Bounding the rank of rational elliptic curves

Arav Karighattam

ABSTRACT. The theory of Selmer and Tate-Shafarevich groups can be used to give bounds on the rank of certain families of elliptic curves. This paper reviews some bounds on this rank and the Cassels bilinear pairing on the Tate-Shafarevich group, which shows that if the conjecture that the Tate-Shafarevich group is finite holds, then the order of the Tate-Shafarevich group must be a square. Finally, we mention another interesting result on the average rank of an elliptic curve.

1. Background

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}$, and let $\bar{\mathcal{E}}$ be its extension to $\overline{\mathbb{Q}}$. Note that to simplify equations, we use this instead of the standard notations $\mathcal{E}[\mathbb{Q}]$ and $\mathcal{E}[\overline{\mathbb{Q}}]$ to also denote the corresponding group. We consider $\bar{\mathcal{E}}$ as a $\mathsf{G} := \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, then $\mathcal{E}$ as the invariant subgroup of $\bar{\mathcal{E}}$. We let $\ker_{\mathcal{E}} \psi$ denote the kernel of the map on $\mathcal{E}$ induced by ψ.
Note that the definition of an isogeny and the definition of the Selmer and Tate-Shafarevich groups can be defined over any other number field as well. Throughout this paper we assume all cohomology groups are taken over G, unless otherwise specified.

ISOGENIES. Consider any isogeny $\psi: \mathcal{E} \to \mathcal{E}'$, that is, a morphism of $\mathcal{E}$ and $\mathcal{E}'$ which preserves the point at infinity which we call O. If ψ has degree m, we can define a dual isogeny $\hat{\psi}: \mathcal{E}' \to \mathcal{E}$ by composing the identifications $\mathcal{E} \leftrightarrow \mathsf{Cl}^{\circ}\mathcal{E}$ and $\mathcal{E}' \leftrightarrow \mathsf{Cl}^{\circ}\mathcal{E}'$ with the map $\mathsf{Cl}^{\circ}\mathcal{E} \to \mathsf{Cl}^{\circ}\mathcal{E}'$ induced by ψ; these maps satisfy $\hat{\psi} \circ \psi = [m]_{\mathcal{E}}$ and $\hat{\hat{\psi}} = \psi$. In Section 4, we will use the relation

$$\begin{aligned}\dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}/p\mathcal{E} &= \dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}/\hat{\psi}\mathcal{E}' + \dim_{\mathbb{Z}/p\mathbb{Z}} \hat{\psi}\mathcal{E}'/p\mathcal{E} \\ &= \dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}/\hat{\psi}\mathcal{E}' + \dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}'/\psi\mathcal{E} - \dim_{\mathbb{Z}/p\mathbb{Z}} \ker_{\mathcal{E}'/\psi\mathcal{E}} \hat{\psi} \\ &= \dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}/\hat{\psi}\mathcal{E}' + \dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}'/\psi\mathcal{E} + \dim_{\mathbb{Z}/p\mathbb{Z}} \psi(\ker\,[p]_{\mathcal{E}}) - \dim_{\mathbb{Z}/p\mathbb{Z}} \ker \hat{\psi}\,; \qquad (1)\end{aligned}$$

the second and third equalities coming from the exact sequences

$$0 \longrightarrow \ker_{\mathcal{E}'/\psi\mathcal{E}} \hat{\psi} \hookrightarrow \mathcal{E}'/\psi\mathcal{E} \xrightarrow{\hat{\psi}} \mathrm{im}_{\mathcal{E}'/\psi\mathcal{E}} \hat{\psi} \cong \hat{\psi}\mathcal{E}'/p\mathcal{E} \longrightarrow 0$$

and

$$0 \longrightarrow \psi(\ker\,[p]_{\mathcal{E}}) \longrightarrow \ker \hat{\psi} \longrightarrow \ker_{\mathcal{E}'/\psi\mathcal{E}} \hat{\psi} \longrightarrow 0.$$

The exactness in the second sequence above comes from the fact that

$$\ker_{\psi\mathcal{E}} \hat{\psi} = \psi(\ker\,[p]_{\mathcal{E}}).$$

Note that isogenies of elliptic curves over $\mathbb{Q}$ of prime degree only exist for a certain finite set of primes [7], the largest of which being 163.
A nontrivial (and hence surjective) isogeny $\psi: \bar{\mathcal{E}} \to \bar{\mathcal{E}}'$ is said to be separable if the corresponding function field extension is separable. We state here for further reference that these separable isogenies have their degree to be the size of their kernel. A proof of this result is given in [1], Chapter III.4. Separability follows for all isogenies over $\overline{\mathbb{Q}}$ from the fact that $\mathsf{char}\ \overline{\mathbb{Q}} = 0$. The kernel property, though, can be checked directly for the specific 2-isogeny relevant in Section 4 of this paper.

Selmer and Tate-Shafarevich Groups. We now introduce the Selmer and Tate-Shafarevich groups associated to $\mathcal{E}$, as described in [1], Chapter X.4. To any isogeny ψ is associated an exact sequence of G-modules $0 \to \ker\psi \xrightarrow{i} \bar{\mathcal{E}} \xrightarrow{\psi} \bar{\mathcal{E}}' \to 0$, since a morphism of projective curves is either surjective or has a zero-dimensional image. This sequence induces a long exact sequence of cohomology

$$\cdots \longrightarrow \mathcal{E} \xrightarrow{\psi} \mathcal{E}' \longrightarrow \mathcal{H}^1(\ker\psi) \xrightarrow{i_\star} \mathcal{H}^1(\bar{\mathcal{E}}) \xrightarrow{\psi_\star} \mathcal{H}^1(\bar{\mathcal{E}}') \longrightarrow \cdots.$$

