TOWARDS HILBERT'S TENTH PROBLEM FOR RINGS OF INTEGERS THROUGH IWASAWA THEORY AND HEEGNER POINTS

NATALIA GARCIA-FRITZ AND HECTOR PASTEN

Abstract. For a positive proportion of primes p and q, we prove that $\mathbb{Z}$ is Diophantine in the ring of integers of $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$. This provides a new and explicit infinite family of number fields K such that Hilbert's tenth problem for O_K is unsolvable. Our methods use Iwasawa theory and congruences of Heegner points in order to obtain suitable rank stability properties for elliptic curves.

1. Introduction

A celebrated result due to Matiyasevich [Ma70] after the work of Davis, Putnam, and Robinson [DPR61], shows that computably enumerable sets over $\mathbb{Z}$ are exactly the same as Diophantine sets over $\mathbb{Z}$. As a consequence, Hilbert's tenth problem is unsolvable: namely, there is no algorithm (Turing machine) that takes as input polynomial equations over $\mathbb{Z}$ and decides whether they have integer solutions.

A natural extension is the analogue of Hilbert's tenth problem for rings of integers of number fields, which remains as one of the main open problems in the area. In the direction of a negative solution, the following conjecture formulated by Denef and Lipshitz [DL78] is widely believed (the notion of Diophantine set is recalled in Section 3):

Conjecture 1.1. *Let K be a number field K. Then $\mathbb{Z}$ is a Diophantine subset of O_K.*

By a standard argument, if $\mathbb{Z}$ is Diophantine in O_K for a number field K, then the analogue of Hilbert's tenth problem for O_K has a negative solution, and moreover, the Diophantine sets over O_K are the same as computably enumerable subsets. Thus, the efforts have concentrated in proving new cases of Conjecture 1.1.

However, progress on Conjecture 1.1 has been slow and extremely difficult. First, one has the following known cases dating back to the eighties:

(i) K is totally real or a quadratic extension of a totally real field [DL78, De80]
(ii) $[K:\mathbb{Q}] = 4$, K is not totally real, and $K/\mathbb{Q}$ has a proper intermediate field [DL78]
(iii) K has exactly one complex place [Ph88, Sh89, Vi89]
(iv) K is contained in a number field L such that $\mathbb{Z}$ is Diophantine in O_L; in particular, this holds when $K/\mathbb{Q}$ is abelian [SS89]

Later work by Poonen [Po02], Cornelissen-Pheidas-Zahidi [CPZ05], and Shlapentokh [Sh08] reduced Conjecture 1.1 to the existence of elliptic curves preserving its (positive) rank in suitable extensions of number fields (cf. Section 3). This allowed to verify Conjecture 1.1 on a case-by-case basis for concrete examples of number fields by exhibiting a suitable elliptic curve (see the Paragraph 3.1 for the worked-out example $K = \mathbb{Q}(\sqrt[5]{2})$). Besides specific examples, the elliptic curve criteria also led to the following more recent result by Mazur and Rubin:

Date: September 23, 2019.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11U05.

Key words and phrases. Hilbert's tenth problem, Diophantine set, rank of elliptic curves, quadratic twists, Iwasawa theory, Heegner points.

N. G.-F. was supported by the FONDECYT Iniciación en Investigación grant 11170192, and the CONICYT PAI grant 79170039. H.P. was supported by FONDECYT Regular grant 1190442.

(v) For any number field F for which $\mathbb{Z}$ is Diophantine in O_F, there is a positive proportion of primes ℓ such that for all $n \geq 1$, there are infinitely many choices of K as a cyclic ℓ^n-extension of F for which $\mathbb{Z}$ is Diophantine in O_K. (cf. [MR18]; see also [MR10]).

This concludes our summary of known cases of Conjecture 1.1.

In this work we develop a method to attack Conjecture 1.1 which allows us to prove it in several new cases. Our main result is the following:

Theorem 1.2. *There are explicit Chebotarev sets of primes $\mathscr{P}$ and $\mathscr{Q}$ having positive density in the primes, such that for all $p \in \mathscr{P}$ and all $q \in \mathscr{Q}$ we have that $\mathbb{Z}$ is Diophantine in the ring of integers of $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$. In particular, for these fields $K = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$, the analogue of Hilbert's tenth problem for O_K is unsolvable.*

The sets $\mathscr{P}$ and $\mathscr{Q}$ can be chosen to have densities $5/16 > 31\%$ and $1/12 > 8\%$ respectively.

The sets of prime numbers $\mathscr{P}$ and $\mathscr{Q}$ from our construction will be made explicit in Section 6.

Theorem 1.2 precisely covers one of the simplest kinds of number fields which is out of the scope of all the available results on Hilbert's tenth problem for rings of integers —see Paragraph 3.3 for details.

Besides the fact that we prove new cases of Conjecture 1.1, the main novelty in our work is the method of proof for Theorem 1.2. Using Shlapentokh's elliptic curve criterion and the result of Pheidas, Shlapentokh and Videla quoted above in item (iii), we reduce the problem to the existence of a suitable elliptic curve E over $\mathbb{Q}$ with $\operatorname{rank} E(\mathbb{Q}(\sqrt[3]{p})) = 0$ and $\operatorname{rank} E(\mathbb{Q}(\sqrt{-q})) > 0$. The first condition is achieved by a study of the variation of cyclotomic Iwasawa invariants under base-change, while the second one is achieved by means of a recent result by Kriz and Li [KL19] on congruences of Heegner points in the context of the celebrated Goldfeld's conjecture. Both methods —Iwasawa theory and Heegner points— impose a series of technical conditions on the admissible elliptic curves E, and a critical aspect of the proof of Theorem 1.2 is to make sure that there exist elliptic curves that are admissible for both methods simultaneously.

Let us remark that the approach by Mazur and Rubin (cf. Item (v) above) is substantially different to ours: they achieve the necessary rank-stability conditions by delicate cohomological computations to modify Selmer ranks under quadratic twists.

We conclude this introduction by recalling that there is strong evidence for Conjecture 1.1, at least if one assumes some standard conjectures on elliptic curves. On the one hand, Mazur and Rubin [MR10] proved that it follows from the squareness conjecture for the 2-torsion of Shafarevich-Tate groups of elliptic curves over number fields. On the other hand, Murty and Pasten [MP18] proved that it follows from rank aspects of the Birch and Swinnerton-Dyer conjecture.

2. Preliminaries on Iwasawa theory

Our main results are relevant on logic aspects of number theory but part of our arguments require some Iwasawa theory. So, it might be useful to include here a brief reminder of the latter subject. Other than for the purpose of checking the notation, experts can safely skip this section.

In this section ℓ denotes a prime number. We specialize to the case of cyclotomic Iwasawa theory for elliptic curves, which suffices for our purposes. All results discussed in this section can be found in [Ma72] and [Gr01].

2.1. **Algebra.** It is a standard fact that if X is a finitely generated torsion $\mathbb{Z}_\ell[[T]]$-module, then X is pseudo-isomorphic[1] to

$$\bigoplus_i \mathbb{Z}_\ell[[T]]/(\ell^{\mu_i}) \oplus \bigoplus_j \mathbb{Z}_\ell[[T]]/(f_j^{m_j})$$

[1] A pseudo isomorphism is a morphism with finite kernel and cokernel.

where μ_i are positive integers and $f_j \in \mathbb{Z}_\ell[T]$ are monic, irreducible polynomials such that all non-leading coefficients are in $\ell\mathbb{Z}_\ell$.

The above decomposition is unique up to order, and one defines the following invariants of X:

- $\mu_X = \sum_i \mu_i$ the μ-invariant
- $f_X = \ell^{\mu_X} \prod_j f_j^{m_j}$ the characteristic polynomial
- $\lambda_X = \deg f_X$ the λ-invariant.

2.2. **Iwasawa algebras and modules.** For a number field k, we let k_∞ be the maximal cyclotomic $\mathbb{Z}_\ell$-extension of k. For each $m \geq 0$ we let k_m/k for the unique cyclotomic $\mathbb{Z}/\ell^m\mathbb{Z}$-extension of k contained in k_∞, and we observe that $k_0 = k$ and $k_\infty = \cup_m k_m$. The Galois group Γ_k of k_∞/k is (non-canonically) isomorphic to $\mathbb{Z}_\ell$ as a profinite group. The *Iwasawa algebra* $\Lambda_k = \mathbb{Z}_\ell[[\Gamma_k]]$ is the profinite completion of the group algebra $\mathbb{Z}_\ell[\Gamma_k]$. The choice of a topological generator $\gamma \in \Gamma_k$ determines a continuous $\mathbb{Z}_\ell$-algebra isomorphism $\Psi_{k,\gamma} : \Lambda_k \to \mathbb{Z}_\ell[[T]]$ by the rule $\gamma \mapsto 1 + T$.

Thus, one can study finitely generated torsion Λ_k-modules by means of the classification theorem of the previous paragraph. Using Selmer groups of elliptic curves, one can construct certain finitely generated modules $X(E/k_\infty)$ that are believed to be Λ_k-torsion.

2.3. **Selmer groups.** Let k be a number field and let E be an elliptic curve over k. For any algebraic extension L/k (not necessarily finite) the ℓ-primary part of the Selmer group of E over L is denoted by $\mathrm{Sel}_{\ell^\infty}(E/L)$. It fits in the exact sequence

$$0 \to E(L) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell/\mathbb{Z}_\ell \to \mathrm{Sel}_{\ell^\infty}(E/L) \to Ш(E/L)[\ell^\infty] \to 0 \tag{2.1}$$

where $Ш(E/L)$ is the Shafarevich-Tate group.

It is known that $\mathrm{Sel}_{\ell^\infty}(E/k) \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\rho_\ell(E/k)} \oplus G$ for certain integer $\rho_\ell(E/k) \geq 0$, where G is a finite group. The number $\rho_\ell(E/k)$ is the co-rank of $\mathrm{Sel}_{\ell^\infty}(E/k)$ and the previous exact sequence gives $\operatorname{rank} E(k) \leq \rho_\ell(E/k)$. Of course, if $Ш(E/k)[\ell^\infty]$ is finite (as conjectured) then $\operatorname{rank} E(k) = \rho_\ell(E/k)$.

A foundational result of Mazur allows one to recover valuable arithmetic information about E over all the number fields k_m from the Γ_k-action on $\mathrm{Sel}_{\ell^\infty}(E/k_\infty)$.

Theorem 2.1 (Mazur's control theorem)**.** *Let E be an elliptic curve over k having good ordinary reduction at each prime of k above ℓ. The natural maps*

$$\mathrm{Sel}_{\ell^\infty}(E/k_m) \to \mathrm{Sel}_{\ell^\infty}(E/k_\infty)^{\mathrm{Gal}(k_\infty/k_m)}$$

have finite kernels and cokernels, whose orders are bounded as m varies.

