm{Sel}_\ell\,(E/k_a)^G \simeq \bigoplus_{v \in S} H^1\left(G_v, E(k_{a,w})\right)[\ell],$$

where w is a prime of k_a lying above v. Just as before, Theorem 2.4 tells us that when v is a prime of good reduction or a prime of multiplicative reduction, the summand $H^1\left(G_v, E(k_{a,w})\right)[\ell]$ vanishes. It remains to study the summands arising from the additive primes. Let v be a prime of additive reduction and write r for the rational prime lying below v. Recall that E has good reduction at ℓ. It tells us that $\ell \neq r$, which implies the following isomorphism

$$H^1\left(G_v, E(k_{a,w})\right)[\ell] \simeq H^1\left(G_v, E(k_{a,w})[\ell]\right).$$

Therefore, it is enough to show that

$$E(k_{a,w})[\ell] = 0. \tag{3}$$

We have assumed that $\ell \nmid \mathrm{Tam}(E/k)$; it follows $\ell \nmid \mathrm{Tam}(E/k_a)$. Since v is a prime of additive reduction and $r \nmid \ell a$, the base change E/k_a still has additive reduction at

w. It follows from [31, Theorem 2.30] that

$$|\widetilde{E}^{\mathrm{ns}}(\kappa_w)| = |\kappa_w| \not\equiv 0 \pmod{\ell}.$$

Recall that (see [26, Chapter VII, Proposition 2.1])

$$|E(k_{a,w})[\ell]| = |E(k_{a,w})/\ell E(k_{a,w})| = |\widetilde{E}^{\mathrm{ns}}(\kappa_w)[\ell]| \times |c_w^{(\ell)}(E/k_a)| = 1,$$

proving (3). Therefore, we conclude that

$$\mathrm{Sel}_\ell\,(E/k_a)^G = \mathrm{Sel}_\ell\,(E/k_a) = 0.$$

□

Remark 3.7 We compare our result with [6, Theorem 4.1]. There are three main differences:

- we can define a larger set $\mathscr{P}(E,\ell)$, i.e., without assuming that $p \equiv 1 \pmod{\ell}$.
- we only need to assume that ℓ is a prime of good reduction (not good ordinary reduction).
- we do not require that the mod ℓ representation be surjective.

The authors in [6] only assume that rank $E(k) = 0$ and that $X(E/k)[\ell] = 0$. However, we have the additional assumption that E/k has no ℓ-torsion. The advantage is that we obtain that the ℓ-Selmer group over k_a is *trivial*, not just finite. But we point out that the auxiliary elliptic curve that is used in [6] also satisfies this extra hypothesis that we impose.

The same Iwasawa theoretic argument used in [6, Theorem 4.1] can be repeated if ℓ is a prime of good ordinary reduction, the set $\mathscr{P}(E,\ell)$ is as in our current theorem, and with no hypothesis on the mod ℓ representation being surjective.

3.2 Step 2: rank jump in a quadratic extension

We will rely heavily on the work of D. Kriz and C. Li [7] to construct a set of primes $\mathscr{Q}$ such that for all $q \in \mathscr{Q}$, the Mordell–Weil rank of $E\left(\mathbb{Q}(\sqrt{-q})\right)$ *or* $E\left(\mathbb{Q}(\sqrt{|d_K|q})\right)$ is 1.

3.2.1 Recollections from [7]

We remind the reader of two results from [7] which will allow us to obtain information on the rank jump upon performing a base-change.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and K be a quadratic field. Define the set of primes

$$\mathscr{Q}_K(E) = \left\{q : q \nmid 2N,\ q \text{ splits in } K,\ \text{ and } a_q(E) \equiv 1 \pmod{2}\right\}.$$

Theorem 3.8 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N with trivial 2-torsion. Let K be an imaginary quadratic field satisfying the Heegner hypothesis for N.*[4] *Let P denote a Heegner point Suppose that*

$$2 \text{ splits in } K \text{ and } \frac{|\widetilde{E}^{\mathrm{ns}}(\mathbb{F}_2)| \cdot \log_{\omega_E}(P)}{2} \not\equiv 0 \pmod 2. \tag{*}$$

Then for each square-free integer $d \equiv 1 \pmod 4$ supported on $\mathcal{Q}_K(E)$, the rank part of the Birch–Swinnerton-Dyer conjecture is true for $E^{(d)}/\mathbb{Q}$ and $E^{(d\cdot d_K)}/\mathbb{Q}$. One of these two curves has (algebraic and analytic) rank zero and the other has (algebraic and analytic) rank one.

If further, the Tamagawa number at 2 is odd,

$$\operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} E^{(d)}(\mathbb{Q}) \text{ if and only if } \Delta_E < 0 \text{ or }, \Delta_E > 0 \text{ and } d > 0,$$

where Δ_E is the minimal discriminant of E.

Proof See [7, Theorem 4.3 and Corollary 5.11]. □

The next two results are restatements of the above theorem, but we record them separately since they will be required for our calculations.

Corollary 3.9 *Let K be an imaginary quadratic field and let $E/\mathbb{Q}$ be an elliptic curve satisfying the following properties:*

(i) $\operatorname{rank} E(\mathbb{Q}) = 0$.
(ii) $E(\mathbb{Q})[2]$ *is trivial.*
(iii) (E, K) *satisfies the Heegner Hypothesis.*
(iv) *Hypothesis (*) holds.*
(v) $c_2(E)$ *is odd.*
(vi) $\Delta_E < 0$.

Then, $\operatorname{rank} E^{(d\cdot d_K)} = 1$ *for all* $d \equiv 1 \pmod 4$ *supported on* $\mathcal{Q}_K(E)$.

Proof Since we assume that $\Delta_E < 0$, this means that for all $d \equiv 1 \mod 4$,

$$\operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} E^{(d)}(\mathbb{Q}).$$

The first assertion of Theorem 3.8 implies that $E^{(d\cdot d_K)}/\mathbb{Q}$ has (analytic and algebraic) rank one. □

In exactly the same way, we can prove the following result.

Corollary 3.10 *Let K be an imaginary quadratic field and let $E/\mathbb{Q}$ be an elliptic curve satisfying the following properties:*

(i) $\operatorname{rank} E(\mathbb{Q}) = 0$.
(ii) $E(\mathbb{Q})[2]$ *is trivial.*

[4] It means that all primes dividing N split completely in K.

(iii) (E, K) *satisfies the Heegner Hypothesis.*
(iv) *Hypothesis (*) holds.*
(v) $c_2(E)$ *is odd.*
(vi) $\Delta_E > 0$ *and* $d < 0$.

Then, rank $E^{(d)} = 1$ *for all* $d \equiv 1 \pmod 4$ *supported on* $\mathscr{Q}_K(E)$.

