ELEMENTS OF GIVEN ORDER IN TATE-SHAFAREVICH GROUPS OF ABELIAN VARIETIES IN QUADRATIC TWIST FAMILIES

MANJUL BHARGAVA, ZEV KLAGSBRUN, ROBERT J. LEMKE OLIVER, AND ARI SHNIDMAN

Abstract. Let A be an abelian variety over a number field F and let p be a prime. Cohen-Lenstra-Delaunay-style heuristics predict that the Tate-Shafarevich group $Ш(A_s)$ should contain an element of order p for a positive proportion of quadratic twists A_s of A. We give a general method to prove instances of this conjecture by exploiting independent isogenies of A. For each prime p, there is a large class of elliptic curves for which our method shows that a positive proportion of quadratic twists have nontrivial p-torsion in their Tate-Shafarevich groups. In particular, when the modular curve $X_0(3p)$ has infinitely many F-rational points the method applies to "most" elliptic curves E having a cyclic $3p$-isogeny. It also applies in certain cases when $X_0(3p)$ has only finitely many rational points. For example, we find an elliptic curve over $\mathbb{Q}$ for which a positive proportion of quadratic twists have an element of order 5 in their Tate-Shafarevich groups.

The method applies to abelian varieties of arbitrary dimension, at least in principle. As a proof of concept, we give, for each prime $p \equiv 1 \pmod 9$, examples of CM abelian threefolds with a positive proportion of quadratic twists having elements of order p in their Tate-Shafarevich groups.

1. Introduction

Let A be an abelian variety over a number field F and let n be a positive integer. The n-Selmer group $\mathrm{Sel}_n(A)$ sits in the short exact sequence

$$0 \to A(F)/nA(F) \to \mathrm{Sel}_n(A) \to Ш(A)[n] \to 0$$

between the weak Mordell-Weil group and the n-torsion of the Tate-Shafarevich group $Ш(A)$. For the definitions of these groups, see [25, §X]. Thus, the presence of n-torsion in $Ш(A)$ is the obstruction to computing the rank of the group of rational points $A(F)$ via n-descent.

One is immediately led to ask how often the group $Ш(A)[n]$ is nontrivial as A varies. Consider, for example, the quadratic twist family A_s for $s \in F^*/F^{*2}$, obtained by twisting A by the different quadratic characters of $\mathrm{Gal}(\overline{F}/F)$. There is a natural notion of height for $s \in F^*/F^{*2}$ (see [3]); when $F = \mathbb{Q}$, the height is the absolute value of the unique squarefree integer in the class. For quadratic twist families, one conjectures that there is often such an obstruction coming from $Ш(A_s)[n]$.

Conjecture 1.1. *If A is an abelian variety over a number field F and $n \geq 2$ is an integer, then $Ш(A_s)$ has an element of order n for a positive proportion of $s \in F^*/F^{*2}$, when ordered by height.*

A more precise conjecture when A is an elliptic curve has been formulated by Delaunay [7], but to date, there is no example of any abelian variety for which even the weaker Conjecture 1.1 is known to hold for any n that is not a power of two. When $n = 2$, the only examples of A for which Conjecture 1.1 has been established either require A to be an elliptic curve over $\mathbb{Q}$ with full rational two-torsion or for A to admit such a curve as an isogeny factor [9, 26, 28], with Smith's work [26] largely confirming the full 2-power case of Delaunay's conjecture for such curves. Away from 2, little is known. If $n = 3, 5$, or 7 and the elliptic curve $E/\mathbb{Q}$ has a rational n-torsion point, then $Ш(E_s)[n] \neq 0$ for infinitely many twists [1], but this result falls far short of obtaining a positive proportion. It is also known that the 3- and 5-parts of Ш can be arbitrarily large for curves over $\mathbb{Q}$ [5, 10], and that the p-part can be arbitrarily large for curves over some number field depending on p [16].

The purpose of the paper at hand is to establish several cases of Conjecture 1.1 when n is not a power of two and for abelian varieties other than elliptic curves over $\mathbb{Q}$. Our first theorem proves the existence of elliptic curves for which Conjecture 1.1 holds with $n = 3$.

Theorem 1.2. *Suppose $E \to E'$ is a cyclic 9-isogeny of elliptic curves over $\mathbb{Q}$. Then either a positive proportion of the twists E_s have rank 0 and $|Ш(E_s)[3]| \geq 9$, or a positive proportion of the twists E'_s have rank 0 and $|Ш(E'_s)[3]| \geq 9$.*

While we enjoy the clean statement of Theorem 1.2, the method typically applies to both E and E'. This is made clear by the quantitative version, Theorem 4.1 below. In fact, one consequence of Theorem 4.1 is that for any fixed number field F and $r \geq 1$, almost all elliptic curves E with a cyclic 9-isogeny defined over F will have a positive proportion of twists E_s with $|Ш(E_s)[3]| \geq 9^r$. For some of these curves, this positive proportion may in fact be taken to be a vast majority:

Theorem 1.3. *Let F be a number field and let $r \geq 1$. For any $\epsilon > 0$, there are infinitely many elliptic curves E/F, not isomorphic over $\overline{F}$, for which a proportion at least $1 - \epsilon$ of twists E_s/F have $|Ш(E_s)[3]| \geq 9^r$.*

The ideas leading to Theorem 1.2 also permit us to find elements of order 6 in Tate-Shafarevich groups for a positive proportion of twists E_s of E, provided that the elliptic curve E has an additional bit of level structure. For convenience, we state this result only over $\mathbb{Q}$, though a less uniform version should hold over any number field.

Theorem 1.4. *Suppose that $E/\mathbb{Q}$ has a cyclic 18-isogeny. Suppose also that E is not a twist of a curve in the isogeny class of the curve $y^2 + xy + y = x^3 + 4x - 6$ with Cremona label 14a1. Then for a positive proportion of twists, $Ш(E_s)$ has an element of order 6.*

The isogeny class 14a is the subject of Section 10. While our methods do not show that twists of curves in this isogeny class have elements of order six in their Tate-Shafarevich groups, we are nevertheless able to obtain strong applications regarding their Mordell-Weil ranks. For example, we prove that at least 25% of their quadratic twists have rank 0, and, assuming finiteness of Tate-Shafarevich groups, that at least 41.6% have rank 1.

For each prime $p \geq 5$, we also provide examples of curves for which Conjecture 1.1 holds for $n = p$. First, we make a definition. Let $x \in X_0(3p)(F)$, and let (E, C) be the corresponding elliptic curve over F with $\Gamma_0(3p)$-level structure. Suppose $\mathfrak{q} \nmid 3p$ is a prime ideal in the ring of integers $\mathcal{O}_F$ such that x reduces to a cusp on $X_0(3p)(\mathcal{O}_F/\mathfrak{q})$. Then the special fiber of the Néron model of E over $\mathcal{O}_{F,\mathfrak{q}}$ is an n-gon, and C intersects i of its components, for some $i \mid 3p$. We say that x *has i-reduction at $\mathfrak{q}$*.[1] With this definition in hand, we have:

Theorem 1.5. *Let F be a number field of degree d and suppose that $x = (E, C) \in X_0(3p)(F)$ is a non-cuspidal point. For $i \mid 3p$, let ω_i denote the number of primes $\mathfrak{q} \nmid 3p$ of i-reduction for x. Then there exists an elliptic curve E/F with $j(E) = j(x)$ such that for a positive proportion of s, we have*

$$|Ш(E_s/F)[p]| \geq p^{2\min(\omega_1,\omega_3)-2d}.$$

We present several corollaries to Theorem 1.5, the first of which shows that the set of curves for which Theorem 1.5 produces a non-trivial result is not empty.

Corollary 1.6. *Let $p \geq 5$ be a prime and let $E/\mathbb{Q}$ be an elliptic curve. Let $r \geq 1$ and suppose that E has multiplicative reduction at $\ell \nmid 3p$ for at least $4p+4+r$ primes ℓ. Also suppose that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts transitively on the set of $\mathbb{F}_\ell$-lines in $E[\ell]$, for each $\ell \in \{3, p\}$. Then there exists a number field F of degree at most $4p + 4$ over which $|Ш(E_s)[p]| \geq p^{2r}$ for a positive proportion of $s \in F^*/F^{*2}$.*

[1] This is equivalent to saying that x reduces to the unique cusp of $X_0(3p)$ of ramification index i.

The constants in Theorem 1.5 are generally not optimal, and using the ideas behind the proof, we find the first example of an elliptic curve over $\mathbb{Q}$ for which a positive proportion of twists have an element of order 5 in the associated Tate-Shafarevich group.

Corollary 1.7. *Let $E\colon y^2+xy+y=x^3+x^2-13x-219$ be the elliptic curve with Cremona label 50b3. For at least 50% of positive squarefree $s\equiv 1 \pmod 8$ that are coprime to 5, $E_s(\mathbb{Q})$ has rank 0 and $|Ш(E_s)[5]|\geq 25$. The same result holds for the elliptic curve with Cremona label 50b4.*

Corollary 1.6 shows that for any $r\geq 1$, there exist some number field over which some elliptic curve E has $|Ш(E_s)[p]|\geq p^{2r}$ for a positive proportion of its twists. The final corollary we present shows that, when $p=5$ or 7, there exist number fields over which for any $r\geq 1$ there are elliptic curves E for which $|Ш(E_s)[p]|\geq p^{2r}$ for a positive proportion of the quadratic twists of E.

Corollary 1.8. *Let $p\in\{5,7\}$ and let $r\geq 1$ be an integer. Let F be a number field over which the modular curve $X_0(3p)$ has infinitely many points over F. Then there are infinitely many elliptic curves over F, not isomorphic over $\bar{F}$, such that $|Ш(E_s)[p]|\geq p^{2r}$ for a positive proportion of $s\in F^*/F^{*2}$.*

For example, $X_0(15)$ and $X_0(21)$ both have infinitely many points over the field $\mathbb{Q}(\sqrt{10})$, so each case of Corollary 1.8 applies. The curves produced by Corollary 1.8 are explicit, in the sense that they can be generated easily in `Magma` [4]. Moreover, the proof suggests that when the points of $X_0(3p)(F)$ are ordered in a natural way, the conclusion of Corollary 1.8 holds for 100% of curves over F with a degree $3p$ isogeny; see Remark 6.2.

As we explain at the end of this section, the proofs of the above results all make use of primes of multiplicative reduction to force a certain Selmer group to be large. In particular, this method does not apply to elliptic curves with (potentially) everywhere good reduction. The next result provides examples of curves with (potentially) everywhere good reduction for which Conjecture 1.1 holds, though as in Corollary 1.6, we must base-change to a larger number field to find them. This second approach, which will also be elaborated on at the end of this section, works for any prime $p\geq 5$:

Theorem 1.9. *Let $p\geq 5$ be a prime and $E/\mathbb{Q}$ an elliptic curve with potentially good and ordinary reduction at both 3 and p. Assume that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts transitively on the set of $\mathbb{F}_\ell$-lines in $E[\ell]$, for $\ell\in\{3,p\}$, and set $K=\mathbb{Q}(E[3p])$. Let E' be any elliptic curve over K that is p-isogenous to E. Then for a positive proportion of $s\in K^*/K^{*2}$, we have*

$$\dim_{\mathbb{F}_p} Ш(E'_s)[p]\geq \frac{d}{2}\left(1-\frac{4}{p+1}\right),$$

where $[K:\mathbb{Q}]=2d$.

We obtain even stronger results for certain curves with complex multiplication.

Theorem 1.10. *Let E be an elliptic curve over a number field F, and assume that $\mathrm{End}_F(E)$ is the quadratic order of discriminant Df^2, with D a fundamental discriminant. Assume that f is odd, that 3 is not inert in $K=\mathbb{Q}(\sqrt{D})$, and that all primes dividing f split in K. Then at least half of the twists E_s have both rank 0 and $|Ш(E_s)[f]|\geq f^d$, where $[F\colon\mathbb{Q}]=2d$.*

Finally, our methods apply equally well to higher-dimensional abelian varieties, though the computations become more difficult and less explicit. We provide the following result concerning certain abelian threefolds with CM by the ninth cyclotomic field $K=\mathbb{Q}(\zeta_9)$ as a proof of concept.

Theorem 1.11. *Let J be the Jacobian of the Picard curve $y^3=x^4-x$. Let $p\equiv 1 \pmod 9$ be a prime, and let F be any number field containing $K(J[p])$. Then there is an abelian variety A/F isogenous to J such that at least 50% of quadratic twists A_s have rank 0 and satisfy $|Ш(A_s)[p]|\geq p^{3d}$, where $[F:\mathbb{Q}]=2d$.*

Theorem 1.11 has already inspired other results for high-dimensional A, and even over $\mathbb{Q}$. For example, the fourth author proved the $n = 3$ case of Conjecture 1.1 for certain quotients A of prime level modular Jacobian $J_0(p)$. The explicit proportion of twists with $Ш(A_s)[3] \neq 0$ is shown to be at least $1/8$ for these A [24, Thm. 1.5d]. In forthcoming work, Bruin, Flynn, and Shnidman give an explicit three-parameter family of abelian surfaces over $\mathbb{Q}$ for which Conjecture 1.1 holds.

We now sketch an outline of the method used to prove the above theorems. The proofs all follow the same general strategy, namely, to exploit abelian varieties that have two independent isogenies. To any isogeny $\phi\colon A \to A'$ of abelian varieties, we attach a Selmer group $\mathrm{Sel}_\phi(A)$, which sits in an exact sequence

$$0 \to A'(F)/\phi(A(F)) \to \mathrm{Sel}_\phi(A) \to Ш(A)[\phi] \to 0. \tag{1.1}$$

In favorable circumstances, the ϕ-Selmer group provides some measure of control over the rank of $A(F)$. However, when A has two independent isogenies ϕ_1 and ϕ_2, the control provided by the two associated Selmer groups need not be the same. We exploit this imbalance to prove our theorems.

More specifically, in the next section, we define the *global Selmer ratio* $c(\phi_s)$ attached to the quadratic twists ϕ_s of an isogeny ϕ, which has the property that

$$|\mathrm{Sel}_{\phi_s}(A_s)| \geq c(\phi_s)$$

for all but finitely many twists s. When ϕ has odd degree, $c(\phi_s)$ is determined by finitely many local conditions. If moreover ϕ is not self-dual, then it is relatively easy to construct quadratic twists for which $\mathrm{Sel}_{\phi_s}(A_s)$ is large by making $c(\phi_s)$ large.[2] On the other hand, when ϕ has degree 3 and A has dimension one, recent work of the authors [3] shows that

$$\mathrm{Avg}_{s\in\Sigma}\, |\mathrm{Sel}_{\phi_s}(A_s)| = 1 + \mathrm{Avg}_{s\in\Sigma}\, c(\phi_s)$$

for any $\Sigma \subseteq F^*/F^{*2}$ defined by finitely many local conditions. In particular, if $c(\phi_s)$ is small for $s \in \Sigma$, then the Selmer group, and hence the rank, is small on average. Our approach is to use the Selmer groups attached to such isogenies to control the rank, while simultaneously finding an independent isogeny ψ whose associated Selmer group is large. The sequence (1.1) will then imply that $Ш(A_s)$ is often non-trivial.

