CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

Elements of prime order in Tate–Shafarevich groups of abelian varieties over $\mathbb{Q}$

Ari Shnidman [ID] 1 and Ariel Weiss [ID] 2

[1] Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Edmund J. Safra Campus, Jerusalem, 9190401, Israel;
E-mail: ariel.shnidman@mail.huji.ac.il.
[2] Department of Mathematics, Ben-Gurion University of the Negev, Be'er Sheva, 8410501, Israel;
E-mail: arielweiss@post.bgu.ac.il.

Abstract

For each prime p, we show that there exist geometrically simple abelian varieties A over $\mathbb{Q}$ with $Ш(A)[p] \neq 0$. Specifically, for any prime $N \equiv 1 \pmod{p}$, let A_f be an optimal quotient of $J_0(N)$ with a rational point P of order p, and let $B = A_f/\langle P \rangle$. Then the number of positive integers $d \leq X$ with $Ш(\widehat{B}_d)[p] \neq 0$ is $\gg X/\log X$, where $\widehat{B}_d$ is the dual of the dth quadratic twist of B. We prove this more generally for abelian varieties of GL_2-type with a p-isogeny satisfying a mild technical condition. In the special case of elliptic curves, we give stronger results, including many examples where $Ш(E_d)[p] \neq 0$ for an explicit positive proportion of integers d.

Contents

1. Introduction

Let A be an abelian variety over $\mathbb{Q}$. The Tate–Shafarevich group of A is the abelian group

$$Ш(A) = \ker\left(H^1(\mathbb{Q}, A) \to \prod_{\ell \leq \infty} H^1(\mathbb{Q}_\ell, A) \right)$$

classifying $\mathbb{Q}$-isomorphism classes of A-torsors that are isomorphic to A over $\mathbb{Q}_\ell$ for every prime ℓ, including the infinite prime $\ell = \infty$. Much is conjectured but little is known about the structure of this group. Famously, the Birch and Swinnerton-Dyer conjecture predicts that $Ш(A)$ is finite. On the other

hand, heuristics suggest that, for each prime p, a positive proportion of elliptic curves $E/\mathbb{Q}$, ordered by height, have $Ш(E)[p] \neq 0$ [Del07, PR12, BKL+15], and one expects something similar for abelian varieties of higher dimension.

In stark contrast to these expectations, it seems to be an open question whether, for each prime p, there exists even a *single* elliptic curve over $\mathbb{Q}$ with $Ш(E)[p] \neq 0$. There are constructions of elliptic curves and higher-dimensional abelian varieties A over number fields K with $Ш(A)[p] \neq 0$ [Klo05, CS10, Cre11], although the degree of K grows as a function of p in these results. Taking Weil restrictions of these examples gives abelian varieties $A'/\mathbb{Q}$ with $Ш(A')[p] \neq 0$. However, there again seem to be no known examples of *geometrically simple* abelian varieties $A/\mathbb{Q}$ with $Ш(A)[p] \neq 0$, for large primes p. The purpose of this paper is to provide such examples.

Theorem 1.1. *For each prime p, there exists a geometrically simple abelian variety $A/\mathbb{Q}$ such that $Ш(A)[p] \neq 0$.*

In fact, for each p, we exhibit infinitely many such $A/\mathbb{Q}$ in distinct $\overline{\mathbb{Q}}$-isogeny classes. Our examples arise from optimal quotients A_f of the modular Jacobian $J_0(N)$, attached to weight two newforms $f \in S_2(\Gamma_0(N))$ of prime level N.

Theorem 1.2. *Let N be a prime, and let $p \geq 3$ be a prime divisor of $(N - 1)/\gcd(12, N - 1)$. Let A_f be any optimal quotient of $J_0(N)$ containing a point $P \in A_f(\mathbb{Q})$ of order p. Let $B = A_f/\langle P \rangle$, let $\phi: A_f \to B$ be the canonical isogeny, and let $\widehat{\phi}: \widehat{B} \to \widehat{A}_f$ be the dual isogeny. Then*

$$\#\left\{ d : 0 < |d| \leq X \text{ and } Ш(\widehat{B}_d)[p] \neq 0 \right\} \gg \frac{X}{\log X},$$

where $\widehat{B}_d$ is the dth quadratic twist of $\widehat{B}$, for each $d \in \mathbb{Z}$.

Theorem 1.1 follows immediately from Theorem 1.2. Indeed, the abelian varieties A_f and $\widehat{B}_d$ are geometrically simple [Rib75, Corollary 1.4]; and for any prime p dividing $\frac{N-1}{(12,N-1)}$, there exists at least one newform $f \in S_2(\Gamma_0(N))$ such that $A_f(\mathbb{Q})$ contains a point of order p [Eme03, Theorem B]. Hence, given a prime p, it suffices to apply Theorem 1.2 to any prime $N \equiv 1 \pmod{p}$. Moreover, Dirichlet's theorem on primes in arithmetic progressions guarantees that there are infinitely many such N. Since N is prime, $J_0(N)$ is semistable with conductor a power of N, and we see that different choices of N give geometrically non-isogenous abelian varieties $A/\mathbb{Q}$ with $Ш(A)[p] \neq 0$.

