Math. Res. Lett. **19** (2012), *no.* 05, 1137–1143

ELLIPTIC CURVES WITH A LOWER BOUND ON 2-SELMER RANKS OF QUADRATIC TWISTS

Zev Klagsbrun

Abstract. For any number field K with a complex place, we present an infinite family of elliptic curves defined over K such that $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E^F/K) \geq \dim_{\mathbb{F}_2} E^F(K)[2] + r_2$ for every quadratic twist E^F of every curve E in this family, where r_2 is the number of complex places of K. This provides a counterexample to a conjecture appearing in work of Mazur and Rubin.

1. Introduction

1.1. Distributions of Selmer ranks. Let E be an elliptic curve defined over a number field K and let $\mathrm{Sel}_2(E/K)$ be its 2-Selmer group (see Section 2 for its definition). The **2-Selmer rank** of E, denoted $d_2(E/K)$, is defined as

$$d_2(E/K) = \dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/K) - \dim_{\mathbb{F}_2} E(K)[2].$$

For a given elliptic curve and positive integer r, we are able to ask whether E has a quadratic twist with 2-Selmer rank equal to r. A single restriction on which r can appear as a 2-Selmer rank within the quadratic twist family of a given curve E is previously known. Using root numbers, Dokchitser and Dokchitser identified a phenomenon called **constant 2-Selmer parity** where $d_2(E^F/K) \equiv d_2(E/K) \pmod 2$ for every quadratic twist E^F of E and showed that E has constant 2-Selmer parity if and only if K is totally imaginary and E acquires everywhere good reduction over an abelian extension of K [2].

In this paper, we show the existence of an additional obstruction to small r appearing as 2-Selmer ranks within the quadratic twist family of E. We prove that there are curves having this obstruction over any number field K with a complex place. Specifically:

Theorem 1. *For any number field K, there exist infinitely many elliptic curves E defined over K such that $d_2(E^F/K) \geq r_2$ for every quadratic F/K. Moreover, these curves do not have constant 2-Selmer parity and none of them become isomorphic over $\overline{K}$.*

This result disproves a conjecture appearing in [7], which predicted that subject only to the restriction of constant 2-Selmer parity, the set of twists of E having 2-Selmer rank r has positive density within the set of all twists of E for every $r \geq 0$.

Received by the editors January 27, 2012.

We prove Theorem 1 by presenting a family of elliptic curves defined over $\mathbb{Q}$ for which each curve in the family has the appropriate property when viewed over K. For $n \in \mathbb{N}$, let $E_{(n)}$ be the elliptic curve defined by the equation

$$E_{(n)} : y^2 + xy = x^3 - 128n^2x^2 - 48n^2x - 4n^2 \tag{1.1}$$

and define $\mathcal{F}$ as $\mathcal{F} = \{E_{(n)} : n \in \mathbb{N}, 1 + 256n^2 \notin (K^\times)^2\}$. Each curve $E \in \mathcal{F}$ has a single point of order 2 in $E(K)$ and a cyclic 4-isogeny defined over $K(E[2])$ but not K. Let $\phi : E \to E'$ be the isogeny whose kernel is $C = E(K)[2]$. Our results are obtained by using local calculations combined with a Tamagawa ratio of Cassels to establish a lower bound on the rank of the Selmer group associated to ϕ (to be defined in Section 2).

Although curves $E \in \mathcal{F}$ have the property that $d_2(E^F/K) \geq r_2$ for every quadratic F/K, this does not hold in general for curves E with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that have a cyclic 4-isogeny defined over $K(E[2])$ but not over K. In particular, the forthcoming work of this author can be used to show that every $r \geq 0$ appears infinitely often as a 2-Selmer rank within the quadratic twist family of E' for every $E \in \mathcal{F}$ [4].

2. Selmer groups

We begin by briefly recalling the constructions of the 2-Selmer and ϕ-Selmer groups along with some of the standard descent machinery. A more detailed explanation can by found in Section X.4 of [8].