As alluded to earlier, we have two different ways of constructing twists with large global Selmer ratios $c(\phi_s)$, and hence large Selmer groups. The first is to consider twists with many primes of split multiplicative reduction; see Sections 4–6. The other systematic way we have of making $c(\phi_s)$ large is by exploiting the Galois action on the canonical subgroups of $A[p]$. This is our approach in Sections 7–9. The analysis is easier when A has ordinary reduction at p and 3, as in Theorem 1.9. In principle, this approach should work in cases of supersingular reduction as well.

Acknowledgements

The authors would like to thank the anonymous referees for their many detailed and thoughtful comments.

MB was supported by a Simons Investigator Grant and NSF grant DMS-1001828. RJLO was partially supported by NSF grant DMS-1601398.

[2] If ϕ is self-dual, e.g. multiplication by n on an elliptic curve, then $c(\phi) = 1$. This explains why we need level structure to make this strategy work.

2. Global Selmer ratios and Selmer groups

Given an isogeny $\phi\colon A \to A'$ over a number field F, the *local Selmer ratio* $c_{\mathfrak{p}}(\phi)$ at a (possibly infinite) place $\mathfrak{p}$ is defined to be

$$c_{\mathfrak{p}}(\phi) := \frac{|A'(F_{\mathfrak{p}})/\phi(A(F_{\mathfrak{p}}))|}{|A(F_{\mathfrak{p}})[\phi]|}. \tag{2.1}$$

We have $c_{\mathfrak{p}}(\phi) = 1$ for all but finitely many primes $\mathfrak{p}$ (see Remark 2.5 below), so we may define the *global Selmer ratio* $c(\phi)$ to be the product of the local Selmer ratios,

$$c(\phi) := \prod_{\mathfrak{p}\le\infty} c_{\mathfrak{p}}(\phi). \tag{2.2}$$

The following proposition records the connection between the Selmer ratio $c(\phi)$ and the two Selmer groups $\mathrm{Sel}_{\phi}(A)$ and $\mathrm{Sel}_{\hat{\phi}}(\hat{A}')$ coming from ϕ and the dual isogeny $\hat{\phi}\colon \hat{A}' \to \hat{A}$.

Proposition 2.1. *Let $\phi\colon A \to A'$ be an isogeny of abelian varieties over a number field F. Then*

$$c(\phi) = \frac{|\mathrm{Sel}_{\phi}(A)|}{|\mathrm{Sel}_{\hat{\phi}}(\hat{A}')|}\frac{|A(F)[\phi]|}{|\hat{A}'(F)[\hat{\phi}]|}.$$

Proof. See Theorem VIII.7.9 in [19], for example. □

If ϕ has prime degree ℓ, then $c(\phi) = \ell^m$ for some $m \in \mathbb{Z}$. Moreover, if A is an elliptic curve the parity of m encodes information about the rank of the ℓ-Selmer group:

Proposition 2.2. *If $\phi : E \to E'$ is an isogeny of elliptic curves of prime degree ℓ and $c(\phi) = \ell^m$, then*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_{\ell}(E) \equiv m + \dim_{\mathbb{F}_\ell} E(F)[\ell] \pmod 2.$$

Proof. This can be deduced from results of Cassels [6]; for a proof see [2, Prop. 42]. □

For each $s \in F^\times/F^{\times 2}$, the twist of ϕ is an isogeny $\phi_s\colon A_s \to A'_s$ between the quadratic twists. There are associated local Selmer ratios $c_{\mathfrak{p}}(\phi_s)$ for each place $\mathfrak{p}$ of F and a global Selmer ratio $c(\phi_s)$.

Corollary 2.3. *If ϕ has odd degree, then $|\mathrm{Sel}_{\phi_s}(A_s)| \ge c(\phi_s)$ for all but finitely many s.*

Proof. If ϕ has odd degree, then there finitely many classes $s \in F^\times/F^{\times 2}$ with $E_s(F)[\phi_s] \neq 0$ and finitely many classes $s' \in F^\times/F^{\times 2}$ with $E'_{s'}(F)[\hat{\phi}_{s'}] \neq 0$. By Proposition 2.1, we therefore have $c(\phi_s) = \frac{|\mathrm{Sel}_{\phi_s}(A_s)|}{|\mathrm{Sel}_{\hat{\phi}_s}(A'_s)|}$ for all but finitely many s. □

If ϕ decomposes as the composition of isogenies $\phi_2 \circ \phi_1$, then Lemma 7.2(b) in [18] shows that $c_p(\phi) = c_p(\phi_1)c_p(\phi_2)$ for every prime p. It therefore follows from (2.2) that $c(\phi) = c(\phi_1)c(\phi_2)$. As a result, we may always reduce the computation of Selmer ratios to those of isogenies of prime degree, in which case, the following result gives a way to compute the local Selmer ratio.

Proposition 2.4. *Let $\phi\colon A \to A'$ be an isogeny of prime degree ℓ. If $\mathfrak{p}$ is a finite prime, then*

$$c_{\mathfrak{p}}(\phi) = \frac{c_{\mathfrak{p}}(A')}{c_{\mathfrak{p}}(A)}\alpha_{\phi,\mathfrak{p}}$$

where $c_{\mathfrak{p}}(A)$ and $c_{\mathfrak{p}}(A')$ are the Tamagawa numbers of A and A' at $\mathfrak{p}$, and $\alpha_{\phi,\mathfrak{p}}$ equals $v_{\mathfrak{p}}(\det\tilde{\phi})$, the normalized valuation of the determinant of the induced map $\tilde{\phi}\colon \mathrm{Lie}\,\mathcal{A} \to \mathrm{Lie}\,\mathcal{A}'$ on tangent spaces of the Néron models at the identity. In particular, $\alpha_{\phi,\mathfrak{p}} = 1$ if $\mathfrak{p} \nmid \ell$. If $\mathfrak{p}$ is an infinite place and ℓ is odd, then

$$c_{\mathfrak{p}}(\phi) = \begin{cases} 1/\ell, & A[\phi] \subseteq A(F_{\mathfrak{p}}) \\ 1, & A[\phi] \not\subseteq A(F_{\mathfrak{p}}). \end{cases}$$

Proof. These statements can all be found in [22, §3]. □

Remark 2.5. If $\mathfrak{p} \nmid \ell$ is a prime, then $\alpha_{\phi,\mathfrak{p}} = 1$. As a result, we have $c_{\mathfrak{p}}(\phi) = \frac{c_{\mathfrak{p}}(A')}{c_{\mathfrak{p}}(A)}$. If A has good reduction at $\mathfrak{p}$, we therefore have $c_{\mathfrak{p}}(\phi) = 1$. It follows that $c_{\mathfrak{p}}(\phi) = 1$ for all but finitely many primes $\mathfrak{p}$, as noted at the beginning of this section.

Remark 2.6. When A is an elliptic curve, the factor $\alpha_{\phi,\mathfrak{p}}$ is simply the valuation of the linear term in the power series giving the induced isogeny on formal groups (using minimal models). In general, if $\dim A = g$, then $\alpha_{\phi,\mathfrak{p}}$ is the valuation of the determinant of a $g \times g$ Jacobian matrix of partial derivatives of the g power series in g variables which describe the induced isogeny on formal groups attached to the Néron models, evaluated at 0.

Computing $c_{\mathfrak{p}}(\phi)$ is a hard task in general, but there are clean formulas when the reduction type is not too bad. For example, when A has a quadratic twist of good reduction, we have:

Lemma 2.7. *Let $\phi\colon A \to A'$ be an isogeny of odd degree d. If $\mathfrak{p} \nmid d$ is a prime such that A_s has good reduction at $\mathfrak{p}$ for some $s \in F^*/F^{*2}$, then $c_{\mathfrak{p}}(\phi) = 1$. If $\mathfrak{p} \mid d$, then we have $c_{\mathfrak{p}}(A') = c_{\mathfrak{p}}(A)$.*

Proof. This follows from Lemmas 4.6 and 4.7 in [8], using that d is odd. While the results in [8] are only stated for elliptic curves, the proofs nonetheless hold verbatim for abelian varieties of arbitrary dimension. □

There are also general formulas for $c_{\mathfrak{p}}(\phi)$ in cases of potential ordinary reduction (good or bad). For example, the following lemma completes the computation of $c_{\mathfrak{p}}(\phi)$ when $\mathfrak{p}$ divides $\deg\phi$, in certain cases of good ordinary reduction.

Lemma 2.8. *Let $\phi\colon A \to A'$ be an isogeny of abelian varieties of dimension g over a number field F. Assume $\deg\phi = p^g$ and $\ker\phi \subset A[p]$, with p an odd prime. Let $\mathfrak{p}$ be a prime of F above p and assume A has good ordinary reduction at $\mathfrak{p}$. Then for all $s \in F^\times/F^{\times 2}$, we have:*

(a) If $\ker\phi$ reduces modulo $\mathfrak{p}$ to the kernel of absolute Frobenius, then $c_{\mathfrak{p}}(\phi_s) = p^{g[F_{\mathfrak{p}}\colon \mathbb{Q}_p]}$.

(b) If $\ker\phi$ (modulo $\mathfrak{p}$) intersects trivially with the kernel of absolute Frobenius, then $c_{\mathfrak{p}}(\phi_s) = 1$.

Proof. We have $c_{\mathfrak{p}}(\phi_s) = \alpha_{\phi_s,\mathfrak{p}}$ by Lemma 2.7. Since A is ordinary, condition (a) is equivalent to $(\ker\phi)(\bar{\mathbb{F}}_{\mathfrak{p}}) = 0$, where $\mathbb{F}_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$, and condition (b) is equivalent to saying that $(\ker\phi)(\bar{\mathbb{F}}_{\mathfrak{p}}) = (\mathbb{Z}/p\mathbb{Z})^g$. Equivalently, (a) says that the points of $\ker\phi$ lie in the formal group, while (b) says that $\ker\phi$ has trivial intersection with the formal group. Note that the latter conditions make sense for ϕ_s and are stable under twisting. In case (b), we see that ϕ_s induces an isomorphism of formal groups, hence Proposition 2.4 shows that $\alpha_{\phi_s,\mathfrak{p}} = 1$. We deduce case (a) from case (b), using the isogeny $\psi\colon A/\ker\phi \to A$ such that $\psi \circ \phi = [p]$. Indeed, if ϕ satisfies condition (a), then ψ satisfies condition (b) and

$$\alpha_{\phi_s,\mathfrak{p}} = \alpha_{[p],\mathfrak{p}}\alpha_{\psi_s,\mathfrak{p}}^{-1} = \alpha_{[p],\mathfrak{p}} = p^{g[F_{\mathfrak{p}}\colon \mathbb{Q}_p]}$$

as desired. Here we have used that $[p]$ induces the multiplication-by-p map on the tangent space. □

Remark 2.9. If $A = E$ is an elliptic curve, one of (a) or (b) holds for ϕ, but if $g > 1$ then $\ker\phi$ may have non-trivial proper intersection with the kernel of Frobenius.

In the cases of bad ordinary reduction (i.e. multiplicative reduction), and in the special case that A is an elliptic curve, there is an explicit formula for $c_{\mathfrak{p}}(\phi)$ using the j-invariants of A and A'.

Lemma 2.10. *Let $\phi\colon E \to E'$ be an isogeny of elliptic curves with odd prime degree ℓ and suppose that E has (potentially) multiplicative reduction at a prime $\mathfrak{p} \nmid \ell$.*

(i) If E has split multiplicative reduction at $\mathfrak{p}$, then $c_{\mathfrak{p}}(\phi) = v_{\mathfrak{p}}(j(E'))/v_{\mathfrak{p}}(j(E))$.

(ii) If E does not have split multiplicative reduction at $\mathfrak{p}$, then $c_{\mathfrak{p}}(\phi) = 1$.

Proof. This follows from Table 1 in [8]. □

As a consequence of Lemma 2.7, we deduce:

Corollary 2.11. *Let $\phi\colon A \to A'$ be an isogeny of odd degree d, and let N_A be the conductor of A. For any $s \in F^*/F^{*2}$, the value of $c(\phi_s)$ depends only on the class of $s \in \prod_{\mathfrak{p}|dN_A\infty} F_\mathfrak{p}^*/F_\mathfrak{p}^{*2}$ and in particular is given by*

$$c(\phi_s) = \prod_{\mathfrak{p}|dN_A\infty} c_\mathfrak{p}(\phi_s).$$

Proof. If $\mathfrak{p} \nmid dN_A\infty$, then A_s and A'_s have quadratic twists of good reduction at $\mathfrak{p}$. By Lemma 2.7, we therefore have $c_\mathfrak{p}(\phi_s) = 1$ for all such primes. □

When ϕ is of odd prime degree ℓ, Corollary 2.11 implies that the sets

$$T_m(\phi) := \{s \in F^*/F^{*2} : c(\phi_s) = \ell^m\},$$

for $m \in \mathbb{Z}$, are defined by finitely many local conditions in the sense of [3]. In particular, they have positive density within F^*/F^{*2} when they are non-empty. Moreover, Corollary 2.3 shows that for all but finitely many $s \in T_m(\phi)$, the following lower bound holds: $|\mathrm{Sel}_\phi(A_s)| \geq \ell^m$.

On the other hand, when $\ell = 3$, the main results of [3] allow us to control the average size of $\mathrm{Sel}_\phi(A_s)$, for $s \in T_m(\phi)$, and to give an *upper bound* on its average rank (or, more precisely, on the lim sup of the average rank, as the limit of the average rank is not known to exist):

Theorem 2.12. *Let $\phi\colon A \to A'$ be an isogeny of degree 3 and for $m \in \mathbb{Z}$, let $T_m(\phi)$ be defined as above. For any non-empty subset $\Sigma \subseteq T_m(\phi)$ defined by finitely many local conditions, the average size of $\mathrm{Sel}_\phi(A_s)$ for $s \in \Sigma$ is exactly $1 + 3^m$. If A is an elliptic curve, the average $\mathbb{F}_3$-rank of $\mathrm{Sel}_3(A_s)$, for $s \in \Sigma$, is at most $|m| + 3^{-|m|}$, and in particular, the average rank of $A_s(F)$ is at most $|m| + 3^{-|m|}$.*

Proof. This is a combination of Theorems 2.1 and 2.4 in [3]. □

When $A = E$ is an elliptic curve, Theorem 2.12 shows that for a positive proportion of $s \in T_m(\phi)$ the Mordell-Weil rank of E_s is at most $|m|$. This is clear for $m \geq 1$; for $m = 0$, use Proposition 2.2 as well. Pulling together the results of this section, we obtain the following key proposition.