The dimensions of the abelian varieties A we produce grow with p. Indeed, the Weil conjectures imply that $\dim A_f \geq \frac{\log p}{2 \log(1+\sqrt{2})}$ [Maz77, Proposition 7.2]; in particular, A_f is not an elliptic curve if $p \geq 7$. One could give a very crude *upper bound* for the minimal dimension of an A with $Ш(A)[p] \neq 0$ by combining bounds for the smallest prime $N \equiv 1 \pmod{p}$ with well-known bounds on the dimension of $J_0(N)$.

Our proof of Theorem 1.2 is fairly short but uses several deep inputs. First, we prove that if $\phi: A \to B$ is a p-isogeny of abelian varieties, whose Selmer ratio $c(\phi)$ equals p^i (see Definition 2.2), then there exists an explicit, positive density set of squarefree integers Σ^+ such that $\mathrm{rk}\, A_d(\mathbb{Q}) + \dim_{\mathbb{F}_p} Ш(A_d)[p] \geq i$ for all but finitely many quadratic twists A_d with $d \in \Sigma^+$ (Theorem 2.4). Our proof uses techniques from Galois cohomology, particularly the Greenberg–Wiles formula.

In the case that $A = A_f$ is an optimal quotient of $J_0(N)$, we then invoke nonvanishing results for special values of L-functions, due to Bump–Friedberg–Hoffstein and Ono–Skinner [BFH90, OS98], to show that $L(f_d, s) \neq 0$ for many quadratic twists f_d of f. By work of Gross–Zagier and Kolyvagin–Logachev [GZ86, KL89] or Kato [Kat04], we have $\mathrm{rk}\, \widehat{B}_d(\mathbb{Q}) = 0$ for such d. It follows that if $A = A_f$ is an optimal quotient of $J_0(N)$ that admits a p-isogeny $\phi: A \to B$ such that $c(\phi) \geq p^2$, then $Ш(A_d)[p] \neq 0$ for infinitely many quadratic twists A_d (Theorem 3.1).

In Section 4, we specialise to prime N, where we use Mazur's study of the Eisenstein ideal [Maz77, Eme03] to show that the condition on $c(\phi)$ is always satisfied, thereby proving Theorem 1.2. Our computation of $c(\phi)$ is a generalisation of [Shn21, §6], which was for the prime $p = 3$.

In the case of elliptic curves, we prove an even stronger bound than the one in Theorem 1.2, by invoking recent work of Smith [Smi20] instead of results on *L*-functions. In Section 5, we prove

Theorem 1.3. *Let E be an elliptic curve over $\mathbb{Q}$ with a degree p isogeny $\phi : E \to E'$, for some prime $p \geq 3$. Assume that $c(\phi) \geq p^2$ and that $E[2](\mathbb{Q}) \neq \mathbb{Z}/2\mathbb{Z}$. Then for a positive proportion of squarefree integers d, we have $\text{III}(E_d)[p] \neq 0$.*

The hypothesis $c(\phi) \geq p^2$ applies to 'most' quadratic twist families of p-isogenies of elliptic curves with $p \geq 3$, in a certain sense (see Proposition 5.1).

For each elliptic curve E in Theorem 1.3, we can give an explicit lower bound on the proportion of d such that $\text{III}(E_d)[p] \neq 0$. Sometimes these bounds are larger than those predicted by a naïve generalisation of the heuristics of Delaunay [Del01] and Poonen–Rains [PR12]. For example, in Section 6, we prove that for the elliptic curve $E : y^2 + y = x^3 - x^2 - 7820x - 263580$ with LMFDB label 11.a1, we have $\text{III}(E_d)[5] \neq 0$ for at least 22.9% of squarefree integers d. This example shows that the heuristics of Delaunay and Poonen–Rains on distributions of p-Selmer groups need to be modified when applied to quadratic twist families of elliptic curves with a rational p-isogeny.

In [BKLOS21, Conjecture 1], Bhargava, Klagsbrun, Lemke Oliver and the first author state a conjecture that for any abelian variety $A/\mathbb{Q}$, we should have $\text{III}(A_d)[p] \neq 0$ for a positive proportion of squarefree integers d. They prove special cases of this conjecture, without invoking Smith's work, when one of E or E' admits an additional 3-isogeny, in addition to a p-isogeny. In general, most known systematic constructions of elements in $\text{III}(A)[p]$ over $\mathbb{Q}$ exploit either multiple isogenies or the Cassels–Tate pairing; see, for example, [Cas64, Fis01, Fly19, Shn21, BH22, BFS21]. One exception is a theorem of Balog–Ono [BO03, Theorem 2], which applies to a large class of elliptic curves $E/\mathbb{Q}$ with a point of order p. As with our proof of Theorem 1.2, their proof relies on nonvanishing results for L-functions, but to prove $\text{Sel}_p(E_d) \neq 0$, they instead use nonvanishing results for class groups. This leads to the weaker bound $\{d : 0 < |d| \leq X, \text{III}(E_d)[p] \neq 0\} \gg X^{\frac{1}{2} + \frac{1}{2p}} / \log^2 X$. Thus, even in the special case of elliptic curves, we improve significantly on the known quantitative results whenever our method applies.