If E is an elliptic curve defined over a field K, then the Kummer map $\delta_{[2]}$ maps $E(K)/2(K)$ into $H^1(K, E[2])$. If K is a number field, then for each place v of K we define a distinguished local subgroup $H^1_f(K_v, E[2]) \subset H^1(K_v, E[2])$ by

$$\text{Image}\left(\delta_{[2]} : E(K_v)/2E(K_v) \hookrightarrow H^1(K_v, E[2])\right).$$

We define the **2-Selmer group** of E, denoted $\mathrm{Sel}_2(E/K)$, by

$$\mathrm{Sel}_2(E/K) = \ker\left(H^1(K, E[2]) \xrightarrow{\sum res_v} \bigoplus_{v \text{ of } K} H^1(K_v, E[2])/H^1_f(K_v, E[2])\right).$$

If E^F is the quadratic twist of E by F/K where F is given by $F = K(\sqrt{d})$, then there is an isomorphism $E \to E^F$ given by $(x, y) \mapsto (dx, d^{3/2}y)$ defined over F. Restricted to $E[2]$, this map gives a canonical G_K isomorphism $E[2] \to E^F[2]$, allowing us to view $H^1_f(K_v, E^F[2])$ as sitting inside $H^1(K_v, E[2])$. The following lemma due to Kramer describes the connection between $H^1_f(K_v E[2])$ and $H^1_f(K_v, E^F[2])$.

Given a place w of F above a place v of K, we get a norm map $E(F_w) \to E(K_v)$, the image of which we denote by $E_{\mathbf{N}}(K_v)$.

Lemma 2.1. *Viewing $H^1_f(K_v, E^F[2])$ as sitting inside $H^1(K_v, E[2])$, we have*

$$H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2]) \simeq E_{\mathbf{N}}(K_v)/2E(K_v)$$

Proof. This is Proposition 7 in [5] and Proposition 5.2 in [6]. The proof in [6] works even at places above 2 and ∞. □

If $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then there is an isogeny $\phi : E \to E'$ with kernel $C = E(K)[2]$ that gives rise to a ϕ-Selmer group, $\mathrm{Sel}_\phi(E/K)$. There is a connecting map arising from Galois cohomology, $\delta_\phi : E'(K)/\phi(E(K)) \to H^1(K, C)$, taking the coset of

$Q \in E'(K)$ to the coset defined by the cocycle $c(\sigma) = \sigma(R) - R$ where R is any point on $E(\overline{K})$ with $\phi(R) = Q$. Identifying C with μ_2, we can view $H^1(K, C)$ as $K^\times/(K^\times)^2$ and under this identification, $\delta_\phi(C) = \langle \Delta_E \rangle$, where Δ_E is the discriminant of (any model of) E. The map δ_ϕ can be defined locally as well and for each place v of K, we define a distinguished local subgroup $H^1_\phi(K_v, C) \subset H^1(K_v, C)$ as the image of $E'(K_v)/\phi(E(K_v))$ under δ_ϕ. We define the **ϕ-Selmer group of E**, denoted $\mathrm{Sel}_\phi(E/K)$, as

$$\mathrm{Sel}_\phi(E/K) = \ker\left(H^1(K, C) \xrightarrow{\sum res_v} \bigoplus_{v \text{ of } K} H^1(K_v, C)/H^1_\phi(K_v, C) \right).$$

The isogeny ϕ on E gives gives rise to a dual isogeny $\hat{\phi}$ on E' whose kernel is $C' = \phi(E[2])$. Exchanging the roles of (E, C, ϕ) and $(E', C', \hat{\phi})$ in the above defines the **$\hat{\phi}$-Selmer group**, $\mathrm{Sel}_{\hat{\phi}}(E'/K)$, as a subgroup of $H^1(K, C')$. The local conditions $H^1_\phi(K_v, C)$ and $H^1_{\hat{\phi}}(K, C')$ are connected via the following exact sequence.

Proposition 2.2. *The sequence*

$$0 \to C'/\phi(E(K_v)[2]) \xrightarrow{\delta_\phi} H^1_\phi(K_v, C) \xrightarrow{i} H^1_f(K_v, E[2]) \xrightarrow{\phi} H^1_{\hat{\phi}}(K_v, C') \to 0 \tag{2.1}$$

is exact.

Proof. This well-known result follows from the sequence of kernels and cokernels arising from the composition $\hat{\phi} \circ \phi = [2]_E$. See Remark X.4.7 in [8] for example. □

The following two theorems allow us to compare the ϕ-Selmer group, the $\hat{\phi}$-Selmer group and the 2-Selmer group.

