TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 10, Pages 482–506 (April 14, 2023)
https://doi.org/10.1090/btran/149

RANK GROWTH OF ELLIPTIC CURVES OVER N-TH ROOT EXTENSIONS

ARI SHNIDMAN AND ARIEL WEISS

Abstract. Fix an elliptic curve E over a number field F and an integer n which is a power of 3. We study the growth of the Mordell–Weil rank of E after base change to the fields $K_d = F(\sqrt[2n]{d})$. If E admits a 3-isogeny, then we show that the average "new rank" of E over K_d, appropriately defined, is bounded as the height of d goes to infinity. When $n = 3$, we moreover show that for many elliptic curves $E/\mathbb{Q}$, there are no new points on E over $\mathbb{Q}(\sqrt[6]{d})$, for a positive proportion of integers d. This is a horizontal analogue of a well-known result of Cornut and Vatsal [*Nontriviality of Rankin-Selberg L-functions and CM points,* L-functions and Galois representations, vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 121–186]. As a corollary, we show that Hilbert's tenth problem has a negative solution over a positive proportion of pure sextic fields $\mathbb{Q}(\sqrt[6]{d})$.

The proofs combine our recent work on ranks of abelian varieties in cyclotomic twist families with a technique we call the "correlation trick", which applies in a more general context where one is trying to show simultaneous vanishing of multiple Selmer groups. We also apply this technique to families of twists of Prym surfaces, which leads to bounds on the number of rational points in sextic twist families of bielliptic genus 3 curves.

1. Introduction

Let E be an elliptic curve over a number field F, and let K/F be a finite extension. Mazur and Rubin define E to be *diophantine stable for* K/F if $E(K) = E(F)$, i.e. if there are no new rational points on E after base change to K [MR18]. There has been much interest and speculation regarding how often E is diophantine stable for K/F, as K varies through a family of Galois extensions K/F of fixed degree and Galois group G [Dok07, DFK07, DT10, Kis12, FKK12, MR07, MR08, MR18, For19, LOT21, KN21, BKR21]. Mazur and Rubin themselves showed that for a positive density set of primes ℓ, the curve E is diophantine stable for infinitely many $\mathbb{Z}/\ell^n\mathbb{Z}$-extensions K/F, under the mild hypothesis that $\mathrm{End}_F(E) = \mathrm{End}_{\bar{F}}(E)$.

In this paper, we study a more refined notion of "new points". Observe that there may be points $P \in E(K)$ defined over intermediate extensions L/F contained in K. Moreover, there may be points $P \in E(K)$ whose minimal field of definition is K, but which are sums of points defined over smaller fields. These types of points

Received by the editors January 23, 2022, and, in revised form, November 22, 2022, and December 27, 2022.

2020 *Mathematics Subject Classification.* Primary 11G05, 14G05, 14K05, 11S25.

The first author was supported by the Israel Science Foundation (grant No. 2301/20). The second author was supported by an Emily Erskine Endowment Fund postdoctoral fellowship at the Hebrew University of Jerusalem, by the Israel Science Foundation (grant No. 1963/20) and by the US-Israel Binational Science Foundation (grant No. 2018250).

are not really new, so we define the *new part* of $E(K)$ to be the quotient

$$E(K/F)^{\mathrm{new}} := E(K)/\sum_{L} E(L),$$

where the sum is over the subfields $F \subset L \subsetneq K$.[1] Note that E is diophantine stable for K/F if and only if $E(L/F)^{\mathrm{new}} = 0$ for all extensions $F \subsetneq L$ contained in K.

1.1. **Rank growth.** Our first result shows that the average rank of $E(K_d/F)^{\mathrm{new}}$ is bounded, for certain elliptic curves E and for certain families of number fields of the form $K_d = F(\sqrt[2n]{d})$. In other words, there are not too many new points on average, as $|\operatorname{Nm}_{F/\mathbb{Q}}(d)| \to \infty$.

Theorem 1.1. *Let E/F be an elliptic curve admitting a 3-isogeny and fix a positive integer $n = 3^m$. As d runs over the elements of $F^\times/F^{\times 2n}$ of order $2n$, ordered by height, the average of $\operatorname{rk} E(K_d/F)^{\mathrm{new}}$ is bounded.*

For the precise definition of height see Definition 3.1. To prove Theorem 1.1, we construct, for each field K_d, an abelian variety A_d over F whose Mordell–Weil rank is equal to the rank of $E(K_d/F)^{\mathrm{new}}$. This uses a version of Serre's tensor construction, as in [MRS07]. Each abelian variety A_d admits a μ_n-action, where $\mu_n = \langle \zeta_n \rangle$ is the group scheme of n-th roots of unity, and the A_d's are all μ_{2n}-twists of each other. Because E has a 3-isogeny, the Galois module $A_1[1-\zeta_n]$ decomposes as a direct sum of characters. This allows us to apply our recent result [SW21, Thm. 1.1], which bounds the average rank of abelian varieties in families of μ_{2n}-twists. As in [SW21], the upper bound on the average rank that is guaranteed by Theorem 1.1 can be made explicit, but the bound depends on the particular curve E.

In the spirit of Mazur and Rubin, we are more interested in proving that $E(K_d/F)^{\mathrm{new}} = 0$ for infinitely many d. Actually, we consider the harder question of whether this is true for a *positive proportion* of $d \in F^\times/F^{\times 2n}$, which is what we will need for our applications to Hilbert's tenth problem below. When $n = 1$ and $F = \mathbb{Q}$, we have $\operatorname{rk} E(K_d/F)^{\mathrm{new}} = \operatorname{rk} E_d(F)$, where E_d is the d-th quadratic twist of E, and Goldfeld conjectures that 50% of these twists have rank 0. This conjecture has been verified in many cases [BKLOS19, KL19, Li19]. Indeed, in his Ph.D. thesis, Smith proves the conjecture for "most" elliptic curves E over $\mathbb{Q}$ [Smi20].

In contrast, when $n > 1$, there may not be a single d for which $\operatorname{rk} E(K_d/F)^{\mathrm{new}} = 0$, due to root number considerations. This phenomenon was already observed by Dokchitser in [Dok07] for cubic twists. For example, if $n = 3$, the Birch and Swinnerton-Dyer conjecture implies that for the elliptic curve $E\colon y^2+y = x^3+x^2+x$ over $\mathbb{Q}$ of conductor 19, the group $E(K_d/\mathbb{Q})^{\mathrm{new}}$ will have odd rank for all squarefree integers d.

Despite these somewhat pathological examples, we prove that for many elliptic curves, we indeed have $E(K_d/\mathbb{Q})^{\mathrm{new}} = 0$ for a positive proportion of $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 6}$. We consider elliptic curves with the model $E\colon y^2+axy+by = x^3$, whose discriminant is $b^3(a^3-27b)$. These are precisely the elliptic curves over $\mathbb{Q}$ with a rational 3-torsion point, which is $(0,0)$ in this model.

[1] As we explain in Section 2.1, this definition is best behaved when K contains no proper subextensions L/F whose normal closure is also a normal closure for K. This will always be the case in the situations we consider.

Theorem 1.2. *Let a and b be coprime integers, and let E be the elliptic curve $y^2 + axy + by = x^3$. Assume that $3 \nmid ab$ and that either:*

(i) *there exists a prime $q \equiv 2 \pmod 3$ such that $q \mid a^3 - 27b$, or*
(ii) *there exist primes $q_1 \equiv 1 \pmod 3$ and $q_2 \equiv 2 \pmod 3$ such that $q_1 \mid a^3 - 27b$ and $q_2 \mid b$.*

Set $K_d = \mathbb{Q}(\sqrt[6]{d})$. Then for a positive proportion of integers d, we have $\operatorname{rk} E(K_d/\mathbb{Q})^{\mathrm{new}} = 0$.

More precisely, the lower density of integers d such that $\operatorname{rk} E(K_d/\mathbb{Q})^{\mathrm{new}} = 0$ is positive. Our proof gives an explicit lower bound on this lower density, but the bound depends on E and tends to be quite small. For example, in Section 5.1, we work out the details for the curve $E\colon y^2 + 2xy - y = x^3$ of conductor 35. In this case, we exhibit a set T of squarefree integers, defined by finitely many congruence conditions, such that a proportion of at least $\frac{1}{18}$ of $d \in T$ satisfy $\operatorname{rk} E(K_d/\mathbb{Q})^{\mathrm{new}} = 0$.

In the setting of Theorem 1.2, the Galois group of the splitting field of $K_d/\mathbb{Q}$ is the dihedral group D_6 of order 12, with the subgroup C_6 cut out by the imaginary quadratic field $\mathbb{Q}(\zeta_3)$. In this context, the groups $E(K_d/\mathbb{Q})^{\mathrm{new}}$ have a systematic source of rational points, namely χ_d-components of Heegner points, where χ_d is the corresponding ring class field character of order 6. In terms of L-functions, the Birch and Swinnerton-Dyer conjecture predicts that the rank of $E(K_d/\mathbb{Q})^{\mathrm{new}}$ is 0 if and only if the twisted L-function $L(E, \chi_d, s)$ is non-vanishing at its central point $s = 1$. Theorem 1.2 should be compared to the non-vanishing results of Cornut–Vatsal [CV07], who showed that for every prime $\mathfrak{p}$ of $\mathcal{O}_K$, and for all large enough n, there exist ring class field characters χ of conductor $\mathfrak{p}^n$ such that $L(E, \chi, 1)$ is non-vanishing. Our result is orthogonal to theirs ("horizontal" instead of "vertical"), since we fix the order of the character while allowing many primes to divide the conductor. Of course, we only consider a very special case, where $K = \mathbb{Q}(\zeta_3)$ and the order of the characters is 6. Our general method could conceivably be adapted to other quadratic fields, but that seems to require some new ideas (one would first of all need to generalize [SW21] appropriately).

1.2. **The correlation trick.** The proof of Theorem 1.2 uses Theorem 1.1 as a starting point, but requires significantly more. The abelian varieties A_d from the proof of Theorem 1.1 are, in this case, abelian surfaces with multiplication by $\mathbb{Z}[\zeta_3]$. In fact, they are twists of the Jacobian of the genus two curve

$$C\colon y^2 = x^6 + \alpha x^3 + 1,$$

where $\alpha = 108b/a^3 - 2$. Notice that $\operatorname{Aut}(C)$ contains the group D_6, and in particular the automorphism $\zeta_3(x, y) = (\zeta_3 x, y)$ of order 3.[2] The endomorphism $2\zeta_3 + 1 = \sqrt{-3} \in \operatorname{End}(A_d)$ is only defined over $\mathbb{Q}(\sqrt{-3})$, but it descends to a $(3,3)$-isogeny over $\mathbb{Q}$, which factors into two 3-isogenies $\phi_d\colon A_d \to B_d$ and $\psi_d\colon B_d \to A_{-27d}$.

Under the mild technical conditions of Theorem 1.2, we show that there exists a positive density set $T \subset \mathbb{Z}$, defined by congruence conditions, such that $\#\operatorname{Sel}(\phi_d) = \#\operatorname{Sel}(\widehat{\phi}_d)$ and $\#\operatorname{Sel}(\psi_d) = \#\operatorname{Sel}(\widehat{\psi}_d)$ for all but finitely many $d \in T$. We reiterate that without some kind of technical condition on E, the parity conjecture implies

[2]The non-hyperelliptic involution is $(x : y : z) \to (z : y : x)$, when written in weighted projective coordinates.

that Theorem 1.2 is false in general. When $d \in T$, we show that $\#\operatorname{Sel}_3(A_d) \leq (\#\operatorname{Sel}(\phi_d)\#\operatorname{Sel}(\psi_d))^2$. Since

$$\operatorname{rk} E(K_d/\mathbb{Q})^{\text{new}} = \operatorname{rk} A_d(\mathbb{Q}) \leq \dim_{\mathbb{F}_3} \operatorname{Sel}_3(A_d),$$

in order to prove Theorem 1.2, it is enough to show that $\operatorname{Sel}(\phi_d) = \operatorname{Sel}(\psi_d) = 0$ for a positive proportion of integers $d \in T$.

Using the results of [SW21], we show that the average size of each of $\operatorname{Sel}(\phi_d)$ and $\operatorname{Sel}(\psi_d)$ is 2, for $d \in T$. Since these Selmer groups are $\mathbb{F}_3$-vector spaces, we immediately deduce that each of these groups vanishes for at least 50% of $d \in T$. The problem is that, a priori, we cannot rule out the possibility that the sets $\{d \in T\colon \operatorname{Sel}(\phi_d) = 0\}$ and $\{d \in T\colon \operatorname{Sel}(\psi_d) = 0\}$ intersect in a set of density 0. Thus, to complete the proof, it remains to rule out the unlikely pathological scenario that half of $d \in T$ satisfy $\#\operatorname{Sel}(\phi_d) = 1$ and $\#\operatorname{Sel}(\psi_d) = 3$, and the other half satisfy $\#\operatorname{Sel}(\phi_d) = 3$ and $\#\operatorname{Sel}(\psi_d) = 1$. In other words, we must show that the random variables $\#\operatorname{Sel}(\phi_d)$ and $\#\operatorname{Sel}(\psi_d)$ are at least a tiny bit correlated, e.g. that they are either both 1 or both greater than 1, for a positive proportion of $d \in T$.