The first cohomology group $\mathcal{H}^1(\bar{\mathcal{E}})$ can be considered as the group of $\bar{\mathcal{E}}$-torsors (also known as principal homogeneous spaces) up to isomorphism. These torsors can be considered as other curves over $\overline{\mathbb{Q}}$; namely, those for which the action of $\bar{\mathcal{E}}$ is a morphism of varieties. Then an $\bar{\mathcal{E}}$-torsor $\mathcal{C}$ is isomorphic to $\bar{\mathcal{E}}$ itself if and only if there is some element of $\mathcal{C}$ which is fixed by G; that is, $\mathcal{C}$ has a rational point. Recall that an isomorphism from $\mathcal{E}$ to an $\bar{\mathcal{E}}$-torsor containing a rational point p_0 is given by $p \mapsto p + p_0$. This same isomorphism turns out to show that homogeneous spaces are actually all isomorphic (as varieties) to $\bar{\mathcal{E}}$. This group of torsors up to isomorphism is known as the Weil-Châtelet group of $\mathcal{E}$, denoted by $\mathsf{WC}(\mathcal{E})$. Using this notation, the previous exact sequence becomes

$$\cdots \longrightarrow \mathcal{E} \xrightarrow{\psi} \mathcal{E}' \longrightarrow \mathcal{H}^1(\ker\psi) \xrightarrow{i_\star} \mathsf{WC}(\mathcal{E}) \xrightarrow{\psi_\star} \mathsf{WC}(\mathcal{E}') \longrightarrow \cdots.$$

The short exact sequence induced by the above sequence is

$$0 \longrightarrow \mathcal{E}'/\psi\mathcal{E} \longrightarrow \mathcal{H}^1(\ker\psi) \xrightarrow{i_\star} \ker\psi_\star \longrightarrow 0. \tag{2}$$

Similar sequences can be defined for the completions $\mathcal{E}_v$ over $\mathbb{Q}_v$ (v being either a prime or ∞). Since $\mathsf{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v) = D_v(\overline{\mathbb{Q}}/\mathbb{Q})$ is the decomposition group, there is a natural inclusion $\mathsf{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v) \hookrightarrow \mathsf{G}$. The exact sequences for $\mathcal{E}$ and $\mathcal{E}_v$ – the latter containing cohomology groups over D_v – with the restriction maps from the inclusion just described yield a short exact sequence

$$\begin{aligned} 0 \longrightarrow \ker\left(\frac{\mathcal{E}'}{\psi\mathcal{E}} \longrightarrow \prod_v \ker\psi_{v\star}\right) &\longrightarrow \ker\left(\mathcal{H}^1(\ker\psi) \xrightarrow{\prod_v \mathsf{Res}_v \circ i_{v\star}} \prod_v \ker\psi_{v\star}\right) \\ &\longrightarrow \ker\left(\ker\psi_\star \xrightarrow{\prod_v \mathsf{Res}_v} \prod_v \ker\psi_{v\star}\right) \longrightarrow 0, \end{aligned}$$

by taking the product of all the completions of the G-module exact-sequence and taking the product of the corresponding restriction maps. The first kernel is just $\mathcal{E}'/\psi\mathcal{E}$ by exactness. The second kernel is called the Selmer group $S^{\psi}(\mathcal{E})$ of $\mathcal{E}$. The Tate-Shafarevich group of $\mathcal{E}$ is defined as the kernel

$$\text{Ш}(\mathcal{E}) \coloneqq \ker\left(\mathsf{WC}(\mathcal{E}) \longrightarrow \prod_v \mathsf{WC}(\mathcal{E}_v)\right),$$

so that the exact sequence above can be rewritten as

$$0 \longrightarrow \mathcal{E}'/\psi\mathcal{E} \longrightarrow S^{\psi}(\mathcal{E}) \longrightarrow \text{Ш}(\mathcal{E}) \cap \ker\psi_\star \longrightarrow 0. \tag{3}$$

Thus, we can determine $\mathcal{E}'/\psi\mathcal{E}$ by determining the Selmer and Tate-Shafarevich groups of $\mathcal{E}$.

The Selmer group $S^{\psi}(\mathcal{E})$ can be shown to be finite since all its elements have trivial image under the restriction map induced by the inclusion of the inertia subgroup $I_p \subseteq \mathsf{G}$ for all but finitely many primes p. We will denote the finite group of elements of $\mathcal{H}^1(\ker\psi)$ having trivial image under the restriction map outside some finite set of prime or Archimedean places $\mathcal{P}_{\mathcal{E}}$ by $\mathcal{H}^1(\ker\psi, \mathcal{P}_{\mathcal{E}})$; the cocycles are said to be unramified at all primes outside

$\mathcal{P}_{\mathcal{E}}$. The relevant set $\mathcal{P}_{\mathcal{E}}$ for the Selmer group can be shown to consist of the primes with bad reduction and the primes dividing the degree of ψ.
The Tate-Shafarevich group is conjectured to be finite and has been verified to be finite in many cases. In Section 3, we discuss the Cassels bilinear pairing $\text{Ш}(\mathcal{E}) \times \text{Ш}(\mathcal{E}) \to \mathbb{Q}/\mathbb{Z}$ (derived in [21]) and its implication that if the Tate-Shafarevich group is finite, then all of its primary subgroups will have its order to be a square.
In the language of torsors, the non-trivial elements of the Tate-Shafarevich group correspond to classes of torsors which have p-adic solutions for all p but have no rational solutions.

Reductions of Elliptic Curves and Supersingularity. We discuss here some properties of elliptic curves over finite fields. The proofs of some of the equivalences stated below can be found in [1], Chapters V and VII. An elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ is said to have good reduction at a prime p if its reduction to $\mathbb{Z}/p\mathbb{Z}$ is nonsingular; this is true if and only if p does not divide the discriminant of $\mathcal{E}$. For such primes p, it can be shown that the reduction map from the torsion subgroup of $\mathcal{E}$ to $\tilde{\mathcal{E}}_p$ is injective. Counting the points in $\tilde{\mathcal{E}}_p$ for many primes p can bound the size of the torsion subgroup of $\mathcal{E}$. If $\tilde{\mathcal{E}}_q$ is an elliptic curve over $\mathbb{F}_q$; $\tilde{\mathcal{E}}_q$ is said to be supersingular if and only if $\tilde{\mathcal{E}}_q$ has no q-torsion points. There are some other equivalent definitions; we note in particular that for q a prime, $\tilde{\mathcal{E}}_q$ is supersingular if and only if it has $q+1$ points over $\mathbb{F}_q$, and that if $\tilde{\mathcal{E}}_q$ has a Weierstrass equation $y^2 = x^3 + ax$, then $\tilde{\mathcal{E}}_q$ is supersingular if and only if $q \equiv 3 \pmod 4$. In the latter case, the size of the torsion subgroup must divide $q+1$ for infinitely many primes $q \equiv 3 \pmod 4$ (as an elliptic curve only has bad reduction at finitely many primes), and by Dirichlet's Theorem, the torsion subgroup $\mathcal{T}$ of $\mathcal{E}$ must have order dividing 4 and hence $\mathcal{T} \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2. Calculating the Selmer group