Theorem 2.3. *The ϕ-Selmer group, the $\hat{\phi}$-Selmer group, and the 2-Selmer group sit inside the exact sequence*

$$0 \to E'(K)[2]/\phi(E(K)[2]) \xrightarrow{\delta_\phi} \mathrm{Sel}_\phi(E/K) \to \mathrm{Sel}_2(E/K) \xrightarrow{\phi} \mathrm{Sel}_{\hat{\phi}}(E'/K). \tag{2.2}$$

Proof. This is a diagram chase based on the exactness of (2.1). See Lemma 2 in [3] for example. □

Theorem 2.4 (Cassels)**.** *The **Tamagawa ratio**, defined as* $\mathcal{T}(E/E') = \frac{\left|\mathrm{Sel}_\phi(E/K)\right|}{\left|\mathrm{Sel}_{\hat{\phi}}(E'/K)\right|}$, *is given by a local product formula*

$$\mathcal{T}(E/E') = \prod_{v \, of \, K} \frac{\left|H^1_\phi(K_v, C)\right|}{2}.$$

Proof. This is a combination of Theorem 1.1 and equations (1.22) and (3.4) in [1]. This product converges since $H^1_\phi(K_v, C)$ equals the unramified local subgroup $H^1_u(K_v, C)$ for all $v \nmid 2\Delta_E\infty$. □

3. Local conditions for curves in $\mathcal{F}$

The goal of this section is to prove the following proposition.

Proposition 3.1. *Let $E = E_{(n)} \in \mathcal{F}$. Then* $\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^F) \geq H^1(K_v, C) - 1$ *for every place v of K, where $C^F = E^F(K)[2]$.*

Let $E = E_{(n)} \in \mathcal{F}$. The point $P = (-\frac{1}{4}, \frac{1}{8})$ on E has order 2 and $E' = E/\langle P \rangle$ can be given by a model $y^2+xy = x^3+64n^2x^2+4n^2(1+256n^2)x$. The discriminants of the model (1.1) for E and this model for E' are given by $\Delta_E = 4n^2(1+256n^2)^3$ and by $\Delta_{E'} = 16n^4(1+256n^2)^3$, respectively. As $1+256n^2 \notin (K^\times)^2$, we have $E(K)[2] = \langle P \rangle$. Since Δ_E and $\Delta_{E'}$ differ by a square, we get that $K(E[2]) = K(E'[2])$ and it follows that $\dim_{\mathbb{F}_2} E(K_v)[2] = \dim_{\mathbb{F}_2} E'(K_v)[2]$ for every place v of K. Proposition 3.1 will follow from some results applicable to all curves that have $K(E[2]) = K(E'[2])$ and some results that are specific to curves in $\mathcal{F}$.

Remark 3.2. Forthcoming work of this author shows if $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then E does not have a cyclic 4-isogeny defined over K but acquires one over $K(E[2])$ if and only if $K(E[2]) = K(E'[2])$. See Section 4 of [4] for more details.

Lemma 3.3. *Let E be an elliptic curve with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and suppose further that $K(E[2]) = K(E'[2])$. If E has additive reduction at a place $v \nmid 2$, then* $\dim_{\mathbb{F}_2} H^1_\phi(K_v, C) = 1$.

Proof. Let $E_0(K_v)$ be the group of points on $E(K_v)$ with non-singular reduction, $E_1(Kv)$ the subgroup of points with trivial reduction, and $\mathbb{F}_v$ the residue field of K_v. The formal group structure on $E_1(K_v)$ shows that $E_1(K_v)$ is uniquely divisible by 2 and since $E_0(K_v)/E_1(K_v) \simeq \mathbb{F}_v^+$, $E_0(K_v)$ is uniquely 2-divisible as well. Since $E(K_v)$ has a point of order 2, Tate's algorithm then shows that $E(K_v)/E_0(K_v)$ – and therefore $E(K_v)[2^\infty]$ – either injects to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or is cyclic of order 4.