To prove this correlation, we use a third 3-isogeny $\eta_d\colon A_d \to C_d$, whose Selmer group $\operatorname{Sel}(\eta_d)$ can be interpreted as lying in the intersection of $\operatorname{Sel}(\phi_d)$ and $\operatorname{Sel}(\psi_d)$. We then apply the results of [SW21] to η_d to show that the average size of the intersection is strictly greater than 1. However, this *does not* show that their intersection is non-trivial a positive proportion of the time, since the bulk of the average size could be supported on a 0-density set. The trick is to observe that since

$$\#\operatorname{Sel}(\phi_d) + \#\operatorname{Sel}(\psi_d) = \min(\#\operatorname{Sel}(\phi_d), \#\operatorname{Sel}(\psi_d)) + \max(\#\operatorname{Sel}(\phi_d), \#\operatorname{Sel}(\psi_d)),$$

we can infer that the average of their maximum size is strictly less than $2+2-1 = 3$. Since we are dealing with $\mathbb{F}_3$-vector spaces, this implies that $\operatorname{Sel}(\phi_d)$ and $\operatorname{Sel}(\psi_d)$ are both trivial for a positive proportion of $d \in T$. By the definition of T, we have $\operatorname{Sel}_3(A_d) = 0$ for such d, and $\operatorname{rk}(A_d) = 0$ as well, which proves the theorem.

1.3. **Application to Hilbert's tenth problem for pure sextic fields.** Hilbert asked whether there is a Turing machine that takes as input a polynomial equation over $\mathbb{Z}$ and correctly decides whether it has a solution over $\mathbb{Z}$. Matijasevič [Mat70], building on work of Davis–Putnam–Robinson [DPR61], showed that no such algorithm exists, i.e. Hilbert's tenth problem has a negative solution over $\mathbb{Z}$.

There has been much work on the analogous question over rings of integers $\mathcal{O}_K$ of number fields K of degree larger than 1; see the introduction to [GFP20] for a brief survey. It is believed that the answer should again be negative, and this has been proven for number fields with at most one complex place. In particular, it is known when K has degree 2 or 3, and for many K of degree 4 as well. While the general case is still open, Mazur and Rubin have shown that a negative answer follows from the finiteness of the Tate–Shafarevich group [MR10]. This uses a result of Shlapentokh [Shl08] which states that Hilbert's tenth problem over $\mathcal{O}_K$ has a negative answer if there exists an elliptic curve $E/\mathbb{Q}$ of positive rank such that $\operatorname{rk} E(K) = \operatorname{rk} E(\mathbb{Q})$, i.e. with no rank gain over K. We combine this criterion with Theorem 1.2 to prove:

Theorem 1.3. *For a positive proportion of pure sextic fields $K = \mathbb{Q}(\sqrt[6]{d})$, ordered by the height of d, the analogue of Hilbert's tenth problem over $\mathcal{O}_K$ has a negative solution.*

Recently, Garcia-Fritz and Pasten [GFP20] proved a similar result for an explicit subset of fields of the form $\mathbb{Q}(\sqrt[6]{-p^2q^3})$, with p and q prime. The set of all such fields has density 0 among all pure sextic fields, so Theorem 1.3 is a quantitative improvement. On the other hand, our result does not give an explicit set of fields. We prove Theorem 1.3 by applying Theorem 1.2 to a single elliptic curve, but to maximize the proportion of pure sextic fields that our method gives, one could try to use many different elliptic curves. We do not attempt such an analysis here.

1.4. **Applications to twists of abelian surfaces.** The correlation trick can be applied in other settings where one needs to simultaneously bound Selmer groups attached to two isogenies whose kernels are isomorphic (as group schemes). As an example, we prove the existence of simple abelian surfaces with low rank in some of the sextic twist families considered in [SW21], partially answering a question we asked there. Recall that if $C \to E$ is a ramified double cover of curves, then the Prym variety is the kernel of the induced map $\mathrm{Jac}(C) \to \mathrm{Jac}(E)$ on Jacobians. As a special case, a smooth genus 3 curve of the form $C\colon y^3 = f(x^2)$, with $f(x)$ quadratic, admits a double cover to the elliptic curve $y^3 = f(x)$. In this case, the Prym variety is an abelian surface.

Theorem 1.4. *Fix integers $a > b > 0$ and let A_d be the twist family of Prym surfaces arising from the genus three bielliptic curves $C_d\colon y^3 = (x^2 - da^2)(x^2 - db^2)$. For a positive proportion of integers d, ordered by absolute value, we have* $\mathrm{rk}\, A_d \leq 1$.

As a corollary, we prove:

Theorem 1.5. *Let C_d be any twist family as above. For a positive proportion of $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 6}$, we have $\#C_d(\mathbb{Q}) \leq 5$.*

Individual cases of these theorems were proven in [SW21, §1.2]; for other results on average Mordell–Weil ranks in families of Prym surfaces see [Lag22] and [ABS22, Thm. 1.13]. As usual, one can extract from the proofs of Theorem 1.4 (resp. Theorem 1.5) an explicit lower bound on the proportion of twists with $\mathrm{rk}\, A_d \leq 1$ (resp. $\#C_d \leq 5$), a bound which in principle depends on a and b. For this particular family of curves, it is conceivable that our bound could be made uniform, independent of a and b, since the abelian surfaces A_d have everywhere potentially good reduction. To prove this, one would want to prove a version of Tate's algorithm for these surfaces and various isogenous surfaces, or find some other way to access their Tamagawa numbers. This is beyond the scope of this paper, but would be an interesting future project.

Another large family of curves for which this intersection method applies is the family of genus two curves C admitting *potential* $\sqrt{3}$-multiplication and a subgroup $(\mathbb{Z}/3\mathbb{Z})^2 \hookrightarrow \mathrm{Jac}(C)[3]$ which is isotropic with respect to the Weil pairing. This family is parameterized by a twist of a certain Hilbert modular surface (since the $\sqrt{3}$-multiplication is not defined over $\mathbb{Q}$). An explicit rational parameterization for this surface was given in [BFS21, §2], on the way to constructing a rational parameterization for the Hilbert modular surface itself. We will not prove any theorems about such abelian surfaces since the ideas are similar. In fact the proofs

are easier in this case since these families only admit quadratic twists, not sextic twists.

1.5. **Outline.** We begin in Section 2 by reinterpreting the notion of "new rank" representation-theoretically. Using this interpretation, we construct an abelian variety B/F such that $\mathbb{Z}[\zeta_n] \subset \operatorname{End}_{\bar{F}} B$, and such that for $d \in H^1(F, \mu_{2n})$, the rank of the corresponding twist B_d/F encodes the new rank of $E(K_d/F)$. Although this family of twists exactly encodes the new rank of E, the abelian variety B does not satisfy the main hypothesis of [SW21, Thm. 1.1]. In Section 3, we construct an isogenous abelian variety A/F that does satisfy this hypothesis. Hence, we may apply [SW21, Thm. 1.1] and deduce Theorem 1.1.

In Section 4, we demonstrate in general how to use intersections of Selmer groups to show that the two Selmer groups $\mathrm{Sel}(\phi_d)$ and $\mathrm{Sel}(\psi_d)$ vanish simultaneously for a positive proportion of d. The key result of this section is Theorem 4.4, whose proof uses the correlation trick described above. Using this result, in Section 5, we prove Theorem 1.2. In Section 5.1, we show how to make Theorem 4.4 quantitative, using the curve $E\colon y^2+2xy-y=x^3$ as an example. In Section 6 we deduce Theorem 1.3 from Theorem 1.2. Finally, in Section 7, we apply Theorem 4.4 in the context of Prym abelian surfaces to prove Theorem 1.4.

2. Encoding the new rank of E

Let F be a number field and let E be an elliptic curve over F. The goal of this section is to construct, for each $d \in F^\times/F^{\times 2n}$, an abelian variety B_d over F, whose rank encodes the "new rank" of E for the extension K_d/F.

First, for any extension K/F, we define a slight variant of the new rank, $\operatorname{rk} E(K/F)^{\text{G-new}}$, which we then interpret from a representation-theoretic point of view. When $K = K_d = F(\sqrt[2n]{d})$, it will turn out that $\operatorname{rk} E(K/F)^{\text{new}} = \operatorname{rk} E(K/F)^{\text{G-new}}$, so the results of this section will be relevant to the proof of Theorem 1.1.

2.1. The new rank of an elliptic curve.

2.1.1. *Galois extensions.* Let K/F be a finite Galois extension and let $G = \mathrm{Gal}(K/F)$. The group $E(K)$ is a G-module, and we define a G-module quotient that corresponds to the "new points".

Definition 2.1. Set $E(K/F)^{\text{G-new}} = E(K)/\sum_L E(L)$, where the sum is over the subfields $F \subset L \subsetneq K$ that are Galois over F.

Since we are concerned only with ranks (and not torsion properties), we will mostly consider the G-representation $V := E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. We can decompose V as a $\mathbb{Q}[G]$-module: $V = \bigoplus_\rho V_\rho$, where the sum is over all irreducible $\mathbb{Q}$-representations ρ of G, and V_ρ is the ρ-isotypic part of V, spanned by the images of all G-morphisms from ρ to V.

Definition 2.2. Let V^{new} denote the representation $\bigoplus_\eta V_\eta$, where the sum is over all *faithful* irreducible $\mathbb{Q}$-representations η of G.

Proposition 2.3. *We have* $E(K/F)^{\text{G-new}} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq V^{\text{new}}$ *and* $\operatorname{rk} E(K/F)^{\text{G-new}} = \dim_{\mathbb{Q}} V^{\text{new}}$.

Proof. Let L be a proper subextension of K that is Galois over F, and let $H = \mathrm{Gal}(K/L)$. If $W \subset V$ is any G-subrepresentation, then since H is normal in G, the subspace $W^H \subset W$ of H fixed vectors is a G-subrepresentation.

Observe that a representation W of G is a direct sum of faithful irreducible representations if and only if $W^H = 0$ for every non-trivial normal subgroup $H \lhd G$. Thus, V^{new} is the largest G-subrepresentation W of V such that $W^H = 0$ for all non-trivial normal subgroups $H \lhd G$.

The kernel of the projection $V \to V^{\mathrm{new}}$ is spanned by the subrepresentations W of V such that $W^H = W$ for some non-trivial $H \lhd G$. In other words, the kernel is spanned by the subspaces $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$, where L is a proper Galois subextension of K/F. It follows that $E(K/F)^{\text{G-new}} \otimes_{\mathbb{Z}} \mathbb{Q} = V^{\mathrm{new}}$. □

Remark 2.4. For any field extension $L/\mathbb{Q}$, define $V_L = E(K) \otimes_{\mathbb{Z}} L$ and define V_L^{new} in the analogous way. Then the same argument shows that $E(K/F)^{\text{G-new}} \otimes_{\mathbb{Z}} L = V_L^{\mathrm{new}}$.

Remark 2.5. Let $W = \mathrm{Ind}^G 1$ be the regular representation. As a representation of G, we can write $W = \bigoplus_\rho W_\rho$, where the sum is over the irreducible rational representations ρ of G. As before, let $W^{\mathrm{new}} = \bigoplus_\eta W_\eta$ be the subrepresentation of W, where the sum is over all faithful irreducible rational representations η of G. Let $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be the ℓ-adic Galois representation attached to E. Then the (equivariant) Birch and Swinnerton-Dyer conjecture predicts the equality

$$\mathrm{rk}\, E(K/F)^{\text{G-new}} \stackrel{?}{=} \mathrm{ord}_{s=1} L(V_\ell(E) \otimes W^{\mathrm{new}}, s),$$

where $V_\ell(E) \otimes W^{\mathrm{new}}$ is viewed as a representation of $\mathrm{Gal}(\overline{F}/F)$. Note that this L-function is defined over F. On the other hand, it does not seem that $E(K/F)^{\mathrm{new}}$, as defined in the introduction, should correspond to an L-function over F in general.

2.1.2. *Non-Galois extensions.* Let K/F be an arbitrary finite extension of number fields. For any extension L/F contained in K we write $\widetilde{L}$ for its Galois closure over F. We let $N = \widetilde{K}$ be the Galois closure of K itself.

Definition 2.6. Let $E(K/F)^{\text{G-new}} = E(K)/\sum_L E(L)$, where the sum is over the subfields $F \subset L \subsetneq K$, such that the Galois closure of L is a proper subfield of N.

Let $V(N) = E(N) \otimes_{\mathbb{Z}} \mathbb{Q}$, and define $V(N)^{\mathrm{new}} = \bigoplus_\eta V_\eta$, as in the previous section, where η runs over the faithful irreducible $\mathbb{Q}$-representations of $\mathrm{Gal}(N/F)$. By Proposition 2.3, we have a short exact sequence of $\mathrm{Gal}(N/F)$-representations

$$0 \to V(N)^{\mathrm{old}} \to V(N) \to V(N)^{\mathrm{new}} \to 0, \tag{2.1}$$

where

$$V(N)^{\mathrm{old}} = \sum_{\substack{F \subset L \subsetneq N \\ L/F \text{ Galois}}} E(L) \otimes_{\mathbb{Z}} \mathbb{Q}. \tag{2.2}$$

The G-new points of E for K/F are compatible with the G-new points of E for N/F in the following sense.