3.3 Step 3: determining the size of these families of extensions

3.3.1 The density of $\mathscr{P}$

We consider the special case where $\overline{\rho}_{E,\ell}$ is surjective. We shall consider more general cases in subsequent sections. We begin with the following elementary lemma:

Lemma 3.11 *Suppose that* $\bar{\rho}_{E,\ell}$ *is surjective. When* $\ell = 3$, *we have*

$$\frac{\#H_{E,\ell}}{\#G_{E,\ell}} = \frac{9}{16}.$$

Proof The group $G_{E,\ell} \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has $\ell(\ell-1)^2(\ell+1) = 48$ elements. As in [8, Appendix A], we may divide $G_{E,\ell}$ into the following conjugacy classes:

- Let $C_{a,b}$ be the set of diagonalizable matrices with eigenvalues $a, b \in {\mathbb{F}_\ell}^\times$ with $a \neq b$. We have $(\ell-1)(\ell-2)/2$ choices of $C_{a,b}$ and for each choice, $\#C_{a,b} = \ell(\ell+1)$.
- Let $\mathcal{C}_a$ be the set of non-diagonal matrices with one single eigenvalue $a \in {\mathbb{F}_\ell}^\times$. There are $(\ell-1)$ choices for $\mathcal{C}_a$ and for each choice, $\#\mathcal{C}_a = \ell^2 - 1$.
- Let $D_a = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \right\}$, $a \in \mathbb{F}_\ell^\times$. Then, there are $(\ell-1)$ choices for a and for each choice $\#D_a = 1$.
- Let $\mathcal{E}_\lambda$ be the set of matrices whose eigenvalues are λ and λ', where $\lambda \in \mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$ and λ' is the conjugate of λ. There are $\ell(\ell-1)/2$ choices for λ and for each choice of λ, $\#\mathcal{E}_\lambda = \ell^2 - \ell$.

All elements in $\mathcal{E}_\lambda$ belong to $H_{E,\ell}$, giving $\ell^2(\ell-1)^2/2 = 18$ elements. For contributions from D_a and $\mathcal{C}_a$, we seek $a \in \mathbb{F}_\ell^\times$ whose order is even. The only choice is $a = 2$. This gives $(\ell^2 - 1) + 1 = 9$ elements. Finally, there is no element in $C_{a,b}$ belonging to $H_{E,\ell}$, since if $g \in C_{a,b}$, the eigenvalues of g are 1 and 2, forcing $f(g) = 2$ and $a^{f(g)} + b^{f(g)} = 2$. Summing up, the result follows. □

Remark 3.12 [6, Proposition 4.6] when applied with $\ell = 3$, yields a proportion equal to $5/16$. The proportion obtained in Lemma 3.11 exceeds this by $1/4$.

Corollary 3.13 *Suppose that* $E/\mathbb{Q}$ *is an elliptic curve satisfying the hypotheses of Theorem 3.6 with* $\ell = 3$. *Then, there exists a Chebotarev set of primes* $\mathscr{P}(E, 3)$ *with density* $\frac{9}{16}$ *such that for all* $p \in \mathscr{P}(E, 3)$, *the Mordell–Weil rank of* $E\left(\mathbb{Q}(\sqrt[3]{p})\right) = 0$.

Proof It follows from Theorem 3.6 (with $\ell = 3$), Lemma 3.11 and the Chebotarev density theorem. □

Remark 3.14 The main improvement in our result compared to [6, Theorem 4.1] is that we work with a larger set of primes $\mathscr{P}(E, \ell)$. In particular, we do not need to impose the hypothesis that the primes $p \in \mathscr{P}(E, \ell)$ satisfy the additional hypothesis that $p \equiv 1 \pmod{\ell}$.

3.3.2 The density of $\mathscr{Q}$

To determine the density of the set $\mathscr{Q}$ we use the following lemma.

Lemma 3.15 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let K be a fixed quadratic field. Define*

$$\begin{aligned}\mathscr{Q}(E, K) &= \left\{q : q \nmid 2N, q \text{ splits in } K,\ a_q(E) \equiv 1 \pmod 2\right\}\\ \mathscr{Q}^+(E, K) &= \{q : q \in \mathscr{Q}(E, K) \text{ and } q \equiv 1 \pmod 4\}\\ \mathscr{Q}^-(E, K) &= \{q : q \in \mathscr{Q}(E, K) \text{ and } q \equiv -1 \pmod 4\}\end{aligned}$$

If the mod 2 representation is surjective and $\mathrm{Gal}\left(\mathbb{Q}(E[2])\right)/\mathbb{Q}$ *does not contain K or $\mathbb{Q}(\sqrt{-1})$, then the density of the sets $\mathscr{Q}(E, K)$, $\mathscr{Q}^+(E, K)$, and $\mathscr{Q}^-(E, K)$ are $\frac{1}{6}$, $\frac{1}{12}$, and $\frac{1}{12}$ respectively.*

Proof See [6, Lemma 5.1]. □

4 Hilbert's 10th problem for rings of integers of $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$

The main goal of this section is to prove Theorem A, which provides an improvement of [6, Theorem 1.2]. Our calculations in Sect. 3.3.1 already allows us to obtain a set $\mathscr{P}$ with larger density. We shall work with two auxiliary imaginary quadratic fields, allowing us to improve [6, Lemma 6.4] by enlarging the set $\mathscr{Q}$. In other words, we are able to larger sets $\mathscr{P}$ and $\mathscr{Q}$ (compared with Theorem 1.1) such that for all $p \in \mathscr{P}$ and $q \in \mathscr{Q}$, Hilbert's 10th Problem has a negative solution for rings of integers of $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$.

4.1 Rank jump in multiple quadratic fields

Fix an elliptic curve $E/\mathbb{Q}$. We work with more than one auxiliary imaginary quadratic fields and study rank jumps of E in any one of these fields.

Lemma 4.1 *Let $K_{(1)}, \ldots, K_{(n)}$ be n distinct imaginary quadratic fields. Suppose that $E/\mathbb{Q}$ is an elliptic curve such that its mod 2 representation is surjective and that the Galois extension $\mathbb{Q}(E[2])/\mathbb{Q}$ does not contain $\mathbb{Q}(\sqrt{-1})$ nor $K_{(i)}$ for $1 \le i \le n$. Then,*

$$\begin{aligned}\mathscr{Q}_{(n)}(E) = \big\{&q : q \equiv -1 \pmod 4,\ q \text{ splits in any one of } K_{(1)} \text{ or } \ldots \text{ or } K_{(n)},\\ &a_q(E) \equiv 1 \pmod 2\big\}\end{aligned}$$

is a Chebotarev set of primes with density $\frac{1}{6} \times \left(1 - \frac{1}{2^n}\right)$.