Therefore, if $E(K_v)$ has a point R of order 4, then $2R \in C$. It follows that $\phi(R) \in E'(K_v)[2] - C'$ and $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This contradicts the fact that $\dim_{\mathbb{F}_2} E(K_v)[2] = \dim_{\mathbb{F}_2} E'(K_v)[2]$ since the 2-part of $E(K_v)$ is cyclic. This shows that $E(K_v)$ cannot have any points of order 4 and similar logic shows that the same is true for $E'(K_v)$. It then follows that $\dim_{\mathbb{F}_2} E'(K_v)/\phi(E(K_v)) = 1$ since $\dim_{\mathbb{F}_2} E(K_v)[2] = \dim_{\mathbb{F}_2} E'(K_v)[2]$ and ϕ has degree 2. □

Lemma 3.4. *Let E be an elliptic curve with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and suppose that $K(E[2]) = K(E'[2])$. If E has split multiplicative reduction at a place v where the Kodaira symbols of E and E' are I_n and I_{2n}, respectively, then $H^1_\phi(K_v, C) = H^1(K_v, C)$. Further, if F/K is a quadratic extension in which v does not split, then $\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^F) = \dim_{\mathbb{F}_2} H^1(K_v, C) - 1$ and $H^1_\phi(K_v, C^F) = N_{F_w/K_v} F_w^\times/(K_v^\times)^2$, where w is the place of F above v.*

Proof. Since E and E' have split multiplicative reduction at v, E/K_v and E'/K_v are G_{K_v} isomorphic to Tate curves E_q and $E_{q'}$, respectively. By the condition on the Kodaira symbols, $|q|_v^2 = |q'|_v$. Observe that E_q can be two-isogenous to three different curves: $E_{q^2}, E_{\sqrt{q}}$, and $E_{-\sqrt{q}}$. The curve $E_{q'}$ must therefore be one of these possibilities and the only possibility with $|q|_v^2 = |q'|_v$ is $q' = q^2$. We therefore get G_{K_v}

isomorphisms $\overline{K_v}^\times/q^{\mathbb{Z}} \to E(\overline{K_v})$ and $\overline{K_v}^\times/q^{2\mathbb{Z}} \to E'(\overline{K_v})$ such that the following diagram commutes.

$$\begin{array}{ccccc} \overline{K_v}^\times/q^{\mathbb{Z}} & \xrightarrow{x\mapsto x^2} & \overline{K_v}^\times/q^{2\mathbb{Z}} & \xrightarrow{x\mapsto x} & \overline{K_v}^\times/q^{\mathbb{Z}} \\ \downarrow & & \downarrow & & \downarrow \\ E(\overline{K_v}) & \xrightarrow{\phi} & E'(\overline{K_v}) & \xrightarrow{\hat{\phi}} & E(\overline{K_v}) \end{array}$$

Since the maps in this diagram are G_{K_v} equivariant, we can restrict to K_v giving the following diagram, where the vertical arrows are isomorphisms.

$$\begin{array}{ccccc} {K_v}^\times/q^{\mathbb{Z}} & \xrightarrow{x\mapsto x^2} & {K_v}^\times/q^{2\mathbb{Z}} & \xrightarrow{x\mapsto x} & {K_v}^\times/q^{\mathbb{Z}} \\ \downarrow & & \downarrow & & \downarrow \\ E(K_v) & \xrightarrow{\phi} & E'(K_v) & \xrightarrow{\hat{\phi}} & E(K_v) \end{array}$$

We therefore get a sequence of G_K-isomorphisms

$$H^1_\phi(K_v, C) \simeq E'(K_v)/\phi(E(K_v)) \simeq ({K_v}^\times/q^{2\mathbb{Z}})/({K_v}^\times/q^{\mathbb{Z}})^2 \simeq K_v^\times/(K_v^\times)^2 \simeq H^1(K_v, C)$$

and that $H^1_{\hat{\phi}}(K_v, C') = 0$ proving the first part of the lemma.

Further, by the exactness of (2.1), the map $i : H^1(K_v, C) \to H^1_f(K_v, E[2])$ is surjective. Because $E'(K_v) \simeq {K_v}^\times/q^{2\mathbb{Z}}$, we see that $E'(K_v)[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $K(E[2]) = K(E'[2])$, we then see that $E(K_v)[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as well. The exactness of (2.1) then shows that i is injective. We therefore get that the restriction $\tilde{i} : H^1_\phi(K_v, C^F) \to H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2])$ is also injective.