Proposition 2.7. *We have* $E(K/F)^{\text{G-new}} \otimes_{\mathbb{Z}} \mathbb{Q} = (V(N)^{\mathrm{new}})^{\mathrm{Gal}(N/K)}$.

Proof. From (2.1), we have a short exact sequence of vector spaces

$$0 \to (V(N)^{\mathrm{old}})^{\mathrm{Gal}(N/K)} \to V(N)^{\mathrm{Gal}(N/K)} \to (V(N)^{\mathrm{new}})^{\mathrm{Gal}(N/K)} \to 0.$$

Since

$$E(K/F)^{\text{G-new}} \otimes_{\mathbb{Z}} \mathbb{Q} = \frac{E(K) \otimes_{\mathbb{Z}} \mathbb{Q}}{\sum_{\substack{F \subsetneq L \subsetneq K \\ L \neq N}} E(L) \otimes_{\mathbb{Z}} \mathbb{Q}},$$

it remains to show that

$$(V(N)^{\text{old}})^{\text{Gal}(N/K)} = \left(\sum_{\substack{F \subsetneq L \subsetneq N \\ L/F \text{ Galois}}} E(L) \otimes_{\mathbb{Z}} \mathbb{Q} \right)^{\text{Gal}(N/K)} = \sum_{\substack{F \subsetneq L \subsetneq K \\ L \neq N}} E(L) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

We have

$$(V(N)^{\text{old}})^{\text{Gal}(N/K)} = \left(\bigoplus_{\mu} V_\mu \right)^{\text{Gal}(N/K)} = \bigoplus_{\mu} V_\mu^{\text{Gal}(N/K)},$$

where the sum is over all $\mathbb{Q}$-representations of $\text{Gal}(N/F)$ that are not faithful.

Let μ be a non-faithful representation of $\text{Gal}(N/F)$ with kernel $\text{Gal}(N/L)$ for some non-trivial Galois extension L/F. Then $L \cap K$ is a subfield of K whose Galois closure is a proper subfield of N. By definition, $V_\mu^{\text{Gal}(N/L)} = V_\mu$. Hence,

$$V_\mu^{\text{Gal}(N/K)} = V_\mu^{\text{Gal}(N/K) \cdot \text{Gal}(N/L)} = V_\mu^{\text{Gal}(N/L \cap K)} \subset E(L \cap K) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

It follows that

$$(V(N)^{\text{old}})^{\text{Gal}(N/K)} = \bigoplus_{\mu} V_\mu^{\text{Gal}(N/K)} \subset \sum_{\substack{F \subsetneq L \subsetneq K \\ L \neq N}} E(L) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Conversely, if $F \subset L \subsetneq N$, then

$$E(L)^{\text{Gal}(N/K)} = E(L)^{\text{Gal}(N/K) \cdot \text{Gal}(N/L)} = E(L)^{\text{Gal}(N/L \cap K)} = E(L \cap K).$$

Moreover, if L/F is Galois, then the Galois closure of $L \cap K$ is not N. Hence, by (2.2), we see that

$$\begin{aligned}(V(N)^{\text{old}})^{\text{Gal}(N/K)} &= \left(\sum_{\substack{F \subsetneq L \subsetneq N \\ L/F \text{ Galois}}} E(L) \otimes_{\mathbb{Z}} \mathbb{Q} \right)^{\text{Gal}(N/K)} \\ &\supset \sum_{\substack{F \subsetneq L \subsetneq N \\ L/F \text{ Galois}}} E(L \cap K) \otimes_{\mathbb{Z}} \mathbb{Q} \\ &= \sum_{\substack{F \subsetneq L \subsetneq K \\ L \neq N}} E(L) \otimes_{\mathbb{Z}} \mathbb{Q},\end{aligned}$$

which finishes the proof. □

2.2. **Abelian varieties with ζ-multiplication.** We recall the definition of an abelian variety over F with ζ-multiplication and its twists; for further details, see [SW21, §2]. Let A/F be an abelian variety, and let $\zeta = \zeta_n \in \overline{F}^\times$ be a primitive n-th root of unity, where n is an odd prime power.

Definition 2.8. An abelian variety A/F has ζ_n-multiplication if there is a G_F-equivariant injective ring homomorphism $\mathbb{Z}[\zeta_n] \hookrightarrow \text{End}_{\bar{F}} A$.

If $d \in F^\times$, then we define A_d to be twist of A corresponding to the cocycle that is the image of d under

$$F^\times \to F^\times/F^{\times 2n} \simeq H^1(F, \mu_{2n}) \to H^1(F, \mathrm{Aut}_{\bar{F}}(A)).$$

If A has ζ-multiplication, then the endomorphism $1-\zeta\colon A_{F(\zeta)} \to A_{F(\zeta)}$ over $F(\zeta)$ descends to an isogeny defined over F, which we denote by $\pi\colon A \to A^{(1)}$ [SW21, §2]. The abelian variety $A^{(1)}$ is the twist of A corresponding to the cocycle $\sigma \mapsto \frac{1-\zeta^\sigma}{1-\zeta} \in H^1(F, \mathbb{Z}[\zeta]^\times)$ [SW21, Lem. 2.3]. In particular, if $\zeta = \zeta_3$, $A^{(1)} \cong A_{-27}$, but, in general, $A^{(1)}$ is not isomorphic to A_d for any d.

The abelian variety $A^{(1)}$ also has ζ-multiplication, and we let $\pi_d\colon A_d \to A_d^{(1)}$ denote the twist of π corresponding to $d \in F^\times/F^{\times 2n}$.

2.3. **An auxiliary abelian variety.** Let $n = 3^m$ for some $m \geq 1$ and let $\zeta = \zeta_n$. Fix an element $d \in F^\times/F^{\times 2n}$ of order $2n$, and let $K_d = F(\sqrt[2n]{d})$. We will define an abelian variety B/F with ζ-multiplication, such that $\mathrm{rk}\, B_d(F) = \mathrm{rk}\, E(K_d/F)^{\mathrm{new}}$.

View $\mathbb{Z}[\zeta]$ as a right G_F-module. Following [MRS07, Thm. 1.8], we define the abelian variety

$$B := \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} E$$

over F, which has dimension $2 \cdot 3^{m-1}$. By [MRS07, Cor. 1.7], there are G_F-equivariant ring embeddings $\mathbb{Z}[\zeta] \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[\zeta]) \hookrightarrow \mathrm{End}_{\bar{F}}(B)$, so that B has ζ-multiplication. Concretely, the ζ-multiplication on B is by left multiplication on the $\mathbb{Z}[\zeta]$-factor.

Example 2.9. Suppose that $m = 1$ and $F = \mathbb{Q}$. Then $\mathbb{Z}[\zeta]$ is a rank two $\mathbb{Z}$-module and B is an abelian surface. The embedding $\tau\colon E \hookrightarrow B$ defined by $P \mapsto 1 \otimes P$, has cokernel $B/\tau(E)$ isomorphic to $(\mathbb{Z}[\zeta]/\mathbb{Z}) \otimes E$. The latter is isomorphic to the quadratic twist E_{-3}, since $\mathbb{Z}[\zeta]/\mathbb{Z}$ is free of rank one with Galois action factoring through $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$. On the other hand, we can embed E_{-3} in B via $P \mapsto \sqrt{-3} \otimes P$. If E and E_{-3} are not isogenous, then both $\mathrm{Hom}_{\mathbb{Q}}(E, B)$ and $\mathrm{Hom}_{\mathbb{Q}}(E_{-3}, B)$ must have rank one. They are visibly generated by the two inclusions already mentioned. Since the composition $E_{-3} \hookrightarrow B \to E_{-3}$ is multiplication by 2, the map $B \to E_{-3}$ has no section, and the intersection of E and E_{-3} in B is via the isomorphism $\eta\colon E[2] \simeq E_{-3}[2]$. The upshot is that $B \simeq (E \times E_{-3})/\Delta$, where Δ is the graph of η. By specialization, this is true even if E is isogenous to E_{-3}.

Lemma 2.10. *If $i \in (\mathbb{Z}/2n\mathbb{Z})^\times$, then $B_d \simeq B_{d^i}$ for any $d \in F^\times/F^{\times 2n}$.*

Proof. Let $\mathcal{I}_d = \mathbb{Z}[\zeta]$ with the following twisted Galois action: if $\sigma \in G_F$ and $x \in \mathcal{I}_d$, we define

$$x^{\sigma_d} = \frac{\sqrt[2n]{d}}{\sqrt[2n]{d}^\sigma} x^\sigma,$$

where x^σ is the usual Galois action on $\mathbb{Z}[\zeta]$. Viewing $\mathcal{I}_d$ as a $\mathbb{Z}$-module with a G_F action, we can define the abelian variety $\mathcal{I}_d \otimes_{\mathbb{Z}} E$.

We show that this abelian variety is isomorphic to B_d. Over $F(\sqrt[2n]{d})$, the isomorphism $\mathcal{I}_d \to \mathcal{I}_1 = \mathbb{Z}[\zeta]$ defines an isomorphism $\psi\colon \mathcal{I}_d \otimes_{\mathbb{Z}} E \to B$ by [MRS07, Cor. 1.9]. The cocycle $\psi^\sigma\psi^{-1} \in \mathrm{Aut}(B)$ is the map $\sigma \mapsto \frac{\sqrt[2n]{d}^\sigma}{\sqrt[2n]{d}}$. Indeed, if $x \otimes P \in B$,

then

$$\begin{aligned}\psi^\sigma\psi^{-1}(x\otimes P) &= \sigma\circ\psi\circ\sigma_d^{-1}\circ\psi^{-1}(x\otimes P)\\ &= \sigma\circ\psi\Big(\frac{\sqrt[2n]{d}}{\sqrt[2n]{d}^{\sigma^{-1}}}x^{\sigma^{-1}}\otimes P^{\sigma^{-1}}\Big)\\ &= \frac{\sqrt[2n]{d}^{\sigma}}{\sqrt[2n]{d}}(x\otimes P).\end{aligned}$$

By Kummer theory, this is precisely the cocycle which classifies B_d. Hence, $\mathcal{I}_d\otimes_{\mathbb{Z}} E\simeq B_d$.

Now, as $\mathbb{Z}[G_F]$-modules, there is an isomorphism $\mathcal{I}_d\simeq\mathcal{I}_{d^i}$ given by $-\zeta\mapsto(-\zeta)^i$. Hence, by [MRS07, Cor. 1.9], $B_d\simeq B_{d^i}$. □

Proposition 2.11. *Let $d\in F^\times/F^{\times 2n}$. If d has order $2n$ as an element of $F(\zeta)^\times/F(\zeta)^{\times 2n}$, then $\operatorname{rk}E(K_d/F)^{\text{new}}=\operatorname{rk}B_d(F)$.*

Proof. First suppose that $\zeta\in F$, so that K_d/F is Galois, and let $G=\operatorname{Gal}(K_d/F)$. For this extension, we have $E(K_d/F)^{\text{new}}=E(K_d/F)^{\text{G-new}}$, so we can use the representation-theoretic interpretation of Section 2.1.

By the assumption that d has order $2n$, we have $G\simeq C_{2n}$. Let $\varepsilon\colon G\to\mathbb{C}^\times$ be the character $\sigma\mapsto\sqrt[2n]{d}^{\sigma-1}$, so that the set of faithful irreducible $\mathbb{C}$-valued representations of G is $\{\varepsilon^i : i\in(\mathbb{Z}/2n\mathbb{Z})^\times\}$. By Proposition 2.3 and the subsequent remark, we have

$$E(K_d/F)^{\text{new}}\otimes_{\mathbb{Z}}\mathbb{C}=\bigoplus_{i\in(\mathbb{Z}/2n\mathbb{Z})^\times}V_i,$$

where

$$V_i:=\left\{v\in E(K_d)\otimes_{\mathbb{Z}}\mathbb{C} : \sigma(v)=\varepsilon^i(\sigma)v,\ \forall\sigma\in G\right\}.$$

On the other hand, we can view $B(K_d)$ as a finitely generated $\mathbb{Z}[\zeta][G]$-module. As in the proof of [MRS07, Thm. 2.2], we have $B(K_d)=(E\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta])(K_d)=E(K_d)\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta]$. Hence, as $\mathbb{C}$-vector spaces, we have $B(K_d)\otimes_{\mathbb{Z}[\zeta]}\mathbb{C}=E(K_d)\otimes_{\mathbb{Z}}\mathbb{C}$.

Thus, we may view V_i as a subspace of $B(K_d)\otimes_{\mathbb{Z}}\mathbb{C}$. But since B_{d^i} is the twist of B corresponding to the cocycle ε^i, we have

$$V_i=B_{d^i}(F)\otimes_{\mathbb{Z}[\zeta]}\mathbb{C},$$

and hence

$$\dim_{\mathbb{C}}V_i=\operatorname{rk}_{\mathbb{Z}[\zeta]}B_{d^i}(F)=\frac{1}{2\cdot 3^{m-1}}\operatorname{rk}B_{d^i}(F).$$

It follows that

$$\operatorname{rk}E(K_d/F)^{\text{new}}=\frac{1}{2\cdot 3^{m-1}}\sum_{i\in(\mathbb{Z}/2n\mathbb{Z})^\times}\operatorname{rk}B_{d^i}(F)=\operatorname{rk}B_d(F),$$

where the final equality follows from Lemma 2.10.