Proposition 2.13. *Let E be an elliptic curve over a number field F, and let ℓ be a prime. Let $\phi\colon E \to E'$ and $\psi\colon E \to E''$ be isogenies over F of degrees 3 and ℓ, respectively, and suppose $E[\phi] \cap E[\psi] = 0$ if $\ell = 3$. Let m and n be integers such that $m > |n|$ and $T_{-m}(\psi) \cap T_n(\phi) \neq \emptyset$. Then a positive proportion of $s \in T_{-m}(\psi) \cap T_n(\phi)$ are such that $E''_s(F)$ has rank at most $|n|$ and $|Ш(E''_s)[\ell]| \geq \ell^{m-|n|}$. If $n = 0$, this proportion is at least $\frac{1}{2}$, and if $|n| = 1$, it is at least $\frac{5}{6}$.*

Proof. As noted, for a positive proportion of $s \in T_{-m}(\psi) \cap T_n(\phi)$, the rank of $E_s(F)$ is at most $|n|$. The same holds for $E''_s(F)$, since rank is preserved by isogeny. Since $c(\hat{\psi}_s) = c(\psi_s)^{-1} = \ell^m$, we also have $|\mathrm{Sel}_\ell(E'')| \geq |\mathrm{Sel}_{\hat{\psi}}(E''_s)| \geq c(\hat{\psi}_s) = \ell^m$ for all but finitely many such s. It follows from the ℓ-descent short exact sequence that $|Ш(E''_s)[\ell]| \geq \ell^{m-|n|}$.

If $n = 0$, then the average $\mathbb{F}_3$-rank of $\mathrm{Sel}_3(E_s)$ is at most 1 and the parity of $\dim_{\mathbb{F}_3} \mathrm{Sel}_3(E_s)$ is even, for $s \in T_{-m}(\psi) \cap T_n(\phi)$. It follows immediately that at least 50% of s have $\mathrm{Sel}_3(E_s) = 0$. Similarly, if $n = 1$, the average of $\dim_{\mathbb{F}_3} \mathrm{Sel}_3(E_s)$ is at most $4/3$ and the parity is odd. It follows immediately that at least $5/6$ of twists E_s have 3-Selmer rank equal to 1, and hence Mordell-Weil rank at most 1. □

In the special case that $\ell = 3$, the discrepancy between the two Selmer groups allows us to strengthen the rank bounds provided by Theorem 2.12.

Corollary 2.14. *Let $\phi\colon E \to E'$ and $\psi\colon E \to E''$ be independent 3-isogenies. If $T_m(\phi) \cap T_n(\psi)$ is non-empty, then the average rank of $E_s(F)$ for $s \in T_m(\phi) \cap T_n(\psi)$ is at most*

$$\min(|m|, |n|) + 3^{-\min(|m|,|n|)}.$$

If $m = 0$ or $n = 0$, at least $1/2$ of $s \in T_m(\phi) \cap T_n(\psi)$ are such that $E_s(F)$ has rank 0. If either $|m| = 1$ or $|n| = 1$, at least $5/6$ of $s \in T_m(\phi) \cap T_n(\psi)$ are such that $E_s(F)$ has rank at most 1.

Proof. We apply Theorem 2.12 with whichever choice of ϕ and ψ yields a stronger bound. □

Remark 2.15. We give examples of elliptic curves for which Corollary 2.14 implies an improved rank bound in Section 10.

3. Local Selmer ratios for curves with two independent 3-isogenies

Throughout this section, let F be a number field and E an elliptic curve with a pair of independent 3-isogenies $\phi_1 : E \to E'$ and $\phi_2 : E \to E''$ over F. By the non-degeneracy of the Weil pairing, E is a quadratic twist of a curve E_s with $E_s[3] \simeq \mathbb{Z}/3\mathbb{Z} \times \mu_3$. This immediately implies:

Lemma 3.1. *Suppose E has two independent 3-isogenies $\phi_1 : E \to E'$ and $\phi_2 : E \to E''$. Then*

(*i*) *Some twist of E obtains full rational 3-torsion over $F(\zeta_3)$.*

(*ii*) *The groups $E[\phi_1]$ and $E[\phi_2]$ are Cartier dual.*

Part (i) of Lemma 3.1 has the following important corollary.

Lemma 3.2. *If E has additive, potentially good reduction at a finite prime $\mathfrak{p} \nmid 3$ of F, then E has a twist E_s with good reduction at $\mathfrak{p}$. In particular, $c_{\mathfrak{p}}(\phi_i) = 1$ for $i = 1, 2$.*

Proof. By Lemma 3.1(i), E has some twist E_s with full rational 3-torsion over the extension $F_{\mathfrak{p}}(\zeta_3)$. It therefore has good reduction over $F_{\mathfrak{p}}(\zeta_3)$ [23, §2]. Since $F_{\mathfrak{p}}(\zeta_3)$ is unramified over $F_{\mathfrak{p}}$, E_s must have good reduction over $F_{\mathfrak{p}}$. It then follows from Lemma 2.7 that $c_{\mathfrak{p}}(\phi_i) = 1$. □

The story when E has multiplicative or additive potential multiplicative reduction at $\mathfrak{p}$ is relatively straightforward as well. For this, we use the *Hesse model*.

Lemma 3.3. *If E is an elliptic curve over F with $E[3] \simeq \mathbb{Z}/3\mathbb{Z} \times \mu_3$, then there are u and v in K, with $v/u \notin \{0, 1, \zeta_3, \zeta_3^2\}$ such that E is isomorphic to*

$$E_{u,v}\colon v(x^3 + y^3 + z^3) = 3uxyz.$$

In this model, $E_{u,v}(\overline{F})[3]$ is generated by $(1 : -1 : 0)$ and $(\zeta_3 : -\zeta_3^2 : 0)$. Moreover, if E' and E'' are the quotients of E by the corresponding subgroups of order 3, we have

$$j(E') = \frac{27u^3(9u^3 - 8v^3)^3}{v^9(u - v)(u^2 + uv + v^2)},$$

$$j(E) = \frac{27u^3(u + 2v)^3(u^2 - 2uv + 4v^2)^3}{v^3(u - v)^3(u^2 + uv + v^2)^3}, \quad \text{and}$$

$$j(E'') = \frac{3(u + 2v)^3(u^3 + 78u^2v + 84uv^2 + 80v^3)^3}{v(u - v)^9(u^2 + uv + v^2)}.$$

Proof. The Hesse model is classical (see [21], e.g.), and the rest follows from a symbolic computation in `Magma` [4]. □

Lemma 3.4. *Suppose that E has (potential) multiplicative reduction at $\mathfrak{p}$, and write $v(\cdot)$ for the $\mathfrak{p}$-valuation. Let j, j', and j'' denote the j-invariants of E, E', and E'', respectively. Then one of the following holds:*

(*i*) *$v(j) = 3v(j')$ and $3v(j) = v(j'')$,*

(*ii*) $v(j) = 3v(j')$ *and* $v(j) = 3v(j'')$, *or*
(*iii*) $3v(j) = v(j')$ *and* $v(j) = 3v(j'')$.
Moreover, (*ii*) *can only occur if* $\mu_3 \subset F_{\mathfrak{p}}$.

Proof. That only the listed possibilities occur follows from examining the denominators of the j-invariants of E, E', and E'' in the Hesse model. This examination also shows that the case $v(j) = 3v(j')$ and $v(j) = 3v(j'')$ occurs if and only if $v(t^2+t+1) \neq 0$, which implies $\mu_3 \subset F_{\mathfrak{p}}$. □

For any 3-isogeny ϕ, define the global log-Selmer ratio $t(\phi)$ and the local log-Selmer ratio $t_p(\phi)$, by $c(\phi) = 3^{t(\phi)}$ and $c_p(\phi) = 3^{t_p(\phi)}$. Thus, $t(\phi) = \sum_{p \leq \infty} t_p(\phi)$.

Lemma 3.5. *If* $F = \mathbb{Q}$, *then*
(*i*) $t(\phi_1) \equiv t(\phi_2) \pmod 2$ *and*
(*ii*) $t_p(\phi_1) \not\equiv t_p(\phi_2) \pmod 2$ *for* $p \in \{3, \infty\}$.

Proof. By Proposition 2.2, both sides of Congruence (i) are equal to the parity of $\dim_{\mathbb{F}_3} \mathrm{Sel}_3(E) - \dim_{\mathbb{F}_3} E(\mathbb{Q})[3]$ and hence must be the same.

Lemma 2.7 and Proposition 2.4 show that $t_p(\phi_1) \equiv t_p(\phi_2) \pmod 2$ for all primes $p \nmid 3$ where E has additive, potentially good reduction and Lemmas 2.10 and 3.4 show that $t_p(\phi_1) \equiv t_p(\phi_2) \pmod 2$ for all prime $p \nmid 3$ where E has (potential) multiplicative reduction. Congruence (i) then gives

$$t_3(\phi_1) + t_\infty(\phi_1) \equiv t_3 + t_\infty(\phi_2) \pmod 2. \tag{3.1}$$

However, by Proposition 2.4 combined with Lemma 3.1, we have $t_\infty(\phi_1) \not\equiv t_\infty(\phi_2) \pmod 2$. Combining this with (3.1), we then get that $t_3(\phi_1) \not\equiv t_3(\phi_2) \pmod 2$. □

Let $\phi_{1,s} \colon E_s \to E'_s$ and $\phi_{2,s} \colon E_s \to E''_s$ denote the isogenies on the twists induced by ϕ_1 and ϕ_2.

Lemma 3.6. *Suppose* $F = \mathbb{Q}$. *Then for each prime* $p \neq 3$, *there exists* $s \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ *such that* $c_p(\phi_{1,s}) = c_p(\phi_{2,s}) = 1$. *There also exists some* $s \in \mathbb{Q}_3^\times/\mathbb{Q}_3^{\times 2}$ *for which there is an equality of sets*

$$\{c_3(\phi_{1,s}), c_3(\phi_{2,s})\} = \{1, 3\}.$$

Proof. First assume $p \neq 3$. There is a unique $s \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ such that $E[\phi_{1,s}](\mathbb{Q}_p) \neq 0$, and similarly for ϕ_2. Thus, we can choose s so that both $E[\phi_{1,s}]$ and $E[\phi_{2,s}]$ have no $\mathbb{Q}_p$-points. Then by part (ii) of Lemma 3.1, the groups $E''[\hat{\phi}_{2,s}]$ and $E'[\hat{\phi}_{1,s}]$ also have no $\mathbb{Q}_p$-points. By (2.1), all four ratios $c_p(\phi_{i,s})$ and $c_p(\hat{\phi}_{i,s})$ are therefore positive integers. Since

$$c_p(\phi_{1,s})c_p(\hat{\phi}_{1,s}) = \frac{c_p(E')}{c_p(E)}\frac{c_p(E)}{c_p(E')} = 1 = c_p(\phi_{2,s})c_p(\hat{\phi}_{2,s}),$$

we conclude that all four local Selmer ratios are equal to 1, as desired.

Since $\alpha_{\phi_{i,s},\mathfrak{p}}\alpha_{\hat{\phi}_{i,s},\mathfrak{p}} = \alpha_{[3],\mathfrak{p}} = 3$, we have

$$c_3(\phi_{1,s})c_3(\hat{\phi}_{1,s}) = 3 = c_3(\phi_{2,s})c_3(\hat{\phi}_{2,s}).$$

Choosing $s \in \mathbb{Q}_3^\times/(\mathbb{Q}_3^\times)^2$ such that all four local Selmer ratios are positive integers, we deduce that one of $c_3(\phi_{1,s})$ and $c_3(\hat{\phi}_{1,s})$ is 1 and the other is 3. The same holds for $c_3(\phi_{2,s})$ and $c_3(\hat{\phi}_{2,s})$. Since $c_3(\phi_{1,s}) \neq c_3(\phi_{2,s})$ by part (ii) of Lemma 3.5, one of $c_3(\phi_{1,s})$ and $c_3(\phi_{2,s})$ is 1 and the other is 3. □

Over general number fields F, similar arguments give the following weak version of Lemma 3.6:

Lemma 3.7. *Let F be a number field of degree d. Then for each $\mathfrak{p} \nmid 3$, there exists $s \in F^*/F^{*2}$ such that $c_\mathfrak{p}(\phi_{1,s}) = c_\mathfrak{p}(\phi_{2,s}) = 1$. There also exists $s \in F^*/F^{*2}$ such that*

$$\prod_{\mathfrak{p}|3} c_\mathfrak{p}(\phi_{1,s}) \in \{1, 3, \dots, 3^d\} \quad \text{and} \quad \prod_{\mathfrak{p}|3} c_\mathfrak{p}(\phi_{2,s}) \in \{1, 3, \dots, 3^d\}.$$

Proof. The proof for $\mathfrak{p} \nmid 3$ is exactly the same as before. For $\mathfrak{p} \mid 3$, we at least know that

$$c_\mathfrak{p}(\phi_{1,s})c_\mathfrak{p}(\hat{\phi}_{1,s}) = 3^{[F_\mathfrak{p}\colon \mathbb{Q}_3]} = c_\mathfrak{p}(\phi_{2,s})c_\mathfrak{p}(\hat{\phi}_{2,s}),$$

and that all four ratios are positive integers for suitable choice of s. Since $\sum_{\mathfrak{p}|3}[F_\mathfrak{p}\colon \mathbb{Q}_3] = d$, the claim follows. □

4. Curves with a 9-isogeny

Continue to let F be a number field. In this section, we prove Theorems 1.2 and 1.3. Let $\phi\colon E' \to E''$ be a cyclic 9-isogeny of elliptic curves over F. Then ϕ factors as a composition of two 3-isogenies

$$E' \xrightarrow{\hat{\phi}_1} E \xrightarrow{\phi_2} E''$$

over F. The intermediate elliptic curve E has two independent 3-isogenies, ϕ_1 and ϕ_2, with $\hat{\phi}_1$ being the dual isogeny of ϕ_1. As E has two independent isogenies, it is subject to Proposition 2.13 and the results of Section 3.

4.1. **Proof of Theorem 1.2.** Assume $F = \mathbb{Q}$. We may replace E', E, and E'' with their quadratic twists, so we may assume that $E[3] \simeq \mathbb{Z}/3\mathbb{Z} \times \mu$. By Lemma 3.3, E is isomorphic to

$$E_{u,v}\colon v(x^3 + y^3 + z^3) = 3uxyz,$$

for some coprime integers u and v, with $v/u \notin \{0, 1\}$.

We first consider the case where there is some prime $\ell \geq 5$ dividing $u^2 + uv + v^2$. We claim that there exists $s \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ such that

(i) $c_\ell(\phi_{1,s}) = \frac{1}{3} = c_\ell(\phi_{2,s})$,
(ii) $c_p(\phi_{1,s}) = 1 = c_p(\phi_{2,s})$ for all $p \nmid 3\ell\infty$, and
(iii) One of $c_3(\phi_{i,s})c_\infty(\phi_{i,s})$, for $i \in \{1, 2\}$, equals 3 and the other equals $\frac{1}{3}$.