2.4. **Iwasawa modules attached to elliptic curves.** The group $\mathrm{Sel}_{\ell^\infty}(E/k_\infty)$ has a natural Λ_k-module structure and it is topologically discrete. Giving $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ the trivial Γ_k-action, we have an induced Λ_k-module structure on

$$X(E/k_\infty) := \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Sel}_{\ell^\infty}(E/k_\infty), \mathbb{Q}_\ell/\mathbb{Z}_\ell).$$

By Pontryagin duality, $X(E/k_\infty)$ is compact. It is a standard result that $X(E/k_\infty)$ is finitely generated as a Λ_k-module.

Conjecture 2.2 (Mazur)**.** *If E has good ordinary reduction at each prime of k above ℓ, then $X(E/k_\infty)$ is a torsion Λ_k-module.*

The general case of this conjecture remains open. For us it suffices to know the following result, which is a consequence of Mazur's control theorem.

Theorem 2.3 (Mazur)**.** *If E has good ordinary reduction at each prime of k above ℓ, and if $\mathrm{Sel}_{\ell^\infty}(E/k)$ is finite, then $X(E/k_\infty)$ is a torsion Λ_k-module.*

2.5. **Iwasawa invariants.** Suppose that $X(E/k_\infty)$ is a torsion Λ_k-module and fix a topological generator $\gamma \in \Gamma_k$. Then we can regard $X(E/k_\infty)$ as a finitely generated torsion $\mathbb{Z}_\ell[[T]]$-module via $\Psi_{k,\gamma}$ (cf. Paragraph 2.2), and we have the associated invariants $\mu_{E/k} := \mu_{X(E/k_\infty)}$, $\lambda_{E/k} := \lambda_{X(E/k_\infty)}$, and $f_{E/k} := f_{X(E/k_\infty)}$. The μ and λ invariants are well-defined integers that only depend on ℓ and E/k. However, the characteristic polynomial $f_{E/k} \in \mathbb{Z}_\ell[T]$ also depends on the choice of topological generator $\gamma \in \Gamma_k$.

Directly from the definitions one has

Lemma 2.4. *Suppose that $X(E/k_\infty)$ is a torsion Λ_k-module. Then:*

- *$\mu_{E/k} = 0$ if and only if $X(E/k_\infty)$ is finitely generated as a $\mathbb{Z}_\ell$-module,*
- *$\mu_{E/k} = \lambda_{E/k} = 0$ if and only if $X(E/k_\infty)$ is a finite group.*

It is quite common that the μ-invariant vanishes, but this is not always the case. On the other hand, we will be mostly interested on the λ-invariant due to the following important consequence of Mazur's control theorem (cf. Theorem 1.9 in [Gr01]).

Theorem 2.5. *Suppose that E has good ordinary reduction at each prime of k above ℓ and that $X(E/k_\infty)$ is a torsion Λ_k-module. Then for each $m \geq 0$ we have*

$$\operatorname{rank} E(k_m) \leq \rho_\ell(E/k_m) \leq \lambda_{E/k}.$$

2.6. **The value of $f_{E/k}(0)$.** We now discuss the characteristic polynomial $f_{E/k}$ assuming, of course, that $X(E/k_\infty)$ is Λ_k-torsion and that a topological generator $\gamma \in \Gamma_k$ is chosen.

Proposition 2.6. *Suppose that E has good ordinary reduction at each prime of k above ℓ and that $X(E/k_\infty)$ is a torsion Λ_k-module. We have that $\mathrm{Sel}_{\ell^\infty}(E/k)$ is finite if and only if $f_{E/k}(0) \neq 0$.*

Proof. By Mazur's control theorem, $\mathrm{Sel}_{\ell^\infty}(E/k)$ is finite if and only if $\mathrm{Sel}_{\ell^\infty}(E/k_\infty)^{\Gamma_k}$ is finite. Choosing a topological generator $\gamma \in \Gamma_k$ and recalling that $\Psi_{k,\gamma}(\gamma) = 1 + T$, we see that the latter is equivalent to the finiteness of $X(E/k_\infty)/T \cdot X(E/k_\infty)$ by duality between $\mathrm{Sel}_{\ell^\infty}(E/k_\infty)$ and $X(E/k_\infty)$. Finally, we note that $X(E/k_\infty)/T \cdot X(E/k_\infty)$ is finite if and only if $T \nmid f_{E/k}$ (cf. Paragraph 2.1). □

It is of great interest to evaluate $f_{E/k}(0) \in \mathbb{Z}_\ell$ when it is non-zero. The precise value depends on the choice of topological generator $\gamma \in \Gamma_k$, but nevertheless the ℓ-adic valuation of $f_{E/k}(0)$ turns out to depend only on ℓ, the number field k, and the elliptic curve E/k. Before giving the formula, we need some notation.

Given a non-archimedean place v of k, we write $\mathbb{F}_v$ for the residue field and k_v for the completion of k at v. If E is an elliptic curve over k, the reduction of E at v is denoted by $\tilde{E}_v$ and its non-singular locus is $\tilde{E}_v^{ns}$. We write $E(k_v)_0$ for the subgroup of $E(k_v)$ consisting of local points whose reduction at v is in $\tilde{E}_v^{ns}$. The Tamagawa factor at v is defined by $c_v(E/k) = [E(k_v) : E(k_v)_0]$, and the the product $\prod_v c_v(E/k)$ over all non-archimedean places v of k is denoted by $\mathrm{Tam}(E/k)$. Let us write $a \sim_\ell b$ if $a, b \in \mathbb{Q}_\ell$ have the same ℓ-adic valuation.

Note that the finiteness assumption on $\mathrm{Sel}_{\ell^\infty}(E/k)$ not only implies $f_{E/k}(0) \neq 0$ (cf. Theorem 2.3 and Proposition 2.6), but also, it implies that both $Ш(E/k)[\ell^\infty]$ and $E(k)$ are finite (cf. the exact sequence (2.1)). So the formula in the next result only involves non-zero finite numbers. See also [Pe84] and [Sc83].

Theorem 2.7 (cf. Theorem 4.1 in [Gr01])**.** *Suppose that E has good ordinary reduction at each prime of k above ℓ and that $\mathrm{Sel}_{\ell^\infty}(E/k)$ is finite. Then $f_{E/k}(0) \in \mathbb{Z}_\ell$ is non-zero and it satisfies*

$$f_{E/k}(0) \sim_\ell \frac{\mathrm{Tam}(E/k) \cdot \#Ш(E/k)[\ell^\infty]}{\#E(k)^2} \cdot \prod_{v|\ell} \#\tilde{E}_v(\mathbb{F}_v)^2.$$

The proof of Theorem 2.7 relies on the theory of the cyclotomic Euler characteristic, which we don't review here.

3. A general construction of integrally Diophantine extensions

3.1. **Integrally Diophantine extensions.** Given a commutative unitary ring A and a positive integer n, let us recall that a subset $S \subseteq A^n$ is *Diophantine* over A if for some $m \geq 0$ there are polynomials $F_1, \dots, F_k \in A[x_1, ..., x_n, y_1, ..., y_m]$ such that

$$S = \{\mathbf{a} \in A^n : \exists \mathbf{b} \in A^m \text{ such that for each } 1 \leq j \leq k \text{ we have } F_j(\mathbf{a}, \mathbf{b}) = 0\}.$$

An extension of number fields K/F is *integrally Diophantine* if O_F is Diophantine in O_K. It is a standard fact that if $K/F/L$ is a tower of number fields and both F/L and K/F are integrally Diophantine, then so is K/L. In particular,

Lemma 3.1. *Let K/F be an extension of number fields. If K/F is integrally Diophantine and $\mathbb{Z}$ is Diophantine in O_F, then $\mathbb{Z}$ is Diophantine in O_K.*

As discussed in the introduction, there are elliptic curve criteria developed by Poonen, Cornelissen-Pheidas-Zahidi, and Shlapentokh to prove that a given extension of number fields is integrally Diophantine. For our purposes, let us recall here Shlapentokh's criterion.

Theorem 3.2 (Shlapentokh [Sh08]). *Let K/F be an extension of number fields. Suppose that there is an elliptic curve E defined over F such that $\operatorname{rank} E(K) = \operatorname{rank} E(F) > 0$. Then K/F is integrally Diophantine.*

This result can be applied on a case-by-case basis to concrete examples of number fields, but it is not known at present how to systematically apply it in general —at least, not without assuming some conjecture on elliptic curves (cf. [MR10] and [MP18]). For instance, the number field $\mathbb{Q}(\sqrt[5]{2})$ is not covered by the results (i)-(v) quoted in the introduction. However, the elliptic curve E of affine equation $y^2 + xy = x^3 - x^2 - x + 1$ (Cremona label $58a1$) satisfies

$$\operatorname{rank} E(\mathbb{Q}(\sqrt[5]{2})) = \operatorname{rank} E(\mathbb{Q}) = 1,$$

as it can be readily checked on Sage. By Shlapentokh's theorem we get that $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ is integrally Diophantine (in fact, already the results of Poonen [Po02] or Cornelissen-Pheidas-Zahidi [CPZ05] suffice here). That is, Conjecture 1.1 holds for $K = \mathbb{Q}(\sqrt[5]{2})$.

3.2. **A general construction.** The general case of Conjecture 1.1 —and in fact, of Hilbert's tenth problem for rings of integers of number fields— remains open, as discussed in the introduction. It is therefore of great importance to develop tools that permit to construct integrally Diophantine extensions. The next result, despite its simple proof, gives a general way to construct such extensions and to prove new cases of Conjecture 1.1.

Proposition 3.3. *Let F/M and L/M be extensions of number fields with L/M quadratic. Let $K = F.L$ be the compositum of F and L over M. Suppose that there is an elliptic curve E over M satisfying the conditions:*

(i) $\operatorname{rank} E(F) = 0$

(ii) $\operatorname{rank} E(L) > 0$.

Then K/F is integrally Diophantine.

Proof. Let E^L be the elliptic curve over M defined as the quadratic twist of E by L. By (i) and (ii) we see that L is not contained in F, so the extension K/F is quadratic and

$$\operatorname{rank} E^L(K) = \operatorname{rank} E(F) + \operatorname{rank} E^L(F) = \operatorname{rank} E^L(F).$$

Since $\operatorname{rank} E^L(K) = \operatorname{rank} E(K) \geq \operatorname{rank} E(L) > 0$ we can apply Theorem 3.2 to the extension K/F with the elliptic curve E^L over F. □

As an example of how this construction readily leads to new cases of Conjecture 1.1, let us point out the following simple consequence.