The Selmer group $S^{\psi}(\mathcal{E})$ can naturally be embedded in the Weil-Châtelet group $\mathrm{WC}(\mathcal{E})$, associating an equivalence class of $\bar{\mathcal{E}}$-torsors to each point. For elliptic curves over $\mathbb{Q}$, we describe two methods of determining the dimension of $\mathcal{E}/p\mathcal{E}$; the first in terms of the dimension of the Tate-Shafarevich group $\text{Ш}(\mathcal{E})$, and the second without using the Tate-Shafarevich group in the case of a 2-isogeny ψ such that there is a point $\mathfrak{p} \in \mathcal{E}$ of order 2 in $\ker\psi$. Finally considered in this section is a method to determine the equations for the corresponding $\bar{\mathcal{E}}$-torsors useful for computing $S^{\psi}(\mathcal{E})$, with the same preceding assumptions.

The rank of an Elliptic Curve in terms of the Selmer and Tate-Shafarevich Groups. Equations (1) and (2) together imply that for any isogeny $\psi\colon \mathcal{E} \to \mathcal{E}'$ of prime degree p,

$$\begin{aligned}\dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}/p\mathcal{E} &= \dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}/\hat{\psi}\mathcal{E}' + \dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}'/\psi\mathcal{E} + \dim_{\mathbb{Z}/p\mathbb{Z}} \psi(\ker\,[p]_{\mathcal{E}}) - \dim_{\mathbb{Z}/p\mathbb{Z}} \ker\hat{\psi} \\ &= \dim_{\mathbb{Z}/p\mathbb{Z}} S^{\psi}(\mathcal{E}) - \dim_{\mathbb{Z}/p\mathbb{Z}} \text{Ш}(\mathcal{E}) \cap \ker\psi_\star + \dim_{\mathbb{Z}/p\mathbb{Z}} S^{\hat{\psi}}(\mathcal{E}') \\ &\quad - \dim_{\mathbb{Z}/p\mathbb{Z}} \text{Ш}(\mathcal{E}') \cap \ker\hat{\psi}_\star + \dim_{\mathbb{Z}/p\mathbb{Z}} \psi(\ker\,[p]_{\mathcal{E}}) - \dim_{\mathbb{Z}/p\mathbb{Z}} \ker\hat{\psi}.\end{aligned}$$

We can check using inhomogeneous cocycles that there is an exact sequence $0 \longrightarrow \ker\psi_\star \longrightarrow \ker\,[p]_{\mathcal{E}\star} \longrightarrow \ker\hat{\psi}_\star \longrightarrow 0$. Considering the analogous exact sequences over the completions of $\mathbb{Q}$, we obtain the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker\psi_\star \arrow[r, hook] \arrow[d, "\prod_\nu \mathrm{Res}_\nu"] & \ker\,[p]_{\mathcal{E}\star} \arrow[r, two heads, "\psi_\star"] \arrow[d, "\prod_\nu \mathrm{Res}_\nu"] & \ker\hat{\psi}_\star \arrow[r] \arrow[d, "\prod_\nu \mathrm{Res}_\nu"] & 0 \\
0 \arrow[r] & \prod\limits_\nu \ker\psi_{\nu\star} \arrow[r, hook] & \prod\limits_\nu \ker\,[p]_{\mathcal{E}_\nu\star} \arrow[r, two heads, "\prod_\nu \psi_{\nu\star}"] & \prod\limits_\nu \ker\hat{\psi}_{\nu\star} \arrow[r] & 0\,.
\end{tikzcd}$$

Since the kernel of a morphism of left exact sequences is a left exact sequence, this diagram yields the exact sequence

$$0 \longrightarrow \text{Ш}(\mathcal{E}) \cap \ker\psi_\star \longrightarrow \text{Ш}(\mathcal{E}) \cap \ker\,[p]_{\mathcal{E}\star} \xrightarrow{\psi_\star^{\mathrm{ind}}} \text{Ш}(\mathcal{E}') \cap \ker\hat{\psi}_\star,$$

where $\psi_\star^{\mathrm{ind}}$ is the restriction of $\psi_\star$ in the commutative diagram. This implies the dimension relation

$$\begin{aligned}\dim_{\mathbb{Z}/p\mathbb{Z}} \mathcal{E}/p\mathcal{E} &= \dim_{\mathbb{Z}/p\mathbb{Z}} S^{\psi}(\mathcal{E}) + \dim_{\mathbb{Z}/p\mathbb{Z}} S^{\hat{\psi}}(\mathcal{E}') + \dim_{\mathbb{Z}/p\mathbb{Z}} \psi(\ker\,[p]_{\mathcal{E}}) \\ &\quad - \dim_{\mathbb{Z}/p\mathbb{Z}} \ker \hat{\psi} - \dim_{\mathbb{Z}/p\mathbb{Z}} Ш(\mathcal{E}) \cap \ker[p]_{\mathcal{E}\star} - \dim_{\mathbb{Z}/p\mathbb{Z}} \operatorname{coker} \psi_\star^{\mathrm{ind}}.\end{aligned} \tag{4}$$

We will use this relation in section 4 to calculate the sum of the rank of an elliptic curve and the dimension of the subgroup of the Tate-Shafarevich group in the kernel of the map induced by multiplication by 2.