2. Selmer groups of abelian varieties with a p-isogeny

Let $\phi \colon A \to B$ be an isogeny of abelian varieties over $\mathbb{Q}$.

2.1. Selmer groups and the Selmer ratio

Definition 2.1. The ϕ-Selmer group is

$$\text{Sel}(\phi) = \ker\left(H^1(\mathbb{Q}, A[\phi]) \to \prod_{\ell \leq \infty} H^1(\mathbb{Q}_\ell, A) \right).$$

In the special case $A = B$ and $\phi = [p]_A$, we write $\text{Sel}_p(A)$ instead of $\text{Sel}([p]_A)$.

Definition 2.2. For ℓ a finite or infinite prime, define the *local Selmer ratio*

$$c_\ell(\phi) = \frac{\# \text{coker}(A(\mathbb{Q}_\ell) \to B(\mathbb{Q}_\ell))}{\# \ker(A(\mathbb{Q}_\ell) \to B(\mathbb{Q}_\ell))}.$$

When $\ell = \infty$, we use the convention that $\mathbb{Q}_\infty = \mathbb{R}$. We then define the *global Selmer ratio*

$$c(\phi) = \prod_{\ell \leq \infty} c_\ell(\phi).$$

These Selmer ratios were defined in [BES20] but were already studied in [Cas65] under a slightly different guise. The notation is meant to recall the Tamagawa number $c_\ell(X)$ of an abelian variety X

over $\mathbb{Q}_\ell$. Indeed, the following lemma shows that for all but finitely many primes ℓ, we have $c_\ell(\phi) = c_\ell(B)/c_\ell(A)$.

Lemma 2.3. *For any finite prime ℓ, we have*

$$c_\ell(\phi) = \frac{c_\ell(B)}{c_\ell(A)} \gamma_{\phi,\ell},$$

where $\gamma_{\phi,\ell}^{-1}$ is the normalised absolute value of the determinant of the map $\mathrm{Lie}(\mathcal{A}) \to \mathrm{Lie}(\mathcal{B})$ on tangent spaces of the Néron models over $\mathbb{Z}_\ell$. In particular, if $\ell \nmid \deg(\phi)$, then $\gamma_{\phi,\ell} = 1$.

Proof. This lemma is [Sch96, Lemma 3.8]. Recall that $c_\ell(A) = \#A(\mathbb{Q}_\ell)/A_0(\mathbb{Q}_\ell)$, where $A_0(\mathbb{Q}_\ell)$ is the subgroup of points that reduce to the identity component in the special fibre of the Néron model $\mathcal{A}$ of A.   □

The local Tamagawa numbers $c_\ell(A), c_\ell(B)$ are equal to 1 for all primes ℓ of good reduction. Hence, we have $c_\ell(\phi) = 1$ for all but finitely many primes, so the global Selmer ratio $c(\phi) = \prod_\ell c_\ell(\phi)$ is well-defined. Moreover, if ϕ has prime degree p, then $c(\phi)$ is an integer power of p.

2.2. Lower bounds on Selmer groups

Let N be the radical of the conductor of A. Thus, a prime ℓ divides N if and only if A has bad reduction at ℓ.

Let Σ^+ be the set of positive squarefree integers d such that $d \in \mathbb{Z}_\ell^{\times 2}$ for all primes $\ell \mid pN$. For any squarefree $d \in \mathbb{Z}$, write $\phi_d : A_d \to B_d$ for the dth quadratic twist of ϕ, which again has degree p.

Theorem 2.4. *Suppose that $\phi \colon A \to B$ is a degree p isogeny, and write $c(\phi) = p^i$ for some $i \in \mathbb{Z}$. Then for all but finitely many $d \in \Sigma^+$, we have $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(A_d) \geq i$, and hence*

$$\mathrm{rk}\, A_d(\mathbb{Q}) + \dim_{\mathbb{F}_p} \mathrm{III}(A_d)[p] \geq i.$$

The proof will require several lemmas.

Lemma 2.5. *If $\ell \nmid pN\infty$, then $c_\ell(\phi_d) = 1$ for all nonzero $d \in \mathbb{Z}$.*

Proof. Let $\chi_d : \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_p^\times$ denote the character corresponding to the (possibly trivial) extension $\mathbb{Q}_\ell(\sqrt{d})/\mathbb{Q}_\ell$. If χ_d is unramified, then A_d has good reduction over $\mathbb{Q}_\ell$, and $c_\ell(\phi_d) = c_\ell(B_d)/c_\ell(A_d) = 1$ by Lemma 2.3. Assume now that χ_d is ramified (and, in particular, nontrivial). Since A has good reduction over $\mathbb{Q}_\ell$, the extension $\mathbb{Q}_\ell(A[\phi])/\mathbb{Q}_\ell$ is unramified. Hence, the $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-action on $A_d[\phi_d] \simeq A[\phi] \otimes_{\mathbb{F}_p} \chi_d$ is via a nontrivial character $\widetilde{\chi}_d$. Thus

$$c_\ell(\phi_d) = \frac{\#\mathrm{im}(B_d(\mathbb{Q}_\ell) \to H^1(\mathbb{Q}_\ell, \widetilde{\chi}_d))}{\#H^0(\mathbb{Q}_\ell, \widetilde{\chi}_d)}.$$

