TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 369, Number 5, May 2017, Pages 3355–3385
http://dx.doi.org/10.1090/tran/6744
Article electronically published on October 12, 2016

SELMER RANKS OF QUADRATIC TWISTS OF ELLIPTIC CURVES WITH PARTIAL RATIONAL TWO-TORSION

ZEV KLAGSBRUN

Abstract. This paper investigates which integers can appear as 2-Selmer ranks within the quadratic twist family of an elliptic curve E defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$. We show that if E does not have a cyclic 4-isogeny defined over $K(E[2])$ with kernel containing $E(K)[2]$, then subject only to constant 2-Selmer parity, each non-negative integer appears infinitely often as the 2-Selmer rank of a quadratic twist of E. If E has a cyclic 4-isogeny with kernel containing $E(K)[2]$ defined over $K(E[2])$ but not over K, then we prove the same result for 2-Selmer ranks greater than or equal to r_2, the number of complex places of K. We also obtain results about the minimum number of twists of E with rank 0 and, subject to standard conjectures, the number of twists with rank 1, provided E does not have a cyclic 4-isogeny defined over K.

1. Introduction

This paper investigates the integers occurring as 2-Selmer ranks within the quadratic twist family of a given elliptic curve E defined over a number field K. Letting $\mathrm{Sel}_2(E/K)$ denote the 2-Selmer group of E (see Section 2 for the definition), we define the 2-Selmer rank of E/K, denoted $d_2(E/K)$, by

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

Definition 1.1. For $X \in \mathbb{R}^+$, define a set

$$S(X) = \{\text{Quadratic } F/K : \mathbf{N}_{K/\mathbb{Q}}\mathfrak{f}(F/K) < X\}$$

where $\mathfrak{f}(F/K)$ is the finite part of the conductor of F/K. For each $r \in \mathbb{Z}^{\geq 0}$ define a quantity $N_r(E, X)$ by

$$N_r(E, X) = \big|\{F/K \in S(X) : d_2(E^F/K) = r\}\big|,$$

where E^F is the quadratic twist of E by F/K.

The 2-Selmer rank of E serves as an upper bound for the Mordell-Weil rank of E, so understanding its distribution within quadratic twist families yields information about the rank distribution within the twist family (see Corollaries 1.8 and 1.9, for example). We are therefore concerned with the limiting behavior of $\frac{N_r(E,X)}{|S(X)|}$

Received by the editors August 9, 2012 and, in revised form, May 7, 2014, March 1, 2015, and May 5, 2015.

2010 *Mathematics Subject Classification.* Primary 11G05.

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 NSF grants DMS-0457481 and DMS-0757807.

as $X \to \infty$. Recent work by Kane, building on work of Swinnerton-Dyer and Heath-Brown showed that if E is defined over $\mathbb{Q}$, $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and E does not have a cyclic 4-isogeny defined over $\mathbb{Q}$, then $\frac{N_r(E,X)}{|S(X)|}$ tends to an explicit non-zero limit α_r for every non-negative integer r such that the sum of the α_r over $r \in Z^{\geq 0}$ is equal to 1 [8], [17], [7]. Additional recent work by the author, Mazur and Rubin proves that if $\mathrm{Gal}(K(E[2])/K) \simeq \mathcal{S}_3$, then a similar result holds using a different method of counting after correcting by some local factors arising over totally complex fields [11].

Far less is known about the behavior $\frac{N_r(E,X)}{|S(X)|}$ for curves with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, and this paper provides a partial answer. One obstacle to obtaining results for these curves is the presence of a cyclic 4-isogeny, either over K – in which case we have been unable to say anything – or over the two-division field $K(E[2])$. If E has a cyclic 4-isogeny ψ defined over $K(E[2])$ that is not defined over K, then ψ proves to be an obstacle only when $E(K)[2] \subset \ker(\psi)$. Our first theorem assumes that E does not have such an isogeny, and the theorems which follow it give similar results for curves which do have such an isogeny ψ. A simple criterion for determining if E has either of these two problematic isogeny types appears in Section 4.

Theorem 1.2. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over $K(E[2])$ with kernel containing $E(K)[2]$. Then, for all non-negative $r \equiv d_2(E/K) \pmod 2$, we have $N_r(E,X) \gg \frac{X}{\log X}$. If E does not have constant 2-Selmer parity, then $N_r(E,X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$.*

This result is similar to Theorem 1.4 in [13] concerning curves with $E(K)[2] = 0$.

Constant 2-Selmer parity is a phenomenon exhibited by certain curves E, where $d_2(E^F/K) \equiv d_2(E/K) \pmod 2$ for all quadratic twists E^F of E. Dokchitser and Dokchitser have shown that E/K 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 (Remark 4.9 in [4]).

Constant 2-Selmer parity is one of two known obstructions to a non-negative integer r appearing as the 2-Selmer rank of some twist of E. A second "lower-bound" obstruction can occur when E has a cyclic 4-isogeny ψ defined over $K(E[2])$ with $E(K)[2] \subset \ker \psi$. The author recently exhibited an infinite family of curves over any number field K with a complex place such that $d_2(E^F/K) \geq r_2$ for every curve E in this family and every quadratic F/K, where r_2 is the number of complex places of K [9]. As the next theorem shows, these curves exhibit the worst possible behavior among all curves without a cyclic 4-isogeny defined over K.

Theorem 1.3. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny defined over K. Then $N_r(E,X) \gg \frac{X}{\log X}$ for all $r \geq r_2$ with $r \equiv d_2(E/K) \pmod 2$, where r_2 is the number of conjugate pairs of complex embeddings of K. If E does not have constant 2-Selmer parity, then $N_r(E,X) \gg \frac{X}{\log X}$ for all $r \geq r_2$.*

The lower-bound obstruction prevents us from making broad statements about the quadratic twists E^F of E with $d_2(E^F/K) < r_2$ when E has a cyclic 4-isogeny ψ defined over $K(E[2])$ with $E(K)[2] \subset \ker \psi$. However, as the next theorems show, we can do better if we have some specific knowledge about E.

Theorem 1.4. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny defined over K. Then $N_r(E,X) \gg \frac{X}{\log X}$ for all non-negative $r \geq \operatorname{ord}_2 \mathcal{T}(E/E')$ (defined in Section 6) with $r \equiv \operatorname{ord}_2 \mathcal{T}(E/E') \pmod 2$. If K has a real place or E has a place of multiplicative reduction, then $N_r(E,X) \gg \frac{X}{\log X}$ for all non-negative $r \geq \operatorname{ord}_2 \mathcal{T}(E/E')$.*

Remark 1.5. By Theorem 6.5, we know that $d_2(E/K) \equiv \operatorname{ord}_2 \mathcal{T}(E/E') \pmod 2$. This allows us to replace the condition $r \equiv \operatorname{ord}_2 \mathcal{T}(E/E') \pmod 2$ in Theorem 1.4 with the equivalent condition $r \equiv d_2(E/K) \pmod 2$.

Theorem 1.6. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K. If E has a twist E^F such that $d_2(E^F/K) = r$, then $N_{r'}(E,X) \gg \frac{X}{\log X}$ for all $r' \geq r$ with $r' \equiv r \pmod 2$.*

The rational point of order two on K gives rise to an isogeny $\phi : E \to E'$ with kernel $E(K)[2]$ and $\mathcal{T}(E'/E) = \mathcal{T}(E/E')^{-1}$. Theorem 1.4 therefore shows that the lower-bound obstruction cannot apply to both E and E' simultaneously.

Theorem 1.7. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K.*

- *(i) Then either $N_r(E,X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ with $r \equiv d_2(E/K) \pmod 2$ or $N_r(E',X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ with $r \equiv d_2(E/K) \pmod 2$.*
- *(ii) If E does not have constant 2-Selmer parity, then we additionally have that either $N_r(E,X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ with $r \not\equiv d_2(E/K) \pmod 2$ or $N_r(E',X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ with $r \not\equiv d_2(E/K) \pmod 2$.*
- *(iii) If either K has a real place or E has a place of multiplicative reduction, then $N_r(E,X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ or $N_r(E',X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$. (That is, the choice of E and E' for parts (i) and (ii) can be taken to be the same.)*

As the 2-Selmer rank of E serves as an upper bound for the Mordell-Weil rank of E and E and E' have the same rank, we get the following corollary.

Corollary 1.8. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K. If either $d_2(E/K) \equiv 0 \pmod 2$ or E does not have constant 2-Selmer parity, then the proportion of twists E^F of E having rank zero grows at least as fast as $\frac{X}{\log X}$.*

In order to say something about E having twists of rank one, we need to rely on the parity conjecture which states that $d_2(E/K) \equiv \operatorname{rank}(E/K) \pmod 2$ for all elliptic curves E.

Corollary 1.9. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K. Assuming that the parity conjecture holds and either $d_2(E/K) \equiv 1 \pmod 2$ or E does not have constant 2-Selmer parity, then the proportion of twists E^F of E having rank one grows at least as fast as $\frac{X}{\log X}$.*

Corollary 1.8 is similar to a result of Ono and Skinner when $K = \mathbb{Q}$ and $E(\mathbb{Q})[2] = 0$. Corollaries 1.8 and 1.9 are similar to results of Rubin and Mazur for

general K when $E(K)[2] = 0$ [13,14]. Similar results when $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are due to Skorobogotav and Swinnerton-Dyer [16].

1.1. **Layout and methods of proof.** The techniques used to prove these theorems grew out of the techniques developed by Mazur and Rubin in [13] to compare the Selmer ranks $d_2(E/K)$ and $d_2(E^F/K)$. We begin in Section 2 by descibing these techniques and using them to identify specific local criteria for fields F/K ramified at a small number of primes to yield twists E^F with $d_2(E^F/K) = d_2(E/K) + d$ for $d = -2, 0, 2$. The local conditions for F/K are dependent on $\mathrm{Sel}_2(E/K)$ and as detailed in this work (see Example 2.13), whether any F/K satisfying these local conditions exist is highly dependent on the image of the ϕ-Selmer group $\mathrm{Sel}_\phi(E/K)$ (which we define in Section 3) in $\mathrm{Sel}_2(E/K)$.

Rather than seeking to directly control this image, we instead focus on controlling the rank of $\mathrm{Sel}_\phi(E/K)$. We do this by developing techniques similar to those of Mazur and Rubin to compare the ranks of $\mathrm{Sel}_\phi(E/K)$ and $\mathrm{Sel}_\phi(E^F/K)$. These are detailed over the course of Sections 5, 6, and 7. Paralleling the applications of the techniques of Rubin and Mazur to 2-Selmer groups in Section 2, Section 7 applies the newly developed technique to give specific local criteria for fields F/K to yield twists E^F with desired values of $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E^F/K)$. We then show how to construct such extensions in Sections 8 and 9, allowing us to prove Theorem 1.2. Section 8 also includes a detailed numerical example showing how to construct a specific extension satisfying the necessary local criteria for one of our control theorems for $\mathrm{Sel}_\phi(E/K)$.

As will become clear in the proofs, we need to be concerned about the structure of the extension $K(E[2], E'[2])/K$. Therefore, prior to focusing on controlling the rank $\mathrm{Sel}_\phi(E/K)$, we first take a brief detour in Section 4 to show that the structure we care about can be expressed in terms of the 4-isogeny structure of E. This characterization is reflected in the main theorems of the paper and in many cases requires us to present different proofs for the cases when E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over $K(E[2])$ and when it does not. To maintain unity of presentation, we attempt to group similar technical results for the two cases together whenever possible.

The case where E has a cyclic 4-isogeny ψ defined over $K(E[2])$ with $E(K)[2] \subset \ker\psi$ requires certain local computations that have no counterpart in the case where E does not have such an isogeny. These calculations are contained in Section 10 where we use them to prove Theorems 1.3, 1.4, and 1.7.

1.2. **Notation.** We lay out some notation used throughout the paper. These terms are defined in the text, but are included here for the reader's convenience.

- $d_2(E/K) = \dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/K) - \dim_{\mathbb{F}_2}E(K)[2]$.
- $d_\phi(E/K) = \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E/K)$.
- $d_{\hat\phi}(E'/K) = \dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat\phi}(E'/K)$.
- $\mathcal{T}(E/E') = \frac{|\mathrm{Sel}_\phi(E/K)|}{|\mathrm{Sel}_{\hat\phi}(E'/K)|}$.
- $C = \ker[\phi : E \to E']$, $C^F = \ker\left[\phi : E^F \to E'^F\right]$.
- $C' = \ker\left[\hat\phi : E' \to E\right]$, $C'^F = \ker\left[\hat\phi : E'^F \to E^F\right]$.
- Δ_E, $\Delta_{E'}$ are discriminants of models of E and E' respectively.
- κ_v, κ'_v are connecting maps whose domain and codomain should be clear from the context.

2. The 2-Selmer group

2.1. **Background.** We begin by recalling the definition of the 2-Selmer group. If E is an elliptic curve defined over a number field K, then $E(K)/2(K)$ maps into $H^1(K, E[2])$ via the Kummer map κ, which is given by taking a point $P \in E(K)$ to the cohomology class represented by the cocycle $\sigma \mapsto \sigma(R) - R$, where R is any point in $E(\overline{K})$ with $2R = P$. The 2-Selmer group of E is a subgroup of $H^1(K, E[2])$ that attempts to bound the part of $H^1(K, E[2])$ cut out by the image of $E(K)/2(K)$. We can map $E(K_v)/2E(K_v)$ into $H^1(K_v, E[2])$ via the local Kummer map κ_v for any completion K_v of K, and the following diagram commutes for every place v of K:

$$\begin{array}{ccc} E(K)/2E(K) & \xrightarrow{\kappa} & H^1(K, E[2]) \\ \downarrow & & \downarrow \mathrm{res}_v \\ E(K_v)/2E(K_v) & \xrightarrow{\kappa_v} & H^1(K_v, E[2]) \end{array}$$

Definition 2.1. The distinguished local subgroup $H^1_f(K_v, E[2]) \subset H^1(K_v, E[2])$ is

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

for each place v of K.

(That is, κ_v gives an isomorphism from $\mathrm{coker}\left[E(K_v) \xrightarrow{[2]} E(K_v)\right]$ to $H^1_f(K_v, E[2])$.)