Proof We can rewrite

$$\mathscr{Q}_{(n)}(E) = \mathscr{Q}_{K_{(1)}}(E) \cup \mathscr{Q}_{K_{(2)}}(E) \cup \cdots \cup \mathscr{Q}_{K_{(n)}}(E).$$

Therefore, it is clear that $\mathscr{Q}_{(n)}(E)$ is a Chebotarev set. Using a matrix counting argument[5] as in [6, Lemma 6.4], it is easy to see that the set

$$\left\{q : q \text{ splits in any one of } K_{(1)} \text{ or } \ldots \text{ or } K_{(n)},\ a_q(E) \equiv 1 \pmod 2\right\}$$

has density $\left(1 - \frac{1}{2^n}\right) \times \frac{1}{3}$. Here, the first factor comes from the fact that we must avoid counting those primes q which are inert in all of the imaginary quadratic fields $K_{(1)}, \ldots, K_{(n)}$. By the Chebotarev density theorem, this happens for exactly $\frac{1}{2^n}$ proportion of the prime numbers. Since we have assumed that $\mathbb{Q}(E[2])/\mathbb{Q}$ does not contain $\mathbb{Q}(\sqrt{-1})$ we can apply Lemma 3.15 to conclude that the desired density is

$$\frac{1}{2} \times \left(1 - \frac{1}{2^n}\right) \times \frac{1}{3}. \qquad \square$$

Lemma 4.2 *Consider the elliptic curve* $E = 557b1$. *We use Cremona's convention of labeling elliptic curves. Then, there exists a Chebotarev set of primes* $\mathscr{Q}$ *with density* $\frac{7}{48}$ *such that for all* $q \in \mathscr{Q}$,

$$\operatorname{rank} E\left(\mathbb{Q}(\sqrt{-q})\right) = 1.$$

Proof One can further verify using [29] that

(i) E has Mordell–Weil rank 0 over $\mathbb{Q}$ and trivial 2-torsion.
(ii) The minimal discriminant of E is positive.
(iii) The Tamagawa number at 2 is odd.
(iv) E has surjective mod 2 representation.
(v) The only degree two subfield of the Galois extension $\mathbb{Q}(E[2])/\mathbb{Q}$ has discriminant 557.

One can check that the Heegner Hypothesis is satisfied for the pairs $(E, \mathbb{Q}(\sqrt{-7}))$, $(E, \mathbb{Q}(\sqrt{-79}))$ and $(E, \mathbb{Q}(\sqrt{-127}))$, and that Hypothesis (*) holds for each of these imaginary quadratic fields.

Choose $\mathscr{Q} = \mathscr{Q}_{\mathbb{Q}(\sqrt{-7})}(E) \cup \mathscr{Q}_{\mathbb{Q}(\sqrt{-79})}(E) \cup \mathscr{Q}_{\mathbb{Q}(\sqrt{-127})}(E)$. We know from Lemma 4.1 that $\mathscr{Q}$ is a Chebotarev set of density $\frac{7}{48}$. Furthermore, Corollary 3.10 tells us that for integers $d = -q \equiv 1 \pmod 4$ that are supported on $\mathscr{Q}_{\mathbb{Q}(\sqrt{-7})}(E)$ or $\mathscr{Q}_{\mathbb{Q}(\sqrt{-79})}(E)$ or $\mathscr{Q}_{\mathbb{Q}(\sqrt{-127})}(E)$, the Mordell–Weil rank of the twisted curve $E^{(d)}$ is 1. It follows that for each $q \in \mathscr{Q}$,

$$\operatorname{rank} E\left(\mathbb{Q}(\sqrt{-q})\right) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E^{(-q)}(\mathbb{Q}) = 1.$$

[5] Alternatively, one may use an inclusion–exclusion argument combined with the fact that the density of the set $\left\{q : q \text{ splits in } K_{(i)},\ a_q(E) \equiv 1 \pmod 2\right\}$ is $\frac{1}{6}$ for each i.

This completes the proof of the lemma. □

4.2 Application to Hilbert's 10th problem

We now prove Theorem A. Our result improves upon [6, Theorem 1.2] and provides a larger class of extensions where Hilbert's 10th Problem is unsolvable.

Theorem 4.3 *There are explicit Chebotarev sets of primes $\mathscr{P}$ and $\mathscr{Q}$ of density $\frac{9}{16}$ and $\frac{7}{48}$, respectively 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 $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$.*

Proof We will work with the rank 0 auxiliary elliptic curve $E = 557b1$. This elliptic curve satisfies the hypotheses of Theorem 3.6, see [6, Lemma 6.2].[6] We set $\mathscr{P}$ and $\mathscr{Q}$ to be the sets of primes given in Corollary 3.13 and Lemma 4.2 respectively. For each $p \in \mathscr{P}$ and $q \in \mathscr{Q}$, the rank of the elliptic curve remains of Mordell–Weil rank 0 over the cubic extension $\mathbb{Q}(\sqrt[3]{p})$ and has rank 1 over the imaginary quadratic extension $\mathbb{Q}(\sqrt{-q})$. Proposition 3.1 asserts that $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})/\mathbb{Q}(\sqrt[3]{p})$ is integrally Diophantine. But, it is well-known that $\mathbb{Q}(\sqrt[3]{p})/\mathbb{Q}$ is integrally Diophantine since $\mathbb{Q}(\sqrt[3]{p})$ has exactly one complex place. The result follows from the Transitive Property. □

5 Hilbert's 10th problem for rings of integers of $\mathbb{Q}(\sqrt[3]{p}, \sqrt{Dq})$

In this section, we work with a fixed elliptic curve of negative minimal discriminant and an imaginary quadratic field of discriminant $-D$. We will show that there exist Chebotarev sets $\mathscr{P}$ and $\mathscr{Q}_D$ of positive density such that for all $p \in \mathscr{P}$, and $q \in \mathscr{Q}_D$, Hilbert's 10th Problem has a negative solution for two families of rings of integers of $\mathbb{Q}(\sqrt[3]{p}, \sqrt{Dq})$. Unlike in the previous section, the extensions we obtain contain a real quadratic subfield, rather than an imaginary one. While these extensions are still deduced from results of Kriz–Li [7] by verifying Hypothesis (*) for an auxiliary elliptic curve and imaginary quadratic fields, we obtain real quadratic fields where we achieve rank jumps since the minimal discriminant of our chosen elliptic curve is negative (see Lemma 5.2 below for details).

Lemma 5.1 *Consider the elliptic curve $E =$704g1.*

(1) *The hypotheses of Theorem 3.6 are satisfied.*
(2) *Hypothesis (*) holds for $K = \mathbb{Q}(\sqrt{-D})$ where D is in the set*[7]

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

Proof (1) The hypotheses can be verified using [29] (see Sect. B.1).

[6] One extra condition we need to check using [29] is that $E(\mathbb{Q}(\mu_3))[3]$ is trivial.

[7] We only checked through the values of D with $D < 700$.

(2) For $\mathbb{Q}(\sqrt{-7})$ this is recorded in [7, Table 2]. For the other values of D, the conditions can be verified using [29]; and the code is provided in Sect. C.1.

□

Lemma 5.2 *Consider the elliptic curve $E =$704g1. Define the set*

$$\mathscr{Q}_D(E) = \left\{ q : q \equiv -1 \pmod 4,\ q \text{ splits in } \mathbb{Q}(\sqrt{-D}),\ a_q(E) \equiv 1 \pmod 2 \right\},$$

such that Hypothesis (*) holds for $\mathbb{Q}(\sqrt{-D})$. This is a Chebotarev set of primes of density $\frac{1}{12}$. Moreover, for all $q \in \mathscr{Q}_D$,

$$\operatorname{rank} E\left(\mathbb{Q}(\sqrt{Dq})\right) = 1.$$

Proof The proof is adapted from [6, Lemma 6.4]. The key difference in the proof is that the elliptic curve 704g1 has negative minimal discriminant. Hence, we must apply Corollary 3.9 (instead of Corollary 3.10). The hypotheses of Corollary 3.9 can be verified directly (for example from LMFDB). The said corollary asserts that for $d \equiv 1 \pmod 4$ supported on $\mathscr{Q}_D(E)$, we have

$$\operatorname{rank} E^{(Dd)} = 1.$$

But note that d can take either positive or negative values. Therefore, choosing d to be the negative of a prime number in $\mathscr{Q}_D(E)$; i.e., $d \equiv -q \equiv 1 \pmod 4$, we have that

$$\operatorname{rank} E^{(Dq)} = 1.$$

In other words,

$$\operatorname{rank} E\left(\mathbb{Q}(\sqrt{Dq})\right) = 1.$$

Since $E =$704g1 has surjective mod 2 representation and $\mathbb{Q}(\sqrt{-11})$ is the unique imaginary quadratic subfield in the Galois extension $\mathbb{Q}(E[2]/\mathbb{Q})$, the density result follows from Lemma 3.15. □

We can now prove Theorem B.