The denominator is 1 since $\widetilde{\chi}_d$ is nontrivial. Let $\epsilon : \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_p^\times$ be the mod p cyclotomic character, which is unramified. We have $\#H^1(\mathbb{Q}_\ell, \widetilde{\chi}_d) = \#H^0(\mathbb{Q}_\ell, \widetilde{\chi}_d)\#H^0(\mathbb{Q}_\ell, \widetilde{\chi}_d^{-1}\epsilon) = 1$, by local Tate duality [Mil06, Corollary I.2.3] and the Euler characteristic formula [Mil06, Theorem I.2.8]. Hence, $c_\ell(\phi_d) = 1$.   □

Lemma 2.6. *We have $c_\infty(\phi) = \#A[\phi](\mathbb{R})^{-1}$.*

Proof. We have

$$\#\mathrm{coker}(A(\mathbb{R}) \to B(\mathbb{R})) = \#\mathrm{im}(B(\mathbb{R}) \to H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), A[\phi])).$$

Since $\#A[\phi] = p$ is odd, we have $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), A[\phi]) = 0$. Hence,

$$c_\infty(\phi) = \#\mathrm{coker}(A(\mathbb{R}) \to B(\mathbb{R})) \cdot \#A[\phi](\mathbb{R})^{-1} = \#A[\phi](\mathbb{R})^{-1}. \qquad \square$$

To prove Theorem 2.4, we will use the Greenberg–Wiles formula [NSW08, Theorem 8.7.9], which is a consequence of Poitou–Tate duality. If $\psi \colon X \to Y$ is an isogeny, it relates the size of $\mathrm{Sel}(\psi)$ to the size of $\mathrm{Sel}(\widehat{\psi})$, where $\widehat{\psi} \colon \widehat{Y} \to \widehat{X}$ is the dual isogeny. Applied to the isogeny $\phi_d \colon A_d \to B_d$, it reads

$$c(\phi_d) = \frac{\#\mathrm{Sel}(\phi_d)}{\#\mathrm{Sel}(\widehat{\phi}_d)} \cdot \frac{\#\widehat{B}_d[\widehat{\phi}_d](\mathbb{Q})}{\#A_d[\phi_d](\mathbb{Q})}. \qquad (2.1)$$

Proof of Theorem 2.4. First note that if A is any abelian variety and $p > 2$, then $A_d[p](\mathbb{Q}) = 0$ for all but finitely many quadratic twists of A. Indeed, if $0 \neq P \in A_d[p](\mathbb{Q})$, then the Galois module $A[p]$ has a subrepresentation isomorphic to the quadratic character $\chi_d \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^\times$ that cuts out the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Since $A[p]$ is finite-dimensional, there can only be finitely many such d. As a consequence, if $\phi \colon A \to B$ is a p-isogeny, then $A[\phi] \subset A[p]$, and we see that $A_d[\phi_d](\mathbb{Q}) = 0$ for all but finitely many d.

We may therefore ignore the finitely many $d \in \Sigma^+$ such that $\#A_d[\phi_d](\mathbb{Q})\#\widehat{B}_d[\widehat{\phi}_d](\mathbb{Q}) \neq 1$. Hence, from (2.1), we have

$$\#\mathrm{Sel}(\phi_d) = c(\phi_d)\#\mathrm{Sel}(\widehat{\phi}_d) \geq c(\phi_d).$$

Now, if $d \in \Sigma^+$, then $\phi_d = \phi$ over $\mathbb{Q}_\ell$, for all primes $\ell \mid pN\infty$. Hence, by Lemma 2.5, we have $c(\phi_d) = c(\phi) = p^i$ for all $d \in \Sigma^+$. It follows that

$$\dim_{\mathbb{F}_p} \mathrm{Sel}(\phi_d) \geq i$$

for all but finitely many $d \in \Sigma^+$.

Finally, we note that for all but finitely many $d \in \Sigma^+$, the inclusion $A_d[\phi_d] \to A_d[p]$ induces an injection

$$\mathrm{Sel}(\phi_d) \hookrightarrow \mathrm{Sel}_p(A_d).$$

Indeed, by [BKLOS19, (9.1)], the kernel of this map is $B_d[\psi_d](\mathbb{Q})/\phi_d(A_d[p](\mathbb{Q}))$, where $\psi_d \colon B_d \to A_d$ is the isogeny such that $\psi_d \circ \phi_d = [p]$. As before, this kernel vanishes for all but finitely many d. Hence, for such d, we have $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(A_d) \geq i$, and the exact sequence

$$0 \to A_d(\mathbb{Q})/pA_d(\mathbb{Q}) \to \mathrm{Sel}_p(A_d) \to \text{Ш}(A_d)[p] \to 0$$

implies that $\mathrm{rk}\, A_d(\mathbb{Q}) + \dim_{\mathbb{F}_p} \text{Ш}(A_d)[p] \geq i$. $\qquad \square$

3. Quotients of $J_0(N)$ with a p-isogeny

For $N \geq 1$, let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$ over $\mathbb{Q}$.