Definition 2.2. The **2-Selmer group** of E/K, denoted $\mathrm{Sel}_2(E/K)$, is defined as

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

That is, the 2-Selmer group is the group of cohomology classes in $H^1(K, E[2])$ whose restrictions locally come from points of $E(K_v)$ in each completion K_v of K.

The 2-Selmer group is a finite dimensional $\mathbb{F}_2$-vector space that sits inside the exact sequence of $\mathbb{F}_2$-vector spaces

$$0 \to E(K)/2E(K) \xrightarrow{\kappa} \mathrm{Sel}_2(E/K) \to Ш(E/K)[2] \to 0, \tag{2.1}$$

where $Ш(E/K)$ is the Tate-Shafaravich group of E.

We would like to examine the behavior of $\mathrm{Sel}_2(E/K)$ under the action of twisting by a quadratic extension.

Definition 2.3. Let E be given by $E : y^2 = x^3 + Ax^2 + Bx + C$ and F/K be a quadratic extension given by $F = K(\sqrt{d})$. The **quadratic twist** of E by F denoted E^F is the elliptic curve given by the model $y^2 = x^3 + dAx^2 + d^2Bx + d^3C$.

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 $H^1(K_v, E[2])$.

Definition 2.4. The distinguished local subgroup $H^1_f(K_v, E^F[2]) \subset H^1(K_v, E[2])$ is the image of $\kappa_v(E^F(K_v))$ in $H^1(K_v, E[2])$.

We will study $\mathrm{Sel}_2(E^F/K)$ by using the following lemmas to compare $H^1_f(K_v, E[2])$ and $H^1_f(K_v, E^F[2])$.

Lemma 2.5. (*i*) *If* $v \nmid 2\infty$, *then* $\dim_{\mathbb{F}_2} H^1_f(K_v, E[2]) = \dim_{\mathbb{F}_2} E(K_v)[2]$.
(*ii*) *If* $v \mid 2$, *then* $\dim_{\mathbb{F}_2} H^1_f(K_v, E[2]) = \dim_{\mathbb{F}_2} E(K_v)[2] + [K_v : \mathbb{Q}_2]$.
(*iii*) *If* $K_v = \mathbb{R}$, *then* $\dim_{\mathbb{F}_2} H^1_f(K_v, E[2]) = \dim_{\mathbb{F}_2} E(K_v)[2] - 1$.
(*iv*) *If* $K_v = \mathbb{C}$, *then* $\dim_{\mathbb{F}_2} H^1_f(K_v, E[2]) = 0$.
(*v*) *For all* v, $\dim_{\mathbb{F}_2} H^1_f(K_v, E[2]) = \dim_{\mathbb{F}_2}(K_v^\times)/(K_v^\times)^2 + \dim_{\mathbb{F}_2} E(K_v)[2] - 2$.

Proof. Parts (*i*) and (*ii*) are Lemma 3.1 in [2]. Part (*iii*) is an immediate consequence of the fact that $E(\mathbb{R}) \simeq S^1$ if $E(\mathbb{R})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $E(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z} \times S^1$ if $E(\mathbb{R})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Part (*iv*) holds trivially since $H^1(\mathbb{C}, E[2]) = 0$. Part (*v*) comes from examining $\dim_{\mathbb{F}_2}(K_v^\times)/(K_v^\times)^2$ (say, by using Proposition 6 in Section II.3 of [12]) and comparing it with parts (*i*) - (*iv*). □

Lemma 2.6. *If* $v \nmid 2\infty$ *and* E *has good reduction at* v, *then we have an evaluation isomorphism*

$$e_v : H^1_f(K_v, E[2]) \xrightarrow{\sim} E[2]/(\mathrm{Frob}_v - 1)E[2]$$

given by $e_v(c) = \hat{c}(\mathrm{Frob}_v)$, *where* $\hat{c}$ *is any cocycle representative for* c *and* Frob_v *is the Frobenius automorphism of* v.

Proof. This is part (*ii*) of Lemma 2.2 in [13]. □

Lemma 2.7. *Let* E *be an elliptic curve defined over* K, v *a place of* K, *and* F/K *a quadratic extension. Then*

(*i*) $H^1_f(K_v, E[2]) = H^1_f(K_v, E^F[2])$ *if either* v *splits in* F/K *or* v *is a prime where* E *has good reduction that is unramified in* F/K;
(*ii*) $H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2]) = 0$ *if* $v \nmid 2\infty$, E *has good reduction at* v, *and* v *is ramified in* F/K.

Proof. Part (*i*) is Lemma 2.10 in [13], and part (*ii*) is Lemma 2.11 in [13]. □

Lemma 2.8. *Let* E *be an elliptic curve defined over* K, v *a prime of* K *away from* 2 *at which* E *has good reduction, and* F/K *a quadratic extension ramified at* v. *Then* $E^F(K_v)$ *contains no points of order* 4, *and it follows that* $H^1_f(K_v, E^F[2])$ *is the image of* $E^F(K_v)[2]$ *under the Kummer map.*

Proof. Since E had good reduction at v, $v \nmid 2$, and F/K is ramified at v, Tate's algorithm gives us that E^F has reduction type I_0^* at v. Let $E_0^F(K_v)$ be the group of points on $E^F(K_v)$ with non-singular reduction at v, $E_1^F(K_v)$ the subgroup of points with trivial reduction, and k_v the residue field of K_v. The formal group structure on $E_1^F(K_v)$ shows that $E_1^F(K_v)$ is uniquely divisible by 2. As $E_0^F(K_v)/E_1^F(K_v) \simeq k_v^+$, $E_0^F(K_v)$ is uniquely 2-divisible as well. Since E^F has reduction type I_0^* at v, Tate's algorithm then shows that $E^F(K_v)/E_0^F(K_v)$ – and therefore $E^F(K_v)[2^\infty]$ – injects into $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It therefore follows that $E^F(K_v)$ has no points of order four and that $E^F(K_v)[2]$ injects into $H^1_f(K_v, E^F[2])$. By part (*i*) of Lemma 2.5, $E^F(K_v)[2]$ and $H^1_f(K_v, E^F[2])$ have the same dimension, which shows that the image of $E^F(K_v)$ under κ_v is generated by $E^F(K_v)[2]$. □

2.2. **The method of Rubin and Mazur.** In [13], Mazur and Rubin developed a method to compare the Selmer groups $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_2(E^F/K)$ by comparing the local conditions for E and E^F. The following theorem is the primary tool they developed and it will be an important tool for us as well.

Let Δ_E be the discriminant of some model of E.

Theorem 2.9. *Let E be an elliptic curve defined over a number field K. Suppose F/K is a quadratic extension such that all places above $2\Delta_E\infty$ split in F/K. Let T be the set of (finite) primes $\mathfrak{p}$ of K such that F/K is ramified at $\mathfrak{p}$ and $E(K_\mathfrak{p})[2] \neq 0$ and define a map*

$$\mathrm{Loc}_T : H^1(K, E[2]) \to \bigoplus_{\mathfrak{p}\in T} H^1(K_\mathfrak{p}, E[2]) \tag{2.2}$$

as the sum of the sum of the restriction maps over the places $\mathfrak{p}$ in T. Letting $V_T = \mathrm{Loc}_T(\mathrm{Sel}_2(E/K))$, we then have

$$d_2(E^F/K) = d_2(E/K) - \dim_{\mathbb{F}_2} V_T + d$$

for some d satisfying

$$0 \leq d \leq \dim_{\mathbb{F}_2} \left(\bigoplus_{\mathfrak{p}\in T} H^1_f(K_\mathfrak{p}, E[2]) \right) / V_T \tag{2.3}$$

and

$$d \equiv \dim_{\mathbb{F}_2} \left(\bigoplus_{\mathfrak{p}\in T} H^1_f(K_\mathfrak{p}, E[2]) \right) / V_T \pmod 2. \tag{2.4}$$

Proof. This is Proposition 3.3 in [13]. □

Theorem 2.9 has some corollaries which will allow us to produce twists of E with a desired 2-Selmer rank.

Corollary 2.10. *Suppose F/K is a quadratic extension ramified only at $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in which all places above $2\Delta_E\infty$ split completely. If $E(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(\mathrm{Sel}_2(E/K)) = 1$, then $d_2(E^F/K) = d_2(E/K)$.*

Corollary 2.11. *Suppose that F/K is a quadratic extension in which all places above $2\Delta_E\infty$ split completely. If F/K is ramified at exactly four primes, $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_4$, such that $E(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3,\mathfrak{p}_4\}}(\mathrm{Sel}_2(E/K)) = 3$, then $d_2(E^F/K) = d_2(E/K) - 2$.*

Corollary 2.12. *Let E/K be an elliptic curve with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and suppose that F/K is a quadratic extension in which all places above $2\Delta_E\infty$ split completely. If F/K is ramified at exactly two primes, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, such that $E(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{res}_{\mathfrak{p}_i}(\mathrm{Sel}_2(E/K)) = 0$, then $d_2(E^F/K) = d_2(E/K) + 2$.*

Proof. Unlike Corollaries 2.10 and 2.11, this result does not follow immediately from Theorem 2.9. Indeed, Theorem 2.9 shows that either $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) + 2$ but does not help us discriminate between the two cases. We therefore argue as follows.

Since $\mathrm{res}_{\mathfrak{p}_i}(\mathrm{Sel}_2(E/K)) = 0$, we have $\mathrm{Sel}_2(E/K) \subset \mathrm{Sel}_2(E^F/K)$. Let P be the point of order two in $E^F(K)$ and c its image in $\mathrm{Sel}_2(E^F/K)$. By Lemma 2.8, we see that P maps non-trivially into $E^F(K_{\mathfrak{p}_i})/2E^F(K_{\mathfrak{p}_i})$, and therefore that c maps non-trivially into $H^1(K_{\mathfrak{p}_i}, E^F[2])$. By Lemma 2.7, we therefore get that $c \notin \mathrm{Sel}_2(E/K)$. This shows that $\mathrm{Sel}_2(E/K) \subsetneq \mathrm{Sel}_2(E^F/K)$ and that it must be the case that $d_2(E^F/K) = d_2(E/K) + 2$. □

If it were always possible to produce extensions satisfying Corollaries 2.10, 2.11, and 2.12, then proving Theorem 1.2 would be straightforward. However, as this next example shows, there are elliptic curves for which no quadratic extensions satisfy the hypotheses of these corollaries. Proceeding in these situations requires technical effort that occupies much of this paper.

Example 2.13. Take E to be the elliptic curve defined over $\mathbb{Q}$ by the equation $y^2 = x^3 - 15x^2 + 5x$ and let c be the image of $P = (0,0)$ in $\mathrm{Sel}_2(E/\mathbb{Q})$ under the Kummer map. A calculation using **magma** [1] shows that $\mathrm{Sel}_2(E/\mathbb{Q})$ is three-dimensional and is generated by c and the cocycles represented by the quadratic characters χ_{-1} and χ_5, where

$$\chi_a(\sigma) = \begin{cases} P & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{a})}, \\ 0 & \text{if } \sigma \notin G_{\mathbb{Q}(\sqrt{a})}. \end{cases}$$

If T is a set of primes where E has good reduction with $E(\mathbb{Q}_p)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ for each $p \in T$, then Lemma 2.6 tells us $\mathrm{res}_{\mathfrak{p}}(\chi_{-1}) = \mathrm{res}_{\mathfrak{p}}(\chi_5) = 0$ for all $\mathfrak{p} \in T$. We therefore get that $\mathrm{Loc}_T(\mathrm{Sel}_2(E/\mathbb{Q}))$ is given by $\mathrm{Loc}_T(c)$, and it follows that $\mathrm{Loc}_T(\mathrm{Sel}_2(E/\mathbb{Q}))$ is at most one-dimensional.

The next section will help us gain a fuller understanding about what is happening in Example 2.13. We will elaborate on this point in Remark 3.5.

3. The ϕ-Selmer group

When $E(K)$ has a point P of order two, it gives rise to an isogenous curve E' and an isogeny $\phi : E \to E'$ with kernel $C = \langle P \rangle$. If we define $C' = \phi(E[2])$, then we get a short exact sequence of G_K modules

$$0 \to C \to E[2] \xrightarrow{\phi} C' \to 0.$$

This short exact sequence gives rise to a long exact sequence of cohomology groups:

(3.1)
$$0 \to C \to E(K)[2] \xrightarrow{\phi} C' \xrightarrow{\kappa} H^1(K,C) \to H^1(K,E[2]) \xrightarrow{\phi} H^1(K,C') \to \dots .$$

The map $\kappa : E'(K)/\phi(E(K)) \to H^1(K,C)$ is given by taking a point $P' \in E'(K)$ to the cohomology class represented by the cocycle $\sigma \mapsto \sigma(R) - R$, where R is any point in $E(\overline{K})$ with $\phi(R) = P'$. We similarly have local connecting maps $\kappa_v : E'(K_v)/\phi(E(K_v)) \to H^1(K_v,C)$ for each place v of K giving the following commutative diagram:

$$\begin{array}{ccc} E'(K)/\phi(E(K)) & \xrightarrow{\kappa} & H^1(K,C) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} \\ E'(K_v)/\phi(E(K_v)) & \xrightarrow{\kappa_v} & H^1(K_v,C) \end{array}$$

Definition 3.1. The distinguished local subgroup $H^1_\phi(K_v,C) \subset H^1(K_v,C)$ is

$$\mathrm{Image}\left[\kappa_v : E'(K_v)/\phi(E(K_v)) \hookrightarrow H^1(K_v,C)\right]$$

for each place v of K.
(That is, κ_v gives an isomorphism from $\mathrm{coker}\,[\phi : E(K_v) \to E'(K_v)]$ to $H^1_\phi(K_v,C)$.)

If $v \nmid 2$ is a prime where E has good reduction, then $H^1_\phi(K_v, C)$ is given by the (one-dimensional) unramified local subgroup

$$H^1_u(K_v, C) = \ker[H^1(K_v, C) \to H^1(\mathcal{I}_v, C)],$$

where $\mathcal{I}_v$ is the inertia subgroup of $\mathrm{Gal}(\overline{K_v}/K_v)$ (see Lemma 4.1 in [3]).

Definition 3.2. The **ϕ-Selmer group** of E/K, denoted $\mathrm{Sel}_\phi(E/K)$, is defined as

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

That is, the ϕ-Selmer group is the group of cohomology classes in $H^1(K, C)$ whose restrictions locally come from points of $E'(K_v)$ in each completion K_v of K.