Proposition 3.4. *Let p be a prime of the form $p \equiv 3 \bmod 4$. Then $\mathbb{Z}$ is Diophantine in the ring of integers of $\mathbb{Q}(\sqrt[5]{2}, \sqrt{p})$.*

Proof. We apply Proposition 3.3 with $M = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt[5]{2})$, and $L = \mathbb{Q}(\sqrt{p})$ for $p \equiv 3 \bmod 4$ a prime number. Consider the elliptic curve E over $\mathbb{Q}$ with affine equation $y^2 = x^3 - 4x$; this is the twist by 2 of the celebrated Congruent Number elliptic curve $y^2 = x^3 - x$. By classical results due to Heegner [He52] and Birch [Bi69] (see also [Mo90]) we have that $2p$ is a congruent number when $p \equiv 3 \bmod 4$. Hence $\operatorname{rank} E(\mathbb{Q}(\sqrt{p})) > 0$ for these primes p. On the other hand, a direct computation on Sage shows that $\operatorname{rank} E(\mathbb{Q}(\sqrt[5]{2})) = 0$. Therefore $K = \mathbb{Q}(\sqrt[5]{2}, \sqrt{p})$ is integrally Diophantine over $F = \mathbb{Q}(\sqrt[5]{2})$. In Paragraph 3.1 we already checked that $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ is integrally Diophantine, hence $K/\mathbb{Q}$ also is (cf. Lemma 3.1). □

In Proposition 3.4, all the number fields that we obtain are quadratic extensions of a single number field —namely, of $\mathbb{Q}(\sqrt[5]{2})$— and of course one can obtain many other results of this sort thanks to Proposition 3.3. Theorem 1.2 instead is much more delicate and the proof lies deeper, as it concerns number fields of the form $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$ where the two parameters p and q can be chosen independently of each other.

3.3. **Comparison with other available results.** The following elementary lemma will help us to check that the families of number fields K for which we prove that $\mathbb{Z}$ is Diophantine in O_K are indeed new.

Lemma 3.5. *Let $\ell > 2$ be a prime and let $F/\mathbb{Q}$ be a degree ℓ extension which is not totally real. Then F is not contained in a quadratic extension of a totally real number field.*

Proof. Suppose that H/N is a quadratic extension with N a totally real number field, such that $F \subseteq H$. Observe that N and F are linearly disjoint over $\mathbb{Q}$, for otherwise an element $\gamma \in F - \mathbb{Q}$ would be conjugate to an element of N, but $F = \mathbb{Q}(\gamma)$ is not totally real. It follows that the compositum $F.N$ has degree ℓ over N, but this is not possible since $F.N \subseteq H$ and $[H : N] = 2$. □

For instance, let us verify that the number fields in Proposition 3.4 are not included in number fields covered by the results in items (i), (ii), (iii) from the introduction: For a prime p, the number field $\mathbb{Q}(\sqrt[5]{2}, \sqrt{p})$ has degree 10 over $\mathbb{Q}$ and it has 4 complex places, hence K is not contained in fields for which (ii) or (iii) apply. By Lemma 3.5, K is not contained in a quadratic extension of a totally real field, so (i) does not apply.

Regarding item (v), we note that the quadratic extensions $\mathbb{Q}(\sqrt[5]{2}, \sqrt{p})/\mathbb{Q}(\sqrt[5]{2})$ are obtained by adjoining the square root of a rational prime, as opposed to using unrestricted primes from $\mathbb{Q}(\sqrt[5]{2})$. So the method of proof in [MR10, MR18] (cf. item (v) above) does not apply either, as the auxiliary primes required by the methods of *loc. cit.* cannot be guaranteed to be chosen in $\mathbb{Q}$.

Finally, we remark that Lemma 3.5 allows us to check in a similar way that the number fields considered in our main result Theorem 1.2 are out of the scope of the available results in the literature. In fact, if p and q are prime numbers, the number field $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$ has degree 6 over $\mathbb{Q}$, it has three complex places, and it contains the non-totally real number field $\mathbb{Q}(\sqrt[3]{p})$.

4. Preserving rank zero: Iwasawa theory

For a positive integer n, the set of complex n-th roots of 1 is denoted by μ_n. The purpose of this section is to prove the following result

Theorem 4.1. *Let $\ell > 2$ be a prime. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and assume the following:*

1. *E has good ordinary reduction at ℓ*
2. *the residual Galois representation $\rho_{E[\ell]} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell])$ is surjective*
3. $\mathrm{rank}\, E(\mathbb{Q}(\mu_\ell)) = 0$
4. $\text{Ш}(E/\mathbb{Q}(\mu_\ell))[\ell] = (0)$
5. $\ell \nmid \mathrm{Tam}(E/\mathbb{Q}(\mu_\ell)) \cdot \#\tilde{E}_\ell(\mathbb{F}_\ell)$.

Consider the set of prime numbers

$$\mathscr{P}(E,\ell) = \{p : p \nmid N,\ p \equiv 1 \bmod \ell,\ \textit{and}\ a_p(E) \not\equiv 2 \bmod \ell\}.$$

Then $\mathscr{P}(E,\ell)$ is a Chebotarev set of primes of density

$$\delta(\mathscr{P}(E,\ell)) = \frac{\ell^2 - \ell - 1}{(\ell-1)(\ell^2-1)} > 0$$

and for every ℓ-power free integer $a > 1$ supported on $\mathscr{P}(E,\ell)$ we have that $\mathrm{Sel}_{\ell^\infty}(E/\mathbb{Q}(\mu_\ell, \sqrt[\ell]{a}))$ is finite. In particular, for these integers a we have $\mathrm{rank}\, E(\mathbb{Q}(\sqrt[\ell]{a})) = \mathrm{rank}\, E(\mathbb{Q}(\mu_\ell, \sqrt[\ell]{a})) = 0$.

For our applications on Hilbert's tenth problem we (crucially) need the case $\ell = 3$. Nevertheless, this more general theorem can be of independent interest. We also remark that the various hypotheses in the statement are amenable for computations; a concrete example is presented in Section 6. Condition (2) is convenient for showing that $\mathscr{P}(E,\ell)$ has positive density, but it can certainly be relaxed —however, it is enough for our purposes.

We remark that a related result is sketched as Theorem 18 in [Do05] for primes $\ell \geq 5$ without verifying the existence of infinitely many integers a. For $\ell = 3$, the special case of $E = X_1(11)$ is worked out in [Do07] where the existence of infinitely many integers a is shown by explicit computations with an equation for the modular curve $X_1(11)$.

Chao Li has pointed out to us another possible approach to achieve rank 0 over cubic extensions, at least for a particular kind of elliptic curves. Namely, given a Mordell elliptic curve $E : y^2 = x^3 + k$ (i.e. an elliptic curve of j-invariant 0) defined over $\mathbb{Q}$ with $\mathrm{rank}\, E(\mathbb{Q}) = 0$, we have $\mathrm{rank}\, E(\mathbb{Q}(\sqrt[3]{p})) = 0$ if $\mathrm{rank}\, E^{[p]}(\mathbb{Q}) = 0$ and $\mathrm{rank}\, E^{[p^2]}(\mathbb{Q}) = 0$, where $E^{[d]} : y^2 = x^3 + d^2 k$ is the cubic twist by d. The theory of [KL19] allows one to achieve $\mathrm{rank}\, E^{[p]}(\mathbb{Q}) = 0$ for many primes p under suitable conditions. For our applications it would be of great interest to extend this theory in order to control the two relevant cubic twists simultaneously. We point out that both cubic twists $E^{[p]}$ and $E^{[p^2]}$ are needed; for instance, for $E : y^2 = x^3 + 1$ and $p = 5$ we have $\mathrm{rank}\, E(\mathbb{Q}) = 0$, $\mathrm{rank}\, E^{[5]}(\mathbb{Q}) = 0$ but $\mathrm{rank}\, E(\mathbb{Q}(\sqrt[3]{5})) = 1$.

4.1. Variation of the λ-invariant.

In view of Theorem 2.5, we will be interested in the variation of the λ-invariant of an elliptic curve under base change. An important result by Hachimori and Matsuno [HM99] gives a precise formula under suitable assumptions. Here we state a special case. As usual, for a number field k the set of places of k is denoted by M_k.

Theorem 4.2 (Hachimori-Matsuno). *Let $\ell > 2$ be a prime and let k be a number field. Let E be an elliptic curve over k with good ordinary reduction at all primes of k above ℓ. Suppose that $X(E/k_\infty)$ is a torsion Λ_k-module and that $\mu_{E/k} = 0$.*

Let k'/k be an ℓ-power Galois extension of number fields such that E does not have additive reduction at the primes that ramify in k'/k. Then $\mu_{E/k'} = 0$ and $X(E/k'_\infty)$ is a torsion $\Lambda_{k'}$-module. Furthermore,

$$\lambda_{E/k'} = [k'_\infty : k_\infty]\lambda_{E/k} + \sum_{w \in P_1} (e_{k'_\infty/k_\infty}(w) - 1) + 2 \sum_{w \in P_2} (e_{k'_\infty/k_\infty}(w) - 1)$$

where

$$P_1 = \{w \in M_{k'} : w \nmid \ell \text{ and } E \text{ has split multiplicative reduction at } w\}$$

$$P_2 = \{w \in M_{k'} : w \nmid \ell,\ E \text{ has good reduction at } w, \text{ and } E(k'_{\infty,w})[\ell^\infty] \neq (0)\}$$

and $e_{k'_\infty/k_\infty}(w)$ denotes the corresponding ramification index.

The following lemma allows one to give a simple alternative description of the set of places P_2 of the previous theorem.

Lemma 4.3 (Dokchitser-Dokchitser, cf. Lemma 3.19 (3) [DD07])**.** *Let $\ell > 2$ be a prime and let k'/k be an ℓ-power Galois extension of number fields. Let E be an elliptic curve over k with good reduction at a prime $v \nmid \ell$ of k and let $w|v$ be a prime of k'. Then, $E(k'_{\infty,w})[\ell^\infty] = (0)$ if and only if $\tilde{E}_v(\mathbb{F}_v)[\ell] = (0)$.*

Theorem 4.2 leads to a simple criterion to ensure that, under favorable conditions, the finiteness of the Iwasawa module $X(E/k_\infty)$ is preserved in prime-power degree field extensions (see also Corollary 3.20 in [DD07]).

Proposition 4.4 (Preserving finiteness of $X(E/k_\infty)$)**.** *Let $\ell > 2$ be a prime and let k be a number field. Let E be an elliptic curve over k with good ordinary reduction at all primes of k above ℓ. Suppose that $X(E/k_\infty)$ is finite.*

Let k'/k be a ℓ-power Galois extension of number fields satisfying the following conditions:

(i) *E has good reduction at each prime v of k that ramifies in k'/k, and*

(ii) *for each prime $v \nmid \ell$ of k that ramifies in k'/k, we have $\tilde{E}_v(\mathbb{F}_v)[\ell] = (0)$.*

Then $X(E/k'_\infty)$ is finite and $\operatorname{rank} E(k') = 0$.