Theorem 5.3 *For all $D \in \mathfrak{D}$, there are explicit Chebotarev sets of primes $\mathscr{P}$ (which is independent of D) and $\mathscr{Q}_D$ of density $\frac{9}{16}$ and $\frac{1}{12}$ respectively 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 $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{Dq})$.*

Proof This result can be proven in the same way as Theorem 4.3. The only difference is that we use $E =$704g1 and the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. □

6 Studying Hilbert's 10th problem problem via a pair of elliptic curves

The goal of this section is to study a slightly different version of Theorem 5.3 by working with two auxiliary elliptic curves. This allows us to obtain a larger set of $\mathscr{P}$, at the expense of a smaller set of $\mathfrak{D}$ with a lower density for $\mathscr{Q}_D$.

6.1 Rank stabilization over cubic extensions for a pair of elliptic curves

The goal of this section is to study a version of Corollary 3.13 for a pair of two elliptic curves (see Corollary 6.3 below). We first introduce the following definition.

Definition 6.1 Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be two elliptic curves, and let ℓ be a prime number.

- Define the sets

$$G_{E_1,E_2,\ell} = \{(A, B) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(A) = \det(B)\}$$
$$H_{E_1,E_2,\ell} = \left\{(A, B) \in G_{E_1,E_2,\ell} : A \in H_{E_1,\ell} \text{ or } B \in H_{E_1,\ell}\right\}.$$

- Elliptic curves E_1 and E_2 are said to be **maximally disjoint** at ℓ if the image of the product of their mod ℓ representations

$$\bar{\rho}_{E_1,E_2,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}(E_1[\ell]) \times \mathrm{GL}(E_2[\ell]) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

  is given by $G_{E_1,E_2,\ell}$.[8]

In particular, the definition of *maximally disjoint* implies that both $\bar{\rho}_{E_1,\ell}$ and $\bar{\rho}_{E_2,\ell}$ are surjective.

Proposition 6.2 *Suppose that $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ are two elliptic curves that are maximally disjoint at $\ell = 3$. Then,*

$$\frac{\#H_{E_1,E_2,\ell}}{\#G_{E_1,E_2,\ell}} = \frac{103}{128}.$$

Proof Under the notation of the proof of Lemma 3.11, the conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_3)$ are given by the following representatives

$$C_{a,b} : \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \text{ (12 elements each)}$$
$$C_a : \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ & -1 \end{pmatrix} \text{ (8 elements each)}$$
$$D_a : \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} -1 & \\ & -1 \end{pmatrix} \text{ (1 element each)}$$

[8] Note that the image of $\bar{\rho}_{E_1,E_2,\ell}$ is always a subgroup of $G_{E_1,E_1,\ell}$ since the determinant of the mod ℓ representation of an elliptic curve is the mod ℓ cyclotomic character.

$$\mathcal{E}_\lambda : \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \begin{pmatrix} 1 & \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix} \text{ (6 elements each)},$$

where we have highlighted the ones lying inside $H_{E,\ell}$ in grey shade. Therefore, we can count the elements in $G_{E_1,E_2,\ell}$ via the following table:

	$\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & \\ 1 & \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$	$\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$	$\begin{pmatrix} 1 & \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$	144✓	96	12	96	12	72	72✓	72✓
$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$	96	64✓	8✓	64✓	8✓	48✓	48	48
$\begin{pmatrix} 1 & \\ 1 & \end{pmatrix}$	12	8✓	1✓	8✓	1✓	6✓	6	6
$\begin{pmatrix} -1 & 1 \\ & -1 \end{pmatrix}$	96	64✓	8✓	64✓	8✓	48✓	48	48
$\begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$	12	8✓	1✓	8✓	1✓	6✓	6	6
$\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$	72	48✓	6✓	48✓	6✓	36✓	36	36
$\begin{pmatrix} 1 & \\ 1 & -1 \end{pmatrix}$	72✓	48	6	48	6	36	36✓	36✓
$\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}$	72✓	48	6	48	6	36	36✓	36✓

A check mark signifies that the product of the conjugacy classes belongs to $G_{E_1,E_2,\ell}$, with those lying inside $H_{E_1,E_2,\ell}$ highlighted in grey shade. We deduce that $\#G_{E_1,E_2,\ell} = 1152$ (this is exactly half of $\#\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ since $G_{E_1,E_2,\ell}$ is the kernel of the group surjective homomorphism from $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to $\mathbb{F}_\ell^\times$ given by $(A, B) \mapsto \det(AB)$) and $\#H_{E_1,E_2,\ell} = 927$. □

Corollary 6.3 *Suppose that $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ are two elliptic curves which are maximally disjoint at 3 and that both E_1 and E_2 satisfy the hypotheses of Theorem 3.6 with $\ell = 3$. Then, there exists a Chebotarev set of primes $\mathscr{P}$ with density $\frac{103}{128}$ such that for all $p \in \mathscr{P}$, either* $\mathrm{rank}\, E_1\left(\mathbb{Q}(\sqrt[3]{p})\right) = 0$ *or* $\mathrm{rank}\, E_2\left(\mathbb{Q}(\sqrt[3]{p})\right) = 0$.

Proof On taking $\mathscr{P}$ to be the union $\mathscr{P}(E_1, 3) \cup \mathscr{P}(E_2, 3)$, the result follows from the Chebotarev density theorem, Proposition 6.2 and Theorem 3.6. □

Analogously, for an integer $n \geq 1$, one may define the set $\mathscr{P}_n$ as the union $\mathscr{P}(E_1, 3) \cup \cdots \cup \mathscr{P}(E_n, 3)$ for elliptic curves $E_1, \ldots, E_n$ that such that the image of the representation $\bar{\rho}_{E_1,3} \times \bar{\rho}_{E_n,3}$ is given by $\left\{(A_1, \cdots, A_n) \in (\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}))^n : \det(A_1) = \cdots \det(A_n)\right\}$.

Lemma 6.4 *The density for $\mathscr{P}_n$ is*

$$\frac{2 \cdot 24^n - 12^n - 9^n}{2 \cdot 24^n} = 1 - \frac{3^n + 4^n}{2^{3n+1}}.$$

Proof There are in total 48^n elements in $(\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}))^n$. Half of the elements of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ have determinant 1, while the other half have determinant 2. Therefore, there are $\frac{1}{2^{n-1}} \times 48^n = 2 \cdot 24^n$ n-tuples with matching determinant. Of those, we exclude those without factors in $H_{E,\ell}$, i.e., the n-tuples of matrices which are

1. all in the same conjugacy class as $\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$, of which there are 12^n, or

2. in all possible combinations of conjugacy classes represented by $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$.

