# Shafarevich–Tate Groups of Nonsquare Order

William A. Stein

**Abstract.** Let $A$ denote an abelian variety over $\mathbb{Q}$. We give the first known examples in which $\#Ш(A/\mathbb{Q})$ is neither a square nor twice a square. For example, let $E$ be the elliptic curve $y^2 + y = x^3 - x$ of conductor 37. We prove that for every odd prime $p < 25000$ (with $p \neq 37$), there is a twist $A$ of $E \times \cdots \times E$ ($p-1$ copies) such that $\#Ш(A/\mathbb{Q}) = pn^2$ for some integer $n$. We prove this by showing under certain hypothesis on $E$ and $p$ that there is an exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to Ш(A/\mathbb{Q})[p^\infty] \to Ш(E/K)[p^\infty] \to Ш(E/\mathbb{Q})[p^\infty] \to 0,$$

where $K$ is a certain abelian extension of $\mathbb{Q}$ of degree $p$.

## 1. Introduction

The Shafarevich–Tate group of an abelian variety $A$ over a number field $F$ is

$$Ш(A/F) := \operatorname{Ker}\left( H^1(F, A) \to \bigoplus_{\text{all } v} H^1(F_v, A) \right).$$

What are the possibilities for the group structure of $Ш(A/F)$? It is conjectured that $Ш(A/F)$ is finite and this is known in some cases.

**Theorem 1.1** (Kato, Kolyvagin, Wiles, et al.). *Suppose $A$ is an elliptic curve over $\mathbb{Q}$. (1) If $\operatorname{ord}_{s=1} L(A, s) \leq 1$, then $Ш(A/\mathbb{Q})$ is finite. (2) If $\chi$ is a character of the Galois group of an abelian extension $K$ of $\mathbb{Q}$ and $L(A, \chi, 1) \neq 0$, then the $\chi$-component of $Ш(A/K) \otimes_{\mathbb{Z}} \mathbb{Z}[\chi]$ is finite. (Here $\mathbb{Z}[\chi]$ is generated by the image of $\chi$.)*

The Cassels–Tate pairing $Ш(A/F) \times Ш(A^\vee/F) \to \mathbb{Q}/\mathbb{Z}$ imposes strong constraints on the structure of $Ш(A/F)$.

**Theorem 1.2** (Tate, Flach). *Let $p$ be a prime and suppose that there is a polarization $\lambda : A \to A^\vee$ of degree coprime to $p$. If $p = 2$ assume also that $\lambda$ arises from an $F$-rational divisor on $A$ (this hypothesis is automatic if $A$ is an elliptic curve, but can fail in general). If $Ш(A/F)[p^\infty]$ is finite then $\#Ш(A/F)[p^\infty]$ is a perfect square.*

*Proof.* If $\lambda$ is $F$-rational, the Cassels–Tate pairing on $Ш(A/F)[p^\infty]$ (induced by $\lambda$) is nondegenerate and alternating (see [Tat63]), so $\#Ш(A/F)[p^\infty]$ is a perfect square. Even when $\lambda$ is not $F$-rational, the Cassels–Tate pairing is nondegenerate and antisymmetric (see [Fla90]), which when $p$ is odd implies that $\#Ш(A/F)[p^\infty]$ is a perfect square. $\square$

It is tempting to conjecture that $\#Ш(A/F)$ is always a perfect square. Perhaps squareness is a fundamental property of Shafarevich–Tate groups? While implementing algorithms based on [PS97] for computing with Jacobians of hyperelliptic curves, M. Stoll was shocked to discover an example of an abelian variety of dimension two such that $\#Ш(A/F)[2^\infty] = 2$. This was surprising because, for example, one finds in the literature [SD67, pg.149] the following statement: "[The group $Ш(A/F)$] is conjectured to be finite, and Tate [26] has shown that if it is finite its order is a perfect square." Stoll and B. Poonen discovered what hid behind this and other similar examples in which $\#Ш(A/F)$ is twice a perfect square.

An algebraic curve $X$ of genus $g$ over a local field $k$ is *deficient* if $X$ has no $k$-rational divisor of degree $g - 1$.

**Theorem 1.3** (Poonen-Stoll [PS99])**.** *Suppose $A$ is the Jacobian of an algebraic curve over $F$ that is deficient at an odd number of places. If $\#Ш(A/F)$ is finite, then $\#Ш(A/F)$ is twice a square.*

For example, they prove that the Jacobian $J$ of the nonsingular projective curve defined by

$$y^2 = -3(x^2 + 1)(x^2 - 6x + 1)(x^2 + 6x + 1)$$

has Shafarevich–Tate group of order 2 (to see that $\#Ш(J) \mid 2$ they observe that $J$ is isogenous to a product of CM elliptic curves and apply a theorem of Rubin; see [PS99, Prop. 27] for details). Also, Jordan and Livné [JL99] give an infinite family of Atkin–Lehner quotients of Shimura curves which are deficient at an odd number of places.

Though $\#Ш(A/F)$ need not be square, one might still be tempted to conjecture that $Ш(A/F)$ must have order either a square or twice a square. Let $p$ be an odd prime. In this paper, we construct (under certain hypotheses that are satisfied for $p < 25000$) abelian varieties $A$ such that $\#Ш(A/\mathbb{Q}) = pn^2$ for some integer $n$. For example (see Section 3):

**Theorem 1.4.** *Let $E$ be the elliptic curve $y^2 + y = x^3 - x$ of conductor 37. For every odd prime $p < 25000$ (with $p \neq 37$), there is a twist $A$ of $E^{\times(p-1)}$ such that $\#Ш(A/\mathbb{Q}) = pn^2$ for some integer $n$.*

This paper was originally motivated by the problem of relating the conjecture of Birch and Swinnerton-Dyer about the ranks of elliptic curves $E$ to the Birch and Swinnerton-Dyer formula for the orders $\#Ш(A)$ for abelian varieties $A$ of analytic rank 0.