Proof. Since $X(E/k_\infty)$ is finite, it is a torsion Λ_k-module and $\mu_{E/k} = \lambda_{E/k} = 0$ (cf. Lemma 2.4). By (i), we can apply Theorem 4.2 and we obtain that $X(E/k'_\infty)$ is $\Lambda_{k'}$-torsion and $\mu_{E/k'} = 0$. Furthermore, $e_{k'_\infty/k_\infty}(w) = 1$ for each $w \in P_1$ by our assumption (i), and $e_{k'_\infty/k_\infty}(w) = 1$ for each $w \in P_2$ by (ii) and Lemma 4.3. Therefore $\lambda_{E/k'} = [k'_\infty : k_\infty]\lambda_{E/k} = 0$.

Since $X(E/k'_\infty)$ is $\Lambda_{k'}$-torsion and $\mu_{E/k'} = \lambda_{E/k'} = 0$, we obtain that $X(E/k'_\infty)$ is finite (cf. Lemma 2.4). In particular, since $\lambda_{E/k'} = 0$ we get $\operatorname{rank} E(k') = 0$ (cf. Theorem 2.5). □

In view of Proposition 4.4, we need a test for finiteness of $X(E/k_\infty)$.

4.2. **Testing finiteness of $X(E/k_\infty)$.** The following test for finiteness of $X(E/k_\infty)$ follows from the theory of the cyclotomic Euler characteristic and it is well-known to experts.

Proposition 4.5 (A test for finiteness of X)**.** *Let ℓ be a prime and let k be a number field. Let E be an elliptic curve over k with good ordinary reduction at all primes of k above ℓ. Assume that $E(k)$ is finite and that that $Ш(E/k)[\ell^\infty]$ is also finite —the latter happens, for instance, if $Ш(E/k)[\ell] = (0)$. Then $X(E/k_\infty)$ is Λ_k-torsion. Furthermore, consider the quantity*

$$\varpi(E/k) := \frac{\operatorname{Tam}(E/k) \cdot \#Ш(E/k)[\ell^\infty]}{\#E(k)^2} \cdot \prod_{v|\ell} \#\tilde{E}_v(\mathbb{F}_v)^2.$$

Then $\varpi(E/k) \in \mathbb{Z}_\ell$, and if $\varpi(E/k)$ is an ℓ-adic unit, then $X(E/k_\infty)$ is finite.

Proof. Since $E(k)$ and $Ш(E/k)[\ell^\infty]$ are finite, the exact sequence (2.1)

$$0 \to E(k) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell/\mathbb{Z}_\ell \to \mathrm{Sel}_{\ell^\infty}(E/k) \to Ш(E/k)[\ell^\infty] \to 0$$

gives that $\mathrm{Sel}_{\ell^\infty}(E/k)$ is also finite —in fact, we get $\mathrm{Sel}_{\ell^\infty}(E/k) \simeq Ш(E/k)[\ell^\infty]$. In particular, Theorem 2.3 gives that $X(E/k_\infty)$ is Λ_k-torsion.

Thus, we can consider the characteristic polynomial $f_{E/k} \in \mathbb{Z}_\ell[T]$ (for a fixed choice of topological generator $\gamma \in \Gamma_k$). By Proposition 2.6 and the fact that $\mathrm{Sel}_{\ell^\infty}(E/k)$ is finite, we get that $f_{E/k}(0)$ is a non-zero ℓ-adic integer. Theorem 2.7 gives $\varpi(E/k) \sim_\ell f_{E/k}(0)$, so $\varpi(E/k) \in \mathbb{Z}_\ell$.

Suppose that $\varpi(E/k)$ is an ℓ-adic unit. Let us recall that $f_{E/k} = \ell^{\mu_{E/k}} \prod_j f_j^{m_j}$ for certain monic irreducible polynomials f_j having all their non-leading coefficients in $\ell\mathbb{Z}_\ell$. Since $f_{E/k}(0) \sim_\ell \varpi(E/k)$ is an ℓ-adic unit, we deduce that in fact $\mu_{E/k} = 0$ and that the product $\prod_j f_j^{m_j}$ equals 1 because it is empty —for otherwise, the constant term of each f_j would be divisible by ℓ. Hence $\lambda_{E/k} = 0$. Since $\mu_{E/k} = \lambda_{E/k} = 0$, we get that $X(E/k_\infty)$ is finite (cf. Lemma 2.4). □

4.3. **Chebotarev sets of primes.** A set of prime numbers $\mathscr{S}$ is called a *Chebotarev set* if there is a Galois extension $K/\mathbb{Q}$ and a conjugacy-stable set $C \subseteq \mathrm{Gal}(K/\mathbb{Q})$ such that S agrees with the set $\{p : \mathrm{Frob}_p \in C\}$ up to a finite set. Finite unions, finite intersections, and complements of Chebotarev sets are again Chebotarev. Let us recall that the Chebotarev density theorem states that if $\mathscr{S}$ arises from K and C as above, then the limit

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

exists and equals $\#C/[K : \mathbb{Q}]$, where $\pi(x)$ is the number of prime numbers $p \leq x$. The quantity $\delta(\mathscr{S})$ is called the *density* of $\mathscr{S}$.

4.4. **Auxiliary primes.** The next result ensures that we have enough primes for the constructions required in the proof of Theorem 4.1. As usual, if E is an elliptic curve over $\mathbb{Q}$ and p is a prime of good reduction, we write $a_p(E) = p + 1 - \#\tilde{E}_p(\mathbb{F}_p)$.

Proposition 4.6. *Let ℓ be a prime number. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. Suppose that the residual Galois representation $\rho_{E[\ell]}$ is surjective. Consider the set of prime numbers*

$$\mathscr{P}(E,\ell) = \{p : p \nmid N,\ p \equiv 1 \bmod \ell, \text{ and } a_p(E) \not\equiv 2 \bmod \ell\}.$$

Then $\mathscr{P}(E,\ell)$ is a Chebotarev set of primes with density

$$\delta(\mathscr{P}(E,\ell)) = \frac{\ell^2 - \ell - 1}{(\ell-1)(\ell^2-1)} > 0.$$

Furthermore, for each $p \in \mathscr{P}(E,\ell)$ and each place $v|p$ of $\mathbb{Q}(\mu_\ell)$ we have that $\tilde{E}_v(\mathbb{F}_v)[\ell] = (0)$.

Proof. The Weil pairing shows that the ℓ-division field $K = \mathbb{Q}(E[\ell])$ contains $\mathbb{Q}(\mu_\ell)$. The cyclotomic character $\chi : \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \to \mathbb{F}_\ell^\times$ extends to $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{F}_\ell^\times$ by means of the quotient $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$. We recall that the residual Galois representation $\rho_{E[\ell]} : \mathrm{Gal}(K/\mathbb{Q}) \to GL_2(\mathbb{F}_\ell)$ is injective and for all $p \nmid \ell N$ it satisfies

- $\det(\rho_{E[\ell]}(\mathrm{Frob}_p)) = \chi(\mathrm{Frob}_p) = p \bmod \ell$, and
- $\mathrm{tr}(\rho_{E[\ell]}(\mathrm{Frob}_p)) = a_p(E) \bmod \ell$.

The map $\rho_{E[\ell]} : \mathrm{Gal}(K/\mathbb{Q}) \to GL_2(\mathbb{F}_\ell)$ is in fact an isomorphism by our surjectivity assumption. Let $C = \{\gamma \in GL_2(\mathbb{F}_\ell) : \det(\gamma) = 1 \text{ and } \mathrm{tr}(\gamma) \neq 2\} \subseteq GL_2(\mathbb{F}_\ell)$. The set C is conjugacy-stable and it is non-empty (e.g. $-I \in C$ when $\ell > 2$). In fact, it is an elementary exercise to check that $\#\{\gamma \in SL_2(\mathbb{F}_\ell) : \mathrm{tr}(\gamma) = 2\} = \ell^2$, which gives

$$\#C = \#SL_2(\mathbb{F}_\ell) - \#\{\gamma \in SL_2(\mathbb{F}_\ell) : \mathrm{tr}(\gamma) = 2\} = \ell(\ell^2-1) - \ell^2 = \ell(\ell^2 - \ell - 1).$$

Since we can write

$$\mathscr{P}(E,\ell) = \{p : p \nmid N \text{ and } \rho_{E[\ell]}(\mathrm{Frob}_p) \in C\}$$

we see that $\mathscr{P}(E,\ell)$ is a Chebotarev set of density

$$\delta(\mathscr{P}(E,\ell)) = \frac{\#C}{\#GL_2(\mathbb{F}_\ell)} = \frac{\ell(\ell^2-\ell-1)}{(\ell^2-1)(\ell^2-\ell)} = \frac{\ell^2-\ell-1}{(\ell-1)(\ell^2-1)} > 0.$$

Finally, let $p \in \mathscr{P}(E,\ell)$. Since $p \equiv 1 \bmod \ell$ we have that p splits completely in $\mathbb{Q}(\mu_\ell)$, hence, for each place $v|p$ of $\mathbb{Q}(\mu_\ell)$ we have that the residue field of $\mathbb{Q}(\mu_\ell)$ at v is $\mathbb{F}_v = \mathbb{F}_p$. Therefore $\tilde{E}_v(\mathbb{F}_v) \simeq \tilde{E}_p(\mathbb{F}_p)$ because E has good reduction at $p \nmid N$, and we get

$$\#\tilde{E}_v(\mathbb{F}_v) = p + 1 - a_p(E) \equiv 1 + 1 - a_p(E) \not\equiv 0 \bmod \ell$$

because $p \in \mathscr{P}(E,\ell)$. Thus, the ℓ-torsion of $\tilde{E}_v(\mathbb{F}_v)$ is trivial. □

4.5. **Rank zero over extensions.** Let us keep the notation of assumptions of Theorem 4.1.

Proof of Theorem 4.1. The fact that $\mathscr{P}(E,\ell)$ is a Chebotarev set of primes of the asserted density follows from Proposition 4.6 and our Condition (2).

Let $k = \mathbb{Q}(\mu_\ell)$. By Condition (1), E has good ordinary reduction at each place $v|\ell$ of k. Furthermore, ℓ ramifies completely in $k/\mathbb{Q}$, thus, there is only one place $v|\ell$ and the residue field satisfies $\mathbb{F}_v = \mathbb{F}_\ell$, which in particular gives $\tilde{E}_v(\mathbb{F}_v) \simeq \tilde{E}_\ell(\mathbb{F}_\ell)$ because E has good reduction at ℓ.

By Condition (4) we get $Ш(E/k)[\ell^\infty] = (0)$, which together with Condition (5) gives that the integer

$$\mathrm{Tam}(E/k) \cdot \#Ш(E/k)[\ell^\infty] \cdot \prod_{v|\ell} \#\tilde{E}_v(\mathbb{F}_v)^2$$

is not divisible by ℓ. By Conditions (1), (3), and (4) we can apply Proposition 4.5 and we deduce that $X(E/k_\infty)$ is a finite group because the ℓ-adic integer $\varpi(E/k)$ is not divisible by ℓ.