As for the size of the latter type of matrices, the conjugacy class for $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ has size 8, while that of the identity matrix is 1, so keeping in mind the possible positions, the latter count is

$$8^n + \binom{n}{1}8^{n-1} + \ldots + \binom{n}{n-1}8 + 1 = (8+1)^n.$$

The result follows. □

In particular, the density of $\mathscr{P}_n$ approaches 1 as $n \to \infty$. In Table 1, we list the densities for $\mathscr{P}_n$ for some small n. The cases $n = 1$ (resp. $n = 2$) correspond to Lemma 3.11 (resp. Corollary 6.3).

6.2 Rank jumps for two elliptic curves

Next, we study families of real quadratic fields where the Mordell–Weil ranks of two elliptic curves increase under base-change simultaneously.

Lemma 6.5 *Let K be an imaginary quadratic field. Suppose that there exist two elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ such that their mod 2 representations are surjective. Further suppose that E_1, E_2 are maximally disjoint at 2 and that the Galois extension $\mathbb{Q}(E_1[2], E_2[2])/\mathbb{Q}$ does not contain $\mathbb{Q}(\sqrt{-1})$ or K. Then,*

$$\mathscr{Q}_K(E_1, E_2) = \{q : q \equiv -1 \pmod 4,\ q \text{ splits in } K,\\ a_q(E_1) \equiv a_q(E_2) \equiv 1 \pmod 2\}$$

is a Chebotarev set of primes with density $\frac{1}{36}$.

Proof We argue as in [6, Proof of Lemma 5.1(ii)], who treated the case of one elliptic curve and obtained a density of $\frac{1}{6}$. For $E = E_1$ or $E = E_2$, the condition $a_q(E) \equiv 1 \pmod 2$ corresponds to the image of Frob_q being the two elements $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]$, i.e., two of the six possible matrices of $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. Note that they each have determinant -1, so the maximally disjoint condition alone would imply that all four combinations of these two matrices occur in the image of $\bar{\rho}_{E_1,E_2,2}$ giving a proportion of $\frac{4}{36}$. The other conditions cut down the proportion by a factor of $\frac{1}{2}$ each by the Chebotarev density theorem and the fact that $q \equiv -1 \pmod 4$ is a splitting condition in $\mathbb{Q}(\sqrt{-1})$, which alongside K we assumed to not be in $\mathbb{Q}(E_1[2], E_2[2])$. We thus obtain a density of $\frac{1}{2} \times \frac{1}{2} \times \frac{4}{36}$, i.e., one-third the proportion compared to when we work with one elliptic curve. □

Corollary 6.6 *Suppose that there are two elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ satisfying the hypotheses of the above Lemma 6.5 and of Corollary 3.9 for some imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. Then for any $q \in \mathscr{Q}_K(E_1, E_2)$,* $\mathrm{rank}\, E_1(\mathbb{Q}(\sqrt{Dq})) = 1 = \mathrm{rank}\, E_2(\mathbb{Q}(\sqrt{Dq}))$.

Proof We argue as in Corollary 6.5 to conclude that the quadratic twists of E_1 and E_2 by $-D$ have $\mathbb{Q}$-rational points of rank 1. Indeed, we can apply the last assertion of Theorem 3.8 to see that rank $E(\mathbb{Q}) = \text{rank } E^{(-q)}(\mathbb{Q}) = 0$ and from the first assertion, conclude that rank $E^{((-q)\cdot(-D))}(\mathbb{Q}) = 1$ for each of $E = E_1$ and $E = E_2$. Hence, rank $E_1(\mathbb{Q}(\sqrt{Dq})) = 1 = \text{rank } E_2(\mathbb{Q}(\sqrt{Dq}))$. □

This when combined with Corollary 6.3 proves Theorem C.

Theorem 6.7 *There are explicit Chebotarev sets of primes $\mathscr{P}$ and $\mathscr{Q}$ (resp. $\mathscr{P}$ and $\mathscr{Q}'$) of density $\frac{103}{128}$ and $\frac{1}{36}$ such that for all $(p, q) \in \mathscr{P} \times \mathscr{Q}$ (resp. $(p, q') \in \mathscr{P} \times \mathscr{Q}'$), the analogue of Hilbert's 10th Problem is unsolvable for the ring of integers of $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{7q})$ (resp. $L' = \mathbb{Q}(\sqrt[3]{p}, \sqrt{615q'})$).*

Proof We combine Corollary 6.3 and Lemma 6.5 with Corollary 6.6. We work with the elliptic curves $E_1 =$704g1 and $E_2 =$1472j1. Using the code in Appendix A, we verify maximal disjointedness at $\ell = 3$, and check that each elliptic curve satisfies the other required conditions, i.e.,

1. the hypotheses of Lemma 6.5 and
2. those of Theorem 3.8.

As for the former conditions, we know that E_1 and E_2 are maximally disjoint at 2, as can be verified in Appendix A. One can verify that $\mathbb{Q}(E_1[2], E_2[2])$ contains three degree 2 subfields of conductors -11, -23, and 253.

To check the conditions of Theorem 3.8, we refer the reader to the SAGE code in Appendix A, where we choose $K = \mathbb{Q}(\sqrt{-7})$ (resp. $K = \mathbb{Q}(\sqrt{-615})$) We let $\mathscr{P} = \mathscr{P}(E_1, 3) \cup \mathscr{P}(E_2, 3)$ (defined in Theorem 3.6), and let $\mathscr{Q} := \mathscr{Q}_{\mathbb{Q}(\sqrt{-7})}(E_1, E_2)$ and $\mathscr{Q}' := \mathscr{Q}_{\mathbb{Q}(\sqrt{-615})}(E_1, E_2)$ as in Lemma 6.5. From this we know that for $p \in \mathscr{P}$ and $q \in \mathscr{Q}$, either rank $E_1\left(\mathbb{Q}(\sqrt[3]{p})\right) = 0$ or rank $E_2\left(\mathbb{Q}(\sqrt[3]{p})\right) = 0$ from Corollary 3.13, and for $q \in \mathscr{Q}$, we have rank $E_1(\mathbb{Q}(\sqrt{Dq})) = \text{rank } E_2(\mathbb{Q}(\sqrt{Dq})) = 1$ for $D = 7$ and for $D = 615$. We can now apply Proposition 3.1 to at least one of E_1 or E_2. The result then follows from Shlapentokh's Theorem. □

Remark 6.8 We included only two elliptic curves, obtaining the density corresponding to $n = 2$ in Table 1. With enough computing power, it should in principle be possible to generalize Theorem 6.7 further using n auxiliary elliptic curves satisfying the appropriate hypotheses for an arbitrary n. It would be interesting to see how big n could be made with the most powerful computers available. The analogue of the set $\mathscr{P}$ should then have density $1 - \frac{3^n+4^n}{2^{3n+1}}$ (cf. Table 1, where the analogue of $\mathscr{P}$ is called $\mathscr{P}_n$). As for the analogue of the set $\mathscr{Q}$ built out of n curves, the "worst case scenario" would occur when the image of the representation $\bar{\rho}_{E_1,\ldots,E_n,2} = \bar{\rho}_{E_1,2} \times \cdots \times \bar{\rho}_{E_n,2}$ is $(\text{GL}_2(\mathbb{Z}/2\mathbb{Z}))^n$. Its density would be $\frac{1}{4} \times \frac{1}{3^n}$. However, it is possible that the density is higher and does not converge to zero. For example, if the image of $\bar{\rho}_{E_1,\ldots,E_n,2}$ is isomorphic to the diagonal embedding of $\text{GL}_2(\mathbb{Z}/2\mathbb{Z})$, then the density would be $\frac{1}{12}$.