An Exact Sequence. Now we add the assumptions mentioned at the beginning of this section. In this case, $\ker \psi \cong \mathbb{Z}/2\mathbb{Z}$ over $\overline{\mathbb{Q}}$ as mentioned earlier, so it is isomorphic as such over $\mathbb{Q}$. Since $\ker \psi$ is a trivial G-module, we find that $\mathcal{H}^1(\ker \psi) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by using Hilbert's Theorem 90 with the long exact sequence in cohomology associated to $0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{(-1)^\bullet} \overline{\mathbb{Q}}^\times \xrightarrow{\bullet^2} \overline{\mathbb{Q}}^\times \longrightarrow 0$. In particular, this connecting isomorphism sends an element $\mathfrak{a} \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ to the cocycle $\mathfrak{g} \mapsto \iota\left(\frac{\mathfrak{g}\sqrt{\mathfrak{a}}}{\sqrt{\mathfrak{a}}}\right)$ for ι the inclusion from $\mathbb{Z}^\times$ to $\mathcal{E}$ sending -1 to $\mathfrak{p}$. Define the subgroup $\mathcal{G}_{\mathcal{P}_\mathcal{E}} \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by

$$\mathcal{G}_{\mathcal{P}_\mathcal{E}} := \left\{\mathfrak{a} \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \,\middle|\, \nu_p(\mathfrak{a}) \in 2\mathbb{Z} \text{ for all } p \notin \mathcal{P}\right\}.$$

If the cocycle corresponding to $\mathfrak{a}$ is in $\mathcal{H}^1(\ker \psi, \mathcal{P}_\mathcal{E})$, then $\mathfrak{g}\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}}$ for all $\mathfrak{g} \in I_p$ and for every $p \notin \mathcal{P}_\mathcal{E}$. For each prime $p \notin \mathcal{P}_\mathcal{E}$ we may consider an element $\mathfrak{g}_p \in \varprojlim_K \operatorname{Gal}(K/\mathbb{Q}) = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for each $p \in \mathcal{P}_\mathcal{E}$ which lies above the automorphism $\sqrt{p} \mapsto -\sqrt{p}$ of $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ and the trivial automorphism of $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ for all primes $q \neq p$; this element lies in I_p. If $\nu_p(\mathfrak{a}) \notin 2\mathbb{Z}$ then $\mathfrak{a}$ has nontrivial image under this automorphism, and the cocycle in correspondence with $\mathfrak{a}$ is ramified at p. Thus $\mathcal{H}^1(\ker \psi, \mathcal{P}_\mathcal{E}) \subseteq \mathcal{G}_{\mathcal{P}_\mathcal{E}}$; it can be seen for similar reasons that the containment is in fact an equality. From equations (2) and (3), we obtain the exact sequence

$$0 \longrightarrow \mathcal{E}'/\psi\mathcal{E} \longrightarrow \mathcal{G}_{\mathcal{P}_\mathcal{E}} \xrightarrow{\jmath_\psi} \ker \psi_\star \subseteq \mathrm{WC}(\mathcal{E}).$$

From the description above, we see that the map $\jmath_\psi$ sends a point in $\mathcal{G}_{\mathcal{P}_\mathcal{E}}$ to the class of the corresponding homogeneous space in $\mathrm{WC}(\mathcal{E})$. This yields that

$$\dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}'/\psi\mathcal{E} = \dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{G}_{\mathcal{P}_\mathcal{E}} - \dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \jmath_\psi,$$

and

$$\begin{aligned}\dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}/2\mathcal{E} &= \dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{G}_{\mathcal{P}_\mathcal{E}} + \dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{G}_{\mathcal{P}_{\mathcal{E}'}} - \dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \jmath_\psi - \dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \jmath_{\hat{\psi}} \\ &\quad + \dim_{\mathbb{Z}/2\mathbb{Z}} \psi(\ker\,[2]_\mathcal{E}) - \dim_{\mathbb{Z}/2\mathbb{Z}} \ker \hat{\psi}.\end{aligned} \tag{5}$$

The Equations Defining the Torsor Corresponding to an Element of the Selmer Group. Since an $\bar{\mathcal{E}}$-torsor corresponds to a non-trivial class in $\mathrm{WC}(\mathcal{E})$ if and only if it has no rational points, we may use the above identifications to write $S^{\psi}(\mathcal{E}) \cong \{\mathfrak{a} \in \mathcal{G}_\mathcal{P} | \mathcal{C}_\mathfrak{a} \text{ has a } \mathbb{Q}_p\text{-point } \forall p \in \mathcal{P}\}$ for $\mathcal{C}_\mathfrak{a}$ the $\bar{\mathcal{E}}$-torsor corresponding to the cocycle in $\mathcal{H}^1(\ker \psi)$ associated to $\mathfrak{a}$. For a specific elliptic curve $\mathcal{E}$, described below is a possible method to compute the equation of the $\bar{\mathcal{E}}$-torsor $\mathcal{C}_\mathfrak{a}$. Consider the morphism ϕ on $\mathcal{E}$ defined by addition by $\mathfrak{p}$, this morphism can be given by two regular functions, $\mathfrak{h}_1(x,y)$ and $\mathfrak{h}_2(x,y)$. Since $\langle\mathfrak{p}\rangle \cong \mathbb{Z}/2\mathbb{Z}$, this morphism defines an action of $\operatorname{Gal}(\mathbb{Q}(\sqrt{\mathfrak{a}})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ on the set of morphisms $\mathcal{E} \to \mathcal{E}$ by $\mathfrak{g} \cdot (\mathfrak{r}_1, \mathfrak{r}_2) = \phi(\mathfrak{r}_1, \mathfrak{r}_2)$, for $\mathfrak{g}$ the nontrivial automorphism; we extend this action to $\mathcal{E}[\mathbb{Q}(\sqrt{\mathfrak{a}})]$ by combining the previous action with the normal action on $\mathbb{Q}(\sqrt{\mathfrak{a}})$. Next, we suppose that there are two independent regular functions $\tilde{z}_1$ and $\tilde{z}_2$ on $\mathcal{E}$ such that the corresponding regular functions $z_1 := \tilde{z}_1\sqrt{\mathfrak{a}}$ and $z_2 := \tilde{z}_2\sqrt{\mathfrak{a}}$ are invariant. Then we can consider a curve $\tilde{\mathcal{C}}_\mathfrak{a}$ in $\mathbb{P}^2_{\mathbb{Q}(\sqrt{\mathfrak{a}})}$ which is the projective closure of the affine curve defined by an equation relating these invariant regular functions. Define the morphism $\tilde{\phi}(x,y) = (z_1(x,y), z_2(x,y))$, then we can consider the point $p_0 := \tilde{\phi}(\mathfrak{p}) \in$