Let $p$ be a prime. Under suitable hypotheses, we construct an abelian variety $A$ and a natural map $E(\mathbb{Q})/pE(\mathbb{Q}) \hookrightarrow Ш(A/\mathbb{Q})$. Thus if $E(\mathbb{Q}) \cong \mathbb{Z}$ then $Ш(A/\mathbb{Q})$ has a natural subgroup of order $p$, and no other natural subgroup of order $p$ presents itself. Moreover, when $E$ is defined by $y^2 + y = x^3 - x$, the Birch and Swinnerton-Dyer formula predicts that $Ш(A/\mathbb{Q})[3]$ is of order 3. Further investigation led to the results of this paper.

**Acknowledgement:** It is a pleasure to thank Kevin Buzzard, Frank Calegari, Sol Friedberg, Benedict Gross, Emmanuel Kowalski, Barry Mazur, Bjorn Poonen, and David Rohrlich for their helpful comments, and in particular Michael Stoll for Lemma 2.10 and Cristian González for carefully reading this paper, making many comments, and sending me a proof of Proposition 2.13.

### 1.1. Notation

If $G$ is an abelian group and $n$ is an integer, then $G[n]$ denotes the subgroup of elements of order $n$ and $G[n^\infty]$ is the subgroup of elements of order any power of $n$. We refer to elliptic curves using the notation of [C97].

## 2. Construction of Nonsquare Shafarevich–Tate Groups

For the rest of this paper we will work with an elliptic curve $E$ over $\mathbb{Q}$. Aside from the significant use of known cases of the Birch and Swinnerton-Dyer conjecture below, much of the construction should generalize to the situation when $E$ is replaced by a principally polarized abelian variety over a global field.

For the rest of this section, fix an elliptic curve $E$ over $\mathbb{Q}$. By [BCDT01], $E$ is modular so there is a newform $f = \sum_{n=1}^{\infty} a_n q^n$ of level equal to the conductor $N = N_E$ of $E$ such that $L(E,s) = L(f,s)$. For each prime $q \mid N$, the Tamagawa number $c_q$ of $E$ at $q$ is the order of the group of rational components of the special fiber of the Néron model of $E$ at $q$.

### 2.1. Twisting By Characters of Prime Order

Let $p$ be a prime number. For any prime $\ell \equiv 1 \pmod{p}$, let

$$\chi_{p,\ell} : (\mathbb{Z}/\ell\mathbb{Z})^* \to \mu_p \subset \mathbb{C}^*$$

be one of the $p-1$ Galois-conjugate Dirichlet characters of order $p$ and conductor $\ell$.

**Conjecture 2.1.** *Suppose $p$ is a prime such that $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$ is surjective. Then there exists a prime $\ell \nmid N$ such that $L(E,\chi_{p,\ell},1) \neq 0$, $\ell \equiv 1 \pmod{p}$ and $a_\ell \not\equiv \ell + 1 \pmod{p}$.*

*Remarks* 2.2.

1. Formulas involving modular symbols imply that $L(E,\chi_{p,\ell},1) \neq 0$ if and only if $L(E,\chi_{p,\ell}^\sigma,1) \neq 0$ for any $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate $\chi_{p,\ell}^\sigma$ of $\chi_{p,\ell}$.
2. J. Fearnley proved related nonvanishing results when $L(E,1) \neq 0$ in [Fea01].
3. If $E$ is the elliptic curve $y^2 + y = x^3 - x$ of conductor 37 and rank 1, then $\ell = 41$ is the only $\ell \equiv 1 \pmod{5}$ with $\ell < 1000$ for which $L(E,\chi_{5,\ell},1) = 0$.

The following proposition gives evidence for Conjecture 2.1 for the lowest-conductor elliptic curves of ranks 1, 2, and 3.

**Proposition 2.3.** *Conjecture 2.1 is true for the rank* 1 *elliptic curve* **37A** *for every odd* $p < 25000$ *(with* $p \neq 37$*). The conjecture is true for the rank* 2 *curve* **389A** *for every odd* $p < 1000$ *(with* $p \neq 389$*). The conjecture is true for the rank* 3 *curve* **5077A** *for every odd* $p < 1000$.

*Proof.* Consider the modular symbol

$$e_{p,\ell} = \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^*} \chi_{p,\ell}(a) \cdot \left\{0,\ \frac{a}{\ell}\right\} \in H_1(X_0(N), \mathbb{Q}(\zeta_p)).$$

Then $L(E, \chi_{p,\ell}, 1) \neq 0$ if and only if the image of $e_{p,\ell}$ under

$$H_1(X_0(N), \mathbb{Q}(\zeta_p)) \to H_1(E, \mathbb{Q}(\zeta_p))$$

is nonzero. In any particular case, we can use modular symbols to determine whether or not this image is nonzero.