By weak approximation, it suffices to shows that each of these can be individually satisfied. Indeed, (i) follows from Lemma 2.10, which connects the local Selmer ratio to the valuations of the j-invariants, and Lemmas 3.3 and 3.4, which provide the valuation of $j(E)$, $j(E')$, and $j(E'')$ for the Hesse model (in particular, $v_\ell(j(E)) = 3v_\ell(j(E')) = 3v_\ell(j(E''))$ since ℓ divides $u^2 + uv + v^2$); (ii) follows from Lemma 3.6; and (iii) follows from combining Proposition 2.4 with Lemma 3.6.

It follows that at least one of the sets $T_{-2}(\phi_1) \cap T_0(\phi_2)$ and $T_0(\phi_1) \cap T_{-2}(\phi_2)$ is non-empty. Theorem 1.2 now follows from Proposition 2.13.

We next consider the case where $q := u^2 + uv + v^2$ is not divisible by any prime $\ell > 3$. Since q is positive definite as a quadratic form in (u, v), we have $q > 0$ and since u and v are coprime, q can't be divisible by either 2 or 9, so it follows that $q \in \{1, 3\}$. Up to quadratic twist, these cases correspond to E with Cremona labels $27a1$ and $54a1$. A computation in `Magma` [4] shows that $T_{-2}(\phi_1) \cap T_0(\phi_2)$ is non-empty and Theorem 1.2 therefore follows from Proposition 2.13 as above.

4.2. **Quantitative version of Theorem 1.2 over number fields.** Suppose now that F has degree d over $\mathbb{Q}$, with r_1 real places and r_2 pairs of complex places. Define sets $\mathcal{P}_1$, $\mathcal{P}_2$, and $\mathcal{P}_3$ by

$$\mathcal{P}_1 = \{\mathfrak{p} : E \text{ has (pot.) mult. red. at } \mathfrak{p} \text{ with } v(j) = 3v(j') \text{ and } 3v(j) = v(j'')\}$$
$$\mathcal{P}_2 = \{\mathfrak{p} : E \text{ has (pot.) mult. red. at } \mathfrak{p} \text{ with } v(j) = 3v(j') \text{ and } v(j) = 3v(j'')\}$$

and

$$\mathcal{P}_3 = \{\mathfrak{p} : E \text{ has (pot.) mult. red. at } \mathfrak{p} \text{ with } 3v(j) = v(j') \text{ and } v(j) = 3v(j'')\}$$

Also set $\mathcal{P}_{\text{mult}} = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3$. The following theorem gives general results about 3-torsion elements in Tate-Shafarevich groups of quadratic twists for elliptic curves with a 9-isogeny over F.

Theorem 4.1. *Let $s_0 \in F^*/F^{*2}$ be any square class such that E_{s_0} does not have split multiplicative reduction at any $\mathfrak{p} \in \mathcal{P}_3$. Let ω_1^{sp} denote the number of $\mathfrak{p} \in \mathcal{P}_1$ at which E_{s_0} has split multiplicative reduction, and define ω_2^{sp} analogously. Then for a positive proportion of $s \in s_0F^{*2}$*

$$\dim_{\mathbb{F}_3} Ш(E'_s)[3] \geq \min(2\omega_1^{\text{sp}} - 2r_2, 2\omega_2^{\text{sp}} - d).$$

Proof. By Lemma 3.2, the only places that contribute to either of the Selmer ratios $c(\phi_1)$ and $c(\phi_2)$ are infinite primes, places of (potentially) multiplicative reduction, and primes $\mathfrak{p} \mid 3$. For any $s \in F^*/F^{*2}$, define $t_1 = \text{ord}_3(c(\phi_{1,s}))$ and $t_2 = \text{ord}_3(c(\phi_{2,s}))$, along with

$$t_{1,\text{mult}} = \text{ord}_3 \prod_{\mathfrak{p} \in \mathcal{P}_{\text{mult}}} c_{\mathfrak{p}}(\phi_{1,s}) \quad \text{and} \quad t_{2,\text{mult}} = \text{ord}_3 \prod_{\mathfrak{p} \in \mathcal{P}_{\text{mult}}} c_{\mathfrak{p}}(\phi_{2,s}).$$

From Lemma 2.10 and Lemma 3.4, it follows that for any $s \in s_0F^{*2}$

$$t_{1,\text{mult}} = -\omega_1^{\text{sp}} - \omega_2^{\text{sp}} \quad \text{and} \quad t_{2,\text{mult}} = \omega_1^{\text{sp}} - \omega_2^{\text{sp}}.$$

It remains to consider the contribution of places $\mathfrak{p} \mid 3\infty$. By Proposition 2.4, we have

$$\prod_{\mathfrak{p}\mid\infty} c_{\mathfrak{p}}(\phi_{1,s}) = 3^{-r_1-r_2} \quad \text{and} \quad \prod_{\mathfrak{p}\mid\infty} c_{\mathfrak{p}}(\phi_{2,s}) = 3^{-r_2}.$$

for the positive proportion of $s \in s_0F^{*2}$ such that $E[\phi_{i,s}](K_v) = \mathbb{Z}/3\mathbb{Z}$ for all complex places v and $E[\phi_{i,1}](K_v) = \mathbb{Z}/3\mathbb{Z}$ and $E[\phi_{i,2}](K_v) = 0$ for all real places.

Appealing to Lemma 3.7, we find for all such s, we have

$$t_1 \in [-\omega_1^{\text{sp}} - \omega_2^{\text{sp}} - d + r_2, -\omega_1^{\text{sp}} - \omega_2^{\text{sp}} + r_2]$$

and

$$t_2 \in [\omega_1^{\text{sp}} - \omega_2^{\text{sp}} - r_2, \omega_1^{\text{sp}} - \omega_2^{\text{sp}} - r_2 + d].$$

We now wish to appeal to Proposition 2.13 with $m = -t_1$ and $n = t_2$. Notice that if t_1 is positive, so that the choice $m = -t_1$ is not admissible, then $\omega_1^{\text{sp}} + \omega_2^{\text{sp}} \leq r_2$. Thus, both ω_1^{sp} and ω_2^{sp} would be bounded by r_2, and the conclusion of the theorem woud be trivial. Thus, we may assume that t_1 is negative, and hence that $m \geq \omega_1^{\text{sp}} + \omega_2^{\text{sp}} - r_2$. If t_2 is positive, then

$$m - |n| = -t_1 - t_2 \geq 2\omega_2^{\text{sp}} - d,$$

while if t_2 is negative,

$$m - |n| = -t_1 + t_2 \geq 2\omega_1^{\text{sp}} - 2r_2.$$

The claim now follows from Proposition 2.13. □

4.3. **Proof of Theorem 1.3.** For this theorem, we wish to construct elliptic curves E/F for which a vast majority of quadratic twists the group $Ш(E_s)[3]$ is large. We first loosely discuss the idea, continuing with the notation of the proof of Theorem 4.1. In particular, to be consistent with this notation, we will in fact prove the claim for the elliptic curve E'.

First, note that the explicit parametrization provided by Lemma 3.3 enables us to construct many elliptic curves for which $\mathcal{P}_3$ is empty by taking $v = 1$. Thus, every $s \in F^*/F^{*2}$ is subject to Theorem 4.1, so if both $\mathcal{P}_1$ and $\mathcal{P}_2$ are large, then a positive proportion of twists will have large 3-torsion in Ш. However, to ensure that this positive proportion is large, we need the rank bound coming from the second isogeny ϕ_2 to be very efficient. This bound is most efficient when $|\mathrm{ord}_3 c(\phi_{2,s})| \approx |\omega_1^{\mathrm{sp}} - \omega_2^{\mathrm{sp}}|$ is small. The elliptic curves we construct, therefore, will be chosen so that the sets $\mathcal{P}_1$ and $\mathcal{P}_2$ are close in size. The following lemma guarantees that we are able to find such curves.

Lemma 4.2. *Let F be a number field. There exists a constant r, depending only of F, such that for any $m \geq 1$ there are elliptic curves E with two independent 3-isogenies over F with $\mathcal{P}_3$ empty and $\#\mathcal{P}_1, \#\mathcal{P}_2 \in \{m, m+1, \ldots, m+r\}$.*

Proof. Suppose first that $F = \mathbb{Q}$ and recall the curve $E_{u,v}$ from Lemma 3.3. By taking $v = 1$ and $u \in \mathbb{Z}$, we may guarantee that $\mathcal{P}_3$ is trivial. In this case, we find that

$$\mathcal{P}_1 = \{p : p \mid u - 1\} \quad \text{and} \quad \mathcal{P}_2 = \{p : p \mid u^2 + u + 1\}.$$

Using a standard lower-bound sieve (e.g., the beta-sieve [11, Theorem 11.13] of dimension $\kappa = 2$), it follows that there are infinitely many u such that neither $u - 1$ nor $u^2 + u + 1$ is divisible by a prime $p \leq |u|^{1/4.84}$. This implies, in particular, that $u - 1$ is divisible by at most 4 primes while $u^2 + u + 1$ is divisible by at most 9 primes. The same conclusion holds for u satisfying any finite set of congruence conditions, apart from any divisibility conditions imposed by these conditions (e.g., if u is required to be 1 (mod p), then there are infintely many u such that $u - 1$ is divisible by p and at most four other primes). To prove the lemma when $F = \mathbb{Q}$, we therefore impose congruence conditions on u to guarantee that $u - 1$ and $u^2 + u + 1$ are divisible by at least m primes, and then appeal to this lower-bound sieve. This is straightforward: let $q_1, \ldots, q_{m-1} \equiv 1 \pmod 3$ be fixed primes, set $q = q_1 \ldots q_{m-1}$, and let α be such that $\alpha^2 + \alpha + 1 \equiv 0 \pmod q$. Let $p_1, \ldots, p_{m-1}$ be prime, distinct from the q_i, and consider $u = p_1 \ldots p_{m-1} u_1$ where $u_1 \equiv \alpha/(p_1 \ldots p_{m-1}) \pmod q$. This construction yields the lemma in the case $F = \mathbb{Q}$ with $r = 8$.

For general F, we again apply a lower-bound sieve, this time to points of bounded height in Minkowski space. The sieve has exponent of distribution at least $1/d - \epsilon$ for any $\epsilon > 0$ and is of dimension $\kappa = 2$ if $\mu_3 \not\subset F$ and of dimension $\kappa = 3$ if $\mu_3 \subset F$. Analogous to the case $F = \mathbb{Q}$, we find there is some constant r such that for infinitely many $u \in \mathcal{O}_F$, neither $u - 1$ nor $u^2 + u + 1$ has more than r prime factors; when $\kappa = 2$, we may take $r = \lfloor 9.68d \rfloor$, and when $\kappa = 3$, we may take $r = 2\lfloor 20d/3 \rfloor$. By imposing finitely many congruence conditions, the lemma follows. □

We are now ready to make explicit the proof of Theorem 1.3 outlined above.

Proof of Theorem 1.3. We will show that for a curve E constructed in Lemma 4.2, a proportion at least $1 - O(m^{-1/8})$ of twists E'_s have $\dim_{\mathbb{F}_3} Ш(E'_s)[3] \geq m - 2m^{7/8}$. Upon taking m sufficiently large, the claim will follow. Thus, let m be large and let E be a curve constructed as in Lemma 4.2. For convenience, assume each $\mathfrak{p}$ of multiplicative reduction has norm at least m.

With the notation of Theorem 4.1, by varying over $s \in F^*/F^{*2}$, we may think of ω_1^{sp} and ω_2^{sp} as sums of independent Bernoulli random variables. In particular, at a given prime $\mathfrak{p}$ of (potentially) multiplicative reduction, the reduction of E'_s is split for a proportion $\frac{1}{2} - \frac{1}{2\mathbf{N}(\mathfrak{p})+2}$ of $s \in F^*/F^{*2}$. Thus, we find the expected value of ω_1^{sp} to be

$$\mathbb{E}[\omega_1^{\mathrm{sp}}] = \sum_{\mathfrak{p} \in \mathcal{P}_1} \frac{1}{2} - \frac{1}{2\mathbf{N}(\mathfrak{p}) + 2} = m/2 + O(1).$$

A similar computation reveals its variance to be $m/4+O(1)$, with exactly the same results holding for ω_2^{sp}. We therefore find $\mathrm{ord}_3 c(\phi_{1,s}) = -\omega_1^{\mathrm{sp}} - \omega_2^{\mathrm{sp}} + O(1)$ to have expected value $-m+O(1)$ with variance $m/2+O(1)$. By Chebyshev's inequality, it follows that a proportion at least $1-O(m^{-3/4})$ of s are such that $\mathrm{ord}_3 c(\phi_{1,s}) \le -m + m^{7/8}$.

Similarly, as $\mathrm{ord}_3 c(\phi_{2,s}) = \omega_1^{\mathrm{sp}} - \omega_2^{\mathrm{sp}} + O(1)$, we find that it has expected value $O(1)$ with variance $m/2+O(1)$. By Chebyshev's inequality again, a proportion at least $1-O(m^{-1/2})$ of twists have $|\mathrm{ord}_3 c(\phi_{2,s})| \le m^{3/4}$. For such twists, the average rank of $\mathrm{Sel}_3(E'_s)$ is at most $m^{3/4} + 3^{-m^{3/4}}$, so that at least $1-O(m^{-1/8})$ of these have rank at most $m^{7/8}$. Pulling this together, we find that a proportion at least $1-O(m^{-1/8})$ of twists E'_s have $\dim_{\mathbb{F}_3} Ш(E'_s)[3] \ge m - 2m^{7/8}$. Upon taking m sufficiently large, the result follows. □

5. Curves with an 18-isogeny

In this section we assume E' is an elliptic curve over $\mathbb{Q}$ admitting a cyclic 18-isogeny. Then it also possess a cyclic 9-isogeny $\phi\colon E' \to E''$, and as before we decompose ϕ as $\phi = \phi_2 \circ \hat{\phi}_1$, where $\phi_1\colon E \to E'$ and $\phi_2\colon E \to E''$ are 3-isogenies.

Using the parametrization in [17], we may replace E', E and E'' with appropriate quadratic twists such that E' has an integral model of the form

$$y^2 - m^3xy = x^3 + (-2n^6 + n^3m^3)x^2 + (n^{12} - n^9m^3)x \tag{5.1}$$

with m, n relatively prime. Examining the Weierstrass c-invariants $c_4(E')$ and $c_6(E')$ of E', we find that the model (5.1) is minimal except possibly at $p=2$. At $p=2$, E' will have multiplicative reduction and the model (5.1) will be non-minimal if and only if $m \equiv n \pmod 2$, in which case $v_2(\Delta') = v_2(\Delta'_{\min}) + 12$.

The corresponding model for E'' is then given by

$$\begin{aligned} y^2 - m^3xy = x^3 + (&-6m^5n + 6m^4n^2 - 23m^3n^3 - 12m^2n^4 - 24mn^5 - 2n^6)x^2 \\ &- n(m-n)^9(m^2+mn+n^2)x. \end{aligned} \tag{5.2}$$

The model (5.2) will be minimal except possibly at 2 and 3. It will be non-minimal at 2 if and only if $m \equiv n \pmod 2$, in which case $v_2(\Delta'') = v_2(\Delta''_{\min}) + 12$. It will be non-minimal at 3 if and only if $m \equiv n \pmod 3$, in which case $v_3(\Delta'') = v_3(\Delta''_{\min}) + 24$ and E' has additive reduction at 3.