Theorem 3.1. *Let A be a simple abelian variety over $\mathbb{Q}$ arising as a quotient of $J_0(N)$ for some integer $N \geq 1$. Assume that A admits a degree p isogeny $\phi \colon A \to B$ over $\mathbb{Q}$ for some prime $p \geq 3$ and that $c(\phi) \geq p^2$. Then*

$$\#\{d : 0 < |d| \leq X \text{ and } \text{Ш}(A_d)[p] \neq 0\} \gg_A \frac{X}{\log X}.$$

Proof. Let $M \mid N$ be the minimal positive integer such that A is a quotient of $J_0(M)$. Then there is a newform $f = \sum a_n q^n \in S_2(\Gamma_0(M))$ such that the coefficient field $E := \mathbb{Q}(\{a_n\})$ is isomorphic to $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ and $L(A, s) = \prod_{\sigma \in \mathrm{Hom}(E, \mathbb{C})} L(f^\sigma, s)$. Since $J_0(M)$ has good reduction at all primes $\ell \nmid M$, so does A.

Let Σ be the set of squarefree integers d such that $d \in \mathbb{Z}_\ell^{\times 2}$ for all primes $\ell \mid pM$. By [OS98, Corollary 3], we have

$$\#\{d \in \Sigma : 0 < |d| \le X \text{ and } L(f_d, 1) \ne 0\} \gg \frac{X}{\log X},$$

where f_d is the dth quadratic twist of f. Moreover, by [Kat04, Corollary 14.3], or alternatively by [GZ86, KL89] and [BFH90, Theorem 1], we have $\mathrm{rk}\, A_d(\mathbb{Q}) = 0$ whenever $L(f_d, 1) \ne 0$.

By Lemma 2.5 and the assumption that $d \in \mathbb{Z}_\ell^{\times 2}$ for all primes $\ell \mid pM$, we have $c_\ell(\phi_d) = c_\ell(\phi)$ for all finite primes ℓ and all $d \in \Sigma$. If $d > 0$, we therefore have $c(\phi_d) = c(\phi) \ge p^2$. If $d < 0$, we have $c_\infty(\phi_d)/c_\infty(\phi) \in \{p, p^{-1}\}$ by Lemma 2.6, so $c(\phi_d) \ge c(\phi)/p \ge p$. Thus, we have $c(\phi_d) \ge p$ for all $d \in \Sigma$. Applying Theorem 2.4 both to A and to A_{-1}, we have

$$\mathrm{rk}\, A_d(\mathbb{Q}) + \dim_{\mathbb{F}_p} \mathrm{III}(A_d) \ge 1$$

for all but finitely many $d \in \Sigma$. It follows that

$$\#\{d \in \Sigma : 0 < |d| \le X \text{ and } \mathrm{III}(A_d)[p] \ne 0\} \gg \frac{X}{\log X},$$

as desired. $\qquad\square$

4. Quotients of $J_0(N)$ with N prime

Let N be a prime, and let $p \ge 3$ be a divisor of $\frac{N-1}{\gcd(12, N-1)}$. Let $\mathbb{T}$ be the finite $\mathbb{Z}$-algebra generated by the Hecke operators acting on the space $S_2(\Gamma_0(N))$ of weight 2 cusp forms on $\Gamma_0(N)$. For each newform $f \in S_2(\Gamma_0(N))$, let $\lambda_f : \mathbb{T} \to \mathbb{C}$ be the homomorphism giving the action of the Hecke operators on f, and let $I_f = \ker \lambda_f$. Let $J = J_0(N)$ be the modular Jacobian. Then $\mathbb{T} \hookrightarrow \mathrm{End}_{\mathbb{Q}} J$, and $A_f := J/I_f J$ is an abelian variety over $\mathbb{Q}$ called the *optimal quotient* corresponding to f [Eme03].

By [Maz77, Theorem 1], the torsion subgroup $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ is cyclic of order $\frac{N-1}{\gcd(12, N-1)}$ and hence is divisible by p. By [Eme03, Theorem B], there exists at least one optimal quotient $A = A_f$ with a point $P \in A(\mathbb{Q})$ of order p. Let $B = A/\langle P \rangle$ be the quotient, let $\phi : A \to B$ be the canonical p-isogeny over $\mathbb{Q}$, and let $\widehat{\phi} : \widehat{B} \to \widehat{A}$ be the dual isogeny.

Proof of Theorem 1.2. By Theorem 3.1, it is enough to prove that $c(\widehat{\phi}) = p^2$. By the Greenberg–Wiles formula in equation (2.1), it is equivalent to show that $c(\phi) = p^{-2}$. By Lemma 2.5, we have $c_\ell(\phi) = 1$ whenever $\ell \notin \{p, N, \infty\}$. Moreover, by Lemma 2.6, we have $c_\infty(\phi) = \#\ker(\phi)(\mathbb{R})^{-1} = p^{-1}$. To compute the remaining two local Selmer ratios, we use some facts about the Néron model of A.