Let $a > 1$ be an ℓ-power free integer supported on $\mathscr{P}(E,\ell)$ and let $k' = \mathbb{Q}(\mu_\ell, \sqrt[\ell]{a}) = k(\sqrt[\ell]{a})$. The extension k'/k is Galois of degree ℓ. Note that $\ell > 2$, E has good ordinary reduction at each prime of k above ℓ (by Condition (1)), and $X(E/k_\infty)$ is finite, so that we can apply Proposition 4.4. For this, note that if a prime $v \in M_k$ ramifies in k'/k then it divides a, hence, v divides a prime $p \in \mathscr{P}(E,\ell)$ and we deduce that (cf. Proposition 4.6):

- E has good reduction at v (as $p \nmid N$ by definition of $\mathscr{P}(E,\ell)$), and
- $\tilde{E}_v(\mathbb{F}_v)[\ell] = (0)$.

Therefore, Proposition 4.4 gives that $X(E/k'_\infty)$ is finite. In particular $\lambda_{E/k'} = 0$ (cf. Lemma 2.4), $\mathrm{Sel}_{\ell^\infty}(E/k')$ is finite, and $\operatorname{rank} E(k') = 0$ (cf. Theorem 2.5). □

5. Achieving positive rank: Heegner points

In this section we present a theorem by Kriz and Li [KL19] regarding congruences of Heegner points on quadratic twists of elliptic curves, along with some additional facts tailored for our intended applications. The results of Kriz and Li are particularly convenient for producing many explicit quadratic twists with positive rank for a given elliptic curve over $\mathbb{Q}$. We also work-out a concrete example that will be needed later.

5.1. **Heegner points.** Let N be a positive integer. Attached to N there is the modular curve $X_0(N)$ over $\mathbb{Q}$ whose non-cuspidal points classify cyclic degree N isogenies of elliptic curves. The cusp $i\infty \in X_0(N)(\mathbb{Q})$ determines an embedding of the modular curve into its Jacobian $j_N : X_0(N) \to J_0(N)$ defined over $\mathbb{Q}$.

A quadratic imaginary field K is said to satisfy the *Heegner hypothesis* for N if each prime $p|N$ splits in K. If K satisfies the Heegner condition for N we can choose a factorization $(N) = \mathfrak{n}\mathfrak{n}'$ in O_K with $\mathfrak{n}'$ the complex conjugate of the ideal $\mathfrak{n}$, and one has $O_K/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$. The map

$$\mathbb{C}/O_K \to \mathbb{C}/\mathfrak{n}^{-1}$$

is a cyclic degree N isogeny of complex elliptic curves, and it defines a non-cuspidal point $Q_{N,K,\mathfrak{n}} \in X_0(N)(H)$ where H is the Hilbert class field of K. Mapping to $J_0(N)$ and taking trace for the extension H/K, we obtain the K-rational point

$$P_{N,K,\mathfrak{n}} = \sum_{\sigma\in\mathrm{Gal}(H/K)} j_N(Q^{\sigma}_{N,K,\mathfrak{n}}) \in J_0(N)(K).$$

The point $P_{N,K,\mathfrak{n}}$ is the *Heegner point in* $J_0(N)$ *attached to* K. It is independent of the choice of factorization $N = \mathfrak{n}\mathfrak{n}'$ up to sign and adding torsion, and we will denote it by $P_{N,K}$ because this ambiguity is irrelevant for our discussion.

5.2. **Modular parametrizations.** Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. The modularity theorem [BCDT01, TW95, Wi95] gives a non-constant map $\varphi_E : X_0(N) \to E$ defined over $\mathbb{Q}$, with $\varphi_E(i\infty) = 0_E$ where 0_E is the neutral point of E. Such a map φ_E is called modular parametrization. It induces a morphism of abelian varieties $\pi_E : J_0(N) \to E$ defined over $\mathbb{Q}$ satisfying $\varphi_E = \pi_E \circ j_N$. Of course φ_E is not unique; however, if the degree of φ_E is assumed to be minimal (which we don't) then φ_E is determined up to multiplication by -1 in E.

Let $\omega_E \in H^0(E, \Omega^1_{E/\mathbb{Q}})$ be a global Néron differential on E; it is unique up to sign. Let $f(q) = q + a_2q^2 + ... \in S_2(\Gamma_0(N))$ be the unique Fourier-normalized Hecke newform attached to E by the modularity theorem. Then there is a rational number $c(\varphi_E, \omega_E)$ such that

$$\varphi_E^*\omega_E = c(\varphi_E, \omega_E) \cdot f(q)\frac{dq}{q}.$$

The absolute value of $c(\varphi_E, \omega_E)$ only depends on φ_E and it will be denoted by $c(\varphi_E)$. By considerations on the formal completion of the standard integral model of $X_0(N)$ at $i\infty$, it is easily seen that $c(\varphi_E)$ is an integer. In concrete examples, the Manin constant of φ_E can be computed.

A modular parametrization $\varphi_E : X_0(N) \to E$ is *optimal* if the kernel of the induced map $\pi_E : J_0(N) \to E$ is connected. If an optimal modular parametrization exists for E we say that E is optimal (sometimes referred to as strong Weil curve). Every E is isogenous over $\mathbb{Q}$ to an optimal elliptic curve. It is a conjecture of Manin that if $\varphi_E : X_0(N) \to E$ is optimal, then $c(\varphi_E) = 1$. Manin's conjecture is proved in a number of cases, e.g. when the conductor N is odd and squarefree (this is Corollary 4.2 in [Ma78] together with Théorème A in [AU96]). See [ARS06] and the references therein for more details on Manin's conjecture.

5.3. **Logarithms.** Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime. By integration, every differential $\omega \in H^0(E, \Omega^1_{E/\mathbb{Q}})$ uniquely determines a logarithm map

$$\log_{p,\omega} : E(\mathbb{Q}_p) \to \mathbb{Q}_p$$

which satisfies the following:

- For all $a, b \in E(\mathbb{Q}_p)$, $\log_{p,\omega}(a + b) = \log_{p,\omega}(a) + \log_{p,\omega}(b)$.
- If $\omega \neq 0$ then the kernel of $\log_{p,\omega}$ is $E(\mathbb{Q}_p)_{tor}$.

Concretely, the construction is as follows: Choose a global minimal Weierstrass equation over $\mathbb{Z}$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.1}$$

and let $t = -x/y$. Then t is a local parameter at the neutral element $0_E \in E(\mathbb{Q})$ and, moreover, a local point $a \in E(\mathbb{Q}_p)$ is congruent to 0_E modulo p if and only if $t(a) \in p\mathbb{Z}_p$. Let us write $\omega = (b_0 + b_1t + b_2t^2 + ...)dt$. Given any $a \in E(\mathbb{Q}_p)$, choose m such that ma is congruent to 0_E modulo p. Then

$$\log_{p,\omega}(a) = \frac{1}{m}\sum_{r=1}^{\infty} \frac{b_{r-1} \cdot t(ma)^r}{r}$$

where the series converges because $t(ma) \in p\mathbb{Z}_p$. The value of $\log_{p,\omega}(a)$ is independent of the choice of m. We note that the series is the formal integral of ω.

We will consider in the following situation: $K/\mathbb{Q}$ is a quadratic field such that p splits in K and $a \in E(K)$ is a point (in fact, we will take $p = 2$). The choice of a prime $\mathfrak{p}|p$ in O_K is equivalent to the choice of an embedding $\sigma : K \to \mathbb{Q}_p$. Such a σ induces an inclusion $\sigma : E(K) \to E(\mathbb{Q}_p)$ and the quantity $\log_{p,\omega} \sigma(a)$ is thus defined.

For explicit computations with logarithms, it will be convenient to recall the following formulas from Section IV.1 in [Si94]. The global Néron differential over $\mathbb{Z}$ for E is (in affine coordinates of the model (5.1)) given by

$$\omega_E = \frac{dx}{2y + a_1x + a_3}$$

where $a_j \in \mathbb{Z}$ are the coefficients in the global minimal Weierstrass equation (5.1). This differential expressed in terms of the local parameter $t = -x/y$ at 0_E is given by

$$\omega_E = (1 + a_1t + (a_1^2 + a_2)t^2 + (a_1^3 + 2a_1a_2 + 2a_3)t^3 + ...)dt \in \mathbb{Z}[[t]]dt \tag{5.2}$$

where the coefficients of the power series are integers that can be computed in terms of the coefficients a_j from (5.1). For our purposes these first few coefficients suffice.

5.4. **Auxiliary primes.** For an elliptic curve $E/\mathbb{Q}$ of conductor N and a quadratic field K, let us define the sets of prime numbers

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

and observe that $\mathscr{Q}(E,K) = \mathscr{Q}_+(E,K) \cup \mathscr{Q}_-(E,K)$.

Lemma 5.1. *The sets $\mathscr{Q}(E,K)$, $\mathscr{Q}_+(E,K)$, and $\mathscr{Q}_-(E,K)$ are Chebotarev sets of primes. If $E[2](\mathbb{Q}) \neq (0)$ then the three sets are empty.*

Suppose that $E[2](\mathbb{Q}) = (0)$ and $K \neq \mathbb{Q}(\sqrt{-1})$.

(i) *If* $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ *then*

$$\delta(\mathscr{Q}(E,K)) = 1/3, \quad \delta(\mathscr{Q}_+(E,K)) = 1/6, \text{ and } \delta(\mathscr{Q}_-(E,K)) = 1/6.$$

(ii) *If* $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3$ *and* $\mathbb{Q}(E[2])$ *does not contain the fields* $\mathbb{Q}(\sqrt{-1})$ *and* K*, then*

$$\delta(\mathscr{Q}(E,K)) = 1/6, \quad \delta(\mathscr{Q}_+(E,K)) = 1/12, \text{ and } \delta(\mathscr{Q}_-(E,K)) = 1/12.$$

(iii) *If* $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3$ *and* $\mathbb{Q}(E[2])$ *contains the field* $\mathbb{Q}(\sqrt{-1})$*, then* $\mathscr{Q}_-(E,K)$ *is empty,* $\mathscr{Q}_+(E,K) = \mathscr{Q}(E,K)$*, and* $\delta(\mathscr{Q}(E,K)) = 1/6$.

Proof. The condition $a_q(E) \equiv 1 \bmod 2$ at a prime $q \nmid N$ is equivalent to the condition

$$\operatorname{tr}(\rho_{E[2]}(\mathrm{Frob}_q)) = 1 \in \mathbb{F}_2$$

for the residual Galois representation $\rho_{E[2]} : \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \to GL_2(\mathbb{F}_2) \simeq S_3$. The only elements of $GL_2(\mathbb{F}_2)$ with trace equal to 1 are

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

i.e. the two 3-cycles in S_3.