The ϕ-Selmer group $\mathrm{Sel}_\phi(E/K)$ is a finite dimensional $\mathbb{F}_2$-vector space and we denote its dimension $\dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E/K)$ by $d_\phi(E/K)$.

The isogeny ϕ on E gives rise to the dual isogeny $\hat{\phi} : E' \to E$ with kernel $C' = \phi(E[2])$. Exchanging the roles of (E, C, ϕ) and $(E', C', \hat{\phi})$ in the above defines the $\hat{\phi}$-Selmer group of E', $\mathrm{Sel}_{\hat{\phi}}(E'/K)$, as a subgroup of $H^1(K, C')$. We likewise denote its dimension $\dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}(E'/K)$ by $d_{\hat{\phi}}(E'/K)$.

The following theorem allows us to relate the ϕ-Selmer group, the $\hat{\phi}$-Selmer group, and the 2-Selmer group.

Theorem 3.3. *The ϕ-Selmer group, the $\hat{\phi}$-Selmer group, and the 2-Selmer group sit inside the exact sequence*

$$0 \to E'(K)[2]/\phi(E(K)[2]) \to \mathrm{Sel}_\phi(E/K) \to \mathrm{Sel}_2(E/K) \xrightarrow{\phi} \mathrm{Sel}_{\hat{\phi}}(E'/K), \tag{3.2}$$

where the map ϕ is the restriction of the map ϕ in (3.1) *to* $\mathrm{Sel}_2(E/K)$.

Proof. This is a well known diagram chase. See Lemma 2 in [6] for example. □

Corollary 3.4. *Let $\iota : H^1(K, C) \to H^1(K, E[2])$ be the map in* (3.1). *Then* $\mathrm{Sel}_2(E/K) \cap \iota(H^1(K, C)) = \iota(\mathrm{Sel}_\phi(E/K))$.

Proof. The fact that $\iota(\mathrm{Sel}_\phi(E/K)) \subset \mathrm{Sel}_2(E/K) \cap \iota(H^1(K, C))$ is a direct consequence of Theorem 3.3. Let $c \in \mathrm{Sel}_2(E/K) \cap \iota(H^1(K, C))$. The exactness of (3.1) tells us that $\phi(c) = 0$. As the map ϕ in (3.2) is the same as that in (3.1), the exactness of (3.2) tells us that $c \in \iota(\mathrm{Sel}_\phi(E/K))$. □

Remark 3.5. We may use Theorem 3.3 and Corollary 3.4 to gain a fuller understanding of Example 2.13. Lemma 2.6 shows that if $c \in \iota\left(H^1(K, C)\right) \cap \mathrm{Sel}_2(E/K)$, then $\mathrm{res}_v(c) = 0$ whenever E has good reduction at v and $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$. If T is a set of prime places such that E has good reduction and $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ for all $v \in T$, then by Corollary 3.4, the map $\mathrm{Loc}_T : \mathrm{Sel}_2(E/K) \to \bigoplus_{v\in T} H^1_f(K_v, E[2])$ factors through $\mathrm{Sel}_2(E/K)/\iota(\mathrm{Sel}_\phi(E/K))$.

A computation in **magma** shows that for the curve E in Example 2.13, the quotient $\mathrm{Sel}_2(E/K)/\iota(\mathrm{Sel}_\phi(E/K))$ is one-dimensional. It therefore follows that the image of Loc_T must be at most one-dimensional as well.

4. Characterization of curves with $E(K) \simeq \mathbb{Z}/2\mathbb{Z}$

The results obtained in this paper are dependent on whether E possesses certain isogenies defined over K or over $K(E[2])$, and we now take a brief detour in order to characterize such curves. In this section, we will assume that $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$.

We recall that if E is defined over a field N, then a subgroup $H \subset E(\overline{N})$ is called *rational over* N if $\sigma(H) \subset H$ for all $\sigma \in G_N$, where $G_N = \mathrm{Gal}(\overline{N}/N)$. Standard results show that an isogeny ψ with kernel H is defined over N if and only if H is rational over N. We then have the following.

Lemma 4.1. *Let E be an elliptic curve defined over a field N, $C_4 = \langle R \rangle \subset E(\overline{N})$ a cyclic subgroup of order four, and $\psi : E \to A$ an isogeny with kernel $\langle 2R \rangle$. The subgroup C_4 is rational over N if and only if $2R \in A(N)$ and $\psi(C_4) \subset A(N)[2]$.*

Proof. Suppose that C_4 is rational over N. Since $2R$ is the unique point of order two in C_4, we get that $2R \in E(N)$. This shows that ψ is defined over N and $\sigma(\psi(R)) = \psi(\sigma(R))$ for all $\sigma \in G_N$. Taking $\sigma \in G_N$, $\sigma(R) \in C_4$ means that $\sigma(R) \in R + \ker\psi$, so $\sigma(\psi(R)) = \psi(\sigma(R)) = \psi(R)$. As all $\sigma \in G_N$ fix $\psi(R)$, we get that $\psi(R) \in A(N)$. As $2\psi(R) = \psi(2R) = 0$, we further have $\psi(R) \subset A(N)[2]$.

Now suppose that $\psi(R) \in A(N)$ and $2R \in E(N)$. For all $\sigma \in G_N$, we then have $\psi(R) = \sigma(\psi(R)) = \psi(\sigma(R))$, showing that $\sigma(R) - R \in \ker\psi = \langle 2R \rangle$. We therefore get that $\sigma(R) \in C_4$ and that C_4 is rational over N. □

Let $\phi : E \to E'$ be the degree-two isogeny with kernel $E(K)[2]$, $M = K(E[2])$, and $M' = K(E'[2])$.

Lemma 4.2. *Let E be an elliptic curve defined over K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$.*

(i) E has a cyclic 4-isogeny defined over K if and only if $M' = K$.

(ii) E has no cyclic 4-isogenies defined over K but has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over M if and only if $M = M'$.

Proof. If $C_4 \subset E[4]$ is a cyclic subgroup of order four which contains $E(K)[2]$, then we may take ψ and A in Lemma 4.1 to be ϕ and E' respectively. We then get that C_4 is rational over K (respectively M) if and only if $\phi(C_4) \subset E'(K)$ (resp. $\phi(C_4) \subset E'(M)$). As $C' = \phi(E[2])$ and $\phi(C_4)$ are distinct order two subgroups of $E'[2]$, this condition is equivalent to E' having full two-torsion over K (resp. M).

Part *(i)* then follows because the kernel of any cyclic 4-isogeny defined over K must contain $E(K)[2]$. Part *(ii)* follows because $M = M'$ if and only if $M' \neq K$ and E' has full two-torsion over M. We have shown that E' has full two-torsion over M if and only if E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over M, and it follows from part *(i)* that $M' \neq K$ if and only if E does not have a cyclic 4-isogeny defined over K. □

Remark 4.3. As $M = K(\sqrt{\Delta_E})$ and $M' = K(\sqrt{\Delta_{E'}})$, the condition that E have a cyclic 4-isogeny defined over K is equivalent to $\Delta_{E'}$ being a square in $K^\times$, and the condition that E does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over K but acquires such an isogeny over M is equivalent to Δ_E and $\Delta_{E'}$ differing by a square in $K^\times$.

The following corollary follows immediately.

Corollary 4.4. *With E as in Lemma 4.2: If E does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over K but acquires such an isogeny over M, then $\dim_{\mathbb{F}_2} E(K_v)[2] = \dim_{\mathbb{F}_2} E'(K_v)[2]$ for all places v of K.*

5. Controlling 2-Selmer rank

In this section, we will assume that $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and let $M = K(E[2])$.

This section will show how to construct extensions satisfying the hypotheses of Corollaries 2.10 and 2.11 when the codimension of the image of $\mathrm{Sel}_\phi(E/\mathbb{Q})$ in $\mathrm{Sel}_2(E/K)$ is sufficiently large. We begin with the following two lemmas.

Lemma 5.1. *Suppose that $c \in \mathrm{Sel}_2(K, E[2])$ and that N/K is a Galois extension containing M such that $\mathrm{res}_N(c) = 0$. If $\mathfrak{p}$ is a prime where E has good reduction and $\gamma \in \mathrm{Gal}(N/K)$ is in the conjugacy class of the Frobenius $\mathrm{Frob}_\mathfrak{p}$ in $\mathrm{Gal}(N/K)$, then the restriction $\mathrm{res}_\mathfrak{p}(c)$ is given by $\mathrm{res}_\mathfrak{p}(c) = \hat{c}(\gamma) \in E[2]/(\gamma - 1)E[2]$, where $\hat{c}$ is any cocycle representative for c.*

Proof. Since $c \in \mathrm{Sel}_2(E/K)$ and E has good reduction at $\mathfrak{p}$, Lemma 2.6 tells us that $\mathrm{res}_\mathfrak{p}(c)$ is given by $\hat{c}(\mathrm{Frob}_\mathfrak{p}) \in E[2]/(\mathrm{Frob}_\mathfrak{p} - 1)E[2]$. As N contains M, the action of $\mathrm{Frob}_\mathfrak{p}$ on $E[2]$ is given by γ and since $\mathrm{res}_N(c) = 0$, we get that $\hat{c}(\mathrm{Frob}_\mathfrak{p})$ is given by $\hat{c}(\gamma)$. □

Lemma 5.2. *Define S to be the image of $H^1(K, C)$ in $H^1(K, E[2])$ under the map in (3.1) and let $V \subseteq H^1(K, E[2])$ be a dimension r subspace of $H^1(K, E[2])$ such that $V \cap S = 0$. Then there exist $\sigma_1, \ldots, \sigma_r \in G_K$ such that $\sigma_i\big|_M \neq 1$ and $\mathrm{Loc}(V)$ has dimension r where the localization map $\mathrm{Loc} : H^1(K, E[2]) \to \bigoplus_{i=1}^r E[2]/C$ is defined by $c \mapsto (c(\sigma_1), \ldots, c(\sigma_r))$.*

Proof. Let $\tilde{Q} \in E[2]/C$ be the image of a point $Q \in E[2]\backslash C$. Take $\tilde{V} \subseteq H^1(K, C')$ to be the image of V in $H^1(K, C') = \mathrm{Hom}(G_K, C')$ and observe that $\tilde{V}$ has dimension r since $V \cap \mathrm{Image}\left(H^1(K, C)\right) = 0$. Take a basis $\{c_1, \ldots, c_r\}$ for $\tilde{V}$. Since the image of the dual map $G_K \to \mathrm{Hom}(\tilde{V}, C')$ is surjective and has dimension r as well, we can find $\tau_1, \ldots, \tau_r \in G_K$ such that

$$c_i(\tau_j) = \begin{cases} \tilde{Q} & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Suppose $\tau_i \in G_M$ for all i. Then the map $G_M \to \mathrm{Hom}(\tilde{V}, C')$ must be surjective as well. So taking any $\tau \in G_K - G_M$, we can therefore find $\gamma_1, \ldots, \gamma_r \in G_M$ such that

$$c_i(\gamma_j) = \begin{cases} \tilde{Q} + c_j(\tau) & \text{if } i = j, \\ c_j(\tau) & \text{if } i \neq j. \end{cases}$$

Thus,

$$c_j(\gamma_i\tau) = c_j(\gamma_i) + c_j(\tau) = \begin{cases} \tilde{Q} & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Taking $\sigma_i = \gamma_i\tau$ then gives the result.

Otherwise, we have $\tau_k \notin G_M$ for some k. Define $\sigma_1, \ldots, \sigma_r$ by

$$\sigma_i = \begin{cases} \tau_i & \text{if } \tau_i \notin G_M, \\ \tau_i\tau_k & \text{if } \tau_i \in G_M. \end{cases}$$

We then get that

$$c(\sigma_i) = 0 \ \forall i \Leftrightarrow c(\tau_i) = 0 \ \forall i,$$

which means that the localization map is injective on V giving us the result. □

We now apply Lemma 5.2 to the following two situations.

Proposition 5.3. *If $d_\phi(E/K) - \dim_{\mathbb{F}_2} E'(K)[2]/\phi(E(K)[2]) \leq d_2(E/K)$, then the number of quadratic extensions F/K in $S(X)$ satisfying the hypotheses of Corollary 2.10 grows at least as fast as $\frac{X}{\log X}$.*

Proof. The assumption that $d_\phi(E/K) - \dim_{\mathbb{F}_2} E'(K)[2]/\phi(E(K)[2]) \leq d_2(E/K)$ tells us that by Theorem 3.3, there exists some $c_0 \in \mathrm{Sel}_2(E/K)$ that is not in the image of $\mathrm{Sel}_\phi(E/K)$. Applying Corollary 3.4, we find that c_0 is not in the image of $H^1(K, C)$. Applying Lemma 5.2 with $V = \langle c_0 \rangle$, we find σ with $\sigma_i\big|_M \neq 1$ and $c_0(\sigma) \neq 0 \in E[2]/C$. Let N be any finite Galois extension of K containing $MK(8\Delta_E\infty)$ such that the restriction of $\mathrm{Sel}_2(E/K)$ to N is zero, where $K(8\Delta_E\infty)$ is the ray class field modulo $8\Delta_E\infty$ and pick two primes $\mathfrak{p}_1, \mathfrak{p}_2$ away from $2\Delta_E$ such that the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}_1}$ in $\mathrm{Gal}(N/K)$ contains $\sigma\big|_N$ and the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}_2}$ in $\mathrm{Gal}(N/K)$ contains $\sigma^{-1}\big|_N$. This gives $\mathrm{Frob}_{\mathfrak{p}_1}\mathrm{Frob}_{\mathfrak{p}_2}\big|_{K(8\Delta_E\infty)} = 1$ and therefore the ideal $\mathfrak{p}_1\mathfrak{p}_2$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta_E}$. Set $F = K(\sqrt{\pi})$.

We then get that all places dividing $2\Delta_E\infty$ split in F/K and that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the only primes ramified in F/K. Because $\mathrm{Frob}_{\mathfrak{p}_i}$ restricts non-trivially into M, we additionally get that $E(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$. By Lemma 5.1, $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(c)$ is given by $(\hat{c}(\mathrm{Frob}_{\mathfrak{p}_1}), \hat{c}(\mathrm{Frob}_{\mathfrak{p}_2})) = \big(\hat{c}(\sigma), \hat{c}(\sigma^{-1})\big) \subset E[2]/C \times E[2]/C$ for every $c \in \mathrm{Sel}_2(E/K)$, where $\hat{c}$ is any cocycle representative for c. It follows from this that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(\mathrm{Sel}_2(E/K))$ is contained in the one-dimensional diagonal subspace of $E[2]/C \times E[2]/C$, and it follows that $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(\mathrm{Sel}_2(E/K)) = 1$ since $\mathrm{res}_{\mathfrak{p}_1}(c_0) \neq 0$ due to our choice of $\mathfrak{p}_1$. The extension F/K therefore satisfies the hypotheses of Corollary 2.10.