Lemma 4.1. *We have $c_p(\phi) = 1$.*

Proof. Since A has good reduction at p, we have $c_p(A) = c_p(B) = 1$. In the notation of Lemma 2.3, we therefore have $c_p(\phi) = \gamma_{\phi, p}$. Now, the generator P of $\ker(\phi)$ is the image of a rational cuspidal divisor under the map $J_0(N) \to A$ by [Eme03, Theorem B]. Thus, by [Maz77, II.11.11], ϕ extends to an étale isogeny of Néron models over $\mathbb{Z}_p$. It follows that $\mathrm{Lie}(\mathcal{A}) \to \mathrm{Lie}(\mathcal{B})$ is an isomorphism and $\gamma_{\phi, p} = 1$. $\quad\square$

Lemma 4.2. *We have $c_N(\phi) = p^{-1}$.*

Proof. The Atkin–Lehner operator W_N acts on A by -1. Indeed, A belongs to the Eisenstein quotient of $J = J_0(N)$, which is itself a quotient of J^-, the maximal quotient of J on which the Atkin–Lehner eigenvalue is -1 [Maz77, Proposition 17.10]. Hence, the global root number of f is $+1$, and by [CS01,

Proposition 7.1], the abelian variety $A = A_f$ has split purely toric reduction. Moreover, the order p point P reduces to a non-identity component of the special fibre of the Néron model of A over $\mathbb{Z}_N$, since specialisation induces an isomorphism from $A(\mathbb{Q})_{\text{tors}}$ to the component group Φ_A by [Eme03, Theorem B]. Thus, the lemma follows from [BFS21, Proposition 5.1]. □

We compute $c(\phi) = \prod_{\ell \leq \infty} c_\ell(\phi) = c_N(\phi) c_\infty(\phi) = p^{-2}$, as desired. □

5. Applications to elliptic curves

Proof of Theorem 1.3. By a recent result of Smith [Smi20, Corollary 1.4], we have

$$\lim_{X \to \infty} \frac{\#\{d : 0 < |d| \leq X : \text{rk } E_d(\mathbb{Q}) \leq 1\}}{2X} = 1,$$

under the assumption that either $E[2](\mathbb{Q}) = 0$ or $E[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$ and E does not admit a cyclic 4-isogeny. In our case, E also admits a p-isogeny. If $E[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$, then E cannot also admit a cyclic 4-isogeny: otherwise, the isogeny class of E would contain a cyclic $8p$-isogeny, but $Y_0(8p)(\mathbb{Q}) = \emptyset$ for $p \geq 3$ [Ken82, Theorem 1]. Thus, E satisfies the hypotheses of Smith's result, and by Theorem 2.4 and our assumption that $c(\phi) \geq p^2$, it follows that $\text{III}(A_d)[p] \neq 0$ for 100% of $d \in \Sigma^+$. □

It is natural to ask about the scope of Theorem 1.3. In this direction, we have:

Proposition 5.1. *Suppose that $p > 2$ and that $\phi \colon E \to E'$ is a p-isogeny of elliptic curves over $\mathbb{Q}$. Suppose also that E has at least three primes, distinct from p, of multiplicative reduction. Then there exists an integer d such that either $c(\phi_d) \geq p^2$ or $c(\widehat{\phi}_d) \geq p^2$. In particular, the conclusion of Theorem 1.3 applies to at least one of E or E'.*

Proof. We apply [DD15, Table 1]. Let ℓ_1, ℓ_2, ℓ_3 be the primes of multiplicative reduction, and write v_i for the corresponding ℓ_i-adic valuation. Let j, j' be the j-invariants of E and E'. Replacing E, E' by quadratic twists, we may assume that all three primes have split multiplicative reduction. Moreover, we may further twist so that, at every other prime, E has either good or additive reduction.

After reordering and possibly replacing ϕ with its dual, we may assume that $v_i(j) = p v_i(j')$ for $i = 1, 2$. Indeed, for each i, we have either $v_i(j) = p v_i(j')$ or $v_i(j') = p v_i(j)$, so, possibly replacing ϕ with its dual, the first option must happen for at least two primes.

Twisting again by an integer d, such that $\ell_3 \mid d$ and $\left(\frac{d}{p}\right) = 1$ for all other primes of bad reduction, we may assume that E, E' have additive, potentially multiplicative reduction at ℓ_3. Similarly, we may assume that $E[\phi](\mathbb{R}) = 0$. Hence, by [DD15, Table 1] and Lemma 2.3, we have $c_{\ell_i}(\phi) = p$ for $i = 1, 2$ and $c_{\ell_3}(\phi) = 1$. Moreover, as in Lemma 2.6, we have $c_\infty(\phi) = 1$.

Twisting at p so that E has additive reduction, we have either $c_p(\phi) = 1$ or p, again by [DD15, Table 1]. Finally, by construction, A has good or additive reduction at all the other primes, so $c_\ell(\phi) = 1$ for all primes $\ell \nmid \ell_1 \ell_2 \ell_3 p \infty$ [DD15, Table 1]. Putting everything together, we have $c(\phi) \geq p^2$. □

Proposition 5.1 shows that in a certain natural sense, Theorem 1.3 applies to 'most' twist families of elliptic curves $E/\mathbb{Q}$ with an isogeny of degree $p > 2$. To make this claim more precise, we first recall that for $p \notin \{3, 5, 7, 13\}$, there are only finitely many j-invariants of elliptic curves with a p-isogeny [Maz78]. The modular curves $X_0(p)$ with $p \in \{3, 5, 7, 13\}$ are all isomorphic to $\mathbb{P}^1$. Hence, there are infinitely many j-invariants of such elliptic curves over $\mathbb{Q}$. However, for any p in this set, and for any $k \geq 1$, one can show that 100% of rational points in $X_0(p)(\mathbb{Q})$, ordered by height, have at least k primes of potentially multiplicative reduction. We will not prove this here, but for arguments along these lines, see [BKLOS21].