Remark 6.9 Suppose that one could find an elliptic curve other than 557b1, which has positive discriminant and satisfies the hypotheses of Theorem 3.6 with $\ell = 3$. If furthermore the new curve and 557b1 are maximally disjoint at 3, then one could obtain

a similar result to Theorem 6.7, where one improves the density of $\mathscr{P}$ in Theorem 4.3 to $\frac{103}{128}$. The density of the resulting $\mathscr{Q}$ would depend on the joint image of the mod 2 representations of the two curves. Due to the limited computing power we have had access to, we have not been able to find such a curve.

7 Congruent number elliptic curves and Hilbert's 10th problem

We study a different version of Theorem 6.7 using congruent number elliptic curves. One advantage of this approach is that one may make use of recent breakthroughs in Goldfeld's conjecture for these curves to study the set $\mathscr{Q}$.

7.1 Congruent number elliptic curves

In this section we study the congruent number elliptic curve $E = 32a2$, defined by the equation $y^2 = x^3 - x$. Note that E has good supersingular reduction at 3 with $a_3(E) = 0$.

Similar to the curve 704g1 studied in Lemma 5.1, we can check that E satisfies the hypotheses of Theorem 3.6 for $\ell = 3$ using [29].

We now calculate the density of the set $\mathscr{P}(E, 3)$ given in Theorem 3.6.

Lemma 7.1 *For $E = 32a2$, we have*

$$\frac{\#H_{E,3}}{\#G_{E,3}} = \frac{11}{16}.$$

In other words, the set $\mathscr{P}(E, 3)$ defined in the statement of Theorem 3.6 is a Chebotarev set of density $\frac{11}{16}$.

Proof The curve E has complex multiplication and the image of $\bar{\rho}_{E,3}$ is maximal, given by the following 16 matrices:

$$\begin{pmatrix}1 & \\ & 1\end{pmatrix}, \begin{pmatrix}2 & 2\\ & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ & 2\end{pmatrix}, \begin{pmatrix}2 & \\ 2 & 1\end{pmatrix}, \begin{pmatrix}1 & \\ 1 & 2\end{pmatrix}, \text{ and } \begin{pmatrix}2 & \\ & 2\end{pmatrix}, \begin{pmatrix}2 & 2\\ 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix},$$
$$\begin{pmatrix}2 & 1\\ 1 & \end{pmatrix}, \begin{pmatrix}1 & 2\\ 2 & \end{pmatrix}, \begin{pmatrix}2 & \\ 2 & 2\end{pmatrix}, \begin{pmatrix}1 & \\ 1 & 1\end{pmatrix}, \begin{pmatrix} & 2\\ 1 & \end{pmatrix}, \begin{pmatrix} & 1\\ 2 & \end{pmatrix}, \begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix}, \begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix},$$

with the ones lying inside $H_{E,3}$ highlighted in grey shade. □

Remark 7.2 Curiously, even though $\bar{\rho}_{E,3}$ is not surjective, we are actually getting a larger proportion than the case where the representation is surjective studied in Lemma 3.11.

A straightforward application of Theorem 3.6 shows that

Corollary 7.3 *There exists a Chebotarev set $\mathscr{P}_{\text{cong}}$ of primes of density $\frac{11}{16}$ such that the Mordell–Weil rank of $E/\mathbb{Q}(\sqrt[3]{p})$ is 0 for all $p \in \mathscr{P}_{\text{cong}}$.*

7.2 Rank jump in real quadratic fields

We now turn our attention to studying real quadratic fields over which E has positive rank. The congruent number problem predicts that for all positive square-free integers n that are congruent to $5, 6, 7 \mod 8$, the quadratic twist of E given by

$$E^{(n)} : ny^2 = x^3 - x$$

has positive Mordell–Weil rank. In particular, it predicts that rank $E\left(\mathbb{Q}(\sqrt{n})\right)$ is positive.

Definition 7.4 Let $\mathscr{Q}_{\text{cong}}$ be the set of primes q such that the elliptic curve $qy^2 = x^3 - x$ has positive Mordell–Weil rank over $\mathbb{Q}$ (or equivalently q is a congruent number).

A result announced by Smith in [27, Theorem 1.5] says that $E^{(n)}$ has positive Mordell–Weil over $\mathbb{Q}$ for at least 62.9% of n that are congruent to 5 and 7 modulo 8. In particular, it says that $\mathscr{Q}_{\text{cong}}$ has density at least 31.45%. More recently, Kriz [9] announced a proof of Goldfeld's conjecture for the family of congruent number elliptic curves. In particular, it says that the density of $\mathscr{Q}_{\text{cong}}$ is precisely $\frac{1}{2}$.

We conclude this section with the following result, which is Theorem D in the introduction.

Theorem 7.5 *Let $\mathscr{P}_{\text{cong}}$ and $\mathscr{Q}_{\text{cong}}$ be the set of primes defined as in Corollary 7.3 and Definition 7.4. Then, the analogue of Hilbert's 10th Problem is unsolvable for the ring of integers of $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{q})$.*