Now suppose that $\zeta\notin F$, let $K_d=F(\sqrt[2n]{d})$, and let $N_d=K_d(\zeta)$ be its Galois closure. Then we have $E(N_d/F)^{\text{G-new}}=E(N_d/F(\zeta))^{\text{G-new}}$. Indeed, by assumption, d has order $2n$ in $F(\zeta)^\times/F(\zeta)^{\times 2n}$. Hence, if L/F is a Galois extension with $L\subsetneq N_d$, then $L(\zeta)/F(\zeta)$ is a Galois extension and $L(\zeta)\subsetneq N_d$.

Therefore, as before, we have

$$E(N_d/F)^{\text{G-new}}\otimes\mathbb{C}=E(N_d/F(\zeta))^{\text{G-new}}\otimes\mathbb{C}=\bigoplus_{i\in(\mathbb{Z}/2n\mathbb{Z})^\times}B_{d^i}(F(\zeta))\otimes_{\mathbb{Z}[\zeta]}\mathbb{C}.$$

By Proposition 2.7, we have

$$E(K_d/F)^{\text{G-new}} \otimes \mathbb{C} = (E(N_d/F)^{\text{G-new}} \otimes \mathbb{C})^{\mathrm{Gal}(N_d/K_d)} = \bigoplus_{i \in (\mathbb{Z}/2n\mathbb{Z})^\times} B_{d^i}(F) \otimes_{\mathbb{Z}[\zeta]} \mathbb{C}.$$

It follows that

$$\operatorname{rk} E(K_d/F)^{\text{new}} = \operatorname{rk} E(K_d/F)^{\text{G-new}} = \frac{1}{2 \cdot 3^{m-1}} \sum_{i \in (\mathbb{Z}/2n\mathbb{Z})^\times} \operatorname{rk} B_{d^i}(F) = \operatorname{rk} B_d(F),$$

where the final equality follows from Lemma 2.10. □

3. The average rank of B_d

In this section we prove Theorem 1.1. Let E be as in the theorem and let B be the abelian variety defined in Section 2.3. By Proposition 2.11, to prove Theorem 1.1, it is enough to prove that the average rank of $B_d(F)$ is bounded.

3.1. **Average ranks in cyclotomic twist families.** We recall a general average rank result for a twist family of an abelian variety A/F with ζ-multiplication (see Section 2.2).

There is a natural height function on $F^\times/F^{\times 2n}$, which we now define. Let M_∞ be the set of archimedean places of F. For each $d \in F^\times/F^{\times 2n}$ we choose a lift $d_0 \in F^\times$, and then define the ideal $I = \{a \in F \colon a^{2n} d_0 \in \mathcal{O}_F\}$.

Definition 3.1. The height of d is $H(d) = \mathrm{Nm}(I)^{2n} \prod_{v \in M_\infty} |d_0|_v$.

This definition is independent of the lift d_0, by the product formula. If $F = \mathbb{Q}$, then $H(d) = |d_0|$, where d_0 is the unique $2n$-th power free integer representing d. For any $X > 0$, the set

$$\Sigma_X = \{d \in F^\times/F^{\times 2n} \colon H(d) < X\}$$

is finite. Thus, we can define the average rank of $A_d(F)$ to be

$$\operatorname{avg}_d \operatorname{rk} A_d(F) = \lim_{X \to \infty} \operatorname*{avg}_{d \in \Sigma_X} \operatorname{rk} A_d(F).$$

If the limsup is finite, we say that the *average rank of $A_d(F)$ is bounded*.

Recall from Section 2.2 that there exists an isogeny $\pi \colon A \to A^{(1)}$, which is a descent of $1 - \zeta$ to F. Let $A[\pi]$ denote the kernel of this isogeny.

Theorem 3.2 ([SW21, Thm. 1.1])**.** *Let A be an abelian variety with ζ_{3^m}-multiplication over F. If the G_F-module $A[\pi]$ is a direct sum of characters, then* $\operatorname{avg}_d \operatorname{rk} A_d(F)$ *is bounded.*

3.2. **An isogenous abelian variety.** To apply Theorem 3.2 to the abelian variety B, we would need to know that the G_F-representation $B[\pi]$ is a direct sum of characters. However, Lemma 3.3 shows that this is not the case in general.

Lemma 3.3. *There is an isomorphism of $\mathbb{F}_3[G_F]$-modules $B[\pi] \xrightarrow{\sim} E_{-3}[3]$.*

Proof. By [MRS07, Thm. 2.2], there is a G_F-equivariant isomorphism

$$B[3] \simeq \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} E[3] \simeq \mathbb{Z}[\zeta]/3\mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} E[3].$$

Let $\mathfrak{p} = (1 - \zeta)\mathbb{Z}[\zeta]$, so that $\mathfrak{p}^r = 3\mathbb{Z}[\zeta]$, for $r = 2 \cdot 3^{m-1}$. Then

$$B[\pi] \simeq \mathfrak{p}^{r-1}/\mathfrak{p}^r \otimes_{\mathbb{Z}} E[3] \simeq \mathfrak{p}^{-1}/\mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} E[3].$$

Let $\chi\colon G_F \to \mathbb{Z}_3^\times \hookrightarrow \mathbb{Z}_3[\zeta]^\times$ denote the 3-adic cyclotomic character, and let $\overline{\chi} \equiv \chi \pmod{1-\zeta}$ be the mod 3 cyclotomic character. Using the identity

$$\left(\frac{1-\zeta^{\chi(\sigma)}}{1-\zeta}\right) = 1 + \zeta + \cdots + \zeta^{\chi(\sigma)-1} \equiv \chi(\sigma) \pmod{(1-\zeta)},$$

we see that the G_F-action on the one-dimensional $\mathbb{F}_3$-vector space $\mathfrak{p}^{-1}/\mathbb{Z}[\zeta]$ is by $\overline{\chi}$. Thus,

$$B[\pi] \simeq \overline{\chi} \otimes_{\mathbb{Z}} E[3] \simeq (\overline{\chi} \otimes E)[3] \simeq E_{-3}[3].$$

Explicitly, if $P \in E[3](\overline{F})$, then $\frac{3}{1-\zeta} \otimes P \in B[\pi](\overline{F})$. □

Hence, to apply Theorem 3.2, we instead consider an abelian variety A that is isogenous to B, for which $A[\pi]$ is completely reducible. Recall that E admits a 3-isogeny $\theta\colon E \to E'$. Let $\tau\colon E_{-3}[\theta_{-3}] \hookrightarrow B[\pi]$ be the embedding induced by Lemma 3.3.

Definition 3.4. Define $A = B/\tau(E_{-3}[\theta_{-3}])$.

By [SW21, Lem. 2.6], the fact that $E_{-3}[\theta_{-3}] \subset B[\pi]$ ensures that A also has ζ-multiplication. We use a slight abuse of notation and write $\pi = \pi_A\colon A \to A^{(1)}$ for the descent of $1-\zeta \in \mathrm{End}_{\bar{F}}(A)$ to F.

Lemma 3.5. *There is an isomorphism $A[\pi] \simeq E'_{-3}[\widehat{\theta}_{-3}] \times E[\theta]$ of $\mathbb{F}_3[G_F]$-modules.*

Proof. We can identify $E'_{-3}[\widehat{\theta}_{-3}] \simeq E_{-3}[3]/E_{-3}[\theta_{-3}] \subset A$. Its image in $A[\pi]$ is represented by elements of the form $\frac{3}{1-\zeta} \otimes P$. On the other hand, we can embed $E[\theta] \hookrightarrow A$ by sending Q to the image of $\frac{3}{(1-\zeta)^2} \otimes Q$ in A. This element is evidently killed by π, since $\frac{3}{1-\zeta} \otimes E[\theta]$ is 0 in A. The image of this copy of $E[\theta]$ is also visibly independent of $E'_{-3}[\widehat{\theta}_{-3}]$. □

Proof of Theorem 1.1. By Lemma 3.5, the finite G_F-module $A[\pi]$ is a direct sum of characters. Hence, by Theorem 3.2, the average $\mathrm{avg}_d \operatorname{rk} A_d(F)$ is bounded. Since A_d and B_d are isogenous, it follows that $\mathrm{avg}_d \operatorname{rk} B_d(F)$ is bounded. Now, all but finitely many $d \in F^\times/F^{\times 2n}$ of order $2n$ have order $2n$ in $F(\zeta)$ as well. Indeed, the kernel of the map $F^\times/F^{\times 2n} \to F(\zeta)^\times/F(\zeta)^{\times 2n}$ is isomorphic to $H^1(\mathrm{Gal}(F(\zeta)/F), \mu_{2n})$, which is a finite group. For these d, we have $\operatorname{rk} B_d(F) = \operatorname{rk} E(K_d/F)^{\mathrm{new}}$, by Proposition 2.11, so the average rank of $E(K_d/F)^{\mathrm{new}}$ is indeed bounded. □

4. Intersecting Selmer groups and the correlation trick

We consider a general situation involving twist families of abelian surfaces with ζ_3-multiplication. The main result of the section is Theorem 4.4, which will be used in the proof of Theorem 1.2.

4.1. **Set-up.** Let F be a number field, and let $\zeta = \zeta_3$ be a primitive cube root of unity in $\overline{F}^\times$. Let A/F be an abelian surface with ζ-multiplication, as in Section 2.2. We assume that A admits a polarization $\lambda\colon A \to \widehat{A}$ whose degree is not divisible by 3 and such that the Rosati involution $\alpha \mapsto \lambda^{-1}\widehat{\alpha}\lambda$ on $\mathrm{End}(A)$ restricts to complex conjugation on the subring $\mathbb{Z}[\zeta]$. We also assume that $A[\pi](F) = \langle P, Q\rangle$, or in other words, that $A[\pi]$ has trivial G_F-action.

For each $d \in F^\times$, recall that A_d is the twist of A corresponding to the cocycle $\xi_\sigma = \sqrt[6]{d}^{\sigma-1}$ in $H^1(F, \mu_6)$. The isomorphism $\mathrm{Aut}(A) \to \mathrm{Aut}(\widehat{A})$ sending $f \mapsto \widehat{f}^{-1}$

induces an isomorphism $H^1(F, \mathrm{Aut}(A)) \simeq H^1(F, \mathrm{Aut}(\widehat{A}))$, which we will denote by $\xi \mapsto \widehat{\xi}^{-1}$.

Definition 4.1. Define $(\widehat{A})_d$ to be the twist of $\widehat{A}$ corresponding to the cocycle $\widehat{\xi}^{-1}$.

Lemma 4.2. *Let $\widehat{A}_d$ be the dual of A_d. Then $(\widehat{A})_d \simeq \widehat{A}_d$.*

Proof. Let $f\colon A \to A_d$ be an isomorphism over K. Then, by definition, we have $\xi_\sigma = f^{-1} f^\sigma$. By duality, we have an isomorphism $\widehat{f}\colon \widehat{A}_d \to \widehat{A}$. Consider the cocycle $\widehat{f}(\widehat{f^{-1}})^\sigma$ corresponding to the twist $\widehat{A}_d$. Then

$$\widehat{f}(\widehat{f^{-1}})^\sigma = (\widehat{f^{-1}})^\sigma f = (\widehat{f^{-1} f^{\sigma^{-1}}})^\sigma = \widehat{\xi^\sigma_{\sigma^{-1}}} = \widehat{\xi^{-1}_\sigma}.$$

Here, the final equality comes from the cocyle relation $1 = \xi_1 = \xi^\sigma_{\sigma^{-1}} \xi_\sigma$. Thus, the cocycle corresponding to $\widehat{A}_d$ is $\widehat{\xi}^{-1}$, the same cocycle used to define $(\widehat{A})_d$. It follows that $\widehat{A}_d \simeq (\widehat{A})_d$. □

For each $d \in F^\times$, let $\pi_d\colon A_d \to A_{-27d}$ be the d-th twist of $\pi\colon A \to A^{(1)} = A_{-27}$. The endomorphism $[3]\colon A_d \to A_d$ factors as $u \circ \pi_{-27d} \circ \pi_d$, for some automorphism u. Let $\widehat{\pi}_d\colon \widehat{A}_{-27d} \to \widehat{A}_d$ denote the isogeny dual to π_d.

Lemma 4.3. *We have* $\mathrm{Sel}(\pi_{-27d}) \simeq \mathrm{Sel}(\widehat{\pi}_d)$.

Proof. Let $K = F(\zeta, \sqrt[6]{d})$ and let $f\colon A_K \to (A_d)_K$ be an isomorphism. By [How01, Prop. 2.2] and the condition on the Rosati involution, the polarization $\widehat{f^{-1}} \lambda_K f^{-1}$ of $(A_d)_K$ descends to a polarization of A_d over F, which we will denote by $\lambda_d\colon A_d \to \widehat{A}_d$. Consider the diagram

$$\begin{array}{ccc} A_d & \xrightarrow{\lambda_d} & \widehat{A}_d \\ \downarrow{\scriptstyle \pi_d} & & \downarrow{\scriptstyle \widehat{\pi}_{-27d}} \\ A_{-27d} & \xrightarrow{\lambda_{-27d}} & \widehat{A}_{-27d} \end{array}$$

The definition of λ_d and the condition on the Rosati involution shows that this diagram commutes. In particular, $\mathrm{Sel}(\lambda_{-27d} \circ \pi_d) \simeq \mathrm{Sel}(\widehat{\pi}_{-27d} \circ \lambda_d)$, and since λ_d is prime-to-3, it follows that $\mathrm{Sel}(\pi_d) \simeq \mathrm{Sel}(\widehat{\pi}_{-27d})$. □

By the Lemma and the equality $[3] = u \circ \pi_{-27} \circ \pi_d$, to control $\mathrm{Sel}_3(A_d)$ it is enough to control the two Selmer groups $\mathrm{Sel}(\pi_d)$ and $\mathrm{Sel}(\widehat{\pi}_d)$.