When $p$ is large, it is difficult to compute in the field $\mathbb{Q}(\zeta_p)$, so instead we compute in the residue class field $\mathbb{F}_\ell = \mathbb{Z}[\zeta_p]/\mathfrak{m} \cong Z/\ell\mathbb{Z}$, where $\mathfrak{m}$ is one of the maximal ideals of $\mathbb{Z}[\zeta_p]$ that lies over $\ell$. (Note that $\ell$ splits completely in $\mathbb{Z}[\zeta_p]$ because $\ell \equiv 1 \pmod{p}$.) After reducing modulo $\mathfrak{m}$, we compute the image of

$$\overline{e}_{p,\ell} = \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^*} a^{(\ell-1)/p} \cdot \left\{0,\ \frac{a}{\ell}\right\} \in H_1(X_0(N), \mathbb{F}_\ell)$$

in $H_1(E, \mathbb{F}_\ell)$. If it is nonzero, then the image of $e_{p,\ell}$ in $H_1(E, \mathbb{Q}(\zeta_p))$ is nonzero.

A big computation (that takes hundreds of hours using Magma [BCP97]) shows that the image of $\overline{e}_{p,\ell}$ is nonzero in the cases asserted by the proposition. So the reader can carry out similar computations, we include the following Magma V2.10-6 code, which illustrates verification of the proposition for **37A** for $p < 100$:

```
procedure VerifyConjecture(E, p)
   assert Type(E) eq CrvEll;
   assert Type(p) eq RngIntElt and IsPrime(p) and IsOdd(p);
   N := Conductor(E);
   assert N mod p ne 0;
   M := ModularSymbols(E,+1);  // takes a long time if N large!
   ell := 3; t := Cputime();
   printf "p=%o: ", p;
   while true do
      while (ell mod p ne 1)  or  (N mod ell eq 0) or
       TraceOfFrobenius(ChangeRing(E,GF(ell))) mod p eq (ell+1) do
         ell := NextPrime(ell);
      end while;
      k := FiniteField(ell);
      printf "trying ell=%o...",ell;
      psi := DirichletGroup(ell,k).1;
      eps := psi^(Order(psi) div p);  // order p character
      M_k := BaseExtend(M,k);
```

```
      phi := RationalMapping(M_k);
      e := TwistedWindingElement(M_k,1,eps);
      if phi(e) ne 0 then
         printf " success! (%o seconds)\n", Cputime(t);
         return;
      end if;
      printf "failed. ";
      ell := NextPrime(ell);
   end while;
end procedure;

E := EllipticCurve([0,0,1,-1,0]);  // 37A
for p in [q : q in [3..100] | IsPrime(q) and q ne 37] do
   VerifyConjecture(E,p);
end for;
```

The above input results in the following abbreviated output:

```
p=3: trying ell=7... success! (0.021 seconds)
p=5: trying ell=11... success! (0.039 seconds)
p=7: trying ell=29... success! (0.121 seconds)
...
p=89: trying ell=179... success! (0.739 seconds)
p=97: trying ell=389... success! (1.491 seconds)
```

□

**2.2. A Restriction of Scalars Exact Sequence**

As above, $E$ is an elliptic curve over $\mathbb{Q}$. Let $p$ be any prime (note that $p = 2$ is allowed). Suppose $\ell \equiv 1 \pmod{p}$ is another prime and that $\ell \nmid N_E$. Let $K \subset \mathbb{Q}(\mu_\ell)$ be the abelian extension of $\mathbb{Q}$ that corresponds to $\chi_{p,\ell}$ (thus $K$ is the unique subfield of $\mathbb{Q}(\mu_\ell)$ of degree $p$).

Let $R = \mathrm{Res}_{K/\mathbb{Q}}(E_K)$ be the restriction of scalars down to $\mathbb{Q}$ of $E$ viewed as an elliptic curve over $K$. Thus $R$ is an abelian variety over $\mathbb{Q}$ of dimension $p = [K : \mathbb{Q}]$. It is characterized by the fact that it represents the following functor on $\mathbb{Q}$-schemes $S$:

$$S \mapsto E_K(S_K).$$

As a Galois module,

$$R(\overline{\mathbb{Q}}) = E(\overline{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})],$$

where $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\sum P_\sigma \otimes \sigma$ by

$$\tau\left(\sum P_\sigma \otimes \sigma\right) = \sum \tau(P_\sigma) \otimes \tau_{|K} \cdot \sigma,$$

where $\tau_{|K}$ is the image of $\tau$ in $\mathrm{Gal}(K/\mathbb{Q})$.

**Proposition 2.4.** *The identity map induces a closed immerion $\iota : E \hookrightarrow R$, and the trace* $\mathrm{Tr} : K \to \mathbb{Q}$ *induces a surjection* $\mathrm{Tr} : R \to E$ *whose kernel is geometrically connected. Thus we have an exact sequence of abelian varieties*

$$0 \to A \to R \xrightarrow{\mathrm{Tr}} E \to 0. \tag{1}$$

*Proof.* The existence of $\iota$ and Tr follows from Yoneda's lemma. The map $\iota$ is induced by the functorial inclusion $E(S) \hookrightarrow E_K(S_K) = R(S)$, so $\iota$ is injective. The Tr map is induced by the functorial trace map on points $R(S) = E_K(S_K) \xrightarrow{\mathrm{Tr}} E(S)$.