These models allow us to easily understand the places where E has bad reduction.

Lemma 5.1. *If E has additive, potentially good reduction at a prime p, then E has a twist E_s with good reduction at p.*

Proof. For $p \neq 3$, this is Lemma 3.2. For $p=3$, we observe that $v_3(c_4(E')) = v_3(c_6(E')) = 0$ if $m \not\equiv n \pmod 3$ and $v_3(c_4(E')) = 2$ and $v_3(c_6(E')) = 3$ if $m \equiv n \pmod 3$. Since E, and therefore E', is assumed to have bad reduction at 3, we therefore must be in the latter case. Twisting by 3, we then obtain a curve of good reduction at 3. □

Lemma 5.2. *If $p \ge 5$ divides $(n^2+nm+m^2)(4n^2-2nm+m^2)$, then E has multiplicative reduction at p with $v_p(j(E')) = 3v_p(j(E)) = v_p(j(E''))$.*

Proof. We have $\Delta_{E'} = m^9n^{18}(n-m)^2(2n+m)(n^2+nm+m^2)^2(4n^2-2nm+m^2)$ and $c_4(E') = (m^3+2n^3)(m^9+6m^6n^3-12m^3n^6+8n^9)$. A resultant computation then shows that any prime $p \ge 5$ dividing $(n^2+nm+m^2)(4n^2-2nm+m^2)$ can't divide $c_4(E')$, so E' must have multiplicative reduction at p. Further, since E' has multiplicative reduction at p, we will have $v_p(j(E')) = -v_p(\Delta_{E'}) = -v_p((n^2+nm+m^2)^2(4n^2-2nm+m^2))$, where the latter equality follows from a resultant computation between $(n^2+nm+m^2)(4n^2-2nm+m^2)$ and each of the other factors of $\Delta_{E'}$.

Since $\Delta_{E''} = mn^2(n-m)^{18}(2n+m)^9(n^2+nm+m^2)^2(4n^2-2nm+m^2)$, similar considerations show that $v_p(j(E'')) = -v_p(\Delta_{E''}) = -v_p((n^2+nm+m^2)^2(4n^2-2nm+m^2))$. We therefore have $v_p(j(E')) = v_p(j(E''))$, and the result follows from Lemma 3.4. □

Corollary 5.3. *If E is a not a twist of a curve in the isogeny class 14a, then there exist distinct primes $\ell_1, \ell_2 \geq 5$ such that E has multiplicative reduction at ℓ_i with $v_{\ell_i}(j(E')) = 3v_{\ell_i}(j(E)) = v_{\ell_i}(j(E''))$.*

Proof. It is an elementary exercise to show that the only coprime pairs (n, m) for which there do not exist distinct primes $\ell_1, \ell_2 \geq 5$ dividing $(n^2+nm+m^2)(4n^2-2nm+m^2)$ are $\pm(1,1)$, $\pm(1,-2)$, $\pm(1,-1)$, $\pm(1,2)$, $\pm(2,-1)$, and $\pm(1,4)$. The first two pairs correspond to singular curves and the final four pairs correspond to curves in the isogeny class $14a$ or twists of such curves by -3, and the result then follows from Lemma 5.2. □

Lemma 5.4. *If $p \neq 3$ divides the denominator of $\Delta_{E'}/\Delta_{E''} = \frac{m^8n^{16}}{(m-n)^{16}(m+2n)^8}$, then E has (potential) multiplicative reduction at p with $9v_p(j(E')) = 3v_p(j(E)) = v_p(j(E''))$. The same holds for $p = 3$ if it divides the denominator of $\Delta_{E'}/\Delta_{E''}$ to order greater than 24.*

Proof. If $p \neq 3$ divides the denominator of $\Delta_{E'}/\Delta_{E''}$, then E must have bad reduction at p. The same holds for $p = 3$ if it divides the denominator of $\Delta_{E'}/\Delta_{E''}$ to order greater than 24. For $p \geq 5$, taking the resultant of each of $(m-n)$ and $(m+2n)$ with $c_4(E')$ shows that E' must have multiplicative reduction at p. For $p = 2$, it suffices, as noted above, that E' always has multiplicative reduction at 2.

For $p = 3$, we will have p dividing the denominator of $\Delta_{E'}/\Delta_{E''}$ to order greater than 24 if and only if $m \equiv n \pmod 9$ or $m \equiv -2n \pmod 9$. In each of these cases, we will have $v_3(\Delta_{E''}) \geq 32$ and $v_3(\Delta_{E''_{\min}}) \geq 8$. As a result, E'' can't have a twist of good reduction, since that would require $v_3(\Delta_{E''_{\min}}) = 6$. Applying Lemma 5.1, we find that E must have potentially multiplicative reduction.

Finally, we observe that by Lemma 3.4, for $p \neq 3$, we will have $9v_p(j(E')) = 3v_p(j(E)) = v_p(j(E''))$ if and only if $v_p(\Delta_{E'}) < v_p(\Delta_{E''})$ and for $p = 3$, we will have $9v_p(j(E')) = 3v_p(j(E)) = v_p(j(E''))$ if and only if $v_p(\Delta_{E'}) < v_p(\Delta_{E''}) - 24$, since the valuation of p in the denominator of the j-invariant will be the same as the valuation of the p in the minimal discriminant. □

Corollary 5.5. *If E is not a twist of a curve in the isogeny class 14a, then there exists a prime ℓ_3 such that E has (potential) multiplicative reduction at ℓ_3 with $9v_{\ell_i}(j(E')) = 3v_{\ell_i}(j(E)) = v_{\ell_i}(j(E''))$.*

Proof. By Lemma 5.4, it suffices to show that the denominator of $\Delta_{E'}/\Delta_{E''} = \frac{m^8n^{16}}{(m-n)^{16}(m+2n)^8}$ is not equal to ± 1 or $\pm 3^{24}$. Elementary arguments show that this is the case for $(n, m) \neq \pm(-2, 1)$, $\pm(1, 4)$, which correspond to curves in the isogeny class $14a$ or twists of such curves by -3. □

As a consequence of these results, we obtain the following:

Proposition 5.6. *If E is not a quadratic twist of a curve in the isogeny class 14a, then $T_{-3}(\phi_1) \cap T_{-1}(\phi_2)$ is non-empty.*

Proof. By Corollary 5.3, we may find primes ℓ_1 and ℓ_2 that fall into case (ii) of Lemma 3.4. Thus, by Lemma 2.10, there is a twist s such that $c_{\ell_j}(\phi_{i,s}) = 1/3$ for all $i, j \in \{1, 2\}$.

By Corollary 5.5, we may also find a prime ℓ_3 such that $v_{\ell_3}(j(E'')) = 3v_{\ell_3}(j(E)) = 9v_{\ell_3}(j(E'))$.

If $\ell_3 \neq 3$, then $c_{\ell_3}(\phi_{1,s}) = 1/3$ and $c_{\ell_3}(\phi_{2,s}) = 3$ for some s by Lemma 2.10. By Lemma 3.6 combined with Lemma 2.4, we may additionally find s such that $c_3(\phi_{1,s})c_\infty(\phi_{1,s}) = c_3(\phi_{2,s})c_\infty(\phi_{2,s}) = 1$. Taking s satisfying all of the above further satisfying $c_p(\phi_{1,s}) = 1 = c_p(\phi_{2,s})$ for all $p \nmid 3\ell_1\ell_2\ell_3\infty$, we will then have $c(\phi_{1,s}) = 1/27$ and $c(\phi_{2,s}) = 1/3$, showing that $T_{-3}(\phi_1) \cap T_{-1}(\phi_2)$ is non-empty.

If $\ell_3 = 3$, then by Table 1 in [8], there is some s such that $c_3(\phi_{1,s}) = 1$ and $c_\infty(\phi_{2,s}) = 3$. By Lemma 2.4, we may therefore find s such that $c_3(\phi_{1,s})c_\infty(\phi_{1,s}) = 1/3$ and $c_3(\phi_{2,s})c_\infty(\phi_{2,s}) = 3$.

The result then follows as before by taking s satisfying all of the above further satisfying $c_p(\phi_{1,s}) = 1 = c_p(\phi_{2,s})$ for all $p \nmid 3\ell_1\ell_2\ell_3\infty$. □

5.1. **Proof of Theorem 1.4.** To prove Theorem 1.4, we need the following result concerning 2-Selmer groups of elliptic curves with rational two-torsion.

Theorem 5.7. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and let E' be the curve which is 2-isogenous to E. Let $r \geq 0$ be an integer and let γ be a specified class in $\prod_{v|2N_E\infty} \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$. If $\Delta_E\Delta_{E'}$ is not a square, then at least $1/2$ of the twists of E by $s \in \gamma$ have $|\mathrm{Sel}_2(E_s)| \geq 2^r$.*

Proof. This is essentially due to the main result of Xiong [27] and of Klagsbrun and Lemke Oliver [15]. While neither result explicitly allows for restricting to $s \in \gamma$, each relies on a variant of the classical Erdős–Kac theorem on the distribution of additive functions, and standard techniques allow for the imposition of a fixed congruence condition. For example, the proof of [15, Theorem 1.3] is heavily based on the methods of Granville and Soundararajan [13] that connect the Erdős–Kac theorem to ideas from sieve theory, where it is straightforward to impose a fixed congruence condition. □

The following lemma shows that the hypothesis of Theorem 5.7 that $\Delta_E\Delta_{E'}$ is not a square is always satisfied in the cases in which we wish to apply the result.

Lemma 5.8. *Suppose that $E/\mathbb{Q}$ is an elliptic curve such that $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and additionally suppose that E has a rational 3-isogeny. If $E'/\mathbb{Q}$ is the curve that is 2-isogenous to E, then $\Delta_E\Delta_{E'}$ is not a square.*

Proof. As the modular curve $X_0(6)$ has genus 0, it follows from a rational parametrization given by Maier [17] that there is some $t \in \mathbb{Q}$ such that

$$j(E) = \frac{(t+6)^3(t^3+18t^2+84t+24)^3}{t(t+8)^3(t+9)^2}, \quad t \neq 0, -8, -9.$$

It follows that E is a quadratic twist of the curve with $c_4 = (t+6)(t^3+18t^2+84t+24)$ and $c_6 = (t^2+12t+24)(t^4+24t^3+192t^2+504t-72)$ and discriminant $t(t+8)^3(t+9)^2 \in t(t+8)\mathbb{Q}^{*2}$. Since taking quadratic twists changes the discriminant by sixth powers, we find that $\Delta_E \in t(t+8)\mathbb{Q}^{*2}$. A similar computation reveals that $\Delta_{E'} \in (t+9)\mathbb{Q}^{*2}$. Thus, $\Delta_E\Delta_{E'}$ is a square if and only if there is a rational $y \neq 0$ such that $y^2 = t(t+8)(t+9)$. This equation defines an elliptic curve, which is observed to have rank 0 and Mordell-Weil group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Q}$. The three points of order two correspond exactly to the trivial solutions $t = 0, -8, -9$ ruled out above, and the lemma follows. □

Proof of Theorem 1.4. Let $E'/\mathbb{Q}$ have a cyclic 18-isogeny, and recall we are trying to show that a positive proportion of twists of E' have an element of order 6 in their Tate-Shafarevich groups. In addition to the 9-isogeny ϕ discussed above, it also follows that E' has a rational two-torsion point. Moreover, by Lemma 5.8 E' is subject to Theorem 5.7.

Suppose that E' is not a twist of a curve in the isogeny class 14a. By Proposition 5.6, the set $T_{-3}(\phi_1) \cap T_{-1}(\phi_2)$ is non-empty, so that by Proposition 2.13, a proportion at least $5/6$ of $s \in T_{-3}(\phi_1) \cap T_{-1}(\phi_2)$ are such that $|Ш(E'_s)[3]| \geq 9$. Combining this with Theorem 5.7, we find that a proportion at least $1/3$ of $s \in T_{-3}(\phi_1) \cap T_{-1}(\phi_2)$ are such that $Ш(E'_s)$ has an element of order 6. This establishes the theorem. □

Theorem 5.7 and Lemma 5.8 together also quickly imply the following result.

Corollary 5.9. *Suppose that $E/\mathbb{Q}$ has a rational degree 6 isogeny. Then for any $r_2 \geq 1$ and $\epsilon > 0$, $|Ш(E_s)[2]| \geq 4^{r_2}$ for a proportion at least $1/2 - \epsilon$ of twists E_s.*

Proof. Since E has a degree 6 isogeny, it also possesses a degree 3 isogeny ϕ. Let m be any integer for which $T_m(\phi)$ is non-empty. By Theorem 2.12, it follows that as $r_3 \to \infty$, a proportion $1-O(1/r_3)$ of twists by $s \in T_m(\phi)$ have $|\mathrm{Sel}_3(E_s)| \leq 3^{r_3}$. Combining this with Theorem 5.7 and Proposition 2.13, the claimed result follows for the relative proportion of such $s \in T_m(\phi)$. Adding these proportions across those m for which $T_m(\phi)$ is non-empty, we obtain the corollary. □

6. Exploiting Modular Curves

In this section, we prove Theorem 1.5 and Corollaries 1.6-1.8 We begin with Theorem 1.5.

Proof of Theorem 1.5. We begin by recalling the setup. We are given a non-cuspidal point $x \in X_0(3p)(F)$. Label the four cusps $\mathfrak{c}_i$, $i \in \{1, 3, p, 3p\}$, of $X_0(3p)(F)$ according to their ramification degree, so that ω_i is the number of primes at which x and $\mathfrak{c}_i$ have the same reduction. Now, let E/F be any elliptic curve corresponding to the point x on $X_0(3p)(F)$. Then E has an F-rational 3-isogeny $\phi\colon E \to E'$ and an F-rational p-isogeny $\psi\colon E \to E''$. We will ultimately apply Proposition 2.13 to these two isogenies, so we begin by analyzing their Selmer ratios.