Let $c \in H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2])$. As $H^1_\phi(K_v, C) = 0$, c maps trivially into $H^1_{\hat{\phi}}(K_v, C'^F)$ under the map ϕ in (2.1). It follows from Proposition 2.2 that c is in the image of $H^1_\phi(K_v, C^F)$ and that $\tilde{i} : H^1_\phi(K_v, C^F) \to H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2])$ is surjective. Therefore $\tilde{i}$ is an isomorphism.

By Lemma 2.1, $H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2]) = N_{F_w/K_v}E(F_w)/2E(K_v)$. The elliptic curve norm map $N_{F_w/K_v} : E(F_w) \to E(K_v)$ translates into the usual field norm $N_{F_w/K_v} : F_w^\times/q^{\mathbb{Z}} \to K_v^\times/q^{2\mathbb{Z}}$, so $H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2])$ can be identified with

$$\left(N_{F_w/K_v}F_w^\times/q^{2Z}\right) / \left(K_v^\times/q^{\mathbb{Z}}\right)^2 \simeq N_{F_w/K_v}F_w^\times/(K_v^\times)^2.$$

The isomorphism $E'^F(K_v)/\phi(E^F(K_v)) \to E(K_v)/2E(K_v) \cap E^F(K_v)/2E^F(K_v)$ is given by $\hat{\phi}$. As $\hat{\phi}$ is given by $x \mapsto x$ in the above diagram, the identification of $H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2])$ with $N_{F_w/K_v}F_w^\times/(K_v^\times)^2$ identifies $H^1_\phi(K_v, C^F)$ with $N_{F_w/K_v}F_w^\times/(K_v^\times)^2$. Standard results from the theory of local fields then give that $\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^F) = \dim_{\mathbb{F}_2} H^1(K_v, C) - 1$. □

Lemma 3.5. *If $E = E_{(n)} \in \mathcal{F}$, then E has multiplicative reduction at primes $\mathfrak{p} \mid 2n$. Further, if $k = \mathrm{ord}_{\mathfrak{p}} 2n$, then E has Kodaira symbol I_{2k} at $\mathfrak{p}$ and E' has Kodaira symbol I_{4k} at $\mathfrak{p}$.*

Proof. If $\mathfrak{p} \mid 2n$, then the model (1.1) is minimal at $\mathfrak{p}$. The reduction of (1.1) mod $\mathfrak{p}$ has a node so E has multiplicative reduction at $\mathfrak{p}$. We can then read the Kodaira symbols for E and E' at $\mathfrak{p}$ off of the denominators of their j-invariants, which are $j(E) = \frac{(1+1024n^2)^3}{4n^2}$ and $j(E') = \frac{(1+64n^2)^3}{16n^4}$ respectively. $\square$

Proof of Proposition 3.1. Lemma 3.5 combined with Lemma 3.4 show that the proposition is true for all places $v \mid 2n$. The j-invariant of E shows that these are the only places where E^F can have multiplicative reduction and the result then follows from Proposition 3.3. $\square$

4. Proof of main theorem

We begin by relating $d_2(E/K)$ to the 2-adic valuation of $\mathcal{T}(E/E')$.

Proposition 4.1. *If $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $K(E[2]) = K(E'[2])$, then*

$$d_2(E/K) \geq \mathrm{ord}_2 \mathcal{T}(E/E').$$

Proof. From the definition, we have

$$\mathrm{ord}_2 \mathcal{T}(E/E') = \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E/K) - \dim_{\mathbb{F}_2} \mathrm{Sel}_{\hat{\phi}}(E'/K). \tag{4.1}$$

Since $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $K(E[2]) = K(E'[2])$, we get that $E'(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ as well. It then follows from Theorem 2.3 that $\dim_{\mathbb{F}_2} \mathrm{Sel}_{\hat{\phi}}(E'/K) \geq 1$ and that the map of $\mathrm{Sel}_\phi(E/K)$ into $\mathrm{Sel}_2(E/K)$ is 2-to-1. Combined with (4.1), we get that the image of $\mathrm{Sel}_\phi(E/K)$ in $\mathrm{Sel}_2(E/K)$ has $\mathbb{F}_2$-dimension at least $\mathrm{ord}_2 \mathcal{T}(E/E')$.