To verify that Ker(Tr) is geometrically connected, we base extend the exact sequence (1) to $\overline{\mathbb{Q}}$. First, note that there is an isomorphism

$$R_{\overline{\mathbb{Q}}} \cong E_{\overline{\mathbb{Q}}} \times \cdots \times E_{\overline{\mathbb{Q}}}.$$

After base extension, we identify the trace map with the summation map

$$+ : E_{\overline{\mathbb{Q}}} \times \cdots \times E_{\overline{\mathbb{Q}}} \longrightarrow E_{\overline{\mathbb{Q}}}.$$

Let $n = [K : \mathbb{Q}]$. The map defined by

$$(a_1, \ldots, a_{n-1}) \mapsto \left(a_1, a_2, \ldots, a_{n-1}, -\sum_{i=1}^{n-1} a_i\right),$$

is an isomorphism from $E_{\overline{\mathbb{Q}}}^{\times(n-1)}$ to $\mathrm{Ker}(+) = \mathrm{Ker}(\mathrm{Tr}_{\overline{\mathbb{Q}}})$. Thus $\mathrm{Ker}(\mathrm{Tr}_{\overline{\mathbb{Q}}})$ is isomorphic to a product of copies of $E_{\overline{\mathbb{Q}}}$, and hence is connected. $\square$

**Corollary 2.5.** $\iota(E) \cap \mathrm{Ker}(\mathrm{Tr}) = \iota(E)[p]$.

*Proof.* The composition $\mathbb{Q} \hookrightarrow K \xrightarrow{\mathrm{Tr}} \mathbb{Q}$ is multiplication by $p$, so the composition $E \xrightarrow{\iota} R \xrightarrow{\mathrm{Tr}} E$ is also multiplication by $p$. Since $\iota(E) \cap \mathrm{Ker}(\mathrm{Tr})$ is the kernel of $\mathrm{Tr} \circ \iota = [p]$, it equals $E[p]$. $\square$

**Lemma 2.6.** *The abelian varieties $A_K$, $R_K$, and $(R/\iota(E))_K$ are all isomorphic to a product of copies of $E_K$.*

**Proposition 2.7.** *The exact sequence $0 \to A \to R \to E \to 0$ of Proposition 2.4 extends to an exact sequence $0 \to \mathcal{A} \to \mathcal{R} \to \mathcal{E} \to 0$ of Néron models over $\mathbb{Z}$.*

*Proof.* We use results of [BLR90, Ch. 7] and the fact that formation of Néron models commutes with unramified base change (see [BLR90, §1.2, Prop. 2]) to prove that for every prime $q$, the complex

$$0 \to \mathcal{A}_{\mathbb{Z}_q} \to \mathcal{R}_{\mathbb{Z}_q} \to \mathcal{E}_{\mathbb{Z}_q} \to 0 \tag{2}$$

is exact.

First suppose that $q \neq \ell$, and let $\mathfrak{q}$ be a prime of $K$ lying over $q$. We use the fact that formation of Néron models commutes with unramified base extension and check exactness of (2) after base extension to the unramified extension $\mathcal{O}_{K,\mathfrak{q}}$ of $\mathbb{Z}_q$. By Lemma 2.6, the generic fiber of the base extension of (2) to $\mathcal{O}_{K,\mathfrak{q}}$ is

$$0 \to E_{K,\mathfrak{q}}^{\oplus(n-1)} \to E_{K,\mathfrak{q}}^{\oplus n} \xrightarrow{\Sigma} E_{K,\mathfrak{q}} \to 0.$$

Thus the corresponding complex of Néron models over $\mathcal{O}_{K,\mathfrak{q}}$ is

$$0 \to \mathcal{E}_{\mathcal{O}_{K,\mathfrak{q}}}^{\oplus(n-1)} \to \mathcal{E}_{\mathcal{O}_{K,\mathfrak{q}}}^{\oplus n} \xrightarrow{\Sigma} \mathcal{E}_{\mathcal{O}_{K,\mathfrak{q}}} \to 0,$$

which is exact, since it is exact on $S$-points for *any* ring $S$.

Suppose that $q = \ell$. Since $p \neq \ell$, [BLR90, Prop. 7.5.3 (a)] asserts that the sequence $0 \to \mathcal{A}_{\mathbb{Z}_q} \to \mathcal{R}_{\mathbb{Z}_q} \to \mathcal{E}_{\mathbb{Z}_q}$ is exact. Since $p \neq q$, the map $[p] : \mathcal{E}_{\mathbb{Z}_q} \to \mathcal{E}_{\mathbb{Z}_q}$ is an étale morphism of smooth schemes. Since $E$ has good reduction at $q$, we also know that the fibers of $\mathcal{E}_{\mathbb{Z}_q}$ are geometrically connected, so $[p]$ is surjective (for more details, see the proof of [AS02, Lem. 3.2]). It follows that $\mathcal{R}_{\mathbb{Z}_q} \to \mathcal{E}_{\mathbb{Z}_q}$ is surjective.

□

### 2.3. The Cokernel of Trace

Let $\ell$ be a prime as in Conjecture 2.1. This section is devoted to computing the cokernel of the trace map $R(\mathbb{Q}) \to E(\mathbb{Q})$. Note that $R(\mathbb{Q}) = E(K)$, so this cokernel is also $E(\mathbb{Q})/\operatorname{Tr}_{K/\mathbb{Q}}(E(K))$.