To see the density result, we observe that we have complete freedom in terms of choosing $\mathfrak{p}_1$ and $\mathfrak{p}_2$ subject only to the conditions on Frobenius in $\mathrm{Gal}(N/K)$, and the result then follows from the Chebotarev density theorem. □

Lemma 5.4. *Suppose that $C = \langle P \rangle$. If $c \in \mathrm{Sel}_2(E/K)$ is the image of P under the map κ in (2.1), then $\phi(c) = \hat{\kappa}(P)$ where ϕ is the map $\mathrm{Sel}_2(E/K) \to \mathrm{Sel}_{\hat{\phi}}(E'/K)$ appearing in (3.2) and $\hat{\kappa}$ is the connecting map $\hat{\kappa} : E(K) \to H^1(K, C')$. In particular, if $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then $\mathrm{res}_v(c)$ and $\mathrm{res}_v(\phi(c))$ are non-trivial.*

Proof. Take $R \in E(\overline{K})$ with $2R = P$. The class c is represented by the cocycle $\tilde{c}(\sigma) = \sigma(R) - R$ and $\phi(c)$ is represented by the cocycle

$$\hat{c}(\sigma) = \phi(\sigma(R) - R) = \phi(\sigma(R)) - \phi(R) = \sigma(\phi(R)) - \phi(R).$$

As $\hat{\phi}(\phi(R)) = 2R = P$, we get that $\hat{c}(\sigma) = \sigma(\phi(R)) - \phi(R)$ is a cocycle representative for $\hat{\kappa}(P)$. When $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, $\hat{\kappa}(P)$ restricts non-trivially into $H^1(K_v, C)$. We then get $\mathrm{res}_v(c) \neq 0$ from the commutativity of the diagram

$$\begin{array}{ccc} H^1(K, E[2]) & \xrightarrow{\phi} & H^1(K, C') \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} \\ H^1(K_v, E[2]) & \xrightarrow{\phi} & H^1(K_v, C') \end{array}$$

□

Corollary 5.5. *If E does not have a cyclic 4-isogeny defined over K, then $d_2(E/K) \geq d_\phi(E/K) - 1$ and E satisfies the hypotheses of Proposition 5.3.*

Proof. By Theorem 3.3, the dimension of the image of $\mathrm{Sel}_\phi(E/K)$ in $\mathrm{Sel}_2(E/K)$ is given by $d_\phi(E/K) - \dim_{\mathbb{F}_2} E'(K)[2]/\phi(E(K)[2])$. As E does not have a cyclic 4-isogeny over K, Lemma 4.2 tells us that $\dim_{\mathbb{F}_2} E'(K)[2]/\phi(E(K)[2]) = 1$ and E will satisfy the conditions of Proposition 5.3 as long as $d_2(E/K) \geq d_\phi(E/K) - 1$.

As $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, we have $d_2(E/K) = \dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/K) - 1$ and therefore $d_2(E/K) \geq d_\phi(E/K) - 1$ as long as $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E/K) > d_\phi(E/K) - 1$. As $d_\phi(E/K) - 1$ is the dimension of the image of $\mathrm{Sel}_\phi(E/K)$ in $\mathrm{Sel}_2(E/K)$ and (3.2) is exact, it therefore suffices to show that $\phi(\mathrm{Sel}_2(E/K))$ is non-trivial. By Lemma 4.2, if E does not have a cyclic 4-isogeny defined over K, then there exists some place v such that $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$. By Lemma 5.4, we then have that $\mathrm{res}_v(\phi(\mathrm{Sel}_2(E/K))) \neq 0$ and the result follows. □

Corollary 5.5 allows us to prove Theorem 1.6.

Proof of Theorem 1.6. We follow the proof of Theorem 1.4 in [13].

Suppose $d_2(E^F/K) = r$. Every twist $(E^F)^{L'}$ of E^F is also a twist E^L of E and

$$\mathfrak{f}(L/K) | \mathfrak{f}(F/K)\mathfrak{f}(L'/K),$$

so $N_r(E, X) \geq N_r\left(E^F, \frac{X}{\mathbf{N}_{K/\mathbb{Q}}\mathfrak{f}(F/K)}\right)$.

Since possession of a cyclic 4-isogeny defined over K is fixed under twisting, E^F does not possess a cyclic isogeny of degree 4 defined over K. Corollary 5.5 allows us to apply Proposition 5.3 to E^F yielding the result. □

We can also apply Lemma 5.2 when the codimension of the image of $\mathrm{Sel}_\phi(E/\mathbb{Q})$ in $\mathrm{Sel}_2(E/K)$ is at least three.

Proposition 5.6. *If $d_\phi(E/K) - \dim_{\mathbb{F}_2} E'(K)[2]/\phi(E(K)[2]) \leq d_2(E/K) - 2$, then there is a quadratic extension F/K satisfying the hypotheses of Corollary* 2.11. *In particular, E has a twist E^F with $d_2(E^F/K) = d_2(E/K) - 2$.*

Proof. Our proof is extremely similar to that of Proposition 5.3 so we only include key details.

By assumption, there is a 3-dimensional subspace $V \subset \mathrm{Sel}_2(E/K)$ that intersects the image of $H^1(K, C)$ trivially, and we can therefore pick $\sigma_1, \sigma_2, \sigma_3 \in G_K$ satisfying the conclusion of Lemma 5.2 and set $\sigma_4 = (\sigma_1\sigma_2\sigma_3)^{-1}$. Letting N be as in the proof of Proposition 5.3, we pick primes $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_4$ such that the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}_i}$ in $\mathrm{Gal}(N/K)$ contains $\sigma_i\big|_N$. It follows that the ideal $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta_E}$ and we set $F = K(\sqrt{\pi})$.

As σ_1, σ_2,and σ_3 were chosen to satisfy the conclusion of Lemma 5.2 and the class of $\mathrm{Frob}_{\mathfrak{p}_i}$ in $\mathrm{Gal}(N/K)$ contains $\sigma_i\big|_N$, $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}}(\mathrm{Sel}_2(E/K))$ has dimension three. Since σ_4 was chosen as $\sigma_4 = (\sigma_1\sigma_2\sigma_3)^{-1}$, $\hat{c}(\sigma_1) + \hat{c}(\sigma_2) + \hat{c}(\sigma_3) + \hat{c}(\sigma_4) \in C$ for all $c \in \mathrm{Sel}_2(E/K)$, where $\hat{c}$ is any cocycle representative for c. It follows that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3,\mathfrak{p}_4\}}(\mathrm{Sel}_2(E/K))$ is contained in a codimension-1 subspace of $(E[2]/C)^4$ and therefore that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3,\mathfrak{p}_4\}}(\mathrm{Sel}_2(E/K))$ has dimension three. The extension F/K therefore satisfies the hypotheses of Corollary 2.11. □

Unlike Proposition 5.3, Proposition 5.6 does not apply to all curves without a cyclic 4-isogeny over K. We will deal with this issue in Section 7.

6. Local conditions for the ϕ-Selmer group

6.1. **Notation.** Before continuing, we recall the definitions of the various distinguished local subgroups encountered thus far.

- $H^1_f(K_v, E[2]) \subset H^1(K_v, E[2])$ is the image of $E(K_v)$ under the local connecting map $\kappa_v : E(K_v) \to H^1(K_v, E[2])$ and is isomorphic to $\operatorname{coker} : E(K_v) \xrightarrow{[2]} E(K_v)$.
- $H^1_\phi(K_v, C) \subset H^1(K_v, C)$ is the image of $E'(K_v)$ under the local connecting map $\kappa_v : E'(K_v) \to H^1(K_v, C)$ defined in Section 3 and is isomorphic to the cokernel of the map $\phi : E(K_v) \to E'(K_v)$.
- $H^1_{\hat\phi}(K_v, C') \subset H^1(K_v, C')$ is the image of $E(K_v)$ under the local connecting map $\kappa'_v : E(K_v) \to H^1(K_v, C')$ which is defined by exchanging the roles of E and E' in the definition of $\kappa_v : E'(K_v) \to H^1(K_v, C)$ and is isomorphic to $\operatorname{coker} : E'(K_v) \xrightarrow{\hat\phi} E(K_v)$.

6.2. **Duality between $H^1_\phi(K_v, C)$ and $H^1_{\hat\phi}(K_v, C')$.** In addition to Theorem 3.3, a second relationship between the ϕ-Selmer group and the $\hat\phi$-Selmer group arises from a duality between their respective local conditions.

Proposition 6.1. *With the maps as in* (3.1)*, the sequence*

$$0 \to C'/\phi\left(E(K_v)[2]\right) \xrightarrow{\kappa_v} H^1_\phi(K_v, C) \to H^1_f(K_v, E[2]) \xrightarrow{\phi} H^1_{\hat\phi}(K_v, C') \to 0 \tag{6.1}$$

is exact.

Proof. It is easy to see that the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C'/\phi\left(E(K_v)[2]\right) & \longrightarrow & E'(K_v)/\phi(E(K_v)) & \xrightarrow{\hat\phi} & E(K_v)/2E(K_v) & \longrightarrow & E(K_v)/\phi(E(K_v)) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \kappa_v} & & \downarrow{\scriptstyle \kappa_v} & & \downarrow{\scriptstyle \kappa'_v} & & \\
0 & \longrightarrow & C'/\phi\left(E(K_v)[2]\right) & \longrightarrow & H^1(K_v, C) & \longrightarrow & H^1(K_v, E[2]) & \xrightarrow{\phi} & H^1(K_v, C') & &
\end{array}$$

is commutative, where the three rightmost vertical maps are the connecting maps recalled in Section 6.1 and the top sequence well known to be exact. (See Remark X.4.7 in [15] for example, where the statement is given for number fields but applies equally well to local fields.) The result then follows, since the distinguished local subgroups in (6.1) are defined to be the images of the three rightmost vertical maps in the diagram. □

Lemma 6.2 (Local duality)**.** *For each place v of K there is a local Tate pairing $H^1(K_v, C) \times H^1(K_v, C') \to \{\pm 1\}$ induced by a pairing $[\ ,\ ] : C \times C' \to \{\pm 1\}$ given by $[Q, \tilde R] = \langle Q, R\rangle$, where $\langle Q, R\rangle$ is the Weil pairing and R is any pre-image of $\tilde R$ under ϕ. The subgroups defining the local conditions $H^1_\phi(K_v, C)$ and $H^1_{\hat\phi}(K_v, C')$ are orthogonal complements under this pairing.*

Proof. Equation (7.15) and the immediately preceding comment in [3] tell us that the pairing $H^1(K_v, C) \times H^1(K_v, C') \to \{\pm 1\}$ is non-degenerate. The fact that $H^1_\phi(K_v, C)$ and $H^1_{\hat\phi}(K_v, C')$ are orthogonal to each other under this pairing is equation (7.17) in [3]. Counting dimensions of the terms in (6.1), we get that

$$\dim_{\mathbb{F}_2} H^1_\phi(K_v, C) + \dim_{\mathbb{F}_2} H^1_{\hat\phi}(K_v, C') = \dim_{\mathbb{F}_2} H^1_f(K_v, E[2]) + 2 - \dim_{\mathbb{F}_2} E(K_v)[2].$$

By part (v) of Lemma 2.5,

$$\dim_{\mathbb{F}_2} H^1_f(K_v, E[2]) + 2 - \dim_{\mathbb{F}_2} E(K_v)[2] = \dim_{\mathbb{F}_2} K_v^\times/(K_v^\times)^2 = \dim_{\mathbb{F}_2} H^1(K_v, C).$$

Combined with the non-degeneracy of the pairing, this shows that $H^1_\phi(K_v, C)$ and $H^1_{\hat\phi}(K_v, C')$ are not only orthogonal, but are in fact orthogonal complements. □

Definition 6.3. The ratio

$$\mathcal{T}(E/E') = \frac{\left|\mathrm{Sel}_\phi(E/K)\right|}{\left|\mathrm{Sel}_{\hat\phi}(E'/K)\right|}$$

is called the **Tamagawa ratio** of E.

The Tamagawa ratio can be computed using a local product formula.

Theorem 6.4 (Cassels)**.** *The Tamagawa ratio $\mathcal{T}(E/E')$ is given by*

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

Proof. This is a combination of Theorem 1.1 and equations (1.22) and (3.4) in [3]. Alternatively, this follows from combining Lemma 6.2 with Theorem 2 in [18]. □

We further have the following parity condition.

Theorem 6.5 (Dokchitser, Dokchitser)**.** *The 2-Selmer rank of E/K and* $\mathrm{ord}_2\mathcal{T}(E/E')$ *satisfy the parity condition*

$$d_2(E/K) \equiv \mathrm{ord}_2\mathcal{T}(E/E') \pmod 2.$$

Proof. This follows from Corollary 5.8 in [4]. The ratio $\frac{C_{E/K}}{C_{E'/K}}$ appearing there is defined by a local product over places of K whose terms are given by $\frac{|H^1_\phi(K_v,C)|}{2}$ (see Notation 5.1 there and recall from Section 6.1 that $H^1_\phi(K_v, C)$ is isomorphic to the cokernel of $\phi : E(K_v) \to E'(K_v)$). □

6.3. **Relationship between $H^1_\phi(K_v, C)$ and $H^1_{\phi^F}(K_v, C)$.** As noted earlier, if F/K is quadratic, then there is a canonical G_K-isomorphsim $E[2] \to E^F[2]$. If C is a subgroup of $E(K)$ of order 2, then we denote the image of C in $E^F(K)[2]$ by C^F. As the map $C^F \to C$ is G_K invariant, we can view $H^1_\phi(K_v, C^F)$ as a subgroup of $H^1(K_v, C)$ and $\mathrm{Sel}_\phi(E^F/K)$ as a subgroup of $H^1(K, C)$. This can be thought of as identifying both $H^1(K, C)$ and $H^1(K, C^F)$ with $K^\times/(K^\times)^2$ and both $H^1(K_v, C)$ and $H^1(K_v, C^F)$ with $K_v^\times/(K_v^\times)^2$. To avoid confusion, we make the following definition.