The three sets of primes are empty if there is a rational 2-torsion point, since in this case every prime $q \nmid 2N$ satisfies $a_q(E) \equiv \operatorname{tr}(\rho_{E[2]}(\mathrm{Frob}_q)) \equiv 0 \bmod 2$.

In case (i), since $\mathbb{Q}(E[2])$ does not contain quadratic fields, the result follows from the Chebotarev density theorem and the fact that the congruence conditions modulo 4 are splitting conditions for the extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$.

In cases (ii) and (iii) we have $\delta(\mathscr{Q}(E,K)) = 1/6$ by the Chebotarev density theorem. Case (ii) follows by linear disjointness of the relevant fields.

In case (iii) it only remains to show that $\mathscr{Q}_-(E,K)$ is empty. Note that $\mathbb{Q}(E[2])$ does not contain K because a hexic extension of $\mathbb{Q}$ contains a unique quadratic subfield. The only non-trivial morphism $s : GL_2(\mathbb{F}_2) \simeq S_3 \to \mu_2$ is the sign map, and it sends the trace 1 matrices (i.e. 3-cycles of S_3) to $1 \in \mu_2$. By uniqueness of s, the composition $s \circ \rho_{E[2]} : \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \to \mu_2$ is the same as the map induced by the non-trivial quadratic character $\chi : \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) \to \mu_2$ via the restriction map $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$. Since each prime $q \equiv -1 \bmod 4$ has $\chi(\mathrm{Frob}_q) = -1$, we get that $\mathscr{Q}_-(E,K)$ is empty. □

Case (iii) in Lemma 5.1 can in fact happen and we must avoid it for our intended applications (cf. the remarks after Corollary 5.4). For instance, the elliptic curve E of Cremona label $121a1$ has the property that $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3$ and $\mathbb{Q}(\sqrt{-1}) \subseteq \mathbb{Q}(E[2])$. Here is the data for this E and the first 20 primes $q \nmid 2N$

$q \nmid 2 \cdot 121$	3	5	7	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79
q mod 4	-1	1	-1	1	1	-1	-1	1	-1	1	1	-1	-1	1	-1	1	-1	-1	1	-1
$a_q(E)$	2	1	2	-1	5	-6	2	-9	-2	-3	5	0	2	9	8	-6	2	12	2	10

Already for these first few values we see that when $q \equiv -1 \bmod 4$ we get $a_q(E)$ even, while for $q \equiv 1 \bmod 4$ we can have $a_q(E)$ even or odd depending on whether $\rho_{E[2]}(\mathrm{Frob}_q) \in GL_2(\mathbb{F}_2) \simeq S_3$ is the identity or a 3-cycle respectively.

Let us point out that in Lemma 5.1 the condition that K is not contained in $\mathbb{Q}(E[2])$ will not be a problem for us, due to the following observation.

Lemma 5.2. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N satisfying $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3$. There is only one quadratic field contained in $\mathbb{Q}(E[2])$ and it does not satisfy the Heegner hypothesis for $2N$.*

Proof. Since $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$, there is only one quadratic field $F \subseteq \mathbb{Q}(E[2])$. The primes that ramify in F divide $2N$, hence the result. □

5.5. Congruences of Heegner points, after Kriz and Li.

The following is a re-statement of Theorem 4.3 in [KL19], keeping track of some choices that are made along the proof in *loc. cit.*

Theorem 5.3 (Kriz-Li [KL19])**.** *Suppose $E/\mathbb{Q}$ is an elliptic curve with $E(\mathbb{Q})[2] = (0)$. Consider a modular parametrization $\varphi_E : X_0(N) \to E$ and the corresponding quotient $\pi_E : J_0(N) \to E$. Let K be an imaginary quadratic field satisfying the Heegner hypothesis for $2N$ and let $\sigma : K \to \mathbb{Q}_2$ be* *an embedding. Assume that*

$$\frac{\#\tilde{E}_2^{ns}(\mathbb{F}_2)}{2\cdot c(\varphi_E)}\cdot \log_{2,\omega_E}(\sigma(\pi_E(P_{N,K})))\in \mathbb{Z}_2^\times . \tag{5.3}$$

Then for each squarefree integer $d\equiv 1 \bmod 4$ supported on $\mathscr{Q}(E,K)$ the following holds:

(i) *Both E and E^d have rank at most 1 over $\mathbb{Q}$, and the rank part of the Birch and Swinnerton-Dyer conjecture holds for them.*

(ii) $\operatorname{rank} E(\mathbb{Q})\neq \operatorname{rank} E^d(\mathbb{Q})$ *if and only if $\psi_d(-N)=-1$, where ψ_d is the quadratic Dirichlet character attached to the quadratic field $\mathbb{Q}(\sqrt{d})$.*

Let us make some observations regarding condition (5.3).

- $\log_{2,\omega_E}$ depends on the choice of the Néron differential ω_E only up to sign, which is irrelevant for condition (5.3).
- The choice of φ_E affects both $c(\varphi_E)$ and $\pi_E(P_{N,K})$, but the quantity in (5.3) remains the same up to sign.
- $P_{N,K}\in J_0(N)(K)$ also depends on the choice of a factorization $(N)=\mathfrak{n}\mathfrak{n}'$ in O_K, but only up to multiplication by -1 and adding torsion. Hence $\log_{2,\omega_E}(\sigma(\pi_E(P_{N,K})))$ remains the same up to sign.
- The proof in [KL19] also shows that the quantity in (5.3) is a 2-adic integer. So, the condition actually is about indivisibility by 2.

It is worth pointing out that Theorem 5.3 (cf. Theorem 4.3 in [KL19]) is a consequence of a very general congruence formula for Heegner points. In fact, the theory in [KL19] (for $p=2$) actually shows that the quantity in (5.3) is congruent modulo 2 to the analogous quantity for the twisted elliptic curve E^d. Thus, condition (5.3) implies that the analogous indivisibility holds for E^d and, in particular, the corresponding Heegner points in $E(K)$ and $E^d(K)$ are non-torsion (as their logarithms are non-zero). This, together with known results on the Birch and Swinnerton-Dyer conjecture (due to Kolyvagin [Ko90], Gross-Zagier [GZ86], Murty-Murty [MM91], and Bump-Friedberg-Hoffstein [BFH90]) implies item (i) in Theorem 5.3.

Regarding item (ii) of Theorem 5.3, the condition $\psi_d(-N)=-1$ ensures that the global root numbers of E and E^d are different, so that (ii) follows from (i). The next result is Corollary 5.11 in [KL19], which shows that this parity condition takes a particularly simple form when (5.3) holds and the Tamagawa factor $c_2(E/\mathbb{Q})$ is odd.

Corollary 5.4. *Let us keep the same notation and assumptions of Theorem 5.3 and let $\Delta_E\in\mathbb{Z}$ be the minimal discriminant of E. Assume condition* (5.3) *for E and that $c_2(E/\mathbb{Q})$ is odd. We have* $\operatorname{rank} E(\mathbb{Q})\neq \operatorname{rank} E^d(\mathbb{Q})$ *if and only if $\Delta_E>0$ and $d<0$.*

In particular, if $\operatorname{rank} E(\mathbb{Q})=0$, then Corollary 5.4 can only ensure $\operatorname{rank} E^d(\mathbb{Q})>0$ for negative values of d, under favorable conditions. Later we will be interested in taking $d=-q$ for q a prime. So, it will be crucial that the set $\mathscr{Q}_-(E,K)$ be non-empty; we must avoid case (iii) in Lemma 5.1.

6. Ranks and Hilbert's tenth problem

In this section we prove Theorem 1.2. For this, we will need an auxiliary elliptic curve to which we will apply Theorem 4.1 (with $\ell=3$) and Theorem 5.3. The chosen elliptic curve is 557b1 in Cremona's notation, which has minimal Weierstrass equation over $\mathbb{Z}$

$$y^2+y=x^3-x^2-268x+1781.$$

When using this elliptic curve, we will simply indicate "$E=557b1$".

6.1. **Compatibility in the Birch and Swinnerton-Dyer conjecture.** The Birch and Swinnerton-Dyer conjecture for abelian varieties over number fields (as formulated in [Ta65]) enjoys a number of compatibility properties, such as compatibility under product, isogenies [Ca65, Ta65, Mi06], and base change [Mi72]. The same compatibilities hold regarding the finiteness of the p-primary part of the Shafarevich-Tate group and the p-adic valuation of the conjectural special value formula (cf. Remark 7.4 in [Mi06]). We will use these compatibilities to reduce the verification of hypothesis in Theorem 4.1 for $\ell = 3$ to a computation involving elliptic curves over $\mathbb{Q}$.

This has a practical purpose, since exact numerical computations with elliptic curves over number fields are more difficult than over $\mathbb{Q}$. More concretely, we will need to check that $Ш(E/\mathbb{Q}(\sqrt{-3})[3]$ is trivial in a specific case, which involves a 3-descent to compute the relevant 3-Selmer group. However, the algorithm to compute 3-Selmer groups seems to be implemented in Magma only for elliptic curves over $\mathbb{Q}$.

We recall that if E is an elliptic curve over $\mathbb{Q}$ with L-function $L(E,s)$ and real period Ω_E, then the modularity of E implies that $L(E,s)$ is entire and that $L(E,1)/\Omega_E$ is a rational number that can be exactly, explicitly, and efficiently computed by the theory of modular symbols: it has small denominator (a divisor of $2 \cdot c(\varphi_E) \cdot \#E(\mathbb{Q})_{tor}$ for any modular parametrization φ_E), so a good numerical approximation suffices.

Proposition 6.1. *Let E be a semi-stable elliptic curve over $\mathbb{Q}$ with good reduction at the prime 3. Let $E' = E^{-3}$ be the quadratic twist of E by -3. Suppose that*

(i) $\operatorname{rank} E(\mathbb{Q}) = 0$ *and* $\operatorname{rank} E'(\mathbb{Q}) = 0$.

(ii) $Ш(E/\mathbb{Q})[3^\infty]$ *and* $Ш(E'/\mathbb{Q})[3^\infty]$ *are finite.*

(iii) *The 3-adic valuation of the rational numbers $L(E,1)/\Omega_E$ and $L(E',1)/\Omega_{E'}$ is as predicted by the 3-part of the Birch and Swinnerton-Dyer conjecture.*

Then $\operatorname{rank} E(\mathbb{Q}(\mu_3)) = 0$*, the group* $Ш(E/\mathbb{Q}(\mu_3))[3^\infty]$ *is finite, and we have*

$$\frac{L(E,1)}{\Omega_E} \cdot \frac{L(E',1)}{\Omega_{E'}} \sim_3 \frac{\operatorname{Tam}(E/\mathbb{Q}(\mu_3)) \cdot \#Ш(E/\mathbb{Q}(\mu_3))[3^\infty]}{\#E(\mathbb{Q}(\mu_3))_{tor}^2}.$$

Furthermore, if $3 \nmid \#\tilde{E}_3(\mathbb{F}_3)$, then $3 \nmid \#E(\mathbb{Q}(\mu_3))_{tor}$.