4.2. **Selmer ratios.** Let $\alpha\colon X \to Y$ be an isogeny of abelian varieties over F. The global Selmer ratio of α is by definition the product $c(\alpha) = \prod_v c_v(\alpha)$ of local Selmer ratios

$$c_v(\alpha) = \frac{\#\mathrm{coker}\,(X(F_v) \to Y(F_v))}{\#\ker\,(X(F_v) \to Y(F_v))},$$

one for each place v of F. If $\deg(\alpha)$ is a power of 3, then for $v \nmid 3\infty$, we have $c_v(\alpha) = c_v(Y)/c_v(X)$, where $c_v(X)$ is the Tamagawa number of X over F_v [Sch96, Lem. 3.8]. Thus, up to some subtle factors at places v above 3 and ∞, the number $c(\alpha)$ is the ratio of the global Tamagawa numbers $c(Y)/c(X)$. In particular, we have $c_v(\alpha) \in 3^{\mathbb{Z}}$, and $c_v(\alpha) = 1$ for all but finitely many v.

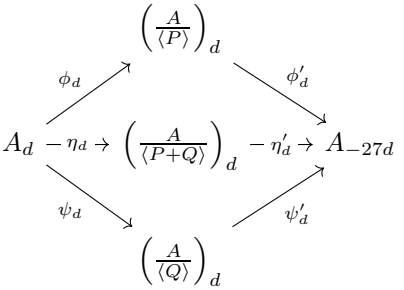
Let $\widehat{\alpha}\colon \widehat{Y} \to \widehat{X}$ be the dual isogeny. Then the Greenberg-Wiles formula [NSW08, 8.7.9] reads

$$c(\alpha) = \frac{\#\operatorname{Sel}(\alpha)}{\#\operatorname{Sel}(\widehat{\alpha})} \cdot \frac{\#\widehat{Y}[\widehat{\alpha}](F)}{\#X[\alpha](F)}. \tag{4.1}$$

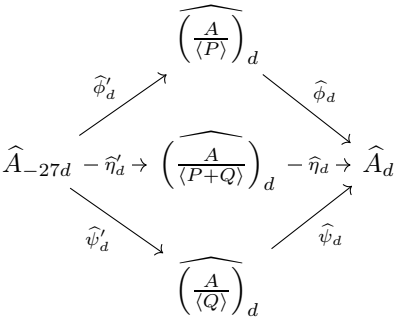
4.3. **The correlation trick.** By Lemma 4.3, we have

(4.2)
$$\operatorname{rk} A_d(F) \le \dim_{\mathbb{F}_3} \operatorname{Sel}_3(A_d) \le \dim_{\mathbb{F}_3}(\operatorname{Sel}(\pi_d) \oplus \operatorname{Sel}(\pi_{-27d})) = \dim_{\mathbb{F}_3}(\operatorname{Sel}(\pi_d) \oplus \operatorname{Sel}(\widehat{\pi}_d)).$$

Now, since $A[\pi](F) = \langle P, Q\rangle$, we can factor π_d in multiple ways as a chain of 3-isogenies:



and by duality, we obtain a corresponding factorisation for $\widehat{\pi}$:



Theorem 4.4 is the main result of this section:

Theorem 4.4. *Let A/F be as above. Suppose that the set*

$$T = \{d \in F^\times/F^{\times 6} : c(\phi_d) = c(\phi'_d) = c(\psi_d) = c(\psi'_d) = 1\}$$

has positive density. Then for a positive lower density of $d \in F^\times/F^{\times 6}$, we have $\operatorname{rk} A_d(F) = 0$.

Lemma 4.5 ([SW21, Lem. 6.2])**.** *Let F be any field, and suppose that there is a commutative diagram of isogenies of abelian varieties over F,*

$$\begin{array}{ccc} A & \xrightarrow{\phi_1} & B_1 \\ \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \psi_2} \\ B_2 & \xrightarrow{\psi_1} & C \end{array}$$

such that ϕ_2 maps $A[\phi_1]$ isomorphically onto $B_2[\psi_1]$. Then ψ_2 induces an injection

$$\frac{B_1(F)}{\phi_1(A(F))} \hookrightarrow \frac{C(F)}{\psi_1(B_2(F))}.$$

As a consequence, if F is a number field, then the map ϕ_2 induces an embedding $\mathrm{Sel}(\phi_1) \hookrightarrow \mathrm{Sel}(\psi_1)$.

Corollary 4.6. *For almost all $d \in T$, we have* $\mathrm{Sel}(\phi_d) = \mathrm{Sel}(\psi'_d)$ *and* $\mathrm{Sel}(\phi'_d) = \mathrm{Sel}(\psi_d)$.

Proof. By Lemma 4.5, we have $\mathrm{Sel}(\phi_d) \hookrightarrow \mathrm{Sel}(\psi'_d)$ and $\mathrm{Sel}(\widehat{\psi}'_d) \hookrightarrow \mathrm{Sel}(\widehat{\phi}_d)$. For almost all $d \in T$, the abelian varieties in the diagram have no non-trivial rational 3-torsion points, so by (4.1) we have $\#\mathrm{Sel}(\phi_d) = \#\mathrm{Sel}(\widehat{\phi}_d)$ and $\#\mathrm{Sel}(\psi'_d) = \#\mathrm{Sel}(\widehat{\psi}'_d)$. Thus

$$\#\mathrm{Sel}(\phi_d) \leq \#\mathrm{Sel}(\psi'_d) = \#\mathrm{Sel}(\widehat{\psi}'_d) \leq \#\mathrm{Sel}(\widehat{\phi}_d) = \#\mathrm{Sel}(\phi_d).$$

It follows that $\mathrm{Sel}(\phi_d) = \mathrm{Sel}(\psi'_d)$. The proof of the second equality is identical. □

Proof of Theorem 4.4. By [SW21, Thm. 5.2], we have

$$\mathrm{avg}_{d\in T} \#\mathrm{Sel}(\phi_d) = \mathrm{avg}_{d\in T} \#\mathrm{Sel}(\phi'_d) = 2,$$

and by [SW21, Thm. 5.3], $\mathrm{avg}_{d\in T} \#\mathrm{Sel}(\eta_d) > 1$. Let $\min_d = \min(\#\mathrm{Sel}(\phi_d), \#\mathrm{Sel}(\phi'_d))$ and $\max_d = \max(\#\mathrm{Sel}(\phi_d), \#\mathrm{Sel}(\phi'_d))$. By Lemma 4.5 and the above diagram, we have $\#\mathrm{Sel}(\eta_d) \leq \#\mathrm{Sel}(\phi'_d)$ and $\#\mathrm{Sel}(\eta_d) \leq \#\mathrm{Sel}(\psi'_d)$ for almost all $d \in T$. Therefore, by Corollary 4.6, we have $\#\mathrm{Sel}(\eta_d) \leq \min_d$ for almost all $d \in T$. Hence $\liminf \mathrm{avg}_{d\in T} \min_d > 1$, where

$$\liminf \mathrm{avg}_{d\in T} \min_d := \liminf_{X\to\infty} \frac{\sum_{d\in T, |d|\leq X} \min_d}{\sum_{d\in T, |D|\leq X} 1}.$$

On the other hand, we have

$$\begin{aligned} 4 &= \mathrm{avg}_{d\in T} \#\mathrm{Sel}(\phi_d) + \mathrm{avg}_{d\in T} \#\mathrm{Sel}(\phi'_d) \\ &= \mathrm{avg}_{d\in T}(\min_d + \max_d) \\ &\geq \liminf \mathrm{avg}_{d\in T} \min_d + \liminf \mathrm{avg}_{d\in T} \max_d \\ &> 1 + \liminf \mathrm{avg}_{d\in T} \max_d, \end{aligned}$$

so that $\liminf \mathrm{avg}_{d\in T} \max_d < 3$. This immediately implies that for a positive lower density of twists $d \in T$, we have

$$\#\mathrm{Sel}(\phi_d) = \#\mathrm{Sel}(\phi'_d) = 1.$$

More quantitatively, let s_0 be the proportion of $d \in T$ such that $\max_d = 1$. Then

$$s_0 + 3(1 - s_0) < 3 \tag{4.3}$$

and hence $s_0 > 0$. By the Greenberg–Wiles formula and the definition of T, we have $\#\mathrm{Sel}(\widehat{\phi}_d) = \#\mathrm{Sel}(\widehat{\phi}'_d) = 1$ for almost all such d as well. By (4.2), we have $\#\mathrm{Sel}_3(A_d) = 1$ for all such d, and hence $\mathrm{rk}\, A_d(F) = 0$ as well. □

Remark 4.7. Suppose that for some $m \in \mathbb{Z}_{\geq 0}$, $c(\eta_d) \geq 3^{-m}$ for all $d \in T$. Then, by [SW21, Thm. 5.2], we have $\mathrm{avg}_{d\in T} \#\mathrm{Sel}(\eta_d) \geq 1 + 3^{-m}$, and (4.3) becomes

$$s_0 + 3(1 - s_0) \leq 3 - 3^{-m}.$$

It follows that $s_0 \geq \frac{1}{2\cdot 3^m}$.

5. Proof of Theorem 1.2

Recall that $E\colon y^2+axy+by=x^3$ is an elliptic curve over $\mathbb{Q}$ with a point $(0,0)$ of order 3. Let $\theta\colon E\to E'=E/\langle(0,0)\rangle$ be the corresponding 3-isogeny. Let $\zeta=\zeta_3$ be a primitive cube root of unity. In Definition 3.4, we defined an abelian variety $A/\mathbb{Q}$ with ζ-multiplication, such that for each $d\in\mathbb{Q}^\times/\mathbb{Q}^{\times 6}$, the rank of $A_d(\mathbb{Q})$ is equal to $\operatorname{rk} E(K_d/\mathbb{Q})^{\mathrm{new}}$ (see Proposition 2.11). To prove Theorem 1.2, we will show that $\operatorname{rk} A_d(\mathbb{Q})=0$ for a positive proportion of twists.

By Lemma 3.5, we have $A[\pi]\simeq E'_{-3}[\widehat{\theta}_{-3}]\times E[\theta]$. We have $E[\theta]=\langle(0,0)\rangle$, and by duality, we have $E[\theta]\simeq E'_{-3}[\widehat{\theta}_{-3}]$ as G_F-modules. Let P and Q denote the images in $A[\pi]$ of generators of $E[\theta]$ and $E'_{-3}[\widehat{\theta}_{-3}]$. Then $A[\pi](\mathbb{Q})=\langle P,Q\rangle$, and we are in the setting of Theorem 4.4. Before proceeding, we need to verify that A admits a prime-to-3 polarization satisfying the assumptions of Theorem 4.4.

Lemma 5.1. *Let C be the hyperelliptic curve $y^2=x^6+\alpha x^3+1$, where $\alpha=108b/a^3-2$. Then $A\simeq\operatorname{Jac}(C)$ and the ζ-multiplication on A is induced from the order 3 automorphism $(x,y)\mapsto(\zeta x,y)$ of C.*

Proof. Set $E^+=E$ and $E^-=E'_{-3}$. It is convenient to use the following symmetric models

$$E^\pm\colon y^2=x^3+(3x+2\pm\alpha)^2.$$

The double covers $f_\pm\colon C\to E^\pm$ given by

$$(x:y:z)\mapsto\left(\frac{(\alpha\pm2)xz}{(x\mp z)^2},\frac{(\alpha\pm2)y}{(x\mp z)^3}\right)$$

may be used to define a morphism $f=f_+^*-f_-^*\colon E^+\times E^-\to\operatorname{Pic}^0(C)\simeq\operatorname{Jac}(C)$, by pullback of divisors. Note that C has an involution $\tau\colon(x:y:z)\mapsto(z:y:x)$ and the two double covers above are the quotients by τ and $\iota\tau$, where ι is the hyperelliptic involution. The kernel of f is therefore the intersection $f_+^*E^+\cap f_-^*E^-$, consisting of divisors fixed by both of these involutions. Thus, the kernel is precisely $f_+^*E^+[2]\cap f_-^*E^-[2]$. Hence, $\operatorname{Jac}(C)\simeq(E^+\times E^-)/\Gamma$, where Γ is the graph of the isomorphism $E^+[2]\simeq E^-[2]$.