Let $\mathfrak{p} \nmid 3p$ be a prime for which $\bar{x} = \bar{\mathfrak{c}}_i$ for some i. If $r \geq 1$ is such that x and $\mathfrak{c}_i$ have the same reduction $\pmod{\mathfrak{p}^r}$ but not $\pmod{\mathfrak{p}^{r+1}}$, then $v_\mathfrak{p}(j(E)) = -ri$. Moreover, by considering the action of the Fricke involutions W_3 and W_p on $X_0(3p)$, we find that

$$(-v_\mathfrak{p}(j(E')), -v_\mathfrak{p}(j(E''))) = \begin{cases} (3r, pr) & \text{if } i = 1, \\ (r, 3pr) & \text{if } i = 3, \\ (3pr, r) & \text{if } i = p, \text{ and} \\ (pr, 3r) & \text{if } i = 3p. \end{cases}$$

Taking E_s to be a twist such that E_s has split multiplicative reduction at $\mathfrak{p}$, we get $c_\mathfrak{p}(\phi_s) = 3$ and $c_\mathfrak{p}(\psi_s) = p$ in the case $i = 1$ and $c_\mathfrak{p}(\phi_s) = 1/3$ and $c_\mathfrak{p}(\psi_s) = p$ in the case $i = 3$ by Lemma 2.10. Thus,

$$\prod_{\mathfrak{p}:\bar{x}=\bar{\mathfrak{c}}_1 \text{ or } \bar{\mathfrak{c}}_3} c_\mathfrak{p}(\phi_s) = 3^{\omega_1-\omega_3} \text{ and } \prod_{\mathfrak{p}:\bar{x}=\bar{\mathfrak{c}}_1 \text{ or } \bar{\mathfrak{c}}_3} c_\mathfrak{p}(\psi_s) = p^{\omega_1+\omega_3}.$$

At all other primes $\mathfrak{p} \nmid 3p$, we may choose s so that $c_\mathfrak{p}(\phi_s) = c_\mathfrak{p}(\psi_s) = 1$. At primes $\mathfrak{p} \mid 3$, we choose s so that $c_\mathfrak{p}(\psi_s) = 1$. At worst, for this s we have

$$3^{-d} \leq \prod_{\mathfrak{p}|3} c_\mathfrak{p}(\phi_s) \leq 3^{2d}.$$

At $\mathfrak{p} \mid p$, we may at the very least choose s so that $c_\mathfrak{p}(\psi_s) \geq 1$ while maintaining $c_\mathfrak{p}(\phi_s) = 1$. Compiling these contributions, we have

$$3^{\omega_1-\omega_3-d} \leq \prod_{\mathfrak{p}<\infty} c_\mathfrak{p}(\phi_s) \leq 3^{\omega_1-\omega_3+2d} \quad \text{and} \quad \prod_{\mathfrak{p}<\infty} c_\mathfrak{p}(\psi_s) \geq p^{\omega_1+\omega_3}.$$

Thus, there are two extremes to be concerned with: either $v_3(c(\phi_s))$ could be large and positive, or $v_3(c(\phi_s))$ could be large and negative. Considering the infinite places, in the first case, there is a choice of s for which $v_p(c(\psi_s)) - v_3(c(\phi_s)) \geq 2\omega_3 - 2d$, while in the latter, there is a choice for which $v_p(c(\psi_s)) - |v_3(c(\phi_s))| \geq 2\omega_1 - 2d$. The result now follows from Proposition 2.13. □

We now proceed to the proofs of the associated corollaries to Theorem 1.5.

Proof of Corollary 1.6. Let x be the point on the modular curve $X(1)$ corresponding to E and let F be the field $\mathbb{Q}(x')$ where x' is a preimage of x under the degree $4p+4$ covering $X_0(3p) \to X(1)$. At each prime ℓ at which E has multiplicative reduction, the point x reduces to the (unique) cusp of $X(1)$, so at any prime $\mathfrak{l}$ of F lying over ℓ, the point x' must reduce to one of the four cusps of $X_0(3p)$. In fact, by our assumption on the Galois action on $E[3p]$, we must have that $\ell\mathcal{O}_F = \mathfrak{l}_1\mathfrak{l}_3\mathfrak{l}_p\mathfrak{l}_{3p}$, where the reduction of x' on $X_0(3p) \pmod{\mathfrak{l}_i}$ is the same as that of $\mathfrak{c}_i$. As we have assumed that there

are at least $4p+4+r$ such primes ℓ, it follows that each $\omega_i \geq 4p+4+r$. The result now follows from Theorem 1.5. □

Proof of Corollary 1.7. Let $E\colon y^2+xy+y = x^3+x^2-13x-219$ be the elliptic curve with Cremona label 50b3. We wish to show that $|Ш(E_s)[5]| \geq 25$ for an explicit set of s. E has both a 3-isogeny $\phi\colon E \to E'$ and a 5-isogeny $\psi\colon E \to E''$, where E' and E'' have Cremona labels 50b4 and 50b1, respectively. We claim that if $s \equiv 1 \pmod 8$ is a positive squarefree integer coprime to 5, then the two global Selmer ratios are given by $c(\phi_s) = 1$ and $c(\psi_s) = 25$. It then follows from Proposition 2.13 that for at least 50% of such s, $E_s(\mathbb{Q})$ will have rank 0 and $|Ш(E_s)[5]| \geq 25$. Thus, the theorem will follow from the claim about the global Selmer ratios of ϕ_s and ψ_s.

The curve E has split multiplicative reduction of Kodaira type I_1 at $p=2$ and additive reduction of Kodaira type II^* at $p=5$. By Proposition 2.4, it follows that $c_2(\phi_s) = 3$ for all squarefree $s \equiv 1 \pmod 8$ and $c_5(\phi_s) = 1$ for all s that are coprime to 5. In addition, a computation in `Magma` [4] shows that $c_3(\phi_s) = 1$ for all s and $c_\infty(\phi_s) = 1/3$ for all positive s. We thus find that for s as claimed, we have $c(\phi_s) = 1$.

We now consider $c(\psi_s)$. From [8, Table 1], we see that $c_2(\psi_s) = 5$ for all squarefree $s \equiv 1 \pmod 8$. The field $\mathbb{Q}(\ker\psi) = \mathbb{Q}\big(\sqrt{5\sqrt{5}-50}\big)$ is totally complex, so it follows that $c_\infty(\psi_s) = 1$ for all positive s. Lastly, $c_5(\psi_s) = c_5(E_s'')/c_5(E_s)\cdot\alpha_{\psi_s,\mathbb{Q}_5}$. Since E has Kodaira type II^* at $p=5$, it follows that $c_5(E_s'')/c_5(E_s) = 1$ for all s. Observe that $\Delta_E = -2\cdot 5^{10}$ while $\Delta_{E''} = -2^5\cdot 5^2$, so that by [12, Theorem 1], $\alpha_{\psi_s,\mathbb{Q}_5} = 5$ for all s coprime to 5. Pulling this together, we find that $c(\psi_s) = 25$ for all positive squarefree $s \equiv 1 \pmod 8$ that are coprime to 5, and the theorem follows. The claim about the elliptic curve 50b4 follows along the same lines. □

We now turn to the proof of Corollary 1.8 concerning fields over which the modular curves $X_0(15)$ and $X_0(21)$ have infinitely many points. Recall that $X_0(15)$ and $X_0(21)$ both have genus one, so that they may be given the structure of an elliptic curve. The following lemma will be used to find rational points which reduce to specified cusps modulo many primes.

Lemma 6.1. *Let E/F be an elliptic curve of positive rank and let $T \in E(F)$ be a non-trivial torsion point. Fix an integral model for E. Given any ω_1 and ω_3, there exist distinct primes $\mathfrak{p}_1,\dots,\mathfrak{p}_{\omega_1}$ and $\mathfrak{q}_1,\dots,\mathfrak{q}_{\omega_3}$ for which there are infinitely many points $P \in E(F)$ for which $P \equiv \mathcal{O} \pmod{\mathfrak{p}_i}$ for each $i \leq \omega_1$ and $P \equiv \bar{T} \pmod{\mathfrak{q}_j}$ for each $j \leq \omega_3$.*

Proof. Let $P \in E(F)$ be of infinite order. Let d be the order of T. Let $w = \max(\omega_1,\omega_3)$, and let $\ell_1,\dots,\ell_w \in \mathbb{Z}$ be any odd primes congruent to 1 (mod d) and sufficiently large that both $\ell_i P$ and $\ell_i P - T$ have a denominator divisible by a prime not dividing the denominator of P or $P-T$; as any elliptic curve has only finitely many S-integral points (see Corollary IX.3.2.1 in [25], for example), this is always possible. Let $\mathfrak{p}_i$ be a prime for which the denominator of $\ell_i P$ has a non-trivial valuation and let $\mathfrak{q}_i$ be such a prime for $\ell_i P - T$. Set $\ell = \ell_1\dots\ell_w$. Then for any integer $n \equiv 1 \pmod d$, the point $n\ell P$ satisfies the desired conditions. □

Proof of Corollary 1.8. Suppose that $p=5$ or $p=7$. The embedding $X_0(3p) \to J_0(3p)$ given by $x \mapsto [x]-[\mathfrak{c}_1]$ is an isomorphism, endowing $X_0(3p)$ with the structure of an elliptic curve E. Moreover, by the Manin-Drinfeld theorem, the cusps $\mathfrak{c}_i$ of $X_0(3p)$ are torsion points in the Mordell-Weil group $E(F)$. For any $r \geq 1$, let $\omega_1 = \omega_3 = r+2d$. Applying Lemma 6.1 with $T = [\mathfrak{c}_3]-[\mathfrak{c}_1]$, we find infinitely many points $x \in X_0(3p)(F)$ for which Theorem 1.5 produces a curve E/F with $|Ш(E_s/F)[p]| \geq p^{2r}$ for a positive proportion of twists. This is Corollary 1.8. □

Remark 6.2. The proof of Lemma 6.1 could likely be adapted to show that when the points P of $E(F)$ are ordered by height, almost all will be such that the conclusion of the lemma holds for fixed values of ω_1 and ω_3. For example, most integers n have at least $\frac{1}{2}\log\log n$ prime factors, so that there are at least $\frac{1}{2}\log\log n$ primes contributing to ω_1 for most points nP. Similarly, most n also

have at least $\frac{1}{2\phi(d)} \log\log n$ prime factors congruent to 1 (mod d). Since $\ell nP - T = \ell \cdot (nP - T)$ for such a prime ℓ, it follows that most points nP will also have $\geq \frac{1}{2\phi(d)} \log\log n$ primes contributing to ω_3. This argument essentially suffices in the case that $E(F)$ has rank 1, and we expect an analogous argument can be made in higher rank.

7. Exploiting primes of (potential) good reduction

Let p be an odd prime. If $E/\mathbb{Q}$ is an elliptic curve with irreducible $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-representation $E[3p]$, then our techniques can say nothing about the average size of $Ш(E_s)[p]$ as s varies over $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, since E admits neither a 3-isogeny nor a p-isogeny over $\mathbb{Q}$.

This is of course no longer the case if we base change E to a sufficiently large extension, a fact that we took advantage of in the proof of Corollary 1.6. However, Corollary 1.6 requires that E have a large number of places of multiplicative reduction, imposing a significant restriction on E.

In the proof of Theorem 1.9 that follows, we show how similar results can be obtained by exploiting primes dividing the degrees of the two isogenies. This allows us to extend our results to many additional curves, including those with everywhere potentially good reduction.

Proof of Theorem 1.9. $E/\mathbb{Q}$ is an elliptic curve with potentially good and ordinary reduction at 3 and p, and $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts transitively on the set of $\mathbb{F}_\ell$-lines in $E[\ell]$ for both $\ell = 3$ and $\ell = p$. It follows that $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the $\mathbb{F}_\ell$-lines in $E_s[\ell]$ as well, where $K = \mathbb{Q}(E[3p])$.

We now replace E by its base change to $K = \mathbb{Q}(E[3p])$; then E/K has everywhere semi-stable reduction. Let $\psi\colon E \to E'$ be any of the $p+1$ isogenies of degree p emanating from E defined over K, and $\phi\colon E \to E_0$ be any of the four 3-isogenies out of E, all of which are defined over K as well. We restrict our focus to the subset S of elements $s \in K^*/K^{*2}$ such that

$$c_\ell(\phi_s) = 1 = c_\ell(\psi_s)$$

for all primes ℓ of K at which E has multiplicative reduction. By Lemmas 2.10 and 2.7, this condition holds whenever E_s does not have split multiplicative reduction at ℓ, so S has positive density. We now claim that the average rank of E_s for $s \in S$ is at most $\frac{d}{2} + 3^{-6}$, where $d = \frac{1}{2}[K:\mathbb{Q}]$.

Since $c_\ell(\phi_s) = 1$ at all places where E has bad reduction, Corollary 2.11 says $c(\phi_s) = c_\infty(\phi_s)c_3(\phi_s)$, where $c_p(\phi) = \prod_{\mathfrak{p}|p} c_\mathfrak{p}(\phi)$. As K is totally complex, we have $c_\infty(\phi_s) = 3^{-d}$. For $\mathfrak{p} \mid 3$, Lemma 2.8 says that $c_\mathfrak{p}(\phi_s)$ is either $3^{[K_\mathfrak{p}:\,\mathbb{Q}_3]}$ or 1, depending on whether $\ker\phi$ reduces mod $\mathfrak{p}$ to the kernel of absolute Frobenius (the "canonical subgroup").

The primes of K above 3 are permuted transitively by $\mathrm{Gal}(K/\mathbb{Q})$ and this Galois action is compatible the $\mathrm{Gal}(K/\mathbb{Q})$-action on the canonical subgroups: if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ then the canonical subgroup of E over $K_{\mathfrak{p}^\sigma}$ is $(\ker\phi)^\sigma$. It follows that $\ker\phi_s$ is the kernel of Frobenius for exactly $1/4$ of all primes $\mathfrak{p}$ of K above 3. Therefore $c_3(\phi_s) = 3^{d/2} \cdot 1^{3d/2} = 3^{d/2}$, which gives $c(\phi_s) = 3^{-d/2}$. Hence, by Theorem 2.12, the average rank of E_s for $s \in S$ is at most $\frac{d}{2} + \frac{1}{3^{d/2}}$. Since K contains ζ_3 and ζ_p, we have $2(p-1) \mid 2d$. Thus, $d/2$ is an integer greater than 1, and the average rank of E_s, for $s \in S$, is at most $\frac{d}{2} + \frac{1}{9}$.

Turning our attention to ψ, we observe that the same reasoning yields $c(\psi_s) = p^{2d/(p+1)-d}$. It follows that $\mathrm{Sel}_p(E'_s)$ has $\mathbb{F}_p$-dimension at least $d - \frac{2d}{p+1}$ for all $s \in S$. However, a positive proportion of twists E'_s by $s \in S$ have rank at most $\frac{d}{2}$. For these s, we conclude that $\dim_{\mathbb{F}_p} Ш(E'_s)[p]$ is at least

$$d - \frac{2d}{p+1} - \frac{d}{2} = \frac{d}{2}\left(1 - \frac{4}{p+1}\right), \tag{7.1}$$

which tends to $\frac{d}{2}$ as $p \to \infty$ and is positive for all $p \geq 5$. ∎

8. Tate-Shafarevich groups of CM elliptic curves

In this section we prove lower bounds for the average order of $Ш(E_s)[n]$, for a large class of elliptic curves E with complex multiplication, which is the content of Theorem 1.10. We will need two preliminary results.