Proof This follows from the same proof as Theorem 4.3. □

Appendix A MAGMA code for verification of maximal disjointedness

The Magma code below, written by Harris B. Daniels, is used to verify whether two elliptic curves are maximally disjoint at a prime p.

```
    function SimpleSplit(f)
    Factors := [vec[1] : vec in Factorization(f) | Degree(vec[1]) gt 1]\\
   ;
    Fields := [NumberField(fac) : fac in Factors];
    K := Rationals();
    for F in Fields do
        K := Compositum(F,K);
    end for;
    return K;
end function;

//Given 2 elliptic curves E1 and E2 and a prime p, it returns true
 if Q(E1[p])
//meet Q(E2[p]) eq Q(zeta_p). Note that if Q(E1[p]) eq Q(E2[p])
 eq Q(zeta_p),
//then this function will return true.
```

```
function HasMaxDisjointPTorsion(E1,E2,p)
    f1 := DivisionPolynomial(E1,p);
    f2 := DivisionPolynomial(E2,p);
    K1<a1> := SimpleSplit(f1);
    K2<a2> := SimpleSplit(f2);
    P1<y1> := PolynomialRing(K1);
    P2<y2> := PolynomialRing(K2);

//Now we see if we need to add any y coordinates.
    rts1 := [vec[1] : vec in Roots(P1!f1) |
                    IsIrreducible(Evaluate(DefiningPolynomial(E1),\\
                [vec[1],y1,1]))];
    rts2 := [vec[1] : vec in Roots(P2!f2) |
                    IsIrreducible(Evaluate(DefiningPolynomial(E2),\\
                  [vec[1],y2,1]))];
//If there are y-coordinates to add, we add them now to K1 and K2 \\
         to make L1 and L2.
    if #rts1 ne 0 then
        p1 := Evaluate(DefiningPolynomial(E1),[rts1[1],y1,1]);
        L1<b1> := AbsoluteField(ext<K1 | p1>);
    else
        L1<b1> := K1;
    end if;

    if #rts2 ne 0 then
        p2 := Evaluate(DefiningPolynomial(E2),[rts2[1],y2,1]);
        L2<b2> := AbsoluteField(ext<K2 | p2>);
    else
        L2<b2> := K2;
    end if;

    dp1 := DefiningPolynomial(L1); //The splitting field of L1 is \\
 Q(E1[p])
    dp2 := DefiningPolynomial(L2); //The splitting field of L2 is\\
           Q(E2[p])

    //This last step checks the degrees are what they should be.
    s1 := #GaloisGroup(dp1);
    s2 := #GaloisGroup(dp2);
    s3 := #GaloisGroup(dp1*dp2);
    return s1*s2 div EulerPhi(p) eq s3;
end function;

E1 := EllipticCurve("704g1");
E2 := EllipticCurve("1472j1");
p := 3; // change the 3 to a 2 to check for maximal disjointness at 2

HasMaxDisjointPTorsion(E1,E2,p);
```

Appendix B SAGE code for preserving the rank in cubic extensions

Appendix B.1 Elliptic curve of conductor 704

Start with the elliptic curve $E = 704g1$ (Cremona label).

1. E has good ordinary reduction at 3.
2. At all the primes p, the residual Galois representation of E has maximal image.
3. We also check that 3 is not a prime of anomalous reduction.
4. The twist of E by -3 has rank 0. To calculate the rank of the twisted elliptic curve use:

```
E = EllipticCurve('704g1')
Et = E.quadratic_twist(-3)
Et.rank()
```

5. It is clear that the base-change of E to $\mathbb{Q}(\sqrt{-3})$ has rank 0. Just to be sure, we can check:

```
E = EllipticCurve('704g1')
K.<t> = QuadraticField(-3)
EK = E.base_extend(K)
EK.rank()
```

6. We check that the order of the torsion group of E over $\mathbb{Q}(\sqrt{-3})$ is not divisible by 3. Just to be sure, we can check:

```
E = EllipticCurve('704g1')
K.<t> = QuadraticField(-3)
EK = E.base_extend(K)
EK.torsion_group()
```

7. The primes of bad reduction are 2, 11 (which are both inert in $\mathbb{Q}(\sqrt{-3})$). This is also clear from [7, Table 2]. To obtain the local data use:

```
E = EllipticCurve('704e1')
K.<t> = QuadraticField(-3)
EK = E.base_extend(K)
EK.local_data(2)
EK.local_data(11)
```

   Output: The Tamagawa number at the inert prime 2 is 1 and at the inert prime 11 is 1.
8. To see that $3 \nmid \#X(E/\mathbb{Q}(\sqrt{-3}))$, we can use [22, Theorem 2.1]. It suffices to check that $\#X(E^{(-3)}/\mathbb{Q})$ is not divisible by 3. For this, use:

```
E = EllipticCurve('704g1')
Et = E.quadratic_twist(-3)
St = Et.sha()
St.an()
```

   Output: The (analytic) Shafarevich–Tate group is trivial for the quadratic twist of E.

Remark B.1 This elliptic curve satisfies the Hypothesis (*) when the imaginary quadratic field is $\mathbb{Q}(\sqrt{-7})$, see [7, Table 2].

Appendix B.2 Elliptic curve of conductor 1472

Now we work with the elliptic curve $E = 1472j1$ (Cremona label). For this curve, we can check all the properties as in the previous section. This elliptic curve is not in the table of Kriz–Li since the conductor is larger than 750. We now check that Hypothesis (*) is satisfied in Appendix C.

Appendix C SAGE code for verifying Hypothesis (*) for curves 704g1, 1472j1, and 557b1

Appendix C.1 When conductor is 704 or 1472

The prime 2 is a prime of bad reduction for the curve of conductor 704 and 1472. Since the Heegner hypothesis is satisfied for $K = \mathbb{Q}(\sqrt{-7})$, it follows immediately that 2 splits in the extension $K/\mathbb{Q}$. The other way to check is to use quadratic reciprocity: since $-7 \equiv 1 \pmod 4$ it follows that the discriminant d_K of K is -7. Since, $d_K \equiv 1 \pmod 8$, we know that 2 splits in K. The same argument shows that 2 splits in $K = \sqrt{-615}$.

Finding the size of $\tilde{E}^{ns}(\mathbb{F}_2)$

Note that 2 is a prime of additive reduction for both the elliptic curves of interest. Hence,

$$|\tilde{E}^{ns}(\mathbb{F}_2)| = |\tilde{E}(\mathbb{F}_2)| - 1 = 3 - 1 = 2.$$

Finding the Heegner Point in K

When K has class number 1

Since $\mathbb{Q}(\sqrt{-7})$ has class number 1, the Heegner point lies in K itself. However, we write a general code suggested by J. Cremona available here which will allow us to change K:

```
E = EllipticCurve('704g1')
a = -7 # conductor of the imaginary quadratic field
P = E.heegner_point(a) # this Heegner point is in H(K)
P1 = P.point_exact()
K = P1[0].parent()
E = P1.curve()
G = K.automorphisms()
def apply(sigma, pt):
     E = pt.curve()
     return E([sigma(c) for c in pt])
sum([apply(sigma,P1) for sigma in G], 0)
```

```
s = K(a).sqrt()
H = sum([apply(sigma,P1) for
 sigma in G if sigma(s)==s], 0)
# this is the Heegner point in K
r1 = -H[0]/-H[1] # r= -x(H)/y(H)
#parameter corresponding to H
H2 = H + H # sum of Heegner points 2H
r2 = -H2[0]/-H2[1] # r= -x(H2)/y(H2)
#parameter corresponding to 2H
```

Calculating the 2-adic valuation of $|\widetilde{E}^{ns}(\mathbb{F}_2)|\log_{\omega_E}(P)$

```
L2=r2.parent()
u=QQ.valuation(2)
vL2=u.extensions(L2); v2=vL2[0]
print(v2(r2), v2(r2-r2^3/3))
# obtain what to evaluate by checking
 the first terms of E.formal_group().log(10)
```

The output is 1 1. This means that Hypothesis (*) is satisfied for $K = \mathbb{Q}(\sqrt{-7})$.

When K does not have class number 1

Our code above works for any imaginary quadratic field, not just those with class number 1. We use it to check that both the elliptic curves of interest, namely $704g1$ and $1472j1$ satisfy Hypothesis (*) when the imaginary quadratic field is $\mathbb{Q}(\sqrt{-615})$.