On the other hand, the abelian surface $B=\mathbb{Z}[\zeta]\otimes E$ is isomorphic to $(E\times E_{-3})/\Delta$, where Δ is the graph of $E[2]\simeq E_{-3}[2]$, by Example 2.9. This gives the claimed isomorphism

$$A\simeq B/E_{-3}[\theta_{-3}]\simeq(E^+\times E^-)/\Gamma\simeq\operatorname{Jac}(C).$$

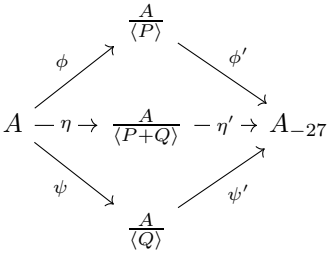
To see that the ζ-actions match up, it is enough to show that $A[1-\zeta]$ maps to $\operatorname{Jac}(C)[1-\zeta]$ (for the respective automorphisms ζ on each) under the above isomorphism. By Lemma 3.5, we have $A[1-\zeta]\simeq E^+[\theta^+]\times E^-[\theta^-]$. This is also $\operatorname{Jac}(C)[1-\zeta]$, since the divisors fixed by ζ are generated by the difference of the four points on C where $xz=0$, and these visibly map to θ-torsion points of $E^\pm$, since these are the points where $x=0$. □

Remark 5.2. The genus two curves $y^2=x^6+\alpha x^3+1$ were considered in [BFT14], where it is remarked that these are precisely the genus two curves with two independent 3-torsion divisors supported on at most 4 points.

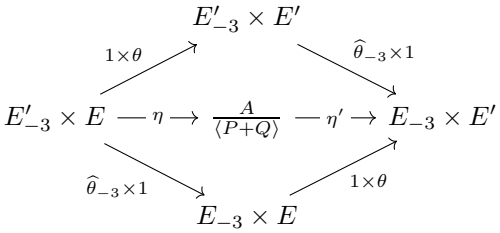
Corollary 5.3. *A is principally polarized and its polarization is preserved by ζ.*

To say that the principal polarization $\lambda\colon A \to \widehat{A}$ is preserved by ζ is equivalent to the condition that the corresponding Rosati involution on $\mathrm{End}(A)$ restricts to complex conjugation on $\mathbb{Z}[\zeta]$. Thus, A satisfies the conditions of Theorem 4.4.

Recall the commutative diagram



from Theorem 4.4. Up to 2-isogenies, this diagram becomes



Let $\mathfrak{f}$ be the conductor of E and let Σ be the set of integers d such that:

- For all p, we have $v_p(d) \in \{0, 1, 3, 5\}$.
- If $p \mid 3\mathfrak{f}$, then $d \in \mathbb{Q}_p^{\times 3}$.

In the next few lemmas, we compute the local Selmer ratios $c_p(\phi_d)$, $c_p(\phi'_d)$, $c_p(\psi_d)$, and $c_p(\psi'_d)$, for all p and all $d \in \Sigma$.

Lemma 5.4. *If $d \in \Sigma$ and if $p \nmid 3\mathfrak{f}d$, then $c_p(\phi_d) = c_p(\phi'_d) = c_p(\psi_d) = c_p(\psi'_d) = 1$*

Proof. By [Sch96, Lem. 3.8], we have $c_p(\phi_d) = \frac{c_p(B_d)}{c_p(A_d)}$, where $c_p(B_d)$ and $c_p(A_d)$ are the local Tamagawa numbers. Since A_d and B_d have good reduction at p, this equals 1. The remaining cases are identical. □

Lemma 5.5. *If $d \in \Sigma$ and if $p \mid d$, then $c_p(\phi_d) = c_p(\phi'_d) = c_p(\psi_d) = c_p(\psi'_d) = c_p(\eta_d) = 1$*

Proof. Let $\alpha \in \{\phi, \phi', \psi, \psi', \eta\}$. By assumption, $A[\alpha]$ is trivial is a $G_{\mathbb{Q}}$-module. Hence, $A_d[\alpha_d] \simeq \chi_d$, where $\chi_d\colon G_{\mathbb{Q}} \to \mathbb{F}_3^{\times}$ is the quadratic character cutting out $\mathbb{Q}_p(\sqrt{d})$, which is non-trivial, since $v_p(d)$ is odd. Hence, the image of the Kummer map lies in $H^1(\mathbb{Q}_p, \chi_d)$, which by [SW21, Lem. 4.6], is trivial. Similarly, since d is not a square, $A_d[\alpha_d](\mathbb{Q}_p) = 0$. Hence, $c_p(\alpha_d) = 1$. □

Lemma 5.6. *If $d \in \Sigma$ and $p \mid 3\mathfrak{f}$, we have $c_p(\phi_d) = c_p(\psi'_d) = c_p(\theta_d)$ and $c_p(\psi_d) = c_p(\phi'_d) = c_p(\widehat{\theta}_{-3d})$. Here, θ_d is the d-th quadratic twist of $\theta\colon E \to E'$.*

Proof. The condition that $d \in \mathbb{Q}_p^{\times 3}$ implies that over $\mathbb{Q}_p$, all the abelian varieties in the above diagram are isogenous to products of elliptic curves. For example, up to 2-isogenies, we have $A_d \approx E_d \times E'_{-3d}$ and $\phi_d \approx 1 \times \theta_d$, and so $c_p(\phi_d) = c_p(\theta_d)$. The other equalities follow by an identical analysis. □

Corollary 5.7. *For all $d \in \Sigma$ and for all p, we have $c_p(\phi_d) = c_p(\psi'_d)$ and $c_p(\phi'_d) = c_p(\psi_d)$.*

Proof. This follows from the previous three lemmas. □

Lemma 5.8. *We have $c_3(\phi_d) = 1$ and $c_3(\phi'_d) = 3$ for all $d \in \Sigma$.*

Proof. Since d is a cube in $\mathbb{Q}_3$, we have $c_3(\phi_d) = c_3(\theta_d)$ and $c_3(\phi'_d) = c_3(\widehat{\theta}_{-3d})$. By [Sch96, Lem. 3.8], we have $c(\theta_d) = c(E'_d)/c(E_d)\gamma$, where γ^{-1} is the normalized absolute value of the determinant of the map $\mathrm{Lie}(\mathcal{E}) \to \mathrm{Lie}(\mathcal{E}')$ on tangent spaces of the Néron models over $\mathbb{Z}_p$.

Since $3 \nmid ab$, E has good reduction over $\mathbb{Q}_3$. The 3-torsion point $(0,0)$ on E reduces to a non-trivial point in $E(\mathbb{F}_3)$, so the reduction is ordinary. It follows from [BKLOS19, Thm. 10.5] that $c(E'_d)/c(E_d) = 1$ and $\gamma = 1$. We therefore have $c_3(\phi_d) = 1$. For $c_3(\phi'_d)$ the argument is similar, except the generator of $\ker(\phi'_d) \simeq \ker(\widehat{\theta}_{-3d})$ reduces to the identity over $\mathbb{F}_3$ (since over $\overline{\mathbb{F}}_3$, the kernel is the Cartier dual of $\mathbb{Z}/3\mathbb{Z}$, which is μ_3) and so $\gamma^{-1} = 3$ and $c_3(\phi'_d) = 3$. □

Lemma 5.9. *We have* $c_\infty(\phi_d) = c_\infty(\phi'_d) = c_\infty(\eta_d) = \begin{cases} \frac{1}{3} & d > 0 \\ 1 & d < 0. \end{cases}$

Proof. Write $B = \frac{A}{\langle P \rangle}$. The numerator of $c_\infty(\phi_d)$ is equal to $\#\,\mathrm{im}(B_d(\mathbb{R}) \to H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), A_d[\phi_d]))$. Since $\#A_d[\phi_d] = 3$ is odd, we have $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), A_d[\phi_d]) = 0$, so this numerator is 1. The denominator is $\#A_d[\phi_d](\mathbb{R})$ which is 3 if and only if d is a square in $\mathbb{R}$, i.e. if $d > 0$. The arguments for ϕ'_d and η_d are identical. □

Lemma 5.10. *Let $d \in \Sigma$. If $p \nmid 3d$ divides $\mathfrak{f}$, then $c_p(\phi_d)$ and $c_p(\phi'_d)$ are as in the following table:*

		$p \mid a^3 - 27b$		$p \mid b$	
		$c_p(\phi_d)$	$c_p(\phi'_d)$	$c_p(\phi_d)$	$c_p(\phi'_d)$
$p = 2$	$d \in \mathbb{Z}_p^{\times 2}$	1	$\frac{1}{3}$	$\frac{1}{3}$	1
	$-3d \in \mathbb{Z}_p^{\times 2}$	3	1	1	3
	$d, -3d \notin \mathbb{Z}_p^{\times 2}$	1	1	1	1
$p \equiv 1 \pmod 3$	$d \in \mathbb{Z}_p^{\times 2}$	3	$\frac{1}{3}$	$\frac{1}{3}$	3
	$d \notin \mathbb{Z}_p^{\times 2}$	1	1	1	1
$p \equiv 2 \pmod 3$	$d \in \mathbb{Z}_p^{\times 2}$	1	$\frac{1}{3}$	$\frac{1}{3}$	1
	$d \notin \mathbb{Z}_p^{\times 2}$	3	1	1	3

Proof. As before, since $d \in \Sigma$, we have $c_p(\phi_d) = c_p(\theta_d)$ and $c_p(\phi'_d) = c_p(\widehat{\theta}_{-3d})$. The assumption that $(a,b) = 1$ ensures that E is semistable (as we will see momentarily), and hence has multiplicative reduction (since $p \mid \mathfrak{f}$, by assumption). We need to determine whether E has split or non-split multiplicative reduction.

First suppose that $p \neq 2$. We have $E\colon y^2 + axy + by = x^3$. If $p \mid b$, then modulo p, E has equation

$$\left(Y - \frac{ax}{2}\right)\left(Y + \frac{ax}{2}\right) = x^3,$$

where $Y = y + \frac{ax}{2}$, i.e. E has split multiplicative reduction. Similarly, if $p \mid a^3 - 27b$, then modulo p, E has equation

$$Y^2 + \frac{a^2}{12}X^2 = X^3$$

with $Y = y + \frac{1}{2}(ax + b)$ and $X = x + \frac{a^2}{9}$. Thus E has split multiplicative reduction if and only if -3 is a square in $\mathbb{Q}_p$, i.e. if $p \equiv 1 \pmod 3$.

When $p = 2$, we compute that $\frac{-c_4}{c_6} \equiv 1 \pmod 8$ when $2 \mid b$, and $\frac{-c_4}{c_6} \equiv -3 \pmod 8$ when $2 \mid a^3 - 27b$. By Hensel's lemma, $\frac{-c_4}{c_6}$ is a square in $\mathbb{Q}_2$ if and only if it is a square in $\mathbb{Z}/8\mathbb{Z}$. From this, one checks that if $2 \mid b$, then E has split multiplicative reduction, while if $2 \mid a^3 - 27b$, then E_{-3} has split multiplicative reduction.

We see that E_d and E'_d have non-split multiplicative reduction whenever $p \mid b$ and $d \notin \mathbb{Q}_p^{\times 2}$ or $p \mid a^3 - 27b$ and $-3d \notin \mathbb{Q}_p^{\times 2}$. In such cases, $c(\phi_d) = c(\theta_d) = 1$ by [BKLOS19, Prop. 10.4].

Otherwise, the formula in *loc. cit.* gives $c_p(\theta_d) = \frac{v_p(j(E'_d))}{v_p(j(E_d))} = \frac{v_p(j(E'))}{v_p(j(E))}$. We have

$$j(E) = \frac{a^3(a^3 - 24b)^3}{b^3(a^3 - 27b)} \text{ and } j(E') = \frac{a^3(a^3 + 216b)^3}{b(a^3 - 27b)^3}.$$

Since $p \neq 3$ and $(a, b) = 1$, p can only divide the denominator of these j-invariants, and the remaining entries for $c_p(\phi_d)$ are easily computed. To compute the entries for $c_p(\phi'_d)$, we use the fact that

$$c_p(\phi'_d) = c_p(\widehat{\theta}_{-3d}) = c_p(\theta_{-3d})^{-1} = c_p(\phi_{-3d})^{-1},$$

so that the values of $c_p(\phi'_d)$ can be computed using the values of $c_p(\phi_{-3d})$. □

Proof of Theorem 1.2. Let A be the abelian surface defined in Definition 3.4, with $m = 1$. Let Σ be the set of integers defined above. For 100% of $d \in \Sigma$, d has order 6 in $\mathbb{Q}(\zeta_3)^\times/\mathbb{Q}(\zeta_3)^{\times 6}$. Hence, by Proposition 2.11, we have $\operatorname{rk} E(K_d/\mathbb{Q})^{\text{new}} = \operatorname{rk} A_d(\mathbb{Q})$ for such d. Thus, it is sufficient to show that $\operatorname{rk} A_d(\mathbb{Q}) = 0$ for a positive proportion of d in Σ.

By Corollary 5.3 and Lemma 3.5, we are in the setting of Theorem 4.4. Hence, it is sufficient to show that the set T in the statement of Theorem 4.4 has positive density.

Define a subset $T' \subset \Sigma$ as follows, based on the two possible cases considered in the theorem:

(i) Suppose that there exists a prime $q \equiv 2 \pmod 3$ with $q \mid a^3 - 27b$. Then $d \in T'$ if and only if:
- if $p \mid \mathfrak{f}$ and $p \neq q$, then
  - if $p = 2$, then either $2 \mid d$ or $d, -3d \notin \mathbb{Z}_2^{\times 2}$.
  - if $p \equiv 1 \pmod 3$, then $p \mid d$ or $d \notin \mathbb{Z}_p^{\times 2}$.
  - if $p \equiv 2 \pmod 3$, then $p \mid d$.
- either $d < 0$ and $d \in \mathbb{Z}_q^{\times 2}$, or $d > 0$ and $-3d \in \mathbb{Z}_q^{\times 2}$.