$\tilde{\mathcal{C}}_{\mathfrak{a}}$. We now add the assumption that $\tilde{\phi}$ is an isomorphism, so that we can define the $\bar{\mathcal{E}}$-module action on $\tilde{\mathcal{C}}_{\mathfrak{a}}$ by $\mathfrak{q} + \mathfrak{Q} = \tilde{\phi}(\tilde{\phi}^{-1}(\mathfrak{q}) + \mathfrak{Q})$ for any $\mathfrak{q} \in \tilde{\mathcal{C}}_{\mathfrak{a}}$ and $\mathfrak{Q} \in \bar{\mathcal{E}}$. To show that $\tilde{\mathcal{C}}_{\mathfrak{a}} = \mathcal{C}_{\mathfrak{a}}$, we must show that the cocycle $\mathfrak{g} \mapsto \mathfrak{g}p_0 - p_0$ is cohomologous to the cocycle $\mathfrak{g} \mapsto \iota\left(\frac{\mathfrak{g}\sqrt{\mathfrak{a}}}{\sqrt{\mathfrak{a}}}\right)$ (in fact, for this choice of p_0, the cocycles are exactly equal). The case for the trivial automorphism is obvious. Now, if we set $\mathfrak{g}$ as the nontrivial automorphism, $\mathfrak{g}p_0 = \mathfrak{g}\left(\sqrt{\mathfrak{a}}\tilde{z}_1(\mathfrak{p}), \sqrt{\mathfrak{a}}\tilde{z}_2(\mathfrak{p})\right) = \left(-\sqrt{\mathfrak{a}}\tilde{z}_1(\mathfrak{p}), -\sqrt{\mathfrak{a}}\tilde{z}_2(\mathfrak{p})\right) = \left(\sqrt{\mathfrak{a}}\tilde{z}_1(O), \sqrt{\mathfrak{a}}\tilde{z}_2(O)\right)$, and the first cocycle has $\mathfrak{g} \mapsto \tilde{\phi}^{-1}(\mathfrak{g}p_0) - \tilde{\phi}^{-1}(p_0) = O - \mathfrak{p} = \mathfrak{p}$ which agrees with the second cocycle. Thus, if the two assumptions are satisfied, this method yields an equation defining the corresponding $\bar{\mathcal{E}}$-torsor.

3. The Cassels bilinear pairing

In this section we describe the bilinear pairing on the Tate-Shafarevich group considered by Cassels [2].

It is a conjecture of Tate and Shafarevich that $\text{Ш}(\mathcal{E})$ is finite for all elliptic curves $\mathcal{E}$; this has been shown for some rank 1 curves (see [3]). One possible step toward this conjecture is presented in [4], which discusses an analogy between elliptic curves and number fields; in particular it relates the group $\mathcal{E}$ with the unit group of the number field K, and the Tate-Shafarevich group with the ideal class group $\mathrm{Cl}(K)$, which has been proven to be finite. If this conjecture holds, then the Cassels pairing will show that the order of $\text{Ш}(\mathcal{E})$ is a square; as a consequence, using the methods discussed in section 4, all the curves $y^2 = x^3 + px$ for all $p \equiv 3, 5, 13$, or $15 \pmod{16}$ will have rank 1.

First, we state the result that $\mathcal{H}^2(\mathbb{I}/\overline{\mathbb{Q}}^{\times}) \cong \mathbb{Q}/\mathbb{Z}$ for reference later in this section, for $\mathbb{I}$ the group of idèles (or ignoring the topological structure, the invertible adèles $\mathbb{A}^{\times}$) on $\overline{\mathbb{Q}}$. We also use the notation $\mathfrak{d}$ to refer to the map from the group of points on a curve to the divisor class group, and δ to refer to the coboundary map. To define the pairing $\langle \bullet, \bullet \rangle$, we consider two classes $[\overline{\mathsf{C}}]$ and $[\chi]$ in $\text{Ш}(\mathcal{E})$, considering C as an $\bar{\mathcal{E}}$-torsor and χ as a cocycle. We refer to C as the curve over $\mathbb{Q}$ and $\overline{\mathsf{C}}$ as the curve over $\overline{\mathbb{Q}}$. The choice of the $\bar{\mathcal{E}}$-torsor we consider corresponding to $[\mathsf{C}]$ does not matter as these are birational over $\mathbb{Q}$, and the only dependence on this choice relates to points on C. We use the cocycle condition in terms of divisors to see that $\mathfrak{d}\left(\chi(\mathfrak{g}_1) + \mathfrak{g}_1\chi(\mathfrak{g}_1^{-1}\mathfrak{g}_2) - \chi(\mathfrak{g}_2)\right)$ is a trivial element of $\mathrm{Cl}^{\circ}\overline{\mathsf{C}}$, and hence is the principal divisor corresponding to some regular function $\mathsf{f}(\mathfrak{g}_1, \mathfrak{g}_2)$ on $\bar{\mathcal{E}}$ (this choice is unique up to scaling), or equivalently, $\overline{\mathsf{C}}$, here assuming that like χ, f is also continuous. By the definition of the Tate-Shafarevich group, for all p there must exist points x_p on the curves C_p over $\mathbb{Q}_p$ – these can be chosen in the domain on which $\mathsf{f}(\mathfrak{g}_1, \mathfrak{g}_2)$ is defined – so that we can define an idèle whose entry corresponding to p is $\mathsf{f}(\mathfrak{g}_1, \mathfrak{g}_2)(x_p)$, and hence a cochain on $\mathbb{I}/\overline{\mathbb{Q}}^{\times}$. But the coboundary of the divisor of f is zero since it itself is a coboundary, thus the coboundary of f as a cocycle over $\overline{\mathbb{Q}}(x)$ must have its corresponding divisor to be zero, so that it is over $\overline{\mathbb{Q}}$, and the coboundary of the cochain $\left(\mathsf{f}(\mathfrak{g}_1, \mathfrak{g}_2)(x_p)\right)_p$ does not depend on the values of x_p, and further all of its components are the same, so it is trivial in the ideal class group. This implies that the cochain is actually is cocycle, we denote its class by $[\mathfrak{t}]$. Note that in the above derivation, the lemma in [2], Section 2, implies that we may choose the points x_p appropriately such that the cocycle does in fact lie in $\mathbb{I}$.