Proof. Note that $\mathbb{Q}(\mu_3) = \mathbb{Q}(\sqrt{-3})$. By (i) we have $\operatorname{rank} E(\mathbb{Q}(\mu_3)) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E'(\mathbb{Q}) = 0$.

Let A be the abelian surface over $\mathbb{Q}$ obtained as Weil restriction of scalars of $E/\mathbb{Q}(\mu_3)$ to $\mathbb{Q}$. Then A is isogenous over $\mathbb{Q}$ to $E \times E'$. By (ii) and compatibilities, we get that $Ш(E/\mathbb{Q}(\mu_3))[3^\infty]$ is finite.

The period of $E/\mathbb{Q}(\mu_3)$ can be computed using a global Néron differential ω_E of a minimal model of E over $\mathbb{Q}$ (as E is semi-stable), which up to powers of 2 gives $|\int_{E(\mathbb{C})} \omega_E \wedge \overline{\omega_E}|$. Up to powers of 2, this is equal to $\Omega_E \Omega_{E'} \sqrt{3}$ because E has good reduction at 3 (cf. [Pa12]).

By (iii) and compatibilities, the 3-part of the Birch and Swinnerton-Dyer conjecture holds for $E/\mathbb{Q}(\mu_3)$. Thus we have

$$\frac{\operatorname{Tam}(E/\mathbb{Q}(\mu_3)) \cdot \#Ш(E/\mathbb{Q}(\mu_3))[3^\infty]}{\#E(\mathbb{Q}(\mu_3))_{tor}^2} \sim_3 \frac{L(E/\mathbb{Q}(\mu_3),1)\sqrt{3}}{|\int_{E(\mathbb{C})} \omega_E \wedge \overline{\omega_E}|}$$

where the $\sqrt{3}$ comes from the discriminant of $\mathbb{Q}(\mu_3)$ (see [DD10] for an explicit statement of the conjectural Birch and Swinnerton-Dyer formula for abelian varieties over number fields). Artin formalism gives $L(E/\mathbb{Q}(\mu_3),s) = L(E,s)L(E',s)$, and the claimed formula follows.

Finally, let v be the only place of $\mathbb{Q}(\mu_3)$ over 3, and note that $v|3$ is ramified. Since E has good reduction at 3, we have that $E(\mathbb{Q}(\mu_3))_{tor}$ injects in $\tilde{E}_v(\mathbb{F}_v) \simeq \tilde{E}_3(\mathbb{F}_3)$, proving the final claim. □

We remark that the semi-stability condition is just for convenience and it can be relaxed with a more careful analysis; for our purposes this is enough.

6.2. **Keeping rank zero in many cubic extensions.**

Lemma 6.2. *Let $E = 557b1$. Define the set of primes*

$$\mathscr{P} = \{p : p \equiv 1 \bmod 3 \text{ and } a_p(E) \not\equiv 2 \bmod 3\}.$$

Then $\mathscr{P}$ is a Chebotarev set of primes of density $5/16$ and for each $p \in \mathscr{P}$ we have

$$\operatorname{rank} E(\mathbb{Q}(\sqrt[3]{p})) = 0.$$

Proof. It suffices to check the conditions (1) - (5) in Theorem 4.1 for $\ell = 3$.

In lmfdb.org [LMFDB] one checks that E has good ordinary reduction at 3 and that $\rho_{E[3]} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_3)$ is surjective, thus Conditions (1) and (2) are satisfied.

Consider the quadratic twist $E' = E^{-3}$, which has Cremona label 5013a1. Let us apply Proposition 6.1. The following code in Magma checks that both $\mathrm{Sel}_3(E/\mathbb{Q})$ and $\mathrm{Sel}_3(E'/\mathbb{Q})$ are trivial:

```
E1:=EllipticCurve("557b1");
E2:=EllipticCurve("5013a1");
Order(ThreeSelmerGroup(E1));
Order(ThreeSelmerGroup(E2));
        1
        1
```

In particular, we obtain:

- $\operatorname{rank} E(\mathbb{Q}) = 0$ and $\operatorname{rank} E'(\mathbb{Q}) = 0$
- $\text{Ш}(E/\mathbb{Q})[3]$ and $\text{Ш}(E/\mathbb{Q})[3]$ are trivial. Hence, $\text{Ш}(E/\mathbb{Q})[3^\infty]$ and $\text{Ш}(E/\mathbb{Q})[3^\infty]$ are also trivial.

The exact analytic order of the Shafarevich-Tate groups of E and E' over $\mathbb{Q}$ is 1 (see for instance lmfdb.org). This is the order predicted by the BSD conjecture, and the computation is exact since the rank is 0.

Therefore, conditions (i), (ii) and (iii) in Proposition 6.1 hold. In addition, $\#\tilde{E}_3(\mathbb{F}_3) = 2$ so $3 \nmid \#E(\mathbb{Q}(\mu_3))_{tor}$ and we get

$$\frac{L(E,1)}{\Omega_E} \cdot \frac{L(E',1)}{\Omega_{E'}} \sim_3 \mathrm{Tam}(E/\mathbb{Q}(\mu_3)) \cdot \#\text{Ш}(E/\mathbb{Q}(\mu_3))[3^\infty].$$

The number on the left is known to be a rational number of small denominator (cf. Paragraph 6.1), so the approximation

$$\frac{L(E,1)}{\Omega_E} \cdot \frac{L(E',1)}{\Omega_{E'}} \approx \frac{4.14294}{4.14294} \cdot \frac{1.36207}{0.68103} \approx 2.00001$$

implies that the number is in fact 2. Thus, Proposition 6.1 and the fact that $\#\tilde{E}_3(\mathbb{F}_3) = 2$ show that conditions (3), (4), and (5) of Theorem 4.1 hold for E and $\ell = 3$. □

6.3. **Increasing the rank in many quadratic extensions.** Our next goal is to produce many twists of $E = 557b1$ having positive rank over $\mathbb{Q}$. For this we will use the results in Section 5, which in particular involve the computation of certain logarithm on p-adic points of elliptic curves. The next observation will allow us to truncate the relevant power series with controlled p-adic precision in our computations.

Lemma 6.3. *Let $F(t) = b_0 + b_1 t + b_2 t^2 + ... \in \mathbb{Z}_p[[t]]$ and let $a \in p\mathbb{Z}_p$. Suppose that for certain $n \geq 1$ the integer*

$$m = v_p\left(ab_0 + \frac{a^2 b_1}{2} + ... + \frac{a^n b_{n-1}}{n}\right)$$

satisfies $m < n - (\log n)/(\log p)$. *Then*

$$v_p\left(\int_0^a F(t)dt\right) = m.$$

Proof. Observe that for all $r \geq 1$ we have

$$v_p(a^r b_{r-1}/r) \geq r + 0 - v_p(r) \geq r - \frac{\log r}{\log p}$$

because $a \in p\mathbb{Z}_p$ and $b_j \in \mathbb{Z}_p$. Using this for $r > n$ we get

$$v_p\left(ab_0 + \frac{a^2 b_1}{2} + ... + \frac{a^n b_{n-1}}{n} - \int_0^a F(t)dt\right) > m,$$

hence the result. □

Next we produce the required twists of positive rank for $E = 557b1$.

Lemma 6.4. *Let* $E = 557b1$. *Define the set of primes*

$$\mathscr{Q} = \{q : q \equiv -1 \bmod 4,\ (q/7) = 1,\ a_q(E) \equiv 1 \bmod 2\}.$$

Then $\mathscr{Q}$ *is a Chebotarev set of primes of density* $1/12$ *and for each* $q \in \mathscr{Q}$ *we have*

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

Proof. We are going to apply Theorem 5.3 and Corollary 5.4 to E and $K = \mathbb{Q}(\sqrt{-7})$. Then we will use Lemma 5.1 to show that the set of primes $\mathscr{Q}$ has the required properties.

First, we note that K satisfies the Heegner hypothesis for $2N = 2 \cdot 557$. This is because a prime ℓ splits in K if and only if ℓ is a quadratic residue modulo 7.

The elliptic curve E has good reduction at 2 and $\#\tilde{E}_2(\mathbb{F}_2) = 1$. It admits an optimal modular parametrization $\varphi : X_0(557) \to E$ (see lmfdb.org) and for this φ the Manin constant is $c(\varphi) = 1$ as 557 is odd and squarefree, cf. Paragraph 5.2 (alternatively, there are efficient algorithms to directly compute $c(\varphi)$). Let $\pi : J_0(557) \to E$ be the corresponding optimal quotient. Choosing an embedding $\sigma : K \to \mathbb{Q}_2$, we need to show that Condition (5.3) holds, i.e.

$$v_2\left(\log_{2,\omega_E} \sigma(\pi(P_{N,K}))\right) = 1 \tag{6.1}$$

where v_2 is the 2-adic valuation in $\mathbb{Q}_2$. According to Table 2 in [KL19] this condition indeed holds. However, the details are not included in *loc. cit.* so we do the computation here. For this we use the explicit description of $\log_{2,\omega_E}$ recalled in Paragraph 5.3.

The equation

$$y^2 + y = x^3 - x^2 - 268x + 1781 \tag{6.2}$$

is the reduced global minimal Weierstrass model for E over $\mathbb{Z}$. The global Néron differential for this model as a power series on $t = -x/y$ (local parameter at 0_E) is

$$\omega_E = (1 - t^2 + 2t^3 + ...)dt$$

where we used (5.2) for the model (6.2) to compute the first few coefficients. All the coefficients in this power series are integers.

Consider the 2-adic neighborhood of 0_E given by $U = \{a \in E(\mathbb{Q}_2) : t(a) \in 2\mathbb{Z}_2\}$. The logarithm map $\log_{2,\omega_E} : U \to \mathbb{Q}_2$ is given by

$$\log_{2,\omega_E}(a) = t(a) - \frac{1}{3}t(a)^3 + \frac{1}{2}t(a)^4 + ... \tag{6.3}$$

The Hilbert class-field of $K = \mathbb{Q}(\sqrt{-7})$ is K itself since the class number is 1 so, in fact, we have (cf. Paragraph 5.1)

$$\pi(P_{N,K}) = \varphi(Q_{N,K,\mathfrak{n}}) \in E(K).$$

Using Sage, we do the following: For a suitable choice of $\mathfrak{n}$, we compute the point $P = \varphi(Q_{N,K,\mathfrak{n}})$ in coordinates over K for the model (6.2). Then $t = -x(P)/y(P)$ is computed and we choose a valuation v on K extending the 2-adic valuation of $\mathbb{Q}$ —this is the same as choosing the embedding $\sigma : K \to \mathbb{Q}_2$. With all of this, we compute $v(t(P))$ and $v(t(P) - t(P)^3/3)$. Here is the code:

```
E=EllipticCurve(’557b1’);
P=E.heegner_point(-7).point_exact(100);
t=-P[0]/P[1];
K=t.parent();
u=QQ.valuation(2);
vK=u.extensions(K); v=vK[0];
v(t); v(t-t^3/3)
      1
      1
```

Since $v(t(P)) = 1$ we see that $\pi(P_{N,K}) \in U$ and we can use (6.3) to compute the logarithm of P. Since $v(t(P) - t(P)^3/3) = 1$ we can apply Lemma 6.3 with $p = 2$, $F(t) = \omega_E$, and $n = 3$, obtaining $v(\log_{2,\omega_E}(P)) = 1$. This proves that (6.1) holds.