Definition 6.6. The distinguished local subgroup $H^1_{\phi^F}(K_v, C) \subset H^1(K_v, C)$ is the image of $E'^F(K_v)$ in $H^1(K_v, C)$ under the map κ_v. The distinguished local subgroup $H^1_{\hat\phi^F}(K_v, C') \subset H^1(K_v, C')$ is the image of $E^F(K_v)$ in $H^1(K_v, C')$ under the map κ'_v.

The following four lemmas are analogues of Lemma 2.7 that allow us to compare $H^1_\phi(K_v, C)$ and $H^1_{\phi^F}(K_v, C)$.

Lemma 6.7. *Suppose v is a prime away from 2 where E has good reduction and v is ramified in F/K. Then $H^1_{\phi^F}(K_v, C) = E'^F(K_v)[2]/\phi(E^F(K_v)[2])$.*

Proof. The proof is very similar to that of Lemma 2.8 and we therefore omit it. □

Lemma 6.8 (Criteria for equality of local conditions after twist)**.** *If any of the following conditions hold:*

(*i*) *v splits in F/K,*
(*ii*) *v is a prime away from 2 where E has good reduction and v is unramified in F/K,*
(*iii*) *v is a prime away from 2 where E has good reduction, v is ramified in F/K, and both $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$,*

then $H^1_\phi(K_v, C) = H^1_{\phi^F}(K_v, C)$ and $H^1_{\hat\phi}(K_v, C') = H^1_{\hat\phi^F}(K_v, C')$.

Proof.

(*i*) In this case $E \simeq E^F$ over K_v.
(*ii*) If v is a prime away from 2 where E has good reduction and v is unramified in F/K, then E^F also has good reduction at v. It then follows that both $H^1_{\phi^F}(K_v, C)$ and $H^1_\phi(K_v, C)$ are equal to $H^1_u(K_v, C)$ and both $H^1_{\hat\phi}(K_v, C')$ and $H^1_{\hat\phi^F}(K_v, C')$ are equal to $H^1_u(K_v, C')$.
(*iii*) Since both $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, Lemma 6.7 tells us that $H^1_{\phi^F}(K_v, C)$ is given by the image of C'^F in $H^1(K_v, C)$. We claim that this image is identical to that of C'. Indeed, if $\langle P\rangle = C'^F$, then $H^1_{\phi^F}(K_v, C)$ is generated by the cocycle $c(\sigma) = \sigma(R) - R$ where $R \in E^F[2]$ with $\phi(R) = P$. As $\sigma(R) \in E^F[2]$, we see that $c(\sigma) = 0$ if and only if σ fixes $E[2]$ and therefore $c = \chi_{\Delta_E}$. A similar calculation shows that the image of C' is generated by χ_{Δ_E} as well. As $H^1_\phi(K_v, C)$ and $H^1_{\phi^F}(K_v, C)$ both have dimension one, we get that they are equal. Exchanging the roles of E and E' then completes the result. □

Lemma 6.9. *Let $v \nmid 2$ be a prime at which E has good reduction and suppose both $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

(*i*) *If F/K is ramified at v, then $\dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C) = \dim_{\mathbb{F}_2} H^1_{\hat\phi^F}(K_v, C') = 1$ and both $H^1_\phi(K_v, C) \cap H^1_{\phi^F}(K_v, C) = 0$ and $H^1_{\hat\phi}(K_v, C') \cap H^1_{\hat\phi^F}(K_v, C') = 0$.*
(*ii*) *If F_1/K_v and F_2/K_v are distinct ramified quadratic extensions of K_v, then $H^1_{\phi^{F_1}}(K_v, C) \cap H^1_{\phi^{F_2}}(K_v, C) = 0$ and $H^1_{\hat\phi^{F_1}}(K_v, C') \cap H^1_{\hat\phi^{F_2}}(K_v, C') = 0$ as well.*

Proof. The fact that $H^1_{\phi^F}(K_v, C)$ and $H^1_{\hat\phi^F}(K_v, C')$ both have $\mathbb{F}_2$ dimension 1 is an immediate consequence of Lemma 6.7.

In the proof of Lemma 5.8 in [10], it is shown that the local subgroups $H^1_f(K_v, E[2])$, $H^1_f(K_v, E^{F_1}[2])$, and $H^1_f(K_v, E^{F_2}[2])$ have trivial pairwise intersection. Because $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, (3.1) shows that the map $H^1(K_v, C) \to H^1(K_v, E[2])$ is injective, and Proposition 6.1 therefore shows that $H^1_\phi(K_v, C)$, $H^1_{\phi^{F_1}}(K_v, C)$, and $H^1_{\phi^{F_2}}(K_v, C)$ have trivial pairwise intersection as well. Exchanging the roles of E and E' completes the result. □

Lemma 6.10. *Suppose E has good reduction at a prime $v \nmid 2$ and F/K is a quadratic extension ramified at v. If $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then $H^1_{\phi^F}(K_v, C) = 0$ and $H^1_{\hat\phi^F}(K_v, C') = H^1(K_v, C)$.*

Proof. This follows immediately from Lemmas 6.2 and 6.7. □

7. Controlling ϕ-Selmer rank under quadratic twist

In order to understand how $\mathrm{Sel}_\phi(E/K)$ and $\mathrm{Sel}_{\hat\phi}(E'/K)$ change under quadratic twist, we prove a pair of analogues of Theorem 2.9 for the ϕ-Selmer and $\hat\phi$-Selmer groups. Let T be a set of primes of K and define a pair of maps

$$\mathrm{Loc}_T : H^1(K,C) \to \bigoplus_{\mathfrak{p}\in T} H^1(K_\mathfrak{p},C) \text{ and } \mathrm{Loc}'_T : H^1(K,C') \to \bigoplus_{\mathfrak{p}\in T} H^1(K_\mathfrak{p},C')$$

as the sum of the restriction maps over the places $\mathfrak{p}$ in T.

Define restricted Selmer groups

$$\mathrm{Sel}_{\phi,T}(E/K) = \ker\left(\mathrm{Loc}_T : \mathrm{Sel}_\phi(E/K) \to \bigoplus_{v\in T} H^1(K_v,C)\right) \text{ and}$$

$$\mathrm{Sel}_{\hat\phi,T}(E'/K) = \ker\left(\mathrm{Loc}_T : \mathrm{Sel}_{\hat\phi}(E'/K) \to \bigoplus_{v\in T'} H^1(K_v,C')\right)$$

and relaxed Selmer groups

$$\mathrm{Sel}^T_\phi(E/K) = \ker\left(H^1(K,C) \to \bigoplus_{v\notin T} H^1(K_v,C)/H^1_\phi(K_v,C)\right) \text{ and}$$

$$\mathrm{Sel}^T_{\hat\phi}(E'/K) = \ker\left(H^1(K,C') \to \bigoplus_{v\notin T} H^1(K_v,C')/H^1_{\hat\phi}(K_v,C')\right).$$

We then have

Lemma 7.1. *Suppose that T is a set of places of K not containing any places dividing 2∞. Then*

$$\dim_{\mathbb{F}_2}\mathrm{Sel}^T_\phi(E/K)/\mathrm{Sel}_{\phi,T}(E/K) + \dim_{\mathbb{F}_2}\mathrm{Sel}^T_{\hat\phi}(E'/K)/\mathrm{Sel}_{\hat\phi,T}(E'/K) = 2|T|.$$

Proof. We first observe that by Lemma 6.2, the local conditions for $\mathrm{Sel}^T_\phi(E/K)$ are exactly dual to those of $\mathrm{Sel}_{\hat\phi,T}(E'/K)$ and that the local conditions for $\mathrm{Sel}^T_{\hat\phi}(E'/K)$ are exactly dual to those of $\mathrm{Sel}_{\phi,T}(E/K)$. We may therefore apply Theorem 2 in [18] and Theorem 6.4, which tell us that

$$\frac{|\mathrm{Sel}^T_\phi(E/K)|}{|\mathrm{Sel}_{\phi,T}(E/K)|}\cdot\frac{|\mathrm{Sel}^T_{\hat\phi}(E'/K)|}{|\mathrm{Sel}_{\hat\phi,T}(E'/K)|} = \frac{|\mathrm{Sel}^T_\phi(E/K)|}{|\mathrm{Sel}_{\hat\phi,T}(E'/K)|}\cdot\frac{|\mathrm{Sel}^T_{\hat\phi}(E'/K)|}{|\mathrm{Sel}_{\phi,T}(E/K)|}$$
$$= \prod_{v\notin T}\frac{|H^1_\phi(K_v,C)|}{2}\frac{|H^1_{\hat\phi}(K_v,C')|}{2}\prod_{v\in T}\frac{|H^1(K_v,C)|}{2}\frac{|H^1(K_v,C')|}{2}.$$

By Lemma 6.2, $|H^1_\phi(K_v,C)||H^1_{\hat\phi}(K_v,C')| = |H^1(K_v,C)|$ and for $v\in T$, we have $|H^1(K_v,C)| = 4$. We therefore get

$$\prod_{v\notin T}\frac{|H^1_\phi(K_v,C)|}{2}\frac{|H^1_{\hat\phi}(K_v,C')|}{2}\prod_{v\in T}\frac{|H^1(K_v,C)|}{2}\frac{|H^1(K_v,C')|}{2}$$
$$= 4^{|T|}\prod_{v\notin T}\frac{|H^1(K_v,C)|}{4} = 4^{|T|}\prod_v\frac{|H^1(K_v,C)|}{4} = 4^{|T|}\prod_v\frac{|K_v^\times/(K_v^\times)^2|}{4}.$$

By Proposition 6 in Section II.3 of [12], $|K_v^\times/(K_v^\times)^2| = \frac{4}{||4||_v}$. The product formula then gives $\prod_v \frac{|K_v^\times/(K_v^\times)^2|}{4} = \prod_v \left|\left|\frac{1}{4}\right|\right|_v = 1$, yielding the result. □

Theorem 7.2. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and suppose that F/K is a quadratic extension such that all places above $2\Delta_E\infty$ split in F/K and $E'(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ for all primes $\mathfrak{p}$ ramified in F/K. Let T be the set of primes ramified in F/K where $E(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Letting $V_T = \mathrm{Loc}_T(\mathrm{Sel}_\phi(E/K))$, we get that*

$$d_\phi(E^F/K) = d_\phi(E/K) - \dim_{\mathbb{F}_2} V_T \text{ and} \tag{7.1}$$

$$d_{\hat\phi}(E'^F/K) = d_{\hat\phi}(E'/K) - \dim_{\mathbb{F}_2} V_T + |T|. \tag{7.2}$$

Proof. By Lemmas 6.8 and 6.10, the local conditions for $\mathrm{Sel}_\phi(E^F/K)$ are identical to those for $\mathrm{Sel}_\phi(E/K)$ for all places not in T and equal to zero for all places in T. We therefore see that $\mathrm{Sel}_\phi(E^F/K) = \mathrm{Sel}_{\phi,T}(E/K)$ and it then follows that $\dim_{\mathbb{F}_2} V_T = \dim_{\mathbb{F}_2}\mathrm{Sel}_\phi(E/K) - \dim_{\mathbb{F}_2}\mathrm{Sel}_{\phi,T}(E/K)$, giving (7.1). By Theorem 6.4, we get that

$$\begin{aligned} &d_\phi(E^F/K) - d_{\hat\phi}(E'^F/K) \\ &\quad = d_\phi(E/K) - d_{\hat\phi}(E'/K) - \sum_{v \text{ of } K} \dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C) - \dim_{\mathbb{F}_2} H^1_\phi(K_v, C). \end{aligned}$$

By Lemma 6.8, we get that $\dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C) - \dim_{\mathbb{F}_2} H^1_\phi(K_v, C) = 0$ for all $v \notin T$. By Lemma 6.10 combined with the fact that $H^1_\phi(K_v, C) = H^1_u(K_v, C)$ at primes $v \nmid 2$ where E has good reduction, we see that $\dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C) - \dim_{\mathbb{F}_2} H^1_\phi(K_v, C) = -1$ for $v \in T$. Combined with (7.1) we get (7.2). □

Theorem 7.3. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and suppose that F/K is a quadratic extension such that all places above $2\Delta_E\infty$ split in F/K and $\dim_{\mathbb{F}_2} E(K_\mathfrak{p})[2] = \dim_{\mathbb{F}_2} E'(K_\mathfrak{p})[2]$ for all primes $\mathfrak{p}$ ramified in F/K.*

Let T be the set of primes ramified in F/K where $E(K_\mathfrak{p})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Letting $V_T = \mathrm{Loc}_T(\mathrm{Sel}_\phi(E/K))$ and $V'_T = \mathrm{Loc}'_T(\mathrm{Sel}_{\hat\phi}(E'/K))$, we then have

$$\begin{aligned} d_\phi(E^F/K) &= d_\phi(E/K) - \dim_{\mathbb{F}_2} V_T + d \text{ and} \\ d_{\hat\phi}(E'^F/K) &= d_{\hat\phi}(E'/K) - \dim_{\mathbb{F}_2} V'_T + d' \end{aligned}$$

for some d and d' satisfying

$$0 \le d + d' \le \dim_{\mathbb{F}_2}\left(\bigoplus_{\mathfrak{p}\in T} H^1_u(K_\mathfrak{p}, C)\right)/V_T + \dim_{\mathbb{F}_2}\left(\bigoplus_{\mathfrak{p}\in T} H^1_u(K_\mathfrak{p}, C')\right)/V'_T \tag{7.3}$$

and

$$d - d' = \dim_{\mathbb{F}_2} V_T - \dim_{\mathbb{F}_2} V'_T. \tag{7.4}$$

Proof. Define $V_T^F = \mathrm{Loc}_T(\mathrm{Sel}_\phi(E^F/K))$ and $V_T'^F = \mathrm{Loc}'_T(\mathrm{Sel}_{\hat\phi}(E'^F/K))$. By Lemma 6.8 the local subgroups $H^1_\phi(K_v, C)$ and $H^1_\phi(K_v, C^F)$ are equal for all v not in T and the same holds for the local subgroups $H^1_{\hat\phi}(K_v, C')$ and $H^1_{\hat\phi^F}(K_v, C')$.