(ii) Suppose that there exist primes $q_1 \equiv 1 \pmod 3$ and $q_2 \equiv 2 \pmod 3$ such that $q_1 \mid a^3 - 27b$ and $q_2 \mid b$. Then $d \in T'$ if and only if:
- if $p \mid \mathfrak{f}$ and $p \notin \{q_1, q_2\}$, then
  - if $p = 2$, then either $2 \mid d$ or $d, -3d \notin \mathbb{Z}_2^{\times 2}$.
  - if $p \equiv 1 \pmod 3$, then $p \mid d$ or $d \notin \mathbb{Z}_p^{\times 2}$.
  - if $p \equiv 2 \pmod 3$, then $p \mid d$.

- $d \in \mathbb{Z}_{q_1}^{\times 2}$.
- either $d < 0$ and $d \in \mathbb{Z}_{q_2}^{\times 2}$, or $d > 0$ and $-3d \in \mathbb{Z}_{q_2}^{\times 2}$.

By Lemmas 5.4–5.5 and 5.8–5.10, we have $c(\phi_d) = c(\phi'_d) = 1$, for all $d \in T'$. By Corollary 5.7, we see that $c(\psi_d) = c(\psi'_d) = 1$ as well. Hence, $T' \subset T$. Since T' has positive density, the result follows from Theorem 4.4. □

5.1. **An explicit example.** Consider the elliptic curve $E\colon y^2 + 2xy - y = x^3$ of conductor 35. Then E satisfies hypothesis (i) of Theorem 1.2. We compute a lower bound on the proportion of d such that $\operatorname{rk} E(K_d/\mathbb{Q})^{\text{new}} = 0$. In this case, we can assume for simplicity that d is squarefree.[3]

Proposition 5.11. *Let T be the set of squarefree integers d such that all of the following hold:*

- $d \equiv \pm 1, \pm 8, \pm 10 \pmod{27}$*;*
- $d \equiv -1, 0 \pmod 7$*;*
- *if $d < 0$, then $d \equiv \pm 1 \pmod 5$; and*
- *if $d > 0$, then $d \equiv \pm 2 \pmod 5$.*

Then for a proportion of at least $1/18$ elements $d \in T$, we have $\operatorname{rk} E(K_d/\mathbb{Q})^{\text{new}} = 0$.

Proof. Observe that T is the set of squarefree integers d such that:

- $d \in \mathbb{Z}_3^{\times 3}$;
- either $7 \mid d$ or $d \in \mathbb{Z}_7^{\times 3} \setminus \mathbb{Z}_7^{\times 6}$;
- if $d < 0$, then $d \in \mathbb{Z}_5^{\times 6}$; and
- if $d > 0$ then $d \in \mathbb{Z}_5^{\times 3} \setminus \mathbb{Z}_5^{\times 6}$.

The set T is contained in the set T' defined in part (i) of the proof of Theorem 1.2. Hence, T is contained in the set in the statement of Theorem 4.4.

Let η, ϕ, ϕ' be the isogenies from the above commutative diagram. We compute the Selmer ratio $c(\eta_d)$ for $d \in T$. By Lemma 5.5, we have $c_p(\eta_d) = 1$ for all $d \in T$, unless $p \in \{3, 5, 7, \infty\}$. Moreover,

$$c_p(\eta_d) = \frac{\#\operatorname{coker} \eta_d(\mathbb{Q}_p)}{\#\ker \eta_d(\mathbb{Q}_p)} \geq \frac{1}{\#A_d[\eta_d](\mathbb{Q}_p)}.$$

Now $\#A_d[\eta_d](\mathbb{Q}_p) = 1$ if and only if $d \notin \mathbb{Q}_p^{\times 2}$. If $d \in T$, then $d \notin \mathbb{Q}_7^{\times 2}$. Thus $c_7(\eta_d) \geq 1$. Otherwise, we have $c_3(\eta_d) \geq \frac{1}{3}$ and $c_\infty(\eta_d)c_5(\eta_d) \geq \frac{1}{3}$. Thus, for all $d \in T$, we have $c(\eta_d) \geq \frac{1}{9}$.

By [SW21, Thm. 5.2], we have $\operatorname{avg}_{d\in T} \#\operatorname{Sel}(\eta_d) \geq 1 + \frac{1}{9}$. On the other hand, as in the proof of Theorem 4.4 (see also Remark 4.7), we have

$$1 + \frac{1}{9} \leq \operatorname{avg}_{d\in T} \#\operatorname{Sel}(\eta_d) \leq \operatorname{avg}_{d\in T} \min_d = 4 - \operatorname{avg}_{d\in T} \max_d,$$

where $\min_d = \min(\#\operatorname{Sel}(\phi_d), \#\operatorname{Sel}(\phi'_d))$ and $\max_d = \max(\#\operatorname{Sel}(\phi_d), \#\operatorname{Sel}(\phi'_d))$. Hence

$$\operatorname{avg}_{d\in T} \max_d \leq 3 - \frac{1}{9}.$$

Let s_0 be the proportion of $d \in T$ with $\max_d = 1$. Then

$$s_0 + 3(1 - s_0) \leq \operatorname{avg}_{d\in T} \max_d \leq 3 - \frac{1}{9}$$

[3]For elliptic curves with many odd primes $p \equiv 2 \pmod 3$ of bad reduction, we must consider sets T' which are not contained in the set of squarefree integers, as in the proof of Theorem 1.2. In this example, we can restrict to just squarefree integers, as there is only one such prime.

from which it follows that $s_0 \geq \frac{1}{18}$.

We see that for a set of $d \in T$ of relative density $\frac{1}{18}$, we have $\max_d = 1$, i.e. $\#\operatorname{Sel}(\phi_d) = \#\operatorname{Sel}(\phi'_d) = 1$. As in the proof of Theorem 4.4, we see that $\operatorname{rk} E(K_d/\mathbb{Q})^{\mathrm{new}} = 0$ for such d. □

6. Application to Hilbert's tenth problem over pure sextic fields

Before giving the proof of Theorem 1.3, we recall from [GFP20] some facts related to diophantine sets over a ring R (i.e. sets characterized as solutions to polynomial equations over R) and Hilbert's tenth problem over number fields.

Definition 6.1. We say that a subset $S \subset R^n$ is *diophantine* over R if there exist integers k, m and polynomials $F_1, \dots, F_k \in R[x_1, \dots, x_n, y_1, \dots, y_m]$ that satisfy the following property: $(a_1, \dots a_n) \in S$ if and only if there exists an element $(b_1, \dots, b_m) \in A^m$ such that for every $j = 1, \dots, k$, we have $F_j(a_1, \dots, a_n, b_1, \dots, b_m) = 0$.

Definition 6.2. An extension K/F is *integrally diophantine* if $\mathcal{O}_F$ is diophantine in $\mathcal{O}_K$.

It is well-known that if $K/\mathbb{Q}$ is integrally diophantine, then Hilbert's tenth problem has a negative solution over $\mathcal{O}_K$, so we aim to show that many pure sextic fields are integrally diophantine. Such sextic fields contain subfields, and we will use:

Lemma 6.3 ([GFP20, Lem. 3.1])**.** *The property of being integrally diophantine is transitive in towers of number fields.*

We will also use the following result of Shlapentokh [Shl08]:

Theorem 6.4. *Let K/F be a finite extension of number fields. If there exists an elliptic curve E/F such that $\operatorname{rk} E(F) = \operatorname{rk} E(K) > 0$, then K/F is integrally diophantine.*

As well as a recent result of Smith [Smi20]:

Theorem 6.5. *Let $E/\mathbb{Q}$ be an elliptic curve with $E[2](\mathbb{Q}) \not\simeq \mathbb{Z}/2\mathbb{Z}$. Then for 100% of integers d, we have $\operatorname{rk} E_d = (-1)^{\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E_d)}$, where E_d is the d-th quadratic twist of E. In particular, for 100% of integers d, if E_d has even 2-Selmer rank, then $\operatorname{rk} E(\mathbb{Q}(\sqrt{d})) = \operatorname{rk} E(\mathbb{Q})$.*

Proof of Theorem 1.3. Let $E = E_{a,b}$ be an elliptic curve over $\mathbb{Q}$ satisfying the conditions of Theorem 1.2 and having positive rank. We also insist that $E[2](\mathbb{Q}) \not\simeq \mathbb{Z}/2\mathbb{Z}$. For example, we may take $E = E_{4,-5}\colon y^2 + 4xy - 5y = x^3$. Theorem 1.2 gives that for a set of positive lower density $\Sigma \subset \mathbb{Z}$ of sixth-power-free integers d, the new rank of E/K_d is 0, where $K_d = \mathbb{Q}(\sqrt[6]{d})$.

Lemma 6.6. *For all $d \in \Sigma$, the 2-Selmer group $\operatorname{Sel}_2(E_d)$ has even $\mathbb{F}_2$-dimension.*

Proof. Let $\theta_d\colon E_d \to E'_d$ be the 3-isogeny. By the construction in the proof of Theorem 1.2, the Selmer ratio $c(\theta_d) = \prod_p c_p(\theta_d) = \prod_p c_p(\phi_d) = c(\phi_d)$ is equal to 1 for all $d \in \Sigma$. Indeed, if $p \mid 3\mathfrak{f}$, where $\mathfrak{f}$ is the conductor of E, then $c_p(\theta_d) = c_p(\phi_d)$ by Lemma 5.6. And if $p \nmid 3\mathfrak{f}$, then $c_p(\theta_d) = c_p(\phi_d) = 1$ by the same arguments as Lemmas 5.4 and 5.5. The formula

$$\log_3 c(\theta_d) \equiv \dim_{\mathbb{F}_3} \operatorname{Sel}_3(E_d) - \dim_{\mathbb{F}_3} E_d[3](\mathbb{Q}) \pmod 2$$

(see [BES20, Prop. 49(b)]) shows that $\dim_{\mathbb{F}_3} \mathrm{Sel}_3(E_d)$ is even for all but finitely many $d \in \Sigma$. By the 3- and 2-parity theorems (due to Dokchitser–Dokchitser [DD10] and Monsky [Mon96], respectively), it follows that $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d)$ is also even. □

Hence by Theorem 6.5, the rank of E_d is 0 for 100% of $d \in \Sigma$. Let $F = \mathbb{Q}(\sqrt[3]{d})$. Since $\mathrm{rk}\, E(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}\, E(\mathbb{Q})$ and $\mathrm{rk}\, E(K_d/\mathbb{Q})^{\mathrm{new}} = 0$, we see that $0 < \mathrm{rk}\, E(F) = \mathrm{rk}\, E(K_d)$, and hence K_d/F is integrally diophantine by Theorem 6.4. Since every cubic field (or more generally, any number field with at most one complex place) is known to be integrally diophantine, it follows from Lemma 6.3 that $K_d/\mathbb{Q}$ is integrally diophantine as well. Hence Hilbert's tenth problem has a negative solution over $\mathcal{O}_{K_d}$. □

7. Ranks of QM abelian surfaces

We recall some facts from [SW21, §10] and then give a proof of Theorem 1.4.

Let $a > b$ be distinct positive integers, and let $f(x) = (x - a^2)(x - b^2)$. Then $y^3 = f(x^2)$ is an affine model of a smooth projective plane quartic curve C that admits a double cover $\pi\colon C \to E$ to the elliptic curve $E\colon y^3 = f(x)$. Let A be the Prym variety, i.e. the kernel of the map $J = \mathrm{Jac}(C) \to E$ induced by Albanese functoriality. The ζ_3-multiplication on J induces ζ_3-multiplication on A, so we may speak of the sextic twists A_d. In fact, A_d is simply the Prym variety of $C_d\colon y^3 = (x^2 - da^2)(x^2 - db^2)$, which covers the elliptic curve $E_d\colon y^3 = (x - da^2)(x - db^2)$.

Recall that π is the descent of $1 - \zeta_3$ to $\mathbb{Q}$, or in other words, a descent of $\sqrt{-3}$. Note that $A[\pi] \simeq (\mathbb{Z}/3\mathbb{Z})^2$ is spanned by the rational points $P = (a, 0) - (-a, 0)$ and $Q = (b, 0) - (-b, 0)$.

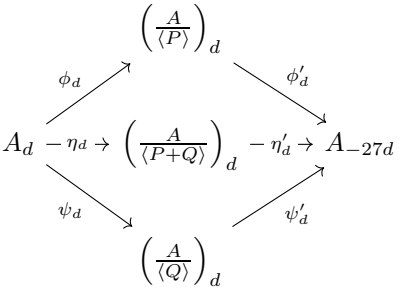
The Prym variety A need not be principally polarized over $\mathbb{Q}$, but it admits a polarization $\lambda\colon A \to \widehat{A}$ whose kernel is order 4 [Mum74]. By [SW21, Lem. 10.4], the Rosati involution restricts to complex conjugation on the subring $\mathbb{Z}[\zeta_3] \subset \mathrm{End}(A)$. Thus, we are in the setting of Theorem 4.4.