Lemma 8.1. *Let E be an elliptic curve over a number field F, and suppose $\mathrm{End}_F(E)$ is the quadratic ring of discriminant Df^2, with D a fundamental discriminant. Then there exists a cyclic f-isogeny $\phi\colon E \to E_0$ such that $\mathrm{End}_F(E_0)$ has discriminant D.*

Proof. Let $K = \mathbb{Q}(\sqrt{D})$, and let $\mathcal{O}_K$ be its ring of integers. We identify $\mathrm{End}_F(E)$ with the order $\mathcal{O}$ of index f inside $\mathcal{O}_K$. Then $f\mathcal{O}_K \subset \mathcal{O}$ is an $\mathcal{O}$-ideal and the desired isogeny ϕ is the isogeny $\phi\colon E \to E/E[f\mathcal{O}_K]$. Indeed, $\ker\phi \simeq E[f\mathcal{O}_K] \simeq \mathcal{O}/f\mathcal{O}_K \simeq \mathbb{Z}/f\mathbb{Z}$, so ϕ is a cyclic f-isogeny. Moreover, if we define $E_0 = E/E[f\mathcal{O}_K]$, then $\mathrm{End}_F(E_0) \simeq \mathcal{O}_K$, by [14, Thm. 20]. □

Proposition 8.2. *Suppose $\phi\colon E \to E_0$ is as in Lemma 8.1, and $f = p^n$ for some prime p. If $\mathfrak{p}$ is a prime of F above p of (potentially) ordinary reduction for E, then $c_{\mathfrak{p}}(\phi) = p^{n[F_{\mathfrak{p}}\colon \mathbb{Q}_p]}$.*

Proof. Since $\mathfrak{p}$ is a prime of potentially ordinary reduction, by [8, Table 1], to compute $c_{\mathfrak{p}}(\phi)$, we may replace $F_{\mathfrak{p}}$ by a finite extension over which E has good ordinary reduction. So we may assume that this is the case already for E over F.

We let $\bar{\phi}\colon \bar{E} \to \bar{E}_0$ be the induced isogeny of elliptic curves over the residue field $\mathbb{F}_{\mathfrak{p}}$. The key point is that $\ker\bar{\phi}$ is connected, i.e. $\bar{\phi}$ is (up to isomorphism) the nth power of the absolute Frobenius isogeny of E over $\mathbb{F}_{\mathfrak{p}}$. In other words, $\ker\phi$ is the canonical subgroup of $E[p^n]$. To see this, note that $\psi \circ \phi = [p^n]$, for some cyclic p^n-isogeny $\psi\colon E_0 \to E$. The canonical subgroup C in $E_0[p]$ is of the form $E_0[\mathfrak{a}]$ for some ideal $\mathfrak{a} \subset \mathcal{O}_K$, so $\mathrm{End}(E_0/C) \simeq \mathcal{O}_K$. It follows that $\ker\psi$ intersects trivially with the canonical subgroup of $E_0[p]$. Indeed, if the intersection were non-trivial, then $\psi\colon E_0 \to E$ would factor through an isogeny of degree $p^{n-1}\colon E_0/C \to E$. This is impossible, since $\mathrm{Disc}(\mathrm{End}(E)) = p^n\mathrm{Disc}(\mathrm{End}(E_0/C))$ and the discriminant changes by at most a factor of p under a p-isogeny (see e.g. [20, Cor. 4.3]).

We conclude that $\ker\bar{\psi}$ is étale, and hence $\ker\bar{\phi}$ is connected. In other words, $\ker\phi$ reduces to the formal group of E. By Lemma 2.8, we conclude that $c_{\mathfrak{p}}(\phi) = p^{n[F_{\mathfrak{p}}\colon \mathbb{Q}_p]}$. □

Proof of Theorem 1.10. On the one hand, by [3, Thm. 2.7], the average rank of E_s is at most 1. Since the rank of $E_s(F)$ is even, this means that at least 50% of these twists have rank 0. On the other hand, we will show that for all but finitely many $s \in F^\times/F^{\times 2}$, the f-Selmer group $\mathrm{Sel}_f(E_s)$ has size at least f^d. For those twists with rank 0, this implies that $|Ш(E_s)[f]| \geq f^d$, proving the theorem.

To give a lower bound for $|\mathrm{Sel}_f(E_s)|$, we choose E_0 over F with $\mathrm{End}_F(E_0) \simeq \mathcal{O}_K$ and such that there is a cyclic isogeny $\phi\colon E \to E_0$ of degree f, as in Lemma 8.1. We will show that $c(\phi_s) = f^d$, for all s. From Proposition 2.1, it will then follow that $\mathrm{Sel}_\phi(E_s)$ has size at least f^d, and hence $\mathrm{Sel}_f(E_s)$ has size at least f^d for all but finitely many s, which will complete the proof.

To compute $c(\phi_s)$, it suffices to consider the case $s = 1$. We need to compute $c_{\mathfrak{p}}(\phi)$ for all primes $\mathfrak{p}$ of F. If $\mathfrak{p}$ is a finite prime not dividing f, then Lemma 2.7 implies that $c_{\mathfrak{p}}(\phi) = 1$ since E_0 has a quadratic twist of good reduction (see [3, Proof of Thm. 11.2]). Next we consider primes p dividing f, and primes $\mathfrak{p}$ of F above p. Then E has potentially ordinary reduction at $\mathfrak{p}$, since p splits in K. We can factor $\phi\colon E \to E_0$ into a $\phi_2 \circ \phi_1$ with ϕ_2 a p-power isogeny and ϕ_1 a prime-to-p isogeny. As noted in Section 2, we then have $c_{\mathfrak{p}}(\phi) = c_{\mathfrak{p}}(\phi_1)c_{\mathfrak{p}}(\phi_2) = c_{\mathfrak{p}}(\phi_2)$ by Lemma 7.2(b) in [18]. Applying Proposition 8.2, this is equal to $p^{n[F_{\mathfrak{p}}\colon \mathbb{Q}_p]}$, where p^n is the highest power of p dividing f.

Finally, if $\mathfrak{p}$ is archimedean, then $\mathfrak{p}$ is complex since F necessarily contains K. We therefore have $\prod_{\mathfrak{p}|\infty} c_{\mathfrak{p}}(\phi) = f^{-[F\colon K]}$. Putting all of the local computations together, we conclude that

$$c(\phi) = \left(\prod_{p|f}\prod_{\mathfrak{p}|p} c_{\mathfrak{p}}(\phi)\right)\prod_{\mathfrak{p}|\infty} c_{\mathfrak{p}}(\phi) = \left(\prod_{p|f}\prod_{\mathfrak{p}|p} p^{n[F_{\mathfrak{p}}\colon \mathbb{Q}_p]}\right) f^{-[F\colon K]} = \left(\prod_{p|f} p^{n[F\colon \mathbb{Q}]}\right) f^{-[F\colon K]}$$
$$= \left(\prod_{p|f} p^{n}\right)^{[F\colon \mathbb{Q}]} f^{-[F\colon K]} = f^{[F\colon \mathbb{Q}]} f^{-[F\colon K]} = f^{[F\colon K]} = f^d \tag{8.1}$$

as desired. □

Note that the interesting cases of Theorem 1.10 are for $f \geq 3$, and in those cases F has degree at least 4 over $\mathbb{Q}$. The degree of such an F necessarily grows with f, since the field of definition for any CM elliptic curve with $\mathrm{End}(E)$ of discriminant Df^2 is the ring class field of K of conductor f.

Example 8.3. If $f = 3$, we can take K to be any imaginary quadratic field in which 3 splits. In this case, F must contain $H(\sqrt{-3})$, where H is the Hilbert class field of K. Indeed, $H(\sqrt{-3})$ is the ring class field of K of conductor 3 whenever 3 splits in K. If K has class number 1, then we can take $F = K(\sqrt{-3})$, which is biquadratic over $\mathbb{Q}$. Theorem 1.10 then says that at least 50% of twists E_s have rank 0 and satisfy $|Ш(E_s)[3]| \geq 9$. If we base change this E to a number field F' of degree $2d$ over $\mathbb{Q}$, then half of all twists over F' have rank 0 and $Ш(E_s)[3]$ of size at least 3^d.

9. Tate-Shafarevich groups of CM abelian varieties

The approach used in the previous section can be extended to more general CM abelian varieties. We spell out the details in a particularly pretty example.

Let J be the Jacobian of the genus three Picard curve $C\colon y^3 = x^4 - x$. Over $\mathbb{Q}$, J has good reduction away from 3. Moreover, J is absolutely simple and has CM by $K = \mathbb{Q}(\zeta_9)$; see [3, §12]. The complex multiplication is defined over all fields containing K, so we will work for now over a general number field F containing K. Also write K^+ for the maximal totally real cubic subfield of K, which is an abelian cubic extension of $\mathbb{Q}$.

Let p be a prime of ordinary good reduction for J over $\mathbb{Q}$. For example, take p to be any prime which splits completely in K, or in other words such that $p \equiv 1 \pmod 9$. We can then write $p\mathcal{O}_K = \prod_{i=1}^6 \mathfrak{p}_i$, and $J[p] \simeq \bigoplus J[\mathfrak{p}_i]$.

Let $\mathfrak{p}$ be a prime of F above p, and let $\mathfrak{p}_i$ be the prime of K below it. Write $J_{\mathbb{F}_{\mathfrak{p}}}$ for the reduction of J over $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_F/\mathfrak{p}$. Over the completion $F_{\mathfrak{p}}$, there is a unique subgroup $C_{\mathfrak{p}}$ of $J[p]$ of order p^3 which lifts the kernel of the absolute Frobenius

$$\mathrm{Fr}\colon J_{\mathbb{F}_{\mathfrak{p}_i}} \to J^{(p)}_{\mathbb{F}_{\mathfrak{p}_i}} \simeq J_{\mathbb{F}_{\mathfrak{p}_i}}.$$

Note that $\mathbb{F}_{\mathfrak{p}_i} \simeq \mathbb{F}_p$. Since Frobenius commutes with the $\mathcal{O}_K$-action on $J_{\mathbb{F}_{\mathfrak{p}_i}}$, the kernel $C_{\mathfrak{p}}$ is more than just a group, it is an $\mathcal{O}_K$-submodule of $J[p] \simeq \mathcal{O}_K/p\mathcal{O}_K$. The $\mathcal{O}_K$-submodules of $\mathcal{O}_K/p\mathcal{O}_K$ of index p^3 are of the form $\mathfrak{n}/p\mathcal{O}_K$, for some ideal $\mathfrak{n} \subset \mathcal{O}_K$ which is a product of three distinct prime ideals above p. Hence $C_{\mathfrak{p}} = J[\mathfrak{n}_{\mathfrak{p}}]$, for some such ideal $\mathfrak{n}_{\mathfrak{p}} \subset \mathcal{O}_K$, which depends only on $\mathfrak{p}_i$, not $\mathfrak{p}$ itself.

Lemma 9.1. *If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then $\mathfrak{n}_{\sigma(\mathfrak{p}_i)} \simeq \sigma(\mathfrak{n}_{\mathfrak{p}_i})$.*

Proof. Given the explicit equations for C and $\zeta_9 \in \mathrm{Aut}(C)$, the lemma follows from transport of structure. More generally, it is a consequence of the Main Theorem of complex multiplication for CM abelian varieties. □

Lemma 9.2. *$C_{\bar{\mathfrak{p}}_i} \cap C_{\mathfrak{p}_i} = 0$, where $\bar{\cdot}$ denotes complex conjugation.*

Proof. Using the principal polarization on J, we may view the dual isogeny $\hat{\alpha}$, for any $\alpha \in \operatorname{End} J$, as an element of $\operatorname{End} J$. Moreover, if $\iota\colon \mathcal{O}_K \simeq \operatorname{End} J$ is our given identification of $\mathcal{O}_K$ with the endomorphism ring of J, then we have $\iota(\bar{\alpha}) = \widehat{\iota(\alpha)}$. Combining with the previous Lemma, we deduce that $C_{\bar{\mathfrak{p}}_i}$ reduces to $\ker \widehat{\mathrm{Fr}}$ over $\mathbb{F}_{\mathfrak{p}_i}$. Since J is ordinary at $\mathfrak{p}_i$, the latter is an étale group scheme. On the other hand, $C_{\mathfrak{p}_i}$ reduces to $\ker \mathrm{Fr}$ over $\mathbb{F}_{\mathfrak{p}_i}$, which is a connected group scheme. It follows that $C_{\bar{\mathfrak{p}}_i} \cap C_{\mathfrak{p}_i} = 0$. □

Since $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$, and complex conjugation has order 2, it follows from the preceding lemmas that the six ideals $\mathfrak{n}_{\mathfrak{p}_i}$ are (after re-indexing):

$$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4,\ \mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5$$

and their complex conjugates

$$\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6,\ \mathfrak{p}_5\mathfrak{p}_6\mathfrak{p}_1,\ \mathfrak{p}_6\mathfrak{p}_1\mathfrak{p}_2.$$

Note that $p\mathcal{O}_K = \mathfrak{n}_{\mathfrak{p}}\bar{\mathfrak{n}}_{\mathfrak{p}}$ and $A[p] = A[\mathfrak{n}_{\mathfrak{p}}] \oplus A[\bar{\mathfrak{n}}_{\mathfrak{p}}]$, where $\bar{\mathfrak{n}}_{\mathfrak{p}}$ denotes the complex conjugate of $\mathfrak{n}_{\mathfrak{p}}$. Also note that $C_{\mathfrak{p}}$ is defined over the number field K, and hence F as well. We refer to the $C_{\mathfrak{p}}$ as *canonical* subgroups.

For simplicity, let us now assume that F also contains the field $K(J[p])$ over which the action of G_K on the Galois module $J[p]$ of order p^6 becomes trivial.

Definition 9.3. A subgroup $C \subset J[p]$ of order p^3 is *anti-canonical* if it intersects trivially with all six canonical subgroups $C_{\mathfrak{p}_i}$.

There are many anti-canonical subgroups of $J[p]$. We describe one such subgroup below.

Example 9.4. Over $\mathbb{C}$ we have $J_{\mathbb{C}} \simeq \mathbb{C}^3/\mathcal{O}_K$, where the embedding of $\mathcal{O}_K$ as a full rank lattice in $\mathbb{C}^3$ is via the CM-type of J. We use this embedding to view all lattices in K as lattices in $\mathbb{C}^3$. Let $\mathcal{O}_p$ be the order $\mathcal{O}_{K^+} + p\mathcal{O}_K$ of index p^3 inside $\mathcal{O}_K$. There are natural $(\mathbb{Z}/p\mathbb{Z})^3$-isogenies of complex tori

$$\mathbb{C}^3/\mathcal{O}_K \simeq \mathbb{C}^3/p\mathcal{O}_K \to \mathbb{C}^3/\mathcal{O}_p \quad \text{and} \quad \mathbb{C}^3/\mathcal{O}_p \to \mathbb{C}^3/\mathcal{O}_K$$

which descend to isogenies of abelian varieties $\psi\colon J \to A$ and $\phi\colon A \to J$ over F. The composition $\phi \circ \psi$ is simply multiplication-by-p on J. Note also that $\operatorname{End}_F(A) \simeq \mathcal{O}_p$ and $\ker \phi = A[p\mathcal{O}_K]$. If we denote the kernel of ψ by C, then we claim that $C \subset J[p]$ has trivial intersection with all six canonical subgroups $C_{\mathfrak{p}} = J[\mathfrak{n}_{\mathfrak{p}}]$. This follows from the fact that $\mathcal{O}_p \cap \mathfrak{n}_{\mathfrak{p}} = p\mathcal{O}_K$.