We therefore get that the four sequences

$$0 \to \mathrm{Sel}_{\phi,T}(E/K) \to \mathrm{Sel}_{\phi}(E/K) \to V_T \to 0, \tag{7.5}$$

$$0 \to \mathrm{Sel}_{\phi,T}(E/K) \to \mathrm{Sel}_{\phi}(E^F/K) \to V_T^F \to 0, \tag{7.6}$$

$$0 \to \mathrm{Sel}_{\hat{\phi},T}(E'/K) \to \mathrm{Sel}_{\hat{\phi}}(E'/K) \to V'_T \to 0, \tag{7.7}$$

$$0 \to \mathrm{Sel}_{\hat{\phi},T}(E'/K) \to \mathrm{Sel}_{\hat{\phi}}(E'^F/K) \to V_T'^F \to 0 \tag{7.8}$$

are exact. Combining (7.5) and (7.6), we get

$$d_\phi(E^F/K) = d_\phi(E/K) - \dim_{\mathbb{F}_2} V_T + \dim_{\mathbb{F}_2} V_T^F, \tag{7.9}$$

and combining (7.7) and (7.8), we get

$$d_{\hat{\phi}}(E'^F/K) = d_{\hat{\phi}}(E'/K) - \dim_{\mathbb{F}_2} V'_T + \dim_{\mathbb{F}_2} V_T'^F. \tag{7.10}$$

By Lemma 6.8, the local conditions for $\mathrm{Sel}_\phi(E/K)$ and $\mathrm{Sel}_\phi(E^F/K)$ are the same for all places not in T so $\mathrm{Sel}_\phi(E/K) + \mathrm{Sel}_\phi(E^F/K) \subset \mathrm{Sel}_\phi^T(E/K)$. By Lemma 6.9, we also get that $\mathrm{Sel}_\phi(E/K) \cap \mathrm{Sel}_\phi(E^F/K) = \mathrm{Sel}_{\phi,T}(E/K)$. We therefore have

$$\begin{aligned} &\dim_{\mathbb{F}_2} V_T + \dim_{\mathbb{F}_2} V_T^F \\ &\quad = \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E/K)/\mathrm{Sel}_{\phi,T}(E/K) + \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi(E^F/K)/\mathrm{Sel}_{\phi,T}(E/K) \\ &\qquad \le \dim_{\mathbb{F}_2} \mathrm{Sel}_\phi^T(E/K)/\mathrm{Sel}_{\phi,T}(E/K). \end{aligned} \tag{7.11}$$

We similarly get that $\dim_{\mathbb{F}_2} V'_T + \dim_{\mathbb{F}_2} V_T'^F \le \dim_{\mathbb{F}_2} \mathrm{Sel}_{\hat{\phi}}^T(E'/K)/\mathrm{Sel}_{\hat{\phi},T}(E'/K)$, and Lemma 7.1 then shows that

$$\dim_{\mathbb{F}_2} V_T^F + \dim_{\mathbb{F}_2} V_T'^F \le 2|T| - \dim_{\mathbb{F}_2} V_T - \dim_{\mathbb{F}_2} V'_T. \tag{7.12}$$

Set $d = \dim_{\mathbb{F}_2} V_T^F$ and $d' = \dim_{\mathbb{F}_2} V_T'^F$. For each $\mathfrak{p} \in T$, the unramified local subgroups $H^1_u(K_\mathfrak{p}, C)$ and $H^1_u(K_\mathfrak{p}, C)$ have dimension one. We therefore have that

$$\begin{aligned} &\dim_{\mathbb{F}_2} \left(\bigoplus_{\mathfrak{p}\in T} H^1_u(K_\mathfrak{p}, C) \right) / V_T + \dim_{\mathbb{F}_2} \left(\bigoplus_{\mathfrak{p}\in T} H^1_u(K_\mathfrak{p}, C') \right) / V'_T \\ &\qquad = 2|T| - \dim_{\mathbb{F}_2} V_T - \dim_{\mathbb{F}_2} V'_T. \end{aligned}$$

Combining this with (7.12) leads to (7.3).

To see (7.4), we observe that $\dim_{\mathbb{F}_2} H^1_\phi(K_v, C) = \dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C)$ for every v of K. Theorem 6.4 then tells us that

$$d_\phi(E^F/K) - d_{\hat{\phi}}(E'^F/K) = d_\phi(E/K) - d_{\hat{\phi}}(E'/K)$$

and (7.4) follows immediately. □

We get a few easy corollaries.

Corollary 7.4. *Let F/K be a quadratic extension in which all places above $2\Delta_E\infty$ split completely and suppose F/K is ramified at exactly two primes, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, such that $E(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E'(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$.*

If $\dim_{\mathbb{F}_2} \mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(\mathrm{Sel}_\phi(E/K)) = 1$ and $\dim_{\mathbb{F}_2} \mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(\mathrm{Sel}_2(E/K)) = 2$, then $d_\phi(E^F/K) = d_\phi(E/K) - 1$, $d_{\hat{\phi}}(E'^F/K) = d_{\hat{\phi}}(E'/K) + 1$, and either $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) - 2$.

Proof. By Theorem 2.9, either $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) - 2$. Applying Theorem 7.2 with $T = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ gives the result. □

Corollary 7.5. *Let F/K be a quadratic extension in which all places above $2\Delta_E\infty$ split completely and suppose F/K is ramified at exactly two primes, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, such that $E(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and $E'(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Assuming that $\mathrm{res}_{\mathfrak{p}_1}(c) \neq 0$ if and only if $\mathrm{res}_{\mathfrak{p}_2}(c) \neq 0$ for every $c \in \mathrm{Sel}_2(E/K)$ and $c \in \mathrm{Sel}_{\hat{\phi}}(E/K)$, we get $d_\phi(E^F/K) = d_\phi(E/K)+2-i$ and $d_{\hat{\phi}}(E'^F/K) = d_{\hat{\phi}}(E'/K)-i$ for some $i \in \{0,1\}$, and either $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K)+2$.*

Proof. The assumption that $\mathrm{res}_{\mathfrak{p}_1}(c) \neq 0$ if and only if $\mathrm{res}_{\mathfrak{p}_2}(c) \neq 0$ for every $c \in \mathrm{Sel}_2(E/K)$ and $c \in \mathrm{Sel}_{\hat{\phi}}(E/K)$ ensures that both $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(\mathrm{Sel}_2(E/K))$ and $\mathrm{Loc}'_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(\mathrm{Sel}_{\hat{\phi}}(E'/K))$ have codimension at least one. Applying Theorem 2.9, we therefore get that either $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K)+2$.

We next apply Theorem 7.2 with the roles of E and E' reversed and $T = \{\mathfrak{p}_1,\mathfrak{p}_2\}$. Because the codimension of $\mathrm{Loc}'_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}(\mathrm{Sel}_{\hat{\phi}}(E'/K))$ is at least one, we get that $\dim_{\mathbb{F}_2}\mathrm{Loc}'_T(\mathrm{Sel}_{\hat{\phi}}(E'/K)) \in \{0,1\}$ and the result follows. □

Corollary 7.6. *Let F/K be a quadratic extension in which all places above $2\Delta_E\infty$ split completely and suppose F/K is ramified at exactly three primes, two of which, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, have $E(K_{\mathfrak{p}_i})[2] \simeq E'(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and the third of which, $\mathfrak{p}_3$, has $E(K_{\mathfrak{p}_3})[2] \simeq E'(K_{\mathfrak{p}_3})[2] \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. If both $\mathrm{Sel}_\phi(E/K)$ and $\mathrm{Sel}_{\hat{\phi}}(E'/K)$ restrict non-trivially at $\mathfrak{p}_3$ and $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}}(\mathrm{Sel}_2(E/K)) \in \{2,3\}$, then we have $d_\phi(E^F/K) = d_\phi(E/K)-1$, $d_{\hat{\phi}}(E'^F/K) = d_{\hat{\phi}}(E'/K)-1$, and we either get $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K)-2$.*

Proof. First off, we note that by Theorem 2.9, we either get $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K)-2$. We then apply Theorem 7.3 with $T = \{\mathfrak{p}_3\}$. The result follows from observing that $d+d' = 0$. □

Corollary 7.7. *Suppose that F_1/K and F_2/K are quadratic extensions in which all places above $2\Delta_E\infty$ split completely with F_1/K ramified as a single prime $\mathfrak{q}$ and F_2/K ramified at three primes $\mathfrak{q}$, $\mathfrak{p}_1$, and $\mathfrak{p}_2$, with $E(K_{\mathfrak{p}_i})[2] \simeq E'(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$, $E(K_{\mathfrak{q}})[2] \simeq E'(K_{\mathfrak{q}})[2] \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Further suppose that the two ramified local extensions $F_{1,\mathfrak{q}_1}/K_{\mathfrak{q}}$ and $F_{2,\mathfrak{q}_2}/K_{\mathfrak{q}}$ of $K_{\mathfrak{q}}$ are distinct.*

If $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}\mathrm{Sel}_2(E/K) = 1$ and $\mathrm{Sel}_2(E/K)$, $\mathrm{Sel}_\phi(E/K)$, and $\mathrm{Sel}_{\hat{\phi}}(E'/K)$ all have trivial restriction at $\mathfrak{q}$, then $d_2(E^{F_i}/K) - d_2(E/K) \in \{0,2\}$ and either

$$d_\phi(E^{F_1}/K) = d_\phi(E/K)+1, d_{\hat{\phi}}(E'^{F_1}/K) = d_{\hat{\phi}}(E'/K)+1$$

and

$$d_\phi(E^{F_2}/K) = d_\phi(E/K), d_{\hat{\phi}}(E'^{F_2}/K) = d_{\hat{\phi}}(E'/K)$$

or

$$d_\phi(E^{F_1}/K) = d_\phi(E/K), d_{\hat{\phi}}(E'^{F_1}/K) = d_{\hat{\phi}}(E'/K)$$

and

$$d_\phi(E^{F_2}/K) = d_\phi(E/K)+1, d_{\hat{\phi}}(E'^{F_2}/K) = d_{\hat{\phi}}(E'/K)+1.$$

Proof. The fact that $d_2(E^{F_i}/K) - d_2(E/K) \in \{0,2\}$ follows from Theorem 2.9.

We now apply Theorem 7.3 to both E^{F_1} and E^{F_2} with $T = \{\mathfrak{q}\}$, showing that $d_\phi(E^{F_i}/K) = d_\phi(E/K)+d_i$ and $d_{\hat{\phi}}(E'^{F_i}/K) = d_{\hat{\phi}}(E'/K)+d'_i$ for some d_i and d'_i satisfying $d_i+d'_i \leq 2$ and $d_i-d'_i = 0$. We would like to show that either $d_1 = d'_1 = 1$ and $d_2 = d'_2 = 0$ or $d_1 = d'_1 = 0$ and $d_2 = d'_2 = 1$.

We note that by Lemma 7.1, we have

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_{\phi}^{T}(E/K)/\mathrm{Sel}_{\phi,T}(E/K)+\dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}^{T}(E'/K)/\mathrm{Sel}_{\hat{\phi},T}(E'/K)=2.$$

We further note that as $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_{\phi}(E/K))=0$, we get $\mathrm{Sel}_{\phi}(E/K)=\mathrm{Sel}_{\phi,T}(E/K)$, and therefore

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_{\phi}^{T}(E/K)/\mathrm{Sel}_{\phi,T}(E/K)=\dim_{\mathbb{F}_2}\mathrm{Sel}_{\phi}^{T}(E/K)/\mathrm{Sel}_{\phi}(E/K)\leq 1.$$

Similar reasoning shows that $\dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}^{T}(E'/K)/\mathrm{Sel}_{\hat{\phi},T}(E'/K)\leq 1$, and we therefore get that

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_{\phi}^{T}(E/K)/\mathrm{Sel}_{\phi,T}(E/K)=\dim_{\mathbb{F}_2}\mathrm{Sel}_{\hat{\phi}}^{T}(E'/K)/\mathrm{Sel}_{\hat{\phi},T}(E'/K)=1.$$

Because $\mathrm{Sel}_{\phi,T}(E/K)\subset\mathrm{Sel}_{\phi}(E^{F_i}/K)\subset\mathrm{Sel}_{\phi}^{T}(E/K)$, we see that $d_i=1$ exactly when $\mathrm{Sel}_{\phi}(E^{F_i}/K)=\mathrm{Sel}_{\phi}^{T}(E/K)$. As $\dim_{\mathbb{F}_2}\mathrm{Sel}_{\phi}^{T}(E/K)/\mathrm{Sel}_{\phi,T}(E/K)=1$, we see that $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_{\phi}^{T}(E/K))$ is a one-dimensional subspace of $H^1(K_{\mathfrak{q}},C)$ and we therefore have $\mathrm{Sel}_{\phi}(E^{F_i}/K)=\mathrm{Sel}_{\phi}^{T}(E/K)$ exactly when $H^1_{\phi^{F_i}}(K_{\mathfrak{q}},C)=\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_{\phi}^{T}(E/K))$. Moreover, since $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_{\phi}(E/K))=0$, we see that $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_{\phi}^{T}(E/K))$ is one of the two one-dimensional ramified subspaces of $H^1(K_{\mathfrak{q}},C)$. The result then follows from Lemma 6.9, which shows that $H^1_{\phi^{F_1}}(K_{\mathfrak{q}},C)$ and $H^1_{\phi^{F_2}}(K_{\mathfrak{q}},C)$ are distinct one-dimensional ramified subspaces of $H^1(K_{\mathfrak{q}},C)$. □

8. Twists with reduced 2-Selmer rank

In this section, we will assume that $E(K)[2]\simeq\mathbb{Z}/2\mathbb{Z}$ and let $M=K(E[2])$ and $M'=K(E'[2])$.

As we saw with Proposition 5.6, if the image of $\mathrm{Sel}_{\phi}(E/K)$ in $\mathrm{Sel}_2(E/K)$ has codimension at least three, then we can construct a quadratic twist E^F of E with $d_2(E^F/K)=d_2(E/K)-2$. We will show that in most cases, it is possible to find a quadratic twist E^L of E such that either $d_2(E^L/K)=d_2(E/K)-2$ or that $d_2(E^L/K)=d_2(E/K)$ and E^L satisfies the hypotheses of Proposition 5.6.