The endomorphism $[3]\colon A \to A$ factors as $[3] = \pi_{-27} \circ \pi$. Hence, for each $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 6}$,

$$\mathrm{rk}(A_d) \le \dim_{\mathbb{F}_3} \mathrm{Sel}_3(A_d) \le \dim_{\mathbb{F}_3}(\mathrm{Sel}(\pi_d) \oplus \mathrm{Sel}(\pi_{-27d})) = \dim_{\mathbb{F}_3}(\mathrm{Sel}(\pi_d) \oplus \mathrm{Sel}(\widehat{\pi}_d)),$$

where the last equality follows from Lemma 4.3.

As in Section 4, for each $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 6}$, the isogeny π_d factors as



Let $\mathfrak{f}$ be the conductor of A, and let Σ be the set of squarefree $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 6}$ such that $d, -3d \notin \mathbb{Q}_p^{\times 2}$ for all $p \mid 3\mathfrak{f}$. To prove Theorem 1.4, we first compute the four Tamagawa ratios $c(\phi_d), c(\phi'_d), c(\psi_d), c(\psi'_d)$.

Lemma 7.1. *Let $\alpha \in \{\phi, \phi', \psi, \psi'\}$. If $d \in \Sigma$ and if $p \nmid 3\mathfrak{f}\infty$, then $c_p(\alpha_d) = 1$.*

Proof. If $p \nmid \mathfrak{f}$, then since d is squarefree, the result follows from [SW21, Thm. 4.7]. If $p \mid \mathfrak{f}$, then, by assumption, $d, -3d \notin \mathbb{Q}_p^{\times 2}$. We have $\ker \alpha \simeq \mathbb{Z}/3\mathbb{Z}$, so $\ker \alpha_d(\mathbb{Q}_p) = 0$. By [SW21, Thm. 4.6], $H^1(\mathbb{Q}, \ker \alpha_d) = 0$ as well. Hence $c_p(\alpha_d) = 1$. □

Lemma 7.2. *Let $\alpha \in \{\phi, \phi', \psi, \psi'\}$. Then* $c_\infty(\alpha_d) = \begin{cases} \frac{1}{3} & d > 0 \\ 1 & d < 0. \end{cases}$

Proof. The proof is identical to Lemma 5.9. □

Now, from the factorisation $[3] = \pi_d \circ \pi_{-27d}$, we see that

$$c_3(\phi_d)c_3(\phi'_d)c_3(\phi_{-27d})c_3(\phi'_{-27d}) = c_3([3]) = 9.$$

By [SW21, Lem. 10.5] and the assumption that $d, -3d \notin \mathbb{Q}_3^{\times 2}$, it follows that each of these four ratios are integers. Hence, exactly two of them are 3 and two of them are 1.

Lemma 7.3. *Let Σ' be the set of $d \in \Sigma$ such that $c_3(\phi_d) \neq c_3(\phi'_d)$. If Σ' has positive density, then for a positive proportion of $d \in \Sigma'$, we have* $\operatorname{rk} A_d(\mathbb{Q}) \leq 1$.

Proof. If $d \in \Sigma'$, then by the above discussion, one of $c_3(\phi_d)$ and $c_3(\phi'_d)$ is 1 and the other is 3. By Lemmas 7.1 and 7.2, it follows that for each $d \in \Sigma'$, one of $c(\phi_d)$ and $c(\phi'_d)$ is 1 and the other is $3^{\pm 1}$. Without loss of generality, we can assume that $c(\phi_d) = 1$. By [SW21, Prop. 5.4], for at least $\frac{1}{2}$ of $d \in \Sigma'$, we have $\operatorname{Sel}(\phi_d) = 0 = \operatorname{Sel}(\widehat{\phi}_d)$, and for at least $\frac{5}{6}$ of $d \in \Sigma'$, we have $\dim_{\mathbb{F}_3} \operatorname{Sel}(\phi'_d) \oplus \operatorname{Sel}(\widehat{\phi}'_d) = 1$. Thus, for at least $\frac{5}{6} - \frac{1}{2} = \frac{1}{3}$ of $d \in \Sigma'$, we have

$$\begin{aligned} \dim_{\mathbb{F}_3} \operatorname{Sel}_3(A_d) &\leq \dim(\operatorname{Sel}(\pi_d) \oplus \operatorname{Sel}(\widehat{\pi}_d)) \\ &\leq \dim(\operatorname{Sel}(\phi_d) \oplus \operatorname{Sel}(\widehat{\phi}_d) \oplus \operatorname{Sel}(\phi'_d) \oplus \operatorname{Sel}(\widehat{\phi}'_d)) \leq 1, \end{aligned}$$

which implies that $\operatorname{rk} A_d(\mathbb{Q}) \leq 1$. □

Proof of Theorem 1.4. By Lemma 7.3, it remains to show that if Σ' has density 0, then $\operatorname{rk} A_d(\mathbb{Q}) \leq 1$ for a positive proportion of $d \in \Sigma$. So assume that Σ' has density 0, and let T be the set of $d \in \Sigma$ such that $c(\phi_d) = c(\phi'_d) = c(\psi_d) = c(\psi'_d) = 1$. By Theorem 4.4, it is sufficient to show that T has positive density, in which case, for a positive proportion of $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 6}$, we have $\operatorname{rk} A_d(\mathbb{Q}) = 0$.

First note that if $d \in \Sigma \setminus \Sigma'$ and if $c(\phi_d) = c(\phi'_d) = 1$, then $c(\psi_d) = c(\psi'_d) = 1$. Indeed, $c_3(\pi_d) = c_3(\phi_d)c_3(\phi'_d) = c_3(\psi_d)c_3(\psi'_d)$. Since $d \notin \Sigma'$, we have $c_3(\phi_d) = c_3(\phi'_d)$, and since all four of $c_3(\phi_d), c_3(\phi'_d), c_3(\psi_d), c_3(\psi'_d)$ are either 1 or 3, we see that $c_3(\phi_d) = c_3(\phi'_d) = c_3(\psi_d) = c_3(\psi'_d)$. Hence, by Lemmas 7.1 and 7.2, we have $c(\phi_d) = c(\phi'_d) = c(\psi_d) = c(\psi'_d)$ for all $d \in \Sigma \setminus \Sigma'$.

Assume at first that there exists a positive density of $d \in \Sigma$ such that $c_3(\phi_d) = c_3(\phi'_d) = 3$. For any such d, if $d > 0$, then $c_\infty(\phi_d) = c_\infty(\phi'_d) = \frac{1}{3}$, so $c(\phi_d) = c(\phi'_d) = 1$, and so T has postive density. If $d < 0$, then let $k \in \mathbb{Z}$ be such that $k \in \mathbb{Z}_p^{\times 2}$ for all $p \mid 3\mathfrak{f}$ and $k < 0$. Then $dk \in \Sigma$, $dk > 0$, and $c_3(\phi_{dk}) = c_3(\phi'_{dk}) = 3$. Thus $dk \in T$. A similar analysis shows that if $c_3(\phi_d) = c_3(\phi'_d) = 1$ then T again has positive density. The result now follows from Theorem 4.4. □

Proof of Theorem 1.5. Given Theorem 1.4, the proof is exactly as in [SW21, Thm. 1.7] □

Acknowledgments

The authors are grateful to Hershy Kisilevsky for helpful comments. They also thank the referees for their very helpful suggestions and comments.

References

[ABS22] Levent Alpöge, Manjul Bhargava, and Ari Shnidman, *Integers expressible as the sum of two rational cubes* (2022).arXiv:2210.10730

[BES20] Manjul Bhargava, Noam Elkies, and Ari Shnidman, *The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$*, J. Lond. Math. Soc. (2) **101** (2020), no. 1, 299–327, DOI 10.1112/jlms.12271. MR4072495

[BFS21] Nils Bruin, E. Victor Flynn, and Ari Shnidman, *Genus two curves with full $\sqrt{3}$-level structure and Tate-Shafarevich groups*, Selecta Mathematica (2021).arXiv:2102.04319

[BFT14] Nils Bruin, E. Victor Flynn, and Damiano Testa, *Descent via $(3,3)$-isogeny on Jacobians of genus 2 curves*, Acta Arith. **165** (2014), no. 3, 201–223. MR3263947

[BKLOS19] Manjul Bhargava, Zev Klagsbrun, Robert J. Lemke Oliver, and Ari Shnidman, *3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field*, Duke Math. J. **168** (2019), no. 15, 2951–2989, DOI 10.1215/00127094-2019-0031. MR4017518

[BKR21] Lea Beneish, Debanjana Kundu, and Anwesh Ray, *Rank Jumps and Growth of Shafarevich–Tate Groups for Elliptic Curves in $\mathbb{Z}/p\mathbb{Z}$-Extensions* (2021).arXiv:2107.09166

[CV07] Christophe Cornut and Vinayak Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 121–186, DOI 10.1017/CBO9780511721267.005. MR2392354

[DD10] Tim Dokchitser and Vladimir Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596, DOI 10.4007/annals.2010.172.567. MR2680426

[DFK07] Chantal David, Jack Fearnley, and Hershy Kisilevsky, *Vanishing of L-functions of elliptic curves over number fields*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 247–259, DOI 10.1017/CBO9780511735158.016. MR2322350

[Dok07] Tim Dokchitser, *Ranks of elliptic curves in cubic extensions*, Acta Arith. **126** (2007), no. 4, 357–360, DOI 10.4064/aa126-4-5. MR2289966

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR133227

[DT10] Henri Darmon and Ye Tian, *Heegner points over towers of Kummer extensions*, Canad. J. Math. **62** (2010), no. 5, 1060–1081, DOI 10.4153/CJM-2010-039-8. MR2730356

[FKK12] Jack Fearnley, Hershy Kisilevsky, and Masato Kuwata, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, J. Lond. Math. Soc. (2) **86** (2012), no. 2, 539–557, DOI 10.1112/jlms/jds018. MR2980924

[For19] Michele Fornea, *Growth of the analytic rank of modular elliptic curves over quintic extensions*, Math. Res. Lett. **26** (2019), no. 6, 1571–1586, DOI 10.4310/MRL.2019.v26.n6.a1. MR4078688

[GFP20] Natalia Garcia-Fritz and Hector Pasten, *Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points*, Math. Ann. **377** (2020), no. 3-4, 989–1013. MR4126887

[How01] Everett W. Howe, *Isogeny classes of abelian varieties with no principal polarizations*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 203–216. MR1827021

[Kis12] Hershy Kisilevsky, *Ranks of elliptic curves in cubic extensions*, Number theory, analysis and geometry, Springer, New York, 2012, pp. 369–383, DOI 10.1007/978-1-4614-1260-1_17. MR2867925

[KL19] Daniel Kriz and Chao Li, *Goldfeld's conjecture and congruences between Heegner points*, Forum Math. Sigma **7** (2019), Paper No. e15, 80, DOI 10.1017/fms.2019.9. MR3954912

[KN21] Hershy Kisilevsky and Jungbae Nam, *Small Algebraic Central Values of Twists of Elliptic L-Functions* (2021).arXiv:2001.03547

[Lag22] Jef Laga, *Arithmetic statistics of Prym surfaces*, Math. Ann. (2022).

[LOT21] Robert J. Lemke Oliver and Frank Thorne, *Rank growth of elliptic curves in non-abelian extensions*, Int. Math. Res. Not. IMRN **24** (2021), 18411–18441, DOI 10.1093/imrn/rnz307. MR4365991

[Mat70] Ju. V. Matijasevič, *The Diophantineness of enumerable sets* (Russian), Dokl. Akad. Nauk SSSR **191** (1970), 279–282. MR0258744

[Mon96] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z. **221** (1996), no. 3, 415–420. MR1381589

[MR07] Barry Mazur and Karl Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612. MR2373150

[MR08] Barry Mazur and Karl Rubin, *Growth of Selmer rank in nonabelian extensions of number fields*, Duke Math. J. **143** (2008), no. 3, 437–461, DOI 10.1215/00127094-2008-025. MR2423759

[MR10] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575. MR2660452

[MR18] Barry Mazur and Karl Rubin, *Diophantine stability*, Amer. J. Math. **140** (2018), no. 3, 571–616. With an appendix by Michael Larsen. MR3805014

[MRS07] B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, J. Algebra **314** (2007), no. 1, 419–438, DOI 10.1016/j.jalgebra.2007.02.052. MR2331769

[Mum74] David Mumford, *Prym varieties. I*, Contributions to analysis (a collection of papers dedicated to Lipman Bers), Academic Press, New York, 1974, pp. 325–350. MR0379510

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008, DOI 10.1007/978-3-540-37889-1. MR2392026

[Sch96] Edward F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114, DOI 10.1006/jnth.1996.0006. MR1370197

[Shl08] Alexandra Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555, DOI 10.1090/S0002-9947-08-04302-X. MR2386235

[Li19] Chao Li, *2-Selmer groups, 2-class groups and rational points on elliptic curves*, Trans. Amer. Math. Soc. **371** (2019), no. 7, 4631–4653, DOI 10.1090/tran/7373. MR3934463

[Smi20] Alexander Smith, *ℓ^∞-Selmer Groups in Degree ℓ Twist Families*, Harvard University, Graduate School of Arts & Sciences (2020).

[SW21] Ari Shnidman and Ariel Weiss, *Ranks of abelian varieties in cyclotomic twist families* (2021).arXiv:2107.06803

Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Edmund J. Safra Campus, Jerusalem 9190401, Israel

Email address: ariel.shnidman@mail.huji.ac.il

Department of Mathematics, Ben-Gurion University of the Negev, Be'er Sheva 8410501, Israel

Email address: arielweiss@post.bgu.ac.il