Since $E(\mathbb{Q})[2] = (0)$ and (6.1) holds, we can apply Theorem 5.3. Furthermore, we have $c_2(E) = 1$ because E has good reduction at 2 (N is odd), so we can apply Corollary 5.4. We have that $\operatorname{rank} E(\mathbb{Q}) = 0$ and $\Delta_E = 557 > 0$. Therefore, for all squarefree integers $d \equiv 1 \bmod 4$ supported on $\mathscr{Q}(E, K)$ with $d < 0$ we have $\operatorname{rank} E^d(\mathbb{Q}) = 1$.

We observe that $\mathscr{Q} = \mathscr{Q}_-(E, K)$ and for each $q \in \mathscr{Q}$, the integer $d = -q$ satisfies the previously required conditions, hence $\operatorname{rank} E^{-q}(\mathbb{Q}) = 1$. Since $\operatorname{rank} E(\mathbb{Q}) = 0$ we deduce $\operatorname{rank} E(\mathbb{Q}(\sqrt{-q}) = 1$ for each $q \in \mathscr{Q}$.

It only remains to check that $\mathscr{Q}$ (i.e. $\mathscr{Q}_-(E, K)$) is a Chebotarev set of density 1/12 (in particular, that it is non-empty!). We apply Lemma 5.1. The degree of the field $L = \mathbb{Q}(E[2])$ and the discriminant of its only quadratic subfield can be computed on Sage as follows:

```
E=EllipticCurve(’557b1’);
L.<a> = E.division_field(2);
L.degree();
L.subfields(2)[0][0].discriminant()
      6
      557
```

Thus, we are in case (ii) of Lemma 5.1, which proves what we wanted. □

6.4. **Proof of the main result.**

Proof of Theorem 1.2. Consider the elliptic curve $E = 557b1$ and let $\mathscr{P}$ and $\mathscr{Q}$ be the sets of primes given by Lemmas 6.2 and 6.4. For each $p \in \mathscr{P}$ and each $q \in \mathscr{Q}$ we have that $\operatorname{rank} E(\mathbb{Q}(\sqrt[3]{p})) = 0$ and $\operatorname{rank} E(\mathbb{Q}(\sqrt{-q})) = 1$. By Proposition 3.3 with $M = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt[3]{p})$ and $L = \mathbb{Q}(\sqrt{-q})$ we get that the extension $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})/\mathbb{Q}(\sqrt[3]{p})$ is integrally Diophantine.

Since $\mathbb{Q}(\sqrt[3]{p})$ has exactly one complex place, the extension $\mathbb{Q}(\sqrt[3]{p})/\mathbb{Q}$ is integrally Diophantine by the Pheidas-Shlapentokh-Videla theorem [Ph88, Sh89, Vi89]. Therefore, Lemma 3.1 gives that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}(\sqrt[3]{p}, \sqrt{q})$. □

7. Acknowledgments

The first author was supported by the FONDECYT Iniciación en Investigación grant 11170192, and the CONICYT PAI grant 79170039. The second author was supported by FONDECYT Regular grant 1190442.

We gratefully acknowledge the hospitality of the IMJ-PRG in Paris during our visit in February 2019, where the final ideas of the project were developed. We heartily thank Loïc Merel for this invitation and for several enlightening discussions on elliptic curves.

The final technical details of this work were worked out and presented in May 2019 at the AIM meeting "Definability and Decidability problems in Number Theory". We thank the AIM for their hospitality and the participants for their valuable feedback. Specially, we thank Karl Rubin and Alexandra Shlapentokh for their interest and technical remarks.

Comments by Matias Alvarado, Chao Li, and Barry Mazur on an earlier version of this manuscript are gratefully acknowledged.

References

[AU96] A. Abbes, E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires.* Compositio Math. 103 (1996), no. 3, 269-286.

[ARS06] A. Agashe, K. Ribet, W. Stein, *The Manin constant.* Pure Appl. Math. Q. 2 (2006), no. 2, Special Issue: In honor of John H. Coates. Part 2, 617-636.

[Bi69] B. J. Birch, *Diophantine analysis and modular functions.* 1969 Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968) pp. 35-42 Oxford Univ. Press, London.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises.* J. Amer. Math. Soc. 14 (2001), no. 4, 843-939.

[BFH90] D. Bump, S. Friedberg, J. Hoffstein, *Eisenstein series on the metaplectic group and non-vanishing theorems for automorphic L-functions and their derivatives.* Annals of Math. 131, 1990, 53-127.

[Ca65] J. Cassels, *Arithmetic on curves of genus 1.* VIII. On conjectures of Birch and Swinnerton-Dyer. J. Reine Angew. Math. 217 (1965) 180-199.

[CPZ05] G. Cornelissen, T. Pheidas, K. Zahidi, *Division-ample sets and the Diophantine problem for rings of integers.* J. Théor. Nombres Bordeaux 17 (2005), no. 3, 727-735.

[DPR61] M. Davis, H. Putnam, J. Robinson, *The decision problem for exponential diophantine equations.* Ann. of Math. (2) 74 (1961) 425-436.

[De80] J. Denef, *Diophantine sets over algebraic integer rings.* II. Trans. Amer. Math. Soc. 257 (1980), no. 1, 227-236.

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

[Do07] T. Dokchitser, *Ranks of elliptic curves in cubic extensions.* Acta Arith. 126 (2007), no. 4, 357-360.

[Do05] V. Dokchitser, *Root numbers of non-abelian twists of elliptic curves.* With an appendix by Tom Fisher. Proc. London Math. Soc. (3) 91 (2005), no. 2, 300-324.

[DD07] T. Dokchitser, V. Dokchitser, *Computations in non-commutative Iwasawa theory.* With an appendix by J. Coates and R. Sujatha. Proc. Lond. Math. Soc. (3) 94 (2007), no. 1, 211-272.

[DD10] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares.* Ann. of Math. (2) 172 (2010), no. 1, 567-596.

[GZ86] B. Gross, D. Zagier, *Heegner points and derivatives of L-series.* Inv. Math. 84, 1986, 225-320.

[Gr01] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves.* Arithmetic algebraic geometry (Park City, UT, 1999), 407-464, IAS/Park City Math. Ser., 9, Amer. Math. Soc., Providence, RI, 2001.

[HM99] Y. Hachimori, K. Matsuno, *An analogue of Kida's formula for the Selmer groups of elliptic curves.* J. Algebraic Geom. 8 (1999), no. 3, 581-601.

[He52] K. Heegner, *Diophantische Analysis und Modulfunktionen.* Math. Z. 56, (1952). 227-253.

[Ko90] V. Kolyvagin, *Euler Systems.* The Grothendieck Festschrift, Eds. P. Cartier, et al., vol. II, Progr. in Math. 87, Birkhäuser, 1990, 435-483.

[KL19] D. Kriz, C. Li, *Goldfeld's conjecture and congruences between Heegner points.* Forum of Mathematics, Sigma, 7, E15 (2019).

[LMFDB] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`

[Ma70] Y. Matiyasevich, *The Diophantineness of enumerable sets.* (Russian) Dokl. Akad. Nauk SSSR 191 (1970) 279-282.

[Ma72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields.* Invent. Math. 18 (1972), 183-266.

[Ma78] B. Mazur, *Rational isogenies of prime degree* (with an appendix by D. Goldfeld). Invent. Math. 44 (1978), no. 2, 129-162.

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

[MR18] B. Mazur, K. Rubin, *Diophantine stability.* With an appendix by Michael Larsen. Amer. J. Math. 140 (2018), no. 3, 571-616.

[Mi72] J. Milne, *On the arithmetic of abelian varieties.* Invent. Math. 17 (1972), 177-190.

[Mi06] J. Milne, *Arithmetic duality theorems.* Second edition. BookSurge, LLC, Charleston, SC, 2006.

[Mo90] P. Monsky, *Mock Heegner points and congruent numbers.* Math. Z. 204 (1990), no. 1, 45-67.

[MM91] M. R. Murty, V. K. Murty, *Mean values of derivatives of modular L-series*, Annals of Math. 133, 1991, 447-475.

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

[Pa12] V. Pal, *Periods of quadratic twists of elliptic curves.* With an appendix by Amod Agashe. Proc. Amer. Math. Soc. 140 (2012), no. 5, 1513-1525.

[Pe84] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa.* (French) [Arithmetic of elliptic curves and Iwasawa theory] Mém. Soc. Math. France (N.S.) No. 17 (1984), 130 pp.

[Ph88] T. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers.* Proc. Amer. Math. Soc. 104 (1988), no. 2, 611-620.

[Po02] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers.* Algorithmic number theory (Sydney, 2002), 33-42, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[Sc83] P. Schneider, *Iwasawa L-functions of varieties over algebraic number fields. A first approach.* Invent. Math. 71 (1983), no. 2, 251-293.

[Si94] J. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

[SS89] H. Shapiro, A. Shlapentokh, *Diophantine relationships between algebraic number fields.* Comm. Pure Appl. Math. 42 (1989), no. 8, 1113-1122.

[Sh89] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields.* Comm. Pure Appl. Math. 42 (1989), no. 7, 939-962.

[Sh08] 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.

[Ta65] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog.* Séminaire Bourbaki, Vol. 9, Exp. No. 306, 415-440, Soc. Math. France, Paris, 1965.

[TW95] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141 (1995), no. 3, 553-572.

[Vi89] C. Videla, *Sobre el décimo problema de Hilbert.* Atas da Xa Escola de Algebra, Vitoria, ES, Brasil. Colecao Atas 16 Sociedade Brasileira de Matematica (1989), 95-108.

[Wi95] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) 141 (1995), no. 3, 443-551.

Departamento de Matemáticas
Pontificia Universidad Católica de Chile
Facultad de Matemáticas
4860 Av. Vicuña Mackenna
Macul, RM, Chile
Email address, N. Garcia-Fritz: natalia.garcia@mat.uc.cl

Departamento de Matemáticas
Pontificia Universidad Católica de Chile
Facultad de Matemáticas
4860 Av. Vicuña Mackenna
Macul, RM, Chile
Email address, H. Pasten: hector.pasten@mat.uc.cl