For our purposes, anti-canonical subgroups $C \subset J[p]$ are interesting because they reduce injectively into $J_{\mathbb{F}_{\mathfrak{p}}}(\mathbb{F}_{\mathfrak{p}})$, for all primes $\mathfrak{p}$ of F above p. In particular, the isogeny $\psi\colon J \to J/C$ induces an isomorphism on formal groups, and so $\alpha_{\psi, F_{\mathfrak{p}}} = 1$ by Lemma 2.8. This is the last bit of input we need to prove the following theorem.

Theorem 9.5. *Let $p \equiv 1 \pmod 9$ be a prime, and let F be a number field containing $K(J[p])$. Let C be any anti-canonical subgroup of $J[p]$, and set $A = J/C$. Then at least 50% of all quadratic twists A_s have rank 0 and satisfy $|Ш(A_s)[p]| \geq p^{3d}$, where $[F\colon \mathbb{Q}] = 2d$.*

Proof. By [3, Thm. 12.5], the average rank of $J_s(F)$ is at most 3, and at least 50% of twists have rank 0. It follows that at least 50% of twists A_s have rank 0 as well. Let $\psi\colon J \to A$ be the natural quotient with kernel C, and let $\phi\colon A \to J$ be the unique isogeny (of degree p^3) such that $\phi \circ \psi = [3]$. We will show that the isogeny $\phi_s\colon A_s \to J_s$ satisfies $c(\phi_s) = p^{3d}$. It will then follow that for all but finitely many $s \in F^\times/F^{\times 2}$, we have $|\mathrm{Sel}_p(A_s)| \geq p^{3d}$. Hence, for those A_s with rank 0, we must have $|Ш(A_s)[p]| \geq p^{3d}$, which proves the theorem.

To compute $c(\phi_s)$, we first argue that $c_{\mathfrak{q}}(\phi_s) = 1$ for any prime $\mathfrak{q} \nmid p\infty$. This follows from Lemma 2.11 and the fact that A_s and J_s have quadratic twists of good reduction at $\mathfrak{q}$. (J has

good reduction at all primes of F above 3 by [23, §2].) On the other hand, $c_\infty(\phi_s) = p^{-3d}$, since F is totally complex. For primes $\mathfrak{p}$ of F above p, we claim that $c_\mathfrak{p}(\phi_s) = p^{3[F_\mathfrak{p}\colon \mathbb{Q}_p]}$. First note that $c_\mathfrak{p}(\phi_s) = \alpha_{\phi_s,F_\mathfrak{p}}$ since A_s and J_s have twists of good reduction. We also have $\alpha_{\phi_s,F_\mathfrak{p}} = \alpha_{[p],F_\mathfrak{p}}\alpha^{-1}_{\psi_s,F_\mathfrak{p}}$. Since C_s is anti-canonical, the extension of C_s to the Néron model of A over $\mathcal{O}_{F_\mathfrak{p}}$ is étale, and hence

$$\alpha_{\phi,F_\mathfrak{p}} = \alpha_{[p],F_\mathfrak{p}}\alpha^{-1}_{\psi,F_\mathfrak{p}} = p^{3[F_\mathfrak{p}\colon \mathbb{Q}_p]} \cdot 1 = p^{3[F_\mathfrak{p}\colon \mathbb{Q}_p]}.$$

Putting everything together, we find that

$$c(\phi_s) = p^{-3d} \cdot \left(\prod_{\mathfrak{p}|p} p^{3[F_\mathfrak{p}\colon \mathbb{Q}_p]}\right) = p^{-3d}\left(p^{3[F:\mathbb{Q}]}\right) = p^{-3d}p^{6d} = p^{3d},$$

which concludes the proof. □

10. Example: The isogeny family 14a

This section concerns the isogeny class of elliptic curves with Cremona label 14a. In particular, the curve with Cremona label 14a1

$$E\colon y^2 + xy + y = x^3 + 4x - 6$$

has conductor 14 and admits two independent 3-isogenies $\phi_1\colon E \to E'$ and $\phi_2\colon E \to E''$, where E' and E'' have Cremona labels 14a3 and 14a4, respectively. Over $\mathbb{Q}_2$, the curves E, E', and E'' have nonsplit multiplicative reduction with Kodaira types I_6, I_{18}, and I_2, respectively. Over $\mathbb{Q}_7$, E has split multiplicative reduction of type I_3, while E' and E'' have type I_1. Additionally, we find that $\ker\phi_1 \simeq \mathbb{Z}/3\mathbb{Z}$ and $\ker\phi_2 \simeq \mu_3$.

Thus, using Proposition 2.4, we find $c_2(\phi_{1,s}) = 3$ and $c_2(\phi_{2,s}) = 1/3$ if $s \equiv 5 \pmod 8$, and $c_2(\phi_{1,s}) = c_2(\phi_{2,s}) = 1$ otherwise. Similarly, we find $c_7(\phi_{1,s}) = 1/3 = c_7(\phi_{2,s})$ if $s \equiv 1, 2, 4 \pmod 7$, and that both are equal to 1 otherwise. Over $\mathbb{Q}_3$, E has good ordinary reduction, and the points of $\ker\phi_1$ reduce injectively modulo 3. By Lemma 2.8, we have $c_3(\phi_{1,s}) = 1$ and $c_3(\phi_{2,s}) = 3$ for all s. Finally, we also find that $c_\infty(\phi_{1,s}) = 1/3$ when s is positive and $c_\infty(\phi_{1,s}) = 1$ when s is negative, and vice versa for $c_\infty(\phi_{2,s})$.

Thus, we see that

$$\mathbb{Z} \setminus \{0\} = T_{-2}(\phi_1) \cup T_{-1}(\phi_1) \cup T_0(\phi_1) \cup T_1(\phi_1)$$

and

$$\mathbb{Z} \setminus \{0\} = T_{-2}(\phi_2) \cup T_{-1}(\phi_2) \cup T_0(\phi_2) \cup T_1(\phi_2).$$

To compute the densities of these sets and their intersections, we find it convenient to use a generating function (in fact, a generating polynomial). From the local computations above, we find

$$\begin{aligned}\sum_{m\in\mathbb{Z}} \mu(T_m(\phi_1))q^m &= \left(\frac{1+q^{-1}}{2}\right)\left(\frac{q}{6}+\frac{5}{6}\right)\left(\frac{27}{48}+\frac{21}{48}q^{-1}\right)\\ &= \frac{35}{192}q^{-2} + \frac{29}{64}q^{-1} + \frac{61}{192} + \frac{3}{64}q.\end{aligned}$$

Thus, for example, the set $T_0(\phi_1)$ has density 61/192, so that by Theorem 2.12 at least $61/384 \approx 15.88\%$ of twists $E_s/\mathbb{Q}$ have rank 0. This expression also yields a bound of $\frac{1183}{864} \approx 1.369$ on the average rank of twists $E_s(\mathbb{Q})$ for s squarefree. Similarly, we compute that

$$\begin{aligned}\sum_{m\in\mathbb{Z}} \mu(T_m(\phi_2))u^m &= u\left(\frac{1+u^{-1}}{2}\right)\left(\frac{u^{-1}}{6}+\frac{5}{6}\right)\left(\frac{27}{48}+\frac{21}{48}u^{-1}\right)\\ &= \frac{7}{192}u^{-2} + \frac{17}{64}u^{-1} + \frac{89}{192} + \frac{15}{64}u.\end{aligned}$$

This yields that a larger proportion $89/384 \approx 23.18\%$ of twists $E_s/\mathbb{Q}$ have rank 0, and a smaller bound of $\frac{1043}{864} \approx 1.207$ on the average rank of $E_s(\mathbb{Q})$ for s squarefree.

We can do much better by combining these isogenies, however. In particular, we find that

$$\sum_{m,n\in\mathbb{Z}} \mu(T_m(\phi_1) \cap T_n(\phi_2))q^m u^n = \frac{3}{64}qu^{-1} + \frac{15}{64}q^{-1}u + \frac{35}{192}q^{-2} + \frac{7}{192}u^{-2} + \frac{7}{32}q^{-1}u^{-1} + \frac{9}{32}.$$

This shows that every squarefree s is in either $T_0(\phi_1)\cup T_0(\phi_2)$ or $T_{-1}(\phi_1)\cup T_1(\phi_1)\cup T_{-1}(\phi_2)\cup T_1(\phi_2)$. Thus, Corollary 2.14 and Proposition 2.2 yield that at least 25% of twists $E_s/\mathbb{Q}$ have rank 0, at least 5/6 have 3-Selmer rank one, and that the average rank of $E_s(\mathbb{Q})$ for s squarefree is at most 7/6. These rank bounds are the best one can hope for using only the methods of this paper.

Moreover, we are also able to exploit the isogenies ϕ_1 and ϕ_2 to produce 3-torsion elements of Tate-Shafarevich groups. In particular, the set $T_{-2}(\phi_1)\cap T_0(\phi_2)$ has density 35/192. By Proposition 2.13, we find that a proportion 35/384 of squarefree s are such that $|Ш(E'_s)[3]| \geq 9$. Similarly, we find that for at least 7/384 of squarefree s, we have $|Ш(E''_s)[3]| \geq 9$.

In fact, each of the curves E, E', and E'' also has a single rational two-torsion point, and hence a rational 2-isogeny. The three additional curves that are the codomain of these 2-isogenies complete the isogeny class 14a, whose isogeny graph is given in Figure 1.

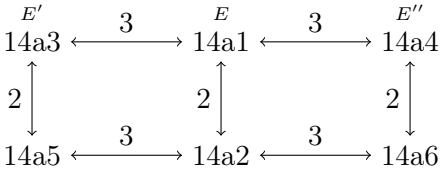

FIGURE 1. The isogeny graph of the isogeny class 14a.

By an easy diagram chase, the global Selmer ratios of the two 3-isogenies in the top row are equal to those of the bottom row, so the analysis for the isogenies in the bottom row is identical to that of the top row. In particular, exactly the same results hold for the proportion of twists with small rank, and exactly the same results hold on 3-torsion in Tate-Shafarevich groups for the curve 14a5 as do for E', and the same for 14a6 as do for E''. In fact, exploiting the 2-isogeny and Theorem 5.7, it is possible to show that each curve in the family has a positive proportion of twists with arbitrarily large 2-torsion in their Tate-Shafarevich groups.

Unfortunately, it is not clear how to prove that any of these curves has a positive proportion of twists with an element of order six in Ш, which is why these curves are the lone exceptional case in Theorem 1.4. For example, to produce elements of order three in $Ш(E'_s)$, we used above that within $T_{-2}(\phi_1) \cap T_0(\phi_2)$, 50% of twists $E'_s(\mathbb{Q})$ have rank 0. We also know by Theorem 5.7 that for 50% of $s \in T_{-2}(\phi_1) \cap T_0(\phi_2)$, we have that $|\mathrm{Sel}_2(E'_s)| \geq 2^{r_2}$ for any $r_2 \geq 0$. To show that there is an element of order six in Ш, we would need these two sets of density 1/2 to intersect, which we currently see no way to guarantee.

REFERENCES

[1] A. Balog and K. Ono. Elements of class groups and Shafarevich-Tate groups of elliptic curves. *Duke Math. J.*, 120(1):35–63, 2003.

[2] M. Bhargava, N. Elkies, and A. Shnidman. The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$. *Journal of the London Mathematical Society*, 101(1):299–327, 2020.

[3] M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver, and A. Shnidman. 3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field. *Duke Math. J.*, 168(15):2951–2989, 2019.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[5] J. W. S. Cassels. Arithmetic on curves of genus 1. VI. The Tate-Šafarevič group can be arbitrarily large. *J. Reine Angew. Math.*, 214/215:65–70, 1964.
[6] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.
[7] C. Delaunay. Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 323–340. Cambridge Univ. Press, Cambridge, 2007.
[8] T. Dokchitser and V. Dokchitser. Local invariants of isogenous elliptic curves. *Trans. Amer. Math. Soc.*, 367(6):4339–4358, 2015.
[9] K. Feng and M. Xiong. On Selmer groups and Tate-Shafarevich groups for elliptic curves $y^2 = x^3 - n^3$. *Mathematika*, 58(2):236–274, 2012.
[10] T. Fisher. Some examples of 5 and 7 descent for elliptic curves over $\mathbf{Q}$. *J. Eur. Math. Soc. (JEMS)*, 3(2):169–201, 2001.
[11] J. Friedlander and H. Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.
[12] M. Gealy and Z. Klagsbrun. Minimal differentials of elliptic curves with a p-isogeny. *Proc. Amer. Math. Soc.*, to appear.
[13] A. Granville and K. Soundararajan. Sieving and the Erdos–Kac theorem. In *Equidistribution in number theory, an introduction*, volume 237 of *NATO Sci. Ser. II Math. Phys. Chem.*, pages 15–27. Springer, Dordrecht, 2007.
[14] E. Kani. Products of CM elliptic curves. *Collect. Math.*, 62(3):297–339, 2011.
[15] Z. Klagsbrun and R. J. Lemke Oliver. The distribution of 2-Selmer ranks of quadratic twists of elliptic curves with partial two-torsion. *Mathematika*, 62(1):67–78, 2016.
[16] R. Kloosterman. The p-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large. *J. Théor. Nombres Bordeaux*, 17(3):787–800, 2005.
[17] R. S. Maier. On rationally parametrized modular equations. *J. Ramanujan Math. Soc.*, 24(1):1–73, 2009.
[18] J. S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, second edition, 2006.
[19] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.
[20] J. Rosen and A. Shnidman. Extensions of CM elliptic curves and orbit counting on the projective line. *Res. Number Theory*, 3:Art. 9, 13, 2017.
[21] K. Rubin and A. Silverberg. Families of elliptic curves with constant mod p representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 148–161. Int. Press, Cambridge, MA, 1995.
[22] E. F. Schaefer. Class groups and Selmer groups. *J. Number Theory*, 56(1):79–114, 1996.
[23] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.
[24] A. Shnidman. Quadratic Twists of Abelian Varieties With Real Multiplication. *International Mathematics Research Notices*, 10 2019. rnz185.
[25] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
[26] A. Smith. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. *Preprint available at http://arxiv.org/abs/1702.02325*, Feb. 2017.
[27] M. Xiong. On Selmer groups of quadratic twists of elliptic curves with a two-torsion over $\mathbb{Q}$. *Mathematika*, 59(2):303–319, 2013.
[28] M. Xiong and A. Zaharescu. Distribution of Selmer groups of quadratic twists of a family of elliptic curves. *Adv. Math.*, 219(2):523–553, 2008.

Department of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address: bhargava@math.princeton.edu

Center for Communications Research, San Diego, CA 92121
E-mail address: zdklags@ccrwest.org

Department of Mathematics, Tufts University, Medford, MA 02155
E-mail address: robert.lemke_oliver@tufts.edu

Einstein Institute of Mathematics, Hebrew University, Jerusalem, Israel
E-mail address: ariel.shnidman@mail.huji.ac.il