**Lemma 2.8.** *Let $K_\ell$ denote the completion of $K$ at the totally ramified prime of $K$ lying over $\ell$. Then $E(K)[p] = E(K_\ell)[p] = 0$.*

*Proof.* The characteristic polynomial of $\mathrm{Frob}_\ell \in \mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell)$ on $E[p] = E(\mathbb{Q}_\ell^{\mathrm{ur}})[p]$ is $x^2 - a_\ell x + \ell \in \mathbb{F}_p[x]$. By hypothesis $a_\ell \not\equiv \ell + 1 \pmod{p}$, so $+1$ is not a root of $x^2 - a_\ell x + \ell$ hence

$$E(\mathbb{Q}_\ell)[p] = E(\mathbb{Q}_\ell^{\mathrm{ur}})[p]^{\mathrm{Frob}_\ell - 1} = 0.$$

Since $K$ is totally ramified at $\ell$ and $E$ has good reduction at $\ell$, $E(K_\ell)[p] = 0$ as well, so $E(K)[p] = 0$, as required. □

**Proposition 2.9.** $\mathrm{Coker}(R(\mathbb{Q}) \to E(\mathbb{Q})) \cong E(\mathbb{Q})/pE(\mathbb{Q})$.

*Proof.* By Corollary 2.5 the the image of $\iota(E(\mathbb{Q})) \subset R(\mathbb{Q})$ in $E(\mathbb{Q})$ is $pE(\mathbb{Q})$, so the cokernel of $R(\mathbb{Q}) \to E(\mathbb{Q})$ is a quotient of $E(\mathbb{Q})/pE(\mathbb{Q})$. Thus it suffices to prove that $R(\mathbb{Q})/\iota(E(\mathbb{Q}))$ is *finite* of order coprime to $p$.

We have an exact sequence $0 \to E \to R \to A' \to 0$, with $A'$ an abelian variety that is isogenous to $A$ (in fact, $A'$ is the abelian variety dual of $A$ since $R$ is self dual, but we will not use this fact.) The $L$-series of $A'$ is $\prod_{i=1}^{p-1} L(E, \chi_{p,\ell}^i, s)$, so by hypothesis $L(A', 1) \neq 0$ and it follows from Kato's theorem (see [Rub98, §8.1]) that $A'(\mathbb{Q})$ is finite. Thus $R(\mathbb{Q})/\iota(E(\mathbb{Q}))$ is finite since $R(\mathbb{Q})/\iota(E(\mathbb{Q})) \subset A'(\mathbb{Q})$. By Lemma 2.6, $A'_K \approx E_K^{\times(p-1)}$ and by Lemma 2.8 $E(K)[p] = 0$, so $A'(\mathbb{Q})[p] = 0$, which proves the proposition. □

### 2.4. Étale Cohomology and Shafarevich–Tate Groups

Fix an elliptic curve $E$ over $\mathbb{Q}$ and a prime $p \nmid \prod c_{E,q}$.

In this section, we use results mostly due to Mazur to relate the Shafarevich–Tate groups of $A$, $R$, and $E$ to certain étale cohomology groups. We maintain the notation and assumptions of the previous sections, except that we abuse notation slightly and let $\mathcal{A}$, $\mathcal{R}$, and $\mathcal{E}$ also denote the étale sheaves on $\mathrm{Spec}(\mathbb{Z})$ defined by the Néron models $\mathcal{A}$, $\mathcal{R}$, and $\mathcal{E}$. Let $\mathcal{B}$ be either $\mathcal{A}$, $\mathcal{R}$, or $\mathcal{E}$ and let $B = \mathcal{B}_{\mathbb{Q}}$ be the corresponding abelian variety. Let $H^q(\mathbb{Z}, \mathcal{B})$ be the $q$th étale cohomology group of $\mathcal{B}$.

**Lemma 2.10.** *There is an isomorphism* $B(\mathbb{Q}_\ell)[p] \cong \mathcal{B}(\mathbb{F}_\ell)[p]$.

*Proof.* This follows from [ST68, Lem. 2, pg. 495], but we sketch a proof for the convenience of the reader. Let $B^1(\mathbb{Q}_\ell)$ denote the kernel of the natural reduction map $r : B(\mathbb{Q}_\ell) \to \mathcal{B}(\mathbb{F}_\ell)$. Using formal groups and that $p \neq \ell$, one sees that $[p] : B^1(\mathbb{Q}_\ell) \to B^1(\mathbb{Q}_\ell)$ is an isomorphism. Since $\mathcal{B}$ is smooth over $\mathbb{Q}_\ell$, Hensel's lemma (see [BLR90, §2.3 Prop. 5]) implies that the reduction map is surjective, so we obtain an exact sequence

$$0 \to B^1(\mathbb{Q}_\ell) \to B(\mathbb{Q}_\ell) \to \mathcal{B}(\mathbb{F}_\ell) \to 0.$$

The snake lemma applied to the multiplication-by-$p$ diagram attached to this exact sequence yields the exact sequence

$$0 \to B(\mathbb{Q}_\ell)[p] \to \mathcal{B}(\mathbb{F}_\ell)[p] \to 0 \to B(\mathbb{Q}_\ell)/pB(\mathbb{Q}_\ell) \to \mathcal{B}(\mathbb{F}_\ell)/p\mathcal{B}(\mathbb{F}_\ell) \to 0,$$

which proves the lemma. □

The *Tamagawa number* of $B$ at a prime $q$ is $c_{B,q} = \#\Phi_{B,q}(\mathbb{F}_q)$, where $\Phi_{B,q}$ is the component group of the closed fiber of the Néron model of $B$ at $q$.