6. An example: an elliptic curve with a 5-isogeny

In this final section, we look at the example $N = 11$ and $p = 5$. In this case, $J_0(11)$ is an elliptic curve with a 5-isogeny $\phi\colon J_0(11) \to E$, and we work out an explicit lower bound on the proportion of squarefree integers d with $\text{III}(E_d)[5] \neq 0$.

In [Del01], Delaunay gives a Cohen–Lenstra type heuristic, which predicts that, for fixed $r \in \{0, 1\}$, and as E varies over all elliptic curves over $\mathbb{Q}$ ordered by conductor,

$$\Pr(\text{III}(E)[p] \neq 0 \mid \text{rk}\, E = r) = 1 - \prod_{k=1}^{\infty}(1 - p^{1-r-2k}).$$

Assuming Goldfeld's conjecture that 50% of elliptic curves have rank 0 and 50% have rank 1, this distribution predicts that

$$\Pr(\text{III}(E)[5] \neq 0) = 1 - \frac{1}{2}\left(\prod_{k=1}^{\infty}(1 - 5^{1-2k}) + \prod_{k=1}^{\infty}(1 - 5^{-2k})\right) \approx 0.124132.$$

Delaunay's heuristics were presented for the family of all elliptic curves over $\mathbb{Q}$; however, it is natural to guess that they should hold in quadratic twist families as well, as is suggested by Delaunay [Del07, Section 4] and Poonen–Rains [PR12, Remark 1.9].

In the following example, we prove that the family of quadratic twists of E *do not* follow this distribution. In particular, in twist families of elliptic curves with a p-isogeny, our example shows that the distribution of the groups $\text{III}(E)[p]$ must follow a different distribution.

Theorem 6.1. *Let $E\colon y^2 + y = x^3 - x^2 - 7820x - 263580$, an elliptic curve of conductor* 11. *Then at least* $11/48 \approx 22.9\%$ *of squarefree integers d satisfy* $\text{III}(E_d)[5] \neq 0$.

Proof. The modular curve $X_0(11)$ is genus 1 and has model $E'\colon y^2 + y = x^3 - x^2 - 10x - 20$. We therefore have $E' \simeq J_0(11) \simeq A_f$, where f is the unique weight two eigenform of level $\Gamma_0(11)$. The torsion subgroup is order 5 generated by the point $(5, 5)$. The curve E in the theorem is the quotient $\phi\colon E' \to E$ by the subgroup generated by $(5, 5)$.

Since $E[2](\mathbb{Q}) = 0$, by [Smi20, Corollary 1.4], we have $\text{rk}\, E_d(\mathbb{Q}) \leq 1$ for 100% of squarefree integers d. Hence, by Theorem 2.4, $\text{III}(E_d)[5] \neq 0$ whenever $c(\widehat{\phi}) \geq 5^2$ or, equivalently, whenever $c(\phi) \leq 5^{-2}$.

By Lemmas 2.6, 4.1 and 4.2, or by [DD15, Table 1], we have $c_{11}(\phi) = \frac{1}{5}$, $c_\infty(\phi) = \frac{1}{5}$ and $c_5(\phi) = 1$. Moreover, by [DD15, Table 1], we have $c_5(\phi_d) = 1$ for all d. If $\ell \nmid 5 \cdot 11 \cdot \infty$, we have $c_\ell(\phi_d) = 1$ by Lemma 2.5. Hence, if Σ^+ denotes the set of positive squarefree integers, such that $d \in \mathbb{Z}_{11}^{\times 2}$, then $c(\phi_d) \leq 5^{-2}$ for all $d \in \Sigma^+$.

As a subset of the set of squarefree integers, Σ^+ has relative density

$$\frac{1}{2} \cdot \frac{5 \cdot 11}{11^2 - 1} = \frac{11}{48}.$$

Hence, at least $11/48$ of squarefree integers d satisfy $\text{III}(E_d)[5] \neq 0$.   □

The fact that Delaunay's heuristics for the distribution of the groups $\text{III}(E_d)[p]$ should be modified in certain cases was already understood in [BKLOS21], which is one reason why the authors formulate [BKLOS21, Conjecture 1] without specifying a conjectural proportion. That paper contains several results that show Delaunay's distribution does not always hold when the (isogeny class of the) elliptic curve admits at least two independent cyclic isogenies. Theorem 1.3 shows that this phenomenon persists even in the presence of a single cyclic isogeny. It would be interesting to develop consistent heuristics that describe a conjectural distribution in all cases.

Conflicts of Interest. The authors have no conflicts of interest to declare.

References

[BES20] M. Bhargava, N. Elkies, and A. Shnidman, 'The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$', *J. Lond. Math. Soc. (2)* **101**(1) (2020), 299–327.

[BFH90] D. Bump, S. Friedberg, and J. Hoffstein, 'Nonvanishing theorems for *L*-functions of modular forms and their derivatives', *Invent. Math.* **102**(3) (1990), 543–618.