Let P generate $E(K)[2]$ and let $c \in \mathrm{Sel}_2(E/K)$ be the image of P in $\mathrm{Sel}_2(E/K)$. We can represent c by a cocycle $\hat{c} : G_K \to E[2]$ given by $\hat{c}(\gamma) = \gamma(R) - R$ for some $R \in E(\overline{K})[4]$ with $2R = P$. Observe that since $2R = P$, it must be that $\phi(R) \in E'[2] - C'$. If $\sigma(R) - R \in C$ for every $\sigma \in G_K$, then $\phi(R) \in E'(K)$ since $\phi(C) = 0$ and $\phi(\sigma(R) - R) = \sigma(\phi(R)) - R$ for $\sigma \in G_K$. Since this would contradict $E'(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, it must be that $\sigma(R) - R \notin C$ for some $\sigma \in G_K$ and c therefore does not come from $H^1(K, C)$. We therefore get that $d_2(E/K) \geq \mathrm{ord}_2 \mathcal{T}(E/E')$. $\square$

Theorem 1 now follows easily from Proposition 3.1.

Proof of Theorem 1. Let $E = E_{(n)} \in \mathcal{F}$ and F/K quadratic.

By Lemma 2.4, $\mathrm{ord}_2 \mathcal{T}(E^F/E'^F)$ is given by

$$\mathrm{ord}_2 \mathcal{T}(E^F/E'^F) = \sum_{v \text{ of } K} \left(\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^F) - 1 \right).$$

By Proposition 3.1, we get that $\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^F) - 1 \geq 0$ for all places $v \nmid 2\infty$. This yields

$$\begin{aligned} \mathrm{ord}_2 \mathcal{T}(E^F/E'^F) &\geq -(r_1 + r_2) + \sum_{v \mid 2} \left(\dim_{\mathbb{F}_2} H^1_\phi(K_v, C^F) - 1 \right) \\ &\geq -(r_1 + r_2) + \sum_{v \mid 2} \left(\dim_{\mathbb{F}_2} H^1(K_v, C) - 2 \right), \end{aligned}$$

with the second inequality following from Proposition 3.1 as well.

As $H^1(K_v, C) \simeq K_v^\times/(K_v^\times)^2$, we get that $\dim_{\mathbb{F}_2} H^1(K_v, C) = 2 + [K_v : \mathbb{Q}_2]$ for places $v \mid 2$. We therefore have

$$\mathrm{ord}_2 \mathcal{T}(E^F/E'^F) \geq -(r_1 + r_2) + \sum_{v|2} [K_v : \mathbb{Q}_2] = -(r_1 + r_2) + [K : \mathbb{Q}] = r_2.$$

Proposition 4.1 then shows that $d_2(E^F/K) \geq r_2$.

The family $\mathcal{F}$ is infinite since every number field K has infinitely many n with $1 + 256n^2 \notin (K^\times)^2$. The curves E_n have distinct j-invariants and therefore are not isomorphic over $\overline{K}$. Since all of the E_n have multiplicative reduction at all places above 2, work of Mazur and Rubin in [7] shows that none of them have constant 2-Selmer parity. □

Acknowledgments

This paper is based on work conducted by the author as part of his doctoral thesis at UC-Irvine under the direction of Karl Rubin and was supported in part by the NSF grants DMS-0457481 and DMS-0757807. I would like to express my utmost gratitude to Karl Rubin for the guidance and assistance he provided while undertaking this research. I would also like to thank the reviewer for making many helpful suggestions, in particular suggesting the model (1.1) for $E_{(n)}$.

References

[1] J. Cassels, *Arithmetic on curves of genus 1. VIII: on the conjectures of Birch and Swinnerton-Dyer*, Journal für die reine und angewandte Mathematik (Crelles Journal), **1965**(217) (1965), 180–199.

[2] T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, Journal für die reine und angewandte Mathematik (Crelles Journal), **658** (2011), 39–64.

[3] E. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43**(4) (2008), 293–303.

[4] Z. Klagsbrun, *Selmer ranks of quadratic twists of elliptic curves with partial rational two-torsion*, Preprint available at `http://arxiv.org/abs/1201.5408` (2011).

[5] K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264**(1) (1981), 121–135.

[6] B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Annal. Math. **166** (2007), 579–612.

[7] ———, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Inventiones mathematicae **181**(3) (2010), 541–575.

[8] J. Silverman, *The arithmetic of elliptic curves*, Vol. 106 (Springer-Verlag, 2009).

Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Drive, Madison, WI 53706, USA

E-mail address: `klagsbru@math.wisc.edu`