**Lemma 2.11.** $p \nmid c_{B,q}$.

*Proof.* First suppose $q = \ell$. The cokernel of $\mathcal{B}(\mathbb{F}_\ell) \to \Phi_{B,\ell}(\mathbb{F}_\ell)$ is contained in $H^1(\mathbb{F}_\ell, \mathcal{B}^0)$, which is 0 by Lang's theorem (see [Lan56] or [Ser88, §VI.4]), so if $\Phi_{B,\ell}(\mathbb{F}_\ell)[p] \neq 0$ then $\mathcal{B}(\mathbb{F}_\ell)[p] \neq 0$. But by Lemmas 2.6, 2.8, and 2.10,

$$\mathcal{B}(\mathbb{F}_\ell)[p] \cong \mathcal{B}(\mathbb{Q}_\ell)[p] \subset \mathcal{B}(K_\ell)[p] \cong E(K_\ell)[p] \times \cdots \times E(K_\ell)[p] = 0.$$

Next suppose that $q \neq \ell$. Since formation of Néron models commutes with unramified base extension, we have

$$\Phi_{B,q}(\overline{\mathbb{F}}_q)[p] \cong \Phi_{E,q}(\overline{\mathbb{F}}_q)[p] \times \cdots \times \Phi_{E,q}(\overline{\mathbb{F}}_q)[p] = 0,$$

by our hypotheses on $p$. □

Following the appendix to [Maz72], let

$$\Sigma(B/\mathbb{Q}) = \ker\left( H^1(\mathbb{Q}, B) \to \bigoplus_{\text{all finite } q} H^1(\mathbb{Q}_q, B) \right),$$

where the sum is over all finite primes $q$ of $\mathbb{Q}$. If $p$ is an odd prime, then $\Sigma(B/\mathbb{Q})[p^\infty] = Ш(B/\mathbb{Q})[p^\infty]$; also one can see easily using Tate cohomology for the cyclic group $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ that

$$\Sigma(B/\mathbb{Q})[2]/Ш(B/\mathbb{Q})[2] \subset H^1(\mathbb{R}, B(\mathbb{C})) \cong B(\mathbb{R})/B(\mathbb{R})^0,$$

where $B(\mathbb{R})/B(\mathbb{R})^0$ has order $2^e$ for some $e \leq \dim B$.

**Proposition 2.12** (Mazur)**.** *Suppose that* $a_\ell \not\equiv \ell + 1 \pmod{p}$*. If* $p$ *is odd, then*

$$H^1(\mathbb{Z}, \mathcal{B})[p^\infty] \cong Ш(B/\mathbb{Q})[p^\infty].$$

*Also,* $\#H^1(\mathbb{Z}, \mathcal{B})[2^\infty]/Ш(B/\mathbb{Q})[2^\infty]$ *divides* $\#(B(\mathbb{R})/B(\mathbb{R})^0)$*.*

*Proof.* It follows from the appendix to [Maz72] that there is an exact sequence

$$0 \to \Sigma(B)[p^\infty] \to H^1(\mathbb{Z}, \mathcal{B})[p^\infty] \to \bigoplus_{\text{all finite } q} H^1\left(\mathbb{F}_q, \Phi_{B,q}(\overline{\mathbb{F}}_q)\right)[p^\infty], \tag{3}$$

where $\Phi_{B,q}$ is the component group of the fiber of $\mathcal{B}$ at $q$. By [Ser79, VIII.4.8],

$$\#H^1(\mathbb{F}_q, \Phi_{B,q}(\overline{\mathbb{F}}_q)) = \#\Phi_{B,q}(\mathbb{F}_q) = c_{B,q},$$

so the proposition follows from Lemma 2.11. □

**Proposition 2.13.** $H^2(\mathbb{Z}, \mathcal{A})[p] = 0$*.*

*Proof.* We apply the lemmas in [Sch83, §III.6]. Note that $A$ has good reduction at $p$ by [Mil72, Prop. 1], and $H^1(\mathbb{Z}, \mathcal{A})[p^\infty]$ is finite by Kato's theorem (see [Rub98, §8.1]) and Proposition 2.12. In the proof of Proposition 2.9, we showed that $A'(\mathbb{Q})$ is finite of order coprime to $p$, where $A'$ is the abelian variety dual of $A$. We now use[1] Lemma 7 of [Sch83, §III.6], which because $A'(\mathbb{Q})[p] = 0$ implies that $H^2(\mathbb{Z}, \mathcal{A}[p^\infty]) = 0$ (Schneider uses $H^q_{\text{fpqf}}$, but this is not a problem since étale and fpqf cohomology agree on the smooth scheme $\mathcal{A}$.) It is easy to see (see, e.g., the proof of Lemma 6 of [Sch83, §III.6]) that the natural map $H^q(\mathbb{Z}, \mathcal{A}[p^\infty]) \to H^q(\mathbb{Z}, \mathcal{A})[p^\infty]$ is surjective for any $q > 0$, in particular, for $q = 2$, so $H^2(\mathbb{Z}, \mathcal{A})[p^\infty] = 0$ which proves the proposition. □

### 2.5. The Main Theorem

Fix an elliptic curve $E$ over $\mathbb{Q}$ and a prime $p \nmid \prod c_{E,q}$ such that $\rho_{E,p} : G_\mathbb{Q} \to \mathrm{Aut}(E[p])$ is surjective. If $p = 2$ assume also that $E(\mathbb{R})$ is connected. Assume that $\ell$ is one of the primes whose existence is predicted by Conjecture 2.1. Let $A$ and $R$ be the corresponding abelian varieties, which fit into an exact sequence $0 \to A \to R \to E \to 0$, and recall that $L(A, 1) \neq 0$ so $A(\mathbb{Q})$ and $Ш(A/\mathbb{Q})$ are both finite (by [Rub98, §8.1] and [Kat, Cor. 14.3]).

---

[1]Note that the proof of Lemma 7 of [Sch83, §III.6] relies on a theorem of Artin and Mazur whose proof they never published; generalizations of this theorem have been published by McCallum [McC86, §5] and Milne [Mil86, §III.3.4], and Mazur assures the author that he and Milne both know the proof of Artin-Mazur duality well.