To see that the Cassels pairing $\langle [\overline{\mathsf{C}}], [\chi] \rangle = [\mathfrak{t}]$ is well-defined, we must check that the class of this cocycle does not depend on the choice of the points x_p (for the proof, see [2]) and the choice of representatives for $[\chi]$. Suppose that χ_1 and χ_2 are two representative cocycles for the class $[\chi]$. Since the divisor of f/g is the difference of the divisors of f and g, working through the steps above, we see that $\langle [\overline{\mathsf{C}}], \chi_1 \rangle - \langle [\overline{\mathsf{C}}], \chi_2 \rangle = \langle [\overline{\mathsf{C}}], \chi_1 - \chi_2 \rangle$ (we have not yet shown independence of the class representative, so we drop the brackets in the notation). Thus, to show independence on $[\chi]$, it suffices to show that for any coboundary χ, the corresponding $\mathfrak{t}$ is also a coboundary. In a similar fashion to what is done above, we can choose some $\chi_0 \in \overline{\mathsf{C}}$ such that $\mathfrak{d}(\chi(\mathfrak{g}_1) - \mathfrak{g}_1\chi_0 + \chi_0)$ is a trivial element of $\mathrm{Cl}^{\circ}\overline{\mathsf{C}}$, and is the principal divisor associated to some regular function F. Then $\mathsf{f}(\mathfrak{g}_1, \mathfrak{g}_2) = c(\mathfrak{g}_1, \mathfrak{g}_2)\left(\frac{\mathrm{F}(\mathfrak{g}_1)\mathfrak{g}_1\mathrm{F}(\mathfrak{g}_1^{-1}\mathfrak{g}_2)}{\mathrm{F}(\mathfrak{g}_2)}\right)$. Plugging in the points $x_p \in \mathsf{C}_p$, we find that $\mathfrak{t}$ must be a coboundary. It can be checked as in [2] that this pairing is bilinear, and is nondegenerate on the quotient of the Tate-Shafarevich group by the subgroup of all infinitely divisible elements.

4. The elliptic curves $y^2 = x^3 + bx$

In this section we explain the methods in [1], Chapter X which bound the rank of the elliptic curve $\mathcal{E}$ defined by $y^2 = x^3 + bx$ for all b, and mention, in particular, the example where b is prime.

A Two-Isogeny. We describe a 2-isogeny defined on a certain class of elliptic curves, so that we can use the bounding estimates described earlier, following the method in ([1], Chapter X.6). Suppose that $\mathcal{E}$ is an elliptic curve over $\mathbb{Q}$ with a rational point of order 2. We can translate $\mathcal{E}$ in the affine plane so that the point of order two is at $(0,0)$, then we may give a Weierstrass equation for $\mathcal{E}$ as $y^2 = x^3 + ax^2 + bx$. We then define an isogeny on $\mathcal{E}$ by

$$\psi(x,y) = \left(\frac{y^2}{x^2}, -\frac{y(x^2-b)}{x^2}\right).$$

This isogeny sends $\mathcal{E}$ to the elliptic curve $\mathcal{E}'$ defined by the equation $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. It follows that $\ker\psi = \{(0,0), O\} \cong \mathbb{Z}/2\mathbb{Z}$. The duplication formula over $\mathcal{E}$ is

$$2 * (x,y) = \left(\left(\frac{x^2-b}{2y}\right)^2, \frac{(x^2-b)(y^4+4bx^4)}{8x^2y^3}\right),$$

hence the corresponding dual isogeny is given by

$$\hat{\psi}(x,y) = \left(\frac{y^2}{4x^2}, \frac{y(a^2-4b-x^2)}{8x^2}\right),$$

with $\ker\hat{\psi} = \{(0,0), O\} \cong \mathbb{Z}/2\mathbb{Z}$.

A Bound on the Rank of some Elliptic Curves. We now restrict to the case where $a = 0$ and b is an integer. To apply the relation on $\dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}/2\mathcal{E}$ mentioned in section 1, we must determine $\psi(\ker\,[2]_{\mathcal{E}})$. Note that $\ker\psi \subseteq \ker\psi \circ \hat{\psi} = \ker\,[2]_{\mathcal{E}}$, hence

$$\begin{aligned}\dim_{\mathbb{Z}/2\mathbb{Z}} \psi(\ker\,[2]_{\mathcal{E}}) &= \dim_{\mathbb{Z}/2\mathbb{Z}} \ker\,[2]_{\mathcal{E}} - \dim_{\mathbb{Z}/2\mathbb{Z}} \ker\psi \\ &= \dim_{\mathbb{Z}/2\mathbb{Z}} \ker\,[2]_{\mathcal{E}} - 1,\end{aligned} \tag{6}$$

The group $\mathcal{G}_{\mathcal{P}_{\mathcal{E}}}$ consists of all products of the prime numbers $p \mid 2b$ and -1 since the discriminant of $\mathcal{E}$ is $4b^2$. This then implies that $\dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{G}_{\mathcal{P}_{\mathcal{E}}} = \dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{G}_{\mathcal{P}_{\mathcal{E}'}} = \wp(2b) + 1$. (Note that for the considerations in the rest of this section, $\mathcal{P}_{\mathcal{E}} = \mathcal{P}_{\mathcal{E}'}$, so we will drop the subscript, $\mathcal{E}$ or $\mathcal{E}'$.) Then equation (5) implies that

$$\begin{aligned} rk\ \mathcal{E} &= \dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}/2\mathcal{E} - \ker\,[2]_{\mathcal{E}} \\ &= 2\wp(2b) + 1 - \left(\dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \jmath_{\psi} + \dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \jmath_{\hat{\psi}}\right) - \ker\hat{\psi} \\ &= 2\wp(2b) - \left(\dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \jmath_{\psi} + \dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \jmath_{\hat{\psi}}\right).\end{aligned} \tag{7}$$