Lemma 8.1. *Suppose that $c\in\mathrm{Sel}_{\phi}(E/K)$ is not in the image of C' under the map κ in (3.1). If N is the quadratic extension cut out by the character c, then $N\cap M=K$.*

Proof. Observe that $C'=\phi(E[2])$. By the exactness of (3.1), the restriction of the image of C' in $H^1(K,C)$ to M is trivial. We therefore see that the non-trivial element of C' maps to the quadratic character in $\mathrm{Sel}_{\phi}(E/K)$ which cuts out the extension M. Therefore, if c is not in the image of C', it must be the case that $N\neq M$. As both are quadratic extensions of K, we then get that $N\cap M=K$. □

Proposition 8.2. *Suppose that E does not have a cyclic 4-isogeny ψ defined over M with $E(K)[2]\subset\ker\psi$. If $d_{\phi}(E/K)\geq 2$, then there is a quadratic extension F/K satifying the hypotheses of Corollary 7.4.*

In particular, E has a quadratic twist E^F such that $d_{\phi}(E^F/K)=d_{\phi}(E/K)-1$ and either $d_2(E^F/K)=d_2(E/K)$ or $d_2(E^F/K)=d_2(E/K)-2$.

Proof. Let $C=\langle P\rangle$ take $c\in\mathrm{Sel}_2(E/K)$ to be the image of P under the map κ in (2.1) and take the cocycle representative $\hat{c}:G_K\to E[2]$ for c defined by $\hat{c}(\sigma)=\sigma(R)-R$ where $R\in E(\overline{K})$ with $2R=P$.

Because we are working under the assumption that E does not have a cyclic 4-isogeny defined over M whose kernel contains $E(K)[2]$, there is some $\tau \in G_M$ such that $\hat{c}(\tau) \notin C$. Applying ϕ to $\hat{c}(\tau) = \tau(R) - R$, we then see that $\tau(\phi(R)) \neq \phi(R)$. As $\phi(R) \in E'[2]$, this shows that $\tau\big|_{M'} \neq 1$.

Because $d_\phi(E/K) \geq 2$, we can find $b \in \mathrm{Sel}_\phi(E/K)$ such that b is not in the image of C' under the map κ in (3.1). Let N_b be the quadratic extension cut out by the character b. Applying Lemma 8.1, we therefore have $N_b \cap M = K$ and we can therefore find $\gamma \in G_K$ such that $\gamma\big|_{MM'} = \tau$ and $\gamma\big|_{N_b} \neq 1$.

Let N be a finite Galois extension of K containing $MM'N_bK(8\Delta_E\infty)$ such that the restrictions of $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_\phi(E/K)$ to N are zero. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be primes of K away from 2 where E has good reduction such that $\mathrm{Frob}_{\mathfrak{p}_1}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of $\gamma\big|_N$ and $\mathrm{Frob}_{\mathfrak{p}_2}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of $\gamma^{-1}\big|_N$. Since $\gamma\gamma^{-1}\big|_{K(8\Delta_E\infty)} = 1$, $\mathfrak{p}_1\mathfrak{p}_2$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta_E}$. Letting $F = K(\sqrt{\pi})$, we get that all places dividing $2\Delta_E\infty$ split in F/K, and that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the only primes that ramify in F/K.

As $\mathrm{Frob}_{\mathfrak{p}_1}\big|_M = \gamma\big|_M = 1$, we get that $E(K_{\mathfrak{p}_1})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and as $\mathrm{Frob}_{\mathfrak{p}_1}\big|_{M'} = \gamma\big|_M \neq 1$, we get that $E'(K_{\mathfrak{p}_1})[2] \simeq \mathbb{Z}/2\mathbb{Z}$. A similar argument with γ^{-1} shows that $E(K_{\mathfrak{p}_2})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E'(K_{\mathfrak{p}_2})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ using the fact that $\mathrm{Frob}_{\mathfrak{p}_2}\big|_N = \gamma^{-1}$.

By our choice of γ, we have $b(\gamma) \neq 0$, and as $\mathrm{Frob}_{\mathfrak{p}_1}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of $\gamma\big|_N$, we therefore get that $\mathrm{res}_{\mathfrak{p}_1}(b) \neq 0$ and therefore that $\dim_{\mathbb{F}_2}\mathrm{res}_{\mathfrak{p}_1}\mathrm{Sel}_\phi(E/K) \neq 0$. Since $\mathrm{res}_{\mathfrak{p}_1}(\mathrm{Sel}_\phi(E/K)) \subset H^1_u(K_v, C)$ and $H^1_u(K_v, C)$ is one-dimensional, it follows that $\dim_{\mathbb{F}_2}\mathrm{res}_{\mathfrak{p}_1}\mathrm{Sel}_\phi(E/K) = 1$.

Let $\tilde{b}$ be the image of b in $\mathrm{Sel}_2(E/K)$. As $\tilde{b}(\gamma) = b(\gamma) \neq 0$, we see that $\tilde{b}(\gamma)$ generates $C \subset E[2]$. As $c(\gamma) = c(\tau) \notin C$, we therefore see that $\tilde{b}(\gamma)$ and $c(\gamma)$ generate $E[2]$. As $\mathrm{Frob}_{\mathfrak{p}_1}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of $\gamma\big|_N$, Lemma 5.1 tells us that the map $\mathrm{res}_{\mathfrak{p}_1}$ is given by evaluation at γ. We therefore get that $\dim_{\mathbb{F}_2}\mathrm{res}_{\mathfrak{p}_1}\mathrm{Sel}_2(E/K) = 2$.

As $\mathrm{Frob}_{\mathfrak{p}_2}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of $\gamma^{-1}\big|_N$, Lemma 5.1 tells us that the restriction map $\mathrm{res}_{\mathfrak{p}_2}$ is given by evaluation at γ^{-1} and the localization map $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}} : \mathrm{Sel}_2(E/K) \to E[2] \times E[2]$ is therefore given by $c \mapsto (\hat{c}(\gamma), \hat{c}(\gamma^{-1}))$, where $\hat{c}$ is any cocycle representative for c. As $E[2]$ has exponent 2, $\hat{c}(\gamma) = \hat{c}(\gamma)^{-1} = \hat{c}(\gamma^{-1})$, and we therefore get that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}\mathrm{Sel}_2(E/K)$ is contained in the diagonal subgroup of $E[2] \times E[2]$. A similar argument show that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}\mathrm{Sel}_\phi(E/K)$ is contained in the diagonal subgroup of $C \times C$.

Therefore,

$$\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}\mathrm{Sel}_\phi(E/K) = 1 \quad \text{and} \quad \dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}\mathrm{Sel}_2(E/K) = 2,$$

yielding the result. □

Corollary 8.3. *Suppose that E does not have a cyclic 4-isogeny ψ defined over M with $E(K)[2] \subset \ker\psi$. If $d_2(E/K) \geq 2$, then E has a twist E^F such that $d_2(E^F/K) = d_2(E/K) - 2$.*

Proof. We iteratively apply Proposition 8.2 until either $d_2(E^F/K) = d_2(E/K) - 2$ or $d_\phi(E^F/K) = 1$. (Note that the total number of iterations may be zero in the case where $d_\phi(E/K) = 1$ and the hypotheses of Proposition 8.2 are not satisfied.) If we terminate with $d_2(E^F/K) = d_2(E/K) - 2$, then we are done.

Otherwise, if $d_\phi(E^F/K) = 1$ and $d_2(E^F/K) = d_2(E/K) - 2$, we observe that E^F satisfies the hypotheses of Proposition 5.6 and E^F therefore has a twist $E^{F'}$ such that $d_2(E^{F'}/K) = d_2(E^F/K) - 2 = d_2(E/K) - 2$. □

We now give a numeric example to show how the proof of Proposition 8.2 can be used to construct an extension in practice.

Example 8.4. Take E given by the equation $y^2 = x^3 - 15x^2 + 5x$ as in Example 2.13. In this instance, $d_2(E/\mathbb{Q}) = 2$, $d_\phi(E/\mathbb{Q}) = 3$, and $d_{\hat\phi}(E/\mathbb{Q}) = 1$.

We have $M = \mathbb{Q}(\sqrt{205})$, $M' = \mathbb{Q}(\sqrt{5})$. By the calculation in Example 2.13, we see that $\mathrm{Sel}_2(E/\mathbb{Q})$ is generated by the quadratic characters χ_{-1}, χ_5, and the element c which is the image of the point $P = (0,0)$ under the Kummer map κ. As explained at the beginning of Section 2, c is represented by the cocycle $\hat c$ defined by $\hat c(\sigma) = \sigma(R) - R$, where R is any point in $E(\overline{\mathbb{Q}})$ with $2R = P$. The cohomology class c therefore trivializes in any extension of $\mathbb{Q}$ which contains a two-division point of P. A calculation in **magma** shows that the minimal such extension is the field $K = \mathbb{Q}[x]/(x^4 + 150x^2 + 5125)$. The splitting field L of the set of polynomials $S = \{x^2 + 1, x^2 - 5, x^2 - 41, x^4 + 150x^2 + 5125\}$ is therefore a Galois extension containing M and M' in which $\mathrm{Sel}_2(E/\mathbb{Q})$ trivializes.

As a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, $\mathrm{Sel}_\phi(E/\mathbb{Q})$ is generated by $\{-1, 5, 41\}$, and the image of C' is generated by the class of $205 = 5{\cdot}41$. We therefore take $b \in \mathrm{Sel}_\phi(E/\mathbb{Q})$ to be the class of -1. If we take $\mathfrak{p}_1 = 7$, we see that $\left(\frac{205}{7}\right) = 1$, $\left(\frac{5}{7}\right) = -1$, and $\left(\frac{-1}{7}\right) = -1$, telling us that $\mathrm{Frob}_7\big|_M = 1$, $\mathrm{Frob}_7\big|_{M'} = -1$, and $\mathrm{Frob}_{\{7\}}\big|_{N_b} = -1$. This shows us that $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{7\}}\mathrm{Sel}_\phi(E/\mathbb{Q}) = 1$.

We now wish to show that $\dim_{\mathbb{F}_2}\mathrm{Loc}_7\mathrm{Sel}_2(E/\mathbb{Q}) = 2$. Letting $\tilde b$ be the image of b in $\mathrm{Sel}_2(E/\mathbb{Q})$, we see that $\mathrm{res}_7\tilde b$ is non-trivial and $\mathrm{res}_7\tilde b$ therefore generates $C = \langle P\rangle \subset E[2] \simeq H^1_u(\mathbb{Q}_7, E[2])$. We therefore only need to show that $\mathrm{res}_7(c)$ as given by $\hat c(\mathrm{Frob}_7)$ generates $E[2]/C$. Let τ be in the class of Frob_7 in $\mathrm{Gal}(L/\mathbb{Q})$ and fix a two-division point R of $P \in K$. A computation in **magma** shows that $Q = \phi(R) \in E'[2]$ is defined over the extension $H = \mathbb{Q}[x]/(x^2 - 5) \subset K$ but not over $\mathbb{Q}$. Since 7 is inert in O_H, we see that $\tau(Q) \neq Q$. We then get that

$$\phi(\hat c(\tau)) = \phi(\tau(R) - R) = \tau(\phi(R)) - R = \tau(Q) - Q \neq 0,$$

and it follows that $\mathrm{res}_7(c) = \hat c(\tau)$ generates $E[2]/C$.

We now need to find $\mathfrak{p}_2$. The primes where E has bad reduction are given by 2, 5, and 41. We therefore need to find $\mathfrak{p}_2$ such that $\mathfrak{p}_1\mathfrak{p}_2 \equiv 1 \pmod{8 \cdot 5 \cdot 41}$ and $\mathrm{Frob}_{p_1}\big|_L = \mathrm{Frob}_{p_2}\big|_L$. The latter condition is equivalent to the polynomials in S having the same splitting behavior modulo $\mathfrak{p}_2$ as they do modulo 7. We find that taking $\mathfrak{p}_2 = 5263$ satisfies all of these conditions.

Taking $d = 7 \cdot 5623 = 39361$, we get $d_2(E^d/\mathbb{Q}) = 2$, $d_\phi(E^d/\mathbb{Q}) = 2$, and $d_{\hat\phi}(E'^d/\mathbb{Q}) = 2$, a result consistent with Proposition 8.2.

The case where E has a cyclic 4-isogeny defined over M whose kernel contains $E(K)[2]$ is more complicated, but we are able to prove the following.

Proposition 8.5. *Suppose E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over M but not over K. If both $d_\phi(E/K) \geq 2$ and $d_{\hat\phi}(E'/K) \geq 2$, then there is a quadratic extension F/K satifying the hypotheses of Corollary 7.6. In particular, E has a twist E^F with $d_\phi(E^F/K) = d_\phi(E/K) - 1$, $d_{\hat\phi}(E'^F/K) = d_{\hat\phi}(E'/K) - 1$, and either $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) - 2$.*

Proof. As above, let $C = \langle P \rangle$, let $c \in \mathrm{Sel}_2(E/K)$ be the image of P under the map κ in (2.1) and let $\hat{c} : G_K \to E[2]$ defined by $\hat{c}(\sigma) = \sigma(R) - R$ where $R \in E(\overline{K})$ with $2R = P$ be a cocycle representative for c.

Since E does not have a cyclic 4-isogeny defined over K, there exists $\tau_1 \in G_K$ with $\hat{c}(\tau_1) \notin C$. Applying ϕ to $\hat{c}(\tau_1)$, we find that $\tau_1(\phi(R)) \neq \phi(R)$ and therefore that $\tau_1 \notin G_{M'}$, as $\phi(R) \in E'[2]$. However, by Lemma 4.2, we have $M = M'$ and therefore $\tau_1\big|_M \neq 1$.

As both $d_\phi(E/K) \geq 2$ and $d_{\hat{\phi}}(E'/K) \geq 2$, we are able to find $b \in \mathrm{Sel}_\phi(E/K)$ and $b' \in \mathrm{Sel}_{\hat{\phi}}(E'/K)$ such that b and b' are not in the images of C' and C respectively under the map κ in (3.1). Letting N_b and $N_{b'}$ be the (not necessarily distinct) quadratic extensions cut out by the characters b and b' respectively, we therefore get $N_b \cap M = K$ and $N_{b'} \cap M = K$ by applying Lemma 8.1. We can therefore find $\tau_3 \in G_K$ such that $\tau_3\big|_M = 1$, $\tau_3\big|_{N_b} \neq 1$, and $\tau_3\big|_{N_{b'}} \neq 1$. We next set $\tau_2 = (\tau_3\tau_1)^{-1}$ and observe that $\tau_2\big|_M \neq 1$.