**Theorem 2.14.** *There is an exact sequence*

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to Ш(A/\mathbb{Q})[p^\infty] \to Ш(E/K)[p^\infty] \to Ш(E/\mathbb{Q})[p^\infty] \to 0.$$

*In particular, if $E$ has odd rank and $Ш(E/\mathbb{Q})[p^\infty]$ is finite, then $\#Ш(A/\mathbb{Q})[p^\infty]$ is not a perfect square.*

*Proof.* By Proposition 2.7 we have an exact sequence of étale sheaves

$$0 \to \mathcal{A} \to \mathcal{R} \to \mathcal{E} \to 0,$$

which gives rise to an exact sequence of étale cohomology groups

$$H^0(\mathbb{Z}, \mathcal{R}) \to H^0(\mathbb{Z}, \mathcal{E}) \to H^1(\mathbb{Z}, \mathcal{A}) \to H^1(\mathbb{Z}, \mathcal{R}) \to H^1(\mathbb{Z}, \mathcal{E}) \to H^2(\mathbb{Z}, \mathcal{A}).$$

We have

$$H^0(\mathbb{Z}, \mathcal{R}) = \mathcal{R}(\mathbb{Z}) = R(\mathbb{Q})$$

and likewise for $\mathcal{E}$, so by Propositions 2.9, 2.12, and 2.13 we obtain an exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to Ш(A/\mathbb{Q})[p^\infty] \to Ш(R/\mathbb{Q})[p^\infty] \to Ш(E/\mathbb{Q})[p^\infty] \to 0.$$

By Shapiro's lemma, there is an isomorphism $Ш(R/\mathbb{Q}) \cong Ш(E/K)$ (see [AS02, §1.3]), which yields the claimed exact sequence.

Kato's theorem ([Rub98, §8.1] and [Kat, Cor. 14.3]) implies that $Ш(E/K)[p^\infty]$ is finite (for the trivial character use our hypothesis that $Ш(E/\mathbb{Q})[p^\infty]$ is finite, and for the nontrivial characters use our hypothesis that $L(E, \chi_{p,\ell}, 1) \neq 0$). Theorem 1.2 then implies that $\#Ш(E/K)[p^\infty]$ is a perfect square. If $E(\mathbb{Q})$ has odd rank then $\#(E(\mathbb{Q})/pE(\mathbb{Q}))$ is an odd power of $p$ (since $E[p]$ is irreducible), so $\#Ш(A/\mathbb{Q})[p^\infty]$ cannot be a perfect square. □

*Remark* 2.15. In the language of visibility of Shafarevich-Tate groups (see [CM00]), Theorem 2.14 asserts that the visible subgroup of $Ш(A)$ with respect to the embedding $A \hookrightarrow R$ is canonically isomorphic to the Mordell-Weil quotient $E(\mathbb{Q})/pE(\mathbb{Q})$.

**Proposition 2.16.** *If $q \neq p$ is a prime, then*

$$Ш(E/K)[q^\infty] \cong Ш(E/\mathbb{Q})[q^\infty] \oplus Ш(A/\mathbb{Q})[q^\infty]. \tag{4}$$

*In particular, if $Ш(E/\mathbb{Q})[q^\infty]$ is finite, then $Ш(A/\mathbb{Q})[q^\infty]$ has order a perfect square.*

*Proof.* The intersection of $E$ and $A$ in $R$ is $E[p]$, so the summation map $E \times A \to R$ is an isogeny with kernel $E[p]$. Considering the long exact sequence associated to $0 \to E[p] \to E \times A \to R \to 0$, we see that

$$H^1(\mathbb{Q}, E \times A)[q^\infty] \cong H^1(\mathbb{Q}, R)[q^\infty], \tag{5}$$

and likewise for any completion $\mathbb{Q}_v$ of $\mathbb{Q}$. We then obtain (4) by combining (5) with the fact that cohomology commutes with products and that $H^1(\mathbb{Q}, R) \cong H^1(K, E)$.

If $Ш(E/\mathbb{Q})[q^\infty]$ is finite, then since $Ш(A/\mathbb{Q})[q^\infty]$ is finite (since $L(A, 1) \neq 0$, by construction), it follows from (4) that $Ш(E/K)[q^\infty]$ is finite. We have by Theorem 1.2 that both $Ш(E/K)[q^\infty]$ and $Ш(E/\mathbb{Q})[q^\infty]$ have order a perfect square, so (4) implies that $Ш(A/\mathbb{Q})[q^\infty]$ has order a perfect square. □

## 3. An Example

Combining Proposition 2.3, Theorem 2.14, and Proposition 2.16 yields the following theorem.

**Theorem 3.1.** *Let $E$ be the elliptic curve $y^2 + y = x^3 - x$ of conductor* 37*. For every odd prime $p < 25000$ (with $p \neq 37$), there is a twist $A$ of $E^{\times(p-1)}$ such that $\#Ш(A/\mathbb{Q}) = pn^2$ for some integer $n$.*

*Remark* 3.2. Using the elliptic curve of conductor 43 in place of $E$ one can construct an abelian variety $A$ with $Ш(A/\mathbb{Q}) = 37n^2$ for some integer $n$.

Though unnecessary for Theorem 3.1, we prove below that $Ш(E/\mathbb{Q}) = 0$, which removes our dependence on Proposition 2.13. We show that $Ш(E/\mathbb{Q})[p^\infty] = 0$ for all odd $p$ using [Kol90, Thm. A], and we use a 2-descent (with [CrB]) to see that $Ш(E/\mathbb{Q})[2] = 0$.