[BFS21] N. Bruin, E. V. Flynn, and A. Shnidman, Genus 2 curves with full $\sqrt{3}$-level structure and Tate-Shafarevich groups. Preprint, 2021, arxiv.org/abs/2102.04319.

[BH22] M. Bhargava and W. Ho, 'On average sizes of Selmer groups and ranks in families of elliptic curves having marked points', Preprint, 2022, arxiv:2207.03309.

[BKL+15] M. Bhargava, D. M. Kane, H. W. Lenstra, Jr., B. Poonen, and E. Rains, 'Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves', *Camb. J. Math.* **3**(3) (2015), 275–321.

[BKLOS19] 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) (2019), 2951–2989.

[BKLOS21] M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver, and A. Shnidman, 'Elements of given order in Tate-Shafarevich groups of abelian varieties in quadratic twist families', *Algebra Number Theory* **15**(3) (2021), 627–655.

[BO03] A. Balog and K. Ono, 'Elements of class groups and Shafarevich-Tate groups of elliptic curves', *Duke Math. J.* **120**(1) (2003), 35–63.

[Cas64] 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** (1964), 65–70.

[Cas65] J. W. S. Cassels, 'Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer', *J. Reine Angew. Math.* **217** (1965), 180–199.

[Cre11] B. Creutz, 'Potential Ш for abelian varieties', *J. Number Theory* **131**(11) (2011), 2162–2174.

[CS01] B. Conrad and W. A. Stein, 'Component groups of purely toric quotients', *Math. Res. Lett.* **8**(5–6) (2001), 745–766.

[CS10] P. L. Clark and S. Sharif, 'Period, index and potential, III', *Algebra Number Theory* **4**(2) (2010), 151–174.

[DD15] T. Dokchitser and V. Dokchitser, 'Local invariants of isogenous elliptic curves', *Trans. Amer. Math. Soc.* **367**(6) (2015), 4339–4358.

[Del01] C. Delaunay, 'Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$', *Experiment. Math.* **10**(2) (2001), 191–196.

[Del07] 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.* (Cambridge Univ. Press, Cambridge, 2007), 323–340.

[Eme03] M. Emerton, 'Optimal quotients of modular Jacobians', *Math. Ann.* **327**(3) (2003), 429–458.

[Fis01] T. Fisher, 'Some examples of 5 and 7 descent for elliptic curves over **Q**', *J. Eur. Math. Soc. (JEMS)* **3**(2) (2001), 169–201.

[Fly19] E. V. Flynn, 'Arbitrarily large 2-torsion in Tate-Shafarevich groups of abelian varieties', *Acta Arith.* **191**(2) (2019), 101–114.

[GZ86] B. H. Gross and D. B. Zagier, 'Heegner points and derivatives of *L*-series', *Invent. Math.* **84**(2) (1986), 225–320.

[Kat04] K. Kato, '*p*-adic Hodge theory and values of zeta functions of modular forms', *Astérisque* **295**, (2004), pages ix, 117–290. Cohomologies *p*-adiques et applications arithmétiques (III).

[Ken82] M. A. Kenku, 'On the number of **Q**-isomorphism classes of elliptic curves in each **Q**-isogeny class', *J. Number Theory* **15**(2) (1982), 199–202.

[KL89] V. A. Kolyvagin and D. Y. Logachëv, 'Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties', *Algebra i Analiz* **1**(5) (1989), 171–196.

[Klo05] R. Kloosterman, 'The *p*-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large', *J. Théor. Nombres Bordeaux* **17**(3) (2005), 787–800.

[Maz77] B. Mazur, 'Modular curves and the Eisenstein ideal', *Inst. Hautes Études Sci. Publ. Math.* (47) (1978), 33–186, 1977. With an appendix by Mazur and M. Rapoport.

[Maz78] B. Mazur, 'Rational isogenies of prime degree (with an appendix by D. Goldfeld)', *Invent. Math.* **44**(2) (1978), 129–162.

[Mil06] J. S. Milne, *Arithmetic Duality Theorems*, second edn. (BookSurge, Charleston, SC, 2006).

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, second edn. (Springer-Verlag, Berlin, 2008). Volume 323 of Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].

[OS98]   K. Ono and C. Skinner, 'Non-vanishing of quadratic twists of modular L-functions', *Invent. Math.* **134**(3) (1998), 651–660.

[PR12]   B. Poonen and E. Rains, 'Random maximal isotropic subspaces and Selmer groups', *J. Amer. Math. Soc.* **25**(1) (2012), 245–269.

[Rib75] K. A. Ribet, 'Endomorphisms of semi-stable abelian varieties over number fields', *Ann. of Math.* **2**(101) (1975), 555–562.

[Sch96] E. F. Schaefer, 'Class groups and Selmer groups', *J. Number Theory* **56**(1) (1996), 79–114.

[Shn21] A. Shnidman, 'Quadratic twists of Abelian varieties with real multiplication', *Int. Math. Res. Not. IMRN* **5** (2021), 3267–3298.

[Smi20] A. Smith, 'ℓ^∞-Selmer groups in degree ℓ twist families', PhD thesis, Harvard University, Graduate School of Arts & Sciences (2020).