Appendix C.2 When conductor is 557

In [7, Table 2], it is already checked that E=$557b1$ satisfies Hypothesis (*) when the imaginary quadratic field is $\mathbb{Q}(\sqrt{-7})$. To check that the same holds for $\mathbb{Q}(\sqrt{-79})$ (resp. $\mathbb{Q}(\sqrt{-127})$), we need to first verify that 2 splits in $\mathbb{Q}(\sqrt{-79})$ (resp. $\mathbb{Q}(\sqrt{-127})$). This follows from the observation that $-127 \equiv 1 \pmod 8$.

For the elliptic curve $E = 557b1$, the prime 2 is a prime of good reduction so we can use the code to know $|\widetilde{E}^{\mathrm{ns}}(\mathbb{F}_2)|$:

```
EllipticCurve(GF(2),'557b1').cardinality()
```

The output is 1.

Now we calculate the 2-adic valuation of $|\widetilde{E}^{\mathrm{ns}}(\mathbb{F}_2)|\log_{\omega_E}(P) = \log_{\omega_E}(P)$:

```
E = EllipticCurve('557b1')
a = -127 # replace with -79 for the other verification
P = E.heegner_point(a)
P1 = P.point_exact(300) #might have to increase precision
K = P1[0].parent()
E = P1.curve()
```

```
G = K.automorphisms()
def apply(sigma, pt):
     E = pt.curve()
     return E([sigma(c) for c in pt])
sum([apply(sigma,P1) for sigma in G], 0)
s = K(a).sqrt()
H = sum([apply(sigma,P1) for sigma in
 G if sigma(s)==s], 0)
# this is the Heegner point in K
r1 = -H[0]/-H[1] # r= -x(H)/y(H)
 #parameter corresponding to H
L1=r1.parent()
u=QQ.valuation(2)
vL1=u.extensions(L1); v1=vL1[0]
print(v1(r1-r1^3/3))
```

The output is 1. This means that Hypothesis (*) is satisfied for $K = \mathbb{Q}(\sqrt{-127})$.

Acknowledgements This project was started as part of the IAS Summer Collaboration Program (2022). We thank the Institute for Advanced Study for its hospitality and financial support. We thank Harris B. Daniels for sharing with us his code on computing joint images of Galois representations attached to two elliptic curves (see Appendix A). We also thank John Cremona, Henri Darmon, Tim Dokchitser, Natalia García-Fritz, Daniel Kriz, Marc Masdeu, Kumar Murty, Robert Pollack, Karl Rubin and Chris Skinner for answering many of our questions and their helpful comments during the preparation of this article. We are grateful to the referee for valuable comments and suggestions on an earlier version of the article, which led to notable improvements. DK is supported by a PIMS Postdoctoral Fellowship. AL is supported by the NSERC Discovery Grants Program RGPIN-2020-04259 and RGPAS-2020-00096. FS is supported by NSF grant 2001280 and Simons Grant 635320. On behalf of all authors, the corresponding author states that there is no conflict of interest. This manuscript has no associated data.

References

1. Brau, J.: Selmer groups of elliptic curves in degree p extensions (2014). Preprint arXiv:1401.3304
2. Cornelissen, G., Pheidas, T., Zahidi, K.: Division-ample sets and the Diophantine problem for rings of integers. J. Théor. Nombres Bordeaux **17**(3), 727–735 (2005)
3. Denef, J.: Diophantine sets over algebraic integer rings. II. Trans. Am. Math. Soc. **257**(1), 227–236 (1980)
4. Denef, J., Lipshitz, L.: Diophantine sets over some rings of algebraic integers. J. Lond. Math. Soc. **2**(3), 385–391 (1978)
5. Davis, M., Putnam, H., Robinson, J.: The decision problem for exponential Diophantine equations. Ann. Math. **74**, 425–436 (1961)
6. Garcia-Fritz, N., Pasten, H.: Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points. Math. Ann. **377**(3–4), 989–1013 (2020)
7. Kriz, D., Li, C.: Goldfeld's conjecture and congruences between Heegner points. Forum Math. Sigma **7**(e15), 80 (2019)
8. Kundu, D., Lei, A., Ray, A.: Arithmetic statistics and noncommutative Iwasawa theory. Doc. Math. **27**, 89–150 (2022)
9. Kriz, D.: Supersingular main conjectures, Sylvester's conjecture and Goldfeld's conjecture (2020). Preprint arXiv:2002.04767
10. Matijasevic, Y.: Enumerable sets are Diophantine. Sov. Math. Dokl. **11**, 354–358 (1970)
11. Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Invent. Math. **18**(3–4), 183–266 (1972)

12. Murty, M.R., Fodden, B.: Hilbert's Tenth Problem: An Introduction to Logic, Number Theory, and Computability, vol. 88. American Mathematical Society, Providence (2019)
13. Milne, J.S.: Arithmetic Duality Theorems. BookSurge, LLC, Charleston, SC (2006)
14. Murty, M.R., Pasten, H.: Elliptic curves, L-functions, and Hilbert's tenth problem. J. Number Theory **182**, 1–18 (2018)
15. Mazur, B., Rubin, K.: Finding large Selmer rank via an arithmetic theory of local constants. Ann. Math. **166**, 579–612 (2007)
16. Mazur, B., Rubin, K.: Ranks of twists of elliptic curves and Hilbert's tenth problem. Invent. Math. **181**(3), 541–575 (2010)
17. Mazur, B., Rubin, K., Larsen, M.: Diophantine stability. Am. J. Math. **140**(3), 571–616 (2018)
18. Mazur, B., Rubin, K., Shlapentokh, A.: Defining $\mathbb{Z}$ using unit groups. Preprint arXiv:2303.02521 (2023)
19. Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields. Fundamental Principles of Mathematical Sciences, vol. 323. Springer, Berlin (2008)
20. Pheidas, T.: Hilbert's tenth problem for a class of rings of algebraic integers. Proc. Am. Math. Soc. **104**(2), 611–620 (1988)
21. Poonen, B.: Using Elliptic Curves of Rank One Towards the Undecidability of Hilbert's Tenth Problem Over Rings of Algebraic Integers. International Algorithmic Number Theory Symposium, pp. 33–42. Springer, Berlin (2002)
22. Qiu, D.: On quadratic twists of elliptic curves and some applications of a refined version of Yu's formula. Commun. Algebra **42**(12), 5050–5064 (2014)
23. Ray, A.: Remarks on Hilbert's tenth problem and the Iwasawa theory of elliptic curves. Bull. Aust. Math. Soc. (to appear) (2022). arXiv:2206.06296
24. Serre, J.-P.: Local Fields, vol. 67. Springer, Berlin (2013)
25. Shlapentokh, A.: Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers. Trans. Am. Math. Soc. **360**(7), 3541–3555 (2008)
26. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106. Springer, Berlin (2009)
27. Smith, A.: The congruent numbers have positive natural density. Preprint arXiv:1603.08479 (2016)
28. Shapiro, H.N., Shlapentokh, A.: Diophantine relationships between algebraic number fields. Commun. Pure Appl. Math. **42**(8), 1113–1122 (1989)
29. The Sage Development Team: Sage Mathematics Software (Version 9.0) (2020). `http://www.sagemath.org`
30. Videla, C.: Sobre el décimo problema de Hilbert, Atas da Xa Escola de Algebra, Vitoria, ES, Brasil. Colecao Atas **16**, 95–108 (1989)
31. Washington, L.C.: Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC, Boca Raton (2008)