**Theorem 3.3** (Kolyvagin)**.** *Let $E$ be an elliptic curve and let $L = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field of odd discriminant $-D$, where all primes dividing the conductor of $E$ split, and assume that $D \neq 3, 4$. If the Heegner point $y_L \in E(L)$ has infinite order (equivalently, by* [GZ86]*, $L'(E/L, 1) \neq 0$), then $\#Ш(E/L) \mid t \cdot [E(L) : \mathbb{Z}y_L]^2$, where the only primes that divide $t$ are* 2 *or primes where $\rho_{E,p}$ is not surjective.*

By [C97], $E$ is isolated in its isogeny class, so $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$ is surjective for all primes $p$ (see [RS01, §1.4]) hence $t$ is a power of 2. Let $L = \mathbb{Q}(\sqrt{-7})$. To compute $[E(L) : \mathbb{Z}y_L]$ up to a power of 2 we use the Gross-Zagier formula and the fact that $[E(L) : E(\mathbb{Q}) + E^D(\mathbb{Q})]$ is a power of 2. By [GZ86, Thm. 6.3],

$$h(y_L) = \frac{u^2|D|^{\frac{1}{2}}}{\|\omega_f\|} L'(E, 1)L(E^D, 1),$$

where $D = -7$, $u = 1$, and $\|\omega_f\|$ is the Peterson norm of the newform $f$ corresponding to $E$. Generators for the period lattice of $E$ are $\omega_1 \sim 2.993459$ and $\omega_2 \sim 2.451389i$, so $\|\omega_f\| \sim 7.338133$. The quadratic twist $E^D$ is the curve **1813B1** in [CrA], and $E^D(\mathbb{Q}) = 0$. From [CrA] we find that $L'(E, 1) \sim 0.306000$ and $L(E^D, 1) \sim 1.853076$, so $h(y_L) \sim 0.204446$. The height of a generator of $E(\mathbb{Q})$ is $\sim 0.051111 \sim h(y_L)/4$, so $[E(L) : \mathbb{Z}y_L]$ is a power of 2. (As a double check, and to avoid dependence on the Gross-Zagier formula, we wrote a program using [BCP97] to compute Heegner points and found that $y_L = (0, 0)$, which is a generator for $E(\mathbb{Q})$.) Thus $\#Ш(E/L)$ is a power of 2.

To connect $Ш(E/L)$ with $Ш(E/\mathbb{Q})$, use the inflation-restriction exact sequence

$$0 \to H^1(L/\mathbb{Q}, E(L)) \to H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})) \to H^1(L, E(\overline{\mathbb{Q}})).$$

Let $p$ be an odd prime. Since $H^1(L/\mathbb{Q}, E(L))$ is a 2-group, the above sequence leads to an injective map

$$H^1(\mathbb{Q}, E(\overline{\mathbb{Q}}))[p] \hookrightarrow H^1(L, E(\overline{\mathbb{Q}}))[p],$$

which induces an inclusion

$$\text{Ш}(E/\mathbb{Q})[p] \hookrightarrow \text{Ш}(E/L)[p] = 0.$$

## References

[AS02] A. Agashe and W. A. Stein, *Visibility of Shafarevich-Tate Groups of Abelian Varieties*, J. of Number Theory, **97** (2002), no. 1, 171–184.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises*, J. Amer. Math. Soc. **15** (2001), no. 4, 843–939.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR **91i:**14034

[C97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[CrA] ———, *Elliptic Curve Data*, http://www.maths.nott.ac.uk/personal/jec/ftp/data/.

[CrB] ———, `mwrank` *(computer software)*, `http://www.maths.nott.ac.uk/personal/jec/ftp/progs/`.

[CM00] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR 1 758 797

[Fea01] J. Fearnley, *Vanishing and Non-Vanishing of L-series of Elliptic Curves Twisted by Dirichlet Characters*, Concordia Ph.D. thesis (2001).

[Fla90] M. Flach, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math. **412** (1990), 113–127. MR **92b:**11037

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR **87j:**11057

[JL99] B. W. Jordan and R. Livné, *On Atkin-Lehner quotients of Shimura curves*, Bull. London Math. Soc. **31** (1999), no. 6, 681–685. MR **2000j:**11090

[Kat] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Preprint, 244 pages.

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR **92g:**11109

[Lan56] S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR 19,174a

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[McC86] W. G. McCallum, *Duality theorems for Néron models*, Duke Math. J. **53** (1986), no. 4, 1093–1124. MR **88c:**14062

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190. MR 48 #8512

[Mil86] ______, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[PS97] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. MR **98k:**11087

[PS99] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR **2000m:**11048

[RS01] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 143–232. MR **2002h:**11047

[Rub98] K. Rubin, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), Cambridge Univ. Press, Cambridge, 1998, pp. 351–367. MR **2001a:**11106

[Sch83] P. Schneider, *Iwasawa L-functions of varieties over algebraic number fields. A first approach*, Invent. Math. **71** (1983), no. 2, 251–293. MR **85d:**11063

[SD67] P. Swinnerton-Dyer, *The conjectures of Birch and Swinnerton-Dyer, and of Tate*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 132–157. MR 37 #6287

[Ser79] J-P. Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Ser88] ______, *Algebraic groups and class fields*, Springer-Verlag, New York, 1988, Translated from the French.

[ST68] J-P. Serre and J. T. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[Tat63] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295. MR 31 #168

515 Science Center, Department of Mathematics, Harvard University,
*E-mail address*: `was@math.harvard.edu`