Now we use the method described earlier to compute the $\bar{\mathcal{E}}$-torsor $\mathcal{C}_{\mathfrak{a}}$ associated to a given $\mathfrak{a} \in \mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2$. Since $\mathfrak{p} = (0,0)$, the addition-by-$\mathfrak{p}$ map is given by

$$\mathfrak{p} + (x,y) = \left(\frac{b}{x}, -\frac{by}{x^2}\right).$$

Then the functions $\tilde{z}_1 := \frac{x}{y}$ and $\tilde{z}_2 := \frac{x^2-b}{x}$ have the desired transformation properties (that is, if $\mathfrak{g}$ is the nontrivial automorphism in $\mathrm{Gal}\big(\mathbb{Q}(\sqrt{\mathfrak{a}})/\mathbb{Q}\big)$, under the group action described in Section 2, $\mathfrak{g}\tilde{z}_i = -\tilde{z}_i$). Next, we find the relation between the $z_i := \tilde{z}_i\sqrt{\mathfrak{a}}$ for $i = 1$ and 2. We have that $z_1^{-2} = \frac{x^2+b}{\mathfrak{a}x}$ and $z_2 = \frac{x^2-b}{x}\sqrt{\mathfrak{a}}$, hence

$\frac{\mathfrak{a}^2}{4b}\left[z_1^{-4} - \frac{z_2^2}{\mathfrak{a}^3}\right] = 1$. For any solution $(z_{1\star}, z_{2\star})$ to this equation, we may define $x \in \overline{\mathbb{Q}}$ such that $\mathfrak{a}z_{1\star}^{-2} = x + b/x$, we can then verify that $\sqrt{\mathfrak{a}}z_{2\star} = \pm(x - b/x)$, note that if $\mathfrak{a}^{-1/2}z_{2\star} = -(x - b/x)$, then we may define $\bar{x} := b/x$ so that $\mathfrak{a}^{-1/2}z_{2\star}^2 = \bar{x} - b/\bar{x}$, so we can find a unique point $(x, y) \in \mathcal{E}$ which maps to $(z_{1\star}, z_{2\star})$. Thus, the curve given by $\mathfrak{a}^2 z_1^{-4} = \frac{z_2^2}{\mathfrak{a}} + 4b$ is isomorphic to $\mathcal{E}$ (in particular, the inverse of this morphism is given by $(z_1, z_2) \mapsto \left(\frac{\mathfrak{a}}{2} z_1^{-2} + \frac{1}{2\sqrt{\mathfrak{a}}} z_2, \frac{\mathfrak{a}^{3/2}}{2} z_1^{-3} + \frac{z_2}{2z_1}\right)$.) To simplify the equation for $\mathcal{C}_\mathfrak{a}$, we make the change-of-variable $(Z_1, Z_2) := \left(z_1, \frac{z_1^2 z_2}{\mathfrak{a}}\right)$ – this is valid since it induces an isomorphism over $\mathbb{Q}$ – so that in terms of the new coordinates, the curve is given by the equation

$$\mathcal{C}_\mathfrak{a}: 4bZ_1^4 + \mathfrak{a}Z_2^2 = \mathfrak{a}^2.$$

Now the dimension of $\operatorname{im} \mathscr{j}_\psi$ is nonzero if there is some $\mathfrak{a} \in \mathcal{G}_\mathcal{P}$ for which the class of $\mathcal{C}_\mathfrak{a}$ is nontrivial in the Weil-Châtelet group, that is, $\mathcal{C}_\mathfrak{a}$ has no rational points. Similarly, the dimension of $\operatorname{im} \mathscr{j}_{\hat{\psi}}$ is nonzero if there is some $\mathfrak{a} \in \mathcal{G}_\mathcal{P}$ for which the curve given by (8), with $4b$ replaced by $-16b$, has no rational points, or equivalently, the curve given by (8), with $4b$ replaced by $-b$, has no rational points.

If $b < 0$, there are no rational solutions to $\mathcal{C}_\mathfrak{a}$ for all negative values of $\mathfrak{a}$. If $b > 0$, then the curve given by (8) with $4b$ replaced by $-b$ has no rational solutions for all negative values of $\mathfrak{a}$, so in all cases, $\dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \mathscr{j}_\psi + \dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \mathscr{j}_{\hat{\psi}} \geq 1$. The equality (7) thus implies the bound

$$rk\, \mathcal{E} \leq 2p(2b) - 1. \tag{9}$$

BOUNDS IN SPECIAL CASES. In this subsection, we consider two cases; the first in which the rank can be directly calculated, and the second in which we only find the sum of the rank and the Tate-Shafarevich group. The rank of $\mathcal{E}$ can be found by considering its associated set of torsors and looking at which of the equations have rational solutions. If it is directly possible to deduce this, the rank of $\mathcal{E}$ can be determined exactly. Otherwise we must solve the equations over the p-adic integers for all $p \in \mathcal{P}$ (using the methods in section 2), and instead determine the sum of the rank and the dimension of the Tate-Shafarevich group.

As an example, we consider the case $b = 4$; here it turns out that $rk\, \mathcal{E} = 0$ (the bound (9) states that $rk\, \mathcal{E} \leq 1$). By the argument above, it suffices to see that $\dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \mathscr{j}_\psi = 1$ and $\dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{im} \mathscr{j}_{\hat{\psi}} = 1$. For any $\mathfrak{a} \in \mathcal{G}_\mathcal{P}$, the corresponding $\bar{\mathcal{E}}$-torsor for ψ has the equation $w_1^4 + \mathfrak{a}w_2^2 = \mathfrak{a}^2$. If $\mathfrak{a} = 2$, then the equation becomes $w_1^4 + 2w_2^2 = 4$. This equation has solutions over $\mathbb{Q}$ if and only if there is a nontrivial solution over $\mathbb{Z}$ to $k^4 + 2l^2 = 4m^4$. This equation has no solutions over $\mathbb{Z}$ (and in fact $\mathbb{Z}_2$) by a descent argument – any solution (k, l, m) must have $2 \mid k$, $4 \mid l$, and $2 \mid m$ – this reduces any solution (k, l, m) to the smaller solution $\left(\frac{k}{2}, \frac{l}{4}, \frac{m}{2}\right)$. If $\mathfrak{a} = -1$, then $(w_1, w_2) = (1,0)$ is a solution. Next consider the $\bar{\mathcal{E}}$-torsor for $\hat{\psi}$ associated to some $\mathfrak{a} \in \mathcal{G}_\mathcal{P}$, its equation is $\mathfrak{a}Z_2^2 = 4Z_1^4 + \mathfrak{a}^2$. Our earlier argument shows that for all negative $\mathfrak{a}$, this equation has no solutions over $\mathbb{Q}$. If $\mathfrak{a} = 2$, then $(Z_1, Z_2) = (1,2)$ is a rational solution. Thus, there are no solutions in this case exactly when $\mathfrak{a}$ is negative, as desired.

We now outline the case where b is an odd prime; the proof is in ([11], Chapter X.6). Here the group $\mathcal{G}_\mathcal{P} = \{\mathfrak{a} \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 : \mathfrak{a} \mid 2b\}$ and the $\bar{\mathcal{E}}$-torsor $\mathcal{C}_\mathfrak{a}$ associated to any $\mathfrak{a} \in \mathcal{G}_\mathcal{P}$ is defined by $4bZ_1^4 + \mathfrak{a}Z_2^2 = \mathfrak{a}^2$. To determine the Selmer group of $\mathcal{E}$ we use casework on $\mathfrak{a}$, we illustrate here the case where $\mathfrak{a} = -2$.

The corresponding equation in this case is $2bZ_1^4 - Z_2^2 = 2$; since $\mathcal{P} = \{2, b\}$, we need to determine if it has solutions in $\mathbb{Q}_2$ and $\mathbb{Q}_b$. By quadratic reciprocity, -2 is a quadratic residue modulo b if and only if $b \equiv 1$ or $3 \pmod 8$. By Hensel's Lemma, it suffices to find solutions modulo 32 and b (since $(2x+1)^4 \equiv 1$ or $17 \pmod{32}$). When taken modulo b, the equation becomes $Z_2^2 = -2$, so that there is a solution in $\mathbb{Q}_b$ if and only if $b \equiv 1$ or $3 \pmod 8$. For the $\mathbb{Q}_2$ case, we determine for which $b \equiv 1$ or $3 \pmod 8$ satisfy the congruence mod 32. We can use casework on $b \pmod{32}$ to see that $b \equiv 1, 3,$ or $9 \pmod{16}$. Thus $-2 \in S^\psi(\mathcal{E})$ if and only if $b \equiv 1, 3,$ or $9 \pmod{16}$.

Using this method, if for example $b \equiv 1 \pmod 8$, we can compute the Selmer group of $\mathcal{E}$ and $\mathcal{E}'$ to be

$$S^{\psi}(\mathcal{E}) = \mathcal{G}_{\mathcal{P}} = \{\pm 1, \pm 2, \pm b\},\ \ S^{\hat{\psi}}(\mathcal{E}') = \{1, b\}.$$

Since $\mathfrak{p} = (0,0)$ is not in the image of $\hat{\psi}$, $\dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}/\hat{\psi}\mathcal{E}' > 0$. But by (3), $\dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}/\hat{\psi}\mathcal{E}' \leq \dim_{\mathbb{Z}/2\mathbb{Z}} S^{\hat{\psi}}(\mathcal{E}') = 1$, hence $\dim_{\mathbb{Z}/2\mathbb{Z}} \operatorname{coker} \psi_{\star}^{\text{ind}} \leq \dim_{\mathbb{Z}/2\mathbb{Z}} Ш(\mathcal{E}) \cap \ker \hat{\psi}_{\star} = \dim_{\mathbb{Z}/2\mathbb{Z}} S^{\hat{\psi}}(\mathcal{E}) - \dim_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}/\hat{\psi}\mathcal{E}' = 0$ in (4). Thus, equations (4) and (6) imply that

$$rk\ \mathcal{E} + \dim_{\mathbb{Z}/2\mathbb{Z}} Ш(\mathcal{E}) \cap \ker\, [2]_{\mathcal{E}\star} = 2.$$

5. Another result

In this section, we note another interesting result in the subject.
Although it is currently not known if the set of ranks of all elliptic curves is bounded, there is a result that shows that the average rank of elliptic curves is bounded (the proof uses a sieve called the square-free sieve). It states [5], [6] that the average size of the 2-Selmer group $S^{[2]}$ is 3, the average size of the 5-Selmer group $S^{[5]}$ is 6, and hence that the average rank of an elliptic curve is less than 1.

References

[1] J. H. Silverman, *Arithmetic of Elliptic Curves*, Springer-Verlag GTM 106, 2009
[2] J. W. S. Cassels, *Arithmetic on curves of genus 1: IV. A proof of the Hauptvermutung*, J. Reine Angew. Math v.211 (1962), pp. 95-112
[3] K. Rubin, *Tate-Shafarevich groups of Elliptic Curves with Complex Multiplication,* Algebraic Number Theory – in honor of K. Iwasawa, Mathematical Society of Japan (1989), pp. 409-419
[4] C. Delaunay, *Heuristics on class groups and on Tate-Shafarevich groups: The magic of the Cohen-Lenstra Heuristics,* Ranks of elliptic curves and random matrix theory, London Math Society Lecture Note Series, Cambridge University Press, v. 341 (2007), pp. 323-340
[5] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Mathematics v. 181, no. 1 (2015), pp. 191-242 arxiv: 1006.1002
[6] M. Bhargava and A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1.* arxiv: 1312.7859
[7] B. Mazur (and D. Goldfeld), *Rational isogenies of prime degree,* Inventiones mathematicae v. 44, no. 2 (1978), pp. 129-162