Let N be a finite Galois extension of K containing $MN_bN_{b'}K(8\Delta_E\infty)$ such that the restrictions of $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_\phi(E/K)$ to N are zero. Let $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ be primes of K away from 2 where E has good reduction such that $\mathrm{Frob}_{\mathfrak{p}_i}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of $\tau_i\big|_N$.

As $\tau_1\tau_2\tau_3\big|_{K(8\Delta_E\infty)} = 1$, $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta_E}$. Letting $F = K(\sqrt{\pi})$, we get that all places dividing $2\Delta_E\infty$ split in F/K, and that $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ are the only primes that ramify in F/K.

By our choice of τ_3, we see that $\mathrm{res}_{\mathfrak{p}_3}(b)$ and $\mathrm{res}_{\mathfrak{p}_3}(b')$ are non-trivial and therefore that $\mathrm{res}_{\mathfrak{p}_3}\mathrm{Sel}_\phi(E/K)$ and $\mathrm{res}_{\mathfrak{p}_3}\mathrm{Sel}_{\hat{\phi}}(E'/K)$ are both non-trivial.

Next, as $\mathrm{Frob}_{\mathfrak{p}_i}\big|_M = \tau_i$, we have $E(K_{\mathfrak{p}_1})[2] \simeq \mathbb{Z}/2\mathbb{Z}$, $E(K_{\mathfrak{p}_2})[2] \simeq \mathbb{Z}/2\mathbb{Z}$, and $E(K_{\mathfrak{p}_3})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and by Lemma 2.6 we get that $H^1_f(K_{\mathfrak{p}_1}, E[2]) \simeq E[2]/C$, $H^1_f(K_{\mathfrak{p}_2}, E[2]) \simeq E[2]/C$, and $H^1_f(K_{\mathfrak{p}_3}, E[2]) \simeq E[2]$. Applying Lemma 5.1, we get that the localization map $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}} : \mathrm{Sel}_2(E/K) \to E[2]/C \times E[2]/C \times E[2]$ is given by $c_0 \mapsto (\hat{c}_0(\tau_i))$, where $\hat{c}_0$ is any cocycle representative for c_0.

Let $\tilde{b} \in \mathrm{Sel}_2(E/K)$ be the image of b under the map κ in (3.1). As $\tilde{b}(\tau_i) = b(\tau_i)$, we see that $\tilde{b}(\tau_i) \in C \subset E[2]$. It therefore follows that $\mathrm{res}_{\mathfrak{p}_1}(\tilde{b}) = \mathrm{res}_{\mathfrak{p}_2}(\tilde{b}) = 0$, since both $H^1_f(K_{\mathfrak{p}_1}, E[2])$ and $H^1_f(K_{\mathfrak{p}_2}, E[2])$ are isomorphic to $E[2]/C$. As $\tau_3\big|_{N_b} \neq 1$, we therefore get that $b(\tau_3)$ generates C and therefore that $\tilde{b}(\tau_3) = P$. We therefore get that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}}(\tilde{b}) = (0, 0, P)$.

The element τ_1 was chosen so that $\mathrm{res}_{\mathfrak{p}_1}(c) \neq 0$. In particular, this says that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}}(c) \notin \langle (0, 0, P) \rangle$, which ensures that $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}}(\mathrm{Sel}_2(E/K)) \geq 2$. However, because $\tau_1\tau_2\tau_3\big|_N = 0$, we see that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}}(\mathrm{Sel}_2(E/K))$ is contained in a codimension-1 subspace of $E[2]/C \times E[2]/C \times E[2]$ and we therefore get that $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}}(\mathrm{Sel}_2(E/K)) \leq 3$. □

Corollary 8.6. *Suppose E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over M but not over K. If $d_2(E/K) \geq 2 + \mathrm{ord}_2\mathcal{T}(E/E')$ and $d_2(E/K) \geq 2$, then E has a twist E^F with $d_2(E^F/K) = d_2(E/K) - 2$ and $\mathcal{T}(E^F/E'^F) = \mathcal{T}(E/E')$.*

Proof. We begin by iteratively applying Proposition 8.5 until either $d_2(E^F/K) = d_2(E/K) - 2$, $d_\phi(E^F/K) = 1$, or $d_{\hat{\phi}}(E'^F/K) = 1$. (Note that the total number of iterations may be zero in the case where either $d_\phi(E/K) = 1$ or $d_{\hat{\phi}}(E'/K) = 1$

and the hypotheses of Proposition 8.5 are not satisfied.) If we terminate with $d_2(E^F/K) = d_2(E/K) - 2$, then we are done.

If we terminate with $d_\phi(E^F/K) = 1$ and $d_2(E^F/K) = d_2(E/K)$, then the hypotheses of Proposition 5.6 are satisfied by E^F since $d_2(E/K) \geq 2$.

Now suppose that we terminate with $d_{\hat{\phi}}(E'^F/K) = 1$ and $d_2(E^F/K) = d_2(E/K)$. Combining the conditions that $d_2(E/K) \geq 2 + \mathrm{ord}_2\mathcal{T}(E/E')$ with the fact that $\mathrm{ord}_2\mathcal{T}(E/E') = \mathrm{ord}_2\mathcal{T}(E^F/E'^F)$ we have

$$\begin{aligned} d_2(E^F/K) = d_2(E/K) \geq 2 + \mathrm{ord}_2\mathcal{T}(E/E') &= 2 + \mathrm{ord}_2\mathcal{T}(E^F/E'^F) \\ &= 2 + d_\phi(E^F/K) - d_{\hat{\phi}}(E'^F/K). \end{aligned}$$

As $d_{\hat{\phi}}(E'^F/K) = 1$, the hypotheses of Proposition 5.6 are satisfied by E^F.

As Proposition 8.5 shows that $\mathcal{T}(E^F/E'^F) = \mathcal{T}(E/E')$, we now only need to show that the extension constructed in Proposition 5.6 does not change the Tamagawa ratio. This will follow from the next lemma. □

Lemma 8.7. *Suppose E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over M but not over K. If F/K is the quadratic extension constructed in Proposition 5.6, then $\mathrm{Sel}_\phi(E^F/K) = \mathrm{Sel}_\phi(E/K)$ and $\mathrm{Sel}_{\hat{\phi}}(E'^F/K) = \mathrm{Sel}_{\hat{\phi}}(E'/K)$.*

Proof. We will show that $H^1_{\phi^F}(K_v, C) = H^1_\phi(K_v, C)$ and $H^1_{\hat{\phi}^F}(K_v, C') = H^1_{\hat{\phi}}(K_v, C')$ for all places v of K. Note that this is trivially true for all places away from 2∞ where E and E^F both have good reduction, since $H^1_{\phi^F}(K_v, C)$ and $H^1_\phi(K_v, C)$ are both equal to the unramified local subgroup $H^1_u(K_v, C)$ and $H^1_{\hat{\phi}^F}(K_v, C')$ and $H^1_{\hat{\phi}}(K_v, C')$ are both equal to the unramified local subgroup $H^1_u(K_v, C')$. We therefore only need to focus on the places above $2\Delta_E\infty$ and those ramified in F/K.

We recall from the proof of Proposition 5.6 that all places above $2\Delta_E\infty$ split in F/K. Part (i) of Lemma 6.8 then tells us that $H^1_\phi(K_v, C) = H^1_{\phi^F}(K_v, C)$ and $H^1_{\hat{\phi}^F}(K_v, C') = H^1_{\hat{\phi}}(K_v, C')$ at all of these places.

We also recall from the proof of Proposition 5.6 that F/K is ramified at exactly four places, $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_4$ (all away from $2\Delta_E\infty$) and that $E(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ for each $\mathfrak{p}_i$. By Corollary 4.4, we therefore get that $E'(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ as well. Part (iii) of Lemma 6.8 then tells us that $H^1_\phi(K_{\mathfrak{p}_i}, C) = H^1_{\phi^F}(K_{\mathfrak{p}_i}, C)$ and that $H^1_{\hat{\phi}^F}(K_{\mathfrak{p}_i}, C') = H^1_{\hat{\phi}}(K_{\mathfrak{p}_i}, C')$ for each $\mathfrak{p}_i$. □

9. Twists with increased 2-Selmer rank

While Corollary 2.12 seems to provide an easy recipe for finding twists E^F of E with $d_2(E^F) = d_2(E) + 2$, finding extensions satisfying its hypotheses turns out to be impossible when $\chi_{\Delta_E} \in \phi\,(\mathrm{Sel}_2(E/K)) \subset \mathrm{Sel}_{\hat{\phi}}(E'/K)$. Because this possibility cannot be discounted without including additional assumptions on E, we take a different path, using Corollaries 7.5 and 7.7 instead.

Proposition 9.1. *If E does not have a cyclic 4-isogeny defined over M whose kernel contains $E(K)[2]$, then there exists a quadratic extension F/K satifying the hypotheses of Corollary 7.5. In particular, E has a quadratic twist E^F with $d_\phi(E^F/K) - d_\phi(E/K) \in \{1, 2\}$ and $d_2(E^F/K) - d_2(E/K) \in \{0, 2\}$.*

Proof. Since E does not have a cyclic 4-isogeny defined over M whose kernel contains $E(K)[2]$, Lemma 4.2 tells us that M and M' are disjoint quadratic extensions

of K. We may therefore find $\sigma \in G_K$ such that $\sigma\big|_M \neq 1$ and $\sigma\big|_{M'} = 1$. Let N be a finite Galois extension of K containing $MM'K(8\Delta_E\infty)$ such that the restrictions of both $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_{\hat{\phi}}(E/K)$ to N are trivial. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be primes of K away from 2 where E has good reduction such that $\mathrm{Frob}_{\mathfrak{p}_1}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of $\sigma\big|_N$ and $\mathrm{Frob}_{\mathfrak{p}_2}$ in $\mathrm{Gal}(N/K)$ is the conjugacy class of $\sigma^{-1}\big|_N$. Since $\sigma\sigma^{-1}\big|_{K(8\Delta_E\infty)} = 1$, $\mathfrak{p}_1\mathfrak{p}_2$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta_E}$. Letting $F = K(\sqrt{\pi})$, we get that all places dividing $2\Delta_E\infty$ split in F/K, and that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the only primes that ramify in F/K.

Since $\sigma\big|_M \neq 1$ and $\sigma\big|_{M'} = 1$, $E(K_{\mathfrak{p}_i}) \simeq \mathbb{Z}/2\mathbb{Z}$ and $E'(K_{\mathfrak{p}_i}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Further, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ satisfy the condition that $\mathrm{res}_{\mathfrak{p}_1}(c) \neq 0$ if and only if $\mathrm{res}_{\mathfrak{p}_2}(c) \neq 0$ for every $c \in \mathrm{Sel}_2(E/K)$ and $c \in \mathrm{Sel}_{\hat{\phi}}(E/K)$ because the restrictions of both $\mathrm{Sel}_2(E/K)$ and $\mathrm{Sel}_{\hat{\phi}}(E/K)$ to N are trivial and the Frobeniuses of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in $\mathrm{Gal}(N/K)$ are inverses of each other. □

Proof of Theorem 1.2. By Theorem 1.6, it suffices to exhibit a single twist E^F of E with $d_2(E^F/K) = r$.

If $r < d_2(E/K)$ and $r \equiv d_2(E/K) \pmod 2$, then we iteratively apply Corollary 8.3 until we obtain a twist E^F of E with $d_2(E^F/K) = r$.

If $r > d_2(E/K)$ and $r \equiv d_2(E/K) \pmod 2$, we may iteratively apply Proposition 9.1 to get a twist E^F of E with $d_2(E^F/K) = r$. Observe that while any one application of Proposition 9.1 is not guaranteed to increase $d_2(E^F/K)$ relative to $d_2(E/K)$, enough applications of Proposition 9.1 will necessarily result in a twist E^F with $d_\phi(E^F/K) > d_2(E/K) + 2$. As $d_2(E^F/K) \geq d_\phi(E^F/K) - 2$, it must be the case that iteratively applying Proposition 9.1 to E will eventually result in increasing $d_2(E^F/K)$ relative to $d_2(E/K)$.

If E does not have contant 2-Selmer parity, then the result follows from applying the above procedure to any twist E^L of E with $d_2(E) \not\equiv d_2(E^L/K) \pmod 2$. □

Proposition 9.2. *If E does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over K but acquires such an isogeny over M, then there is a pair of quadratic extensions F_1/K and F_2/K satifying the hypotheses of Corollary* 7.7. *In particular, E has a quadratic twist E^F such that $d_\phi(E^F/K) = d_\phi(E/K) + 1$, $d_{\hat{\phi}}(E'^F/K) = d_{\hat{\phi}}(E'/K) + 1$ and $d_2(E^F/K) - d_2(E/K) \in \{0, 2\}$.*

Proof. By assumption, Lemma 4.2 shows that $M = M' \neq K$. We can therefore find $\gamma \in \mathrm{Gal}(M/K)$ with $\gamma\big|_M \neq 1$. Let N be a finite Galois extension of K containing $MK(8\Delta_E\infty)$ such that the restrictions of $\mathrm{Sel}_2(E/K)$, $\mathrm{Sel}_\phi(E/K)$, and $\mathrm{Sel}_{\hat{\phi}}(E'/K)$ to N are all trivial. Choose $\sigma \in \mathrm{Gal}(N/K)$ such that $\sigma_1\big|_M = \gamma$. Now choose two primes, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, away from $2\Delta_E$ such that $\mathrm{Frob}_{\mathfrak{p}_1}\big|_N = \sigma$ and $\mathrm{Frob}_{\mathfrak{p}_2}\big|_N = \sigma^{-1}$. As $\mathrm{Frob}_{\mathfrak{p}_1}\mathrm{Frob}_{\mathfrak{p}_2}\big|_{K(8\Delta_E\infty)} = 1$, we get that $\mathfrak{p}_1\mathfrak{p}_2$ has a totally positive generator π' with $\pi' \equiv 1 \pmod{8\Delta_E}$. Define $L = K(\sqrt{\pi'})$.

Now take $\tau \in \mathrm{Gal}(NL/K)$ such that $\tau\big|_N = 1$ and $\tau\big|_L \neq 1$. Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are ramified in L/K and not in N/K, we have $L \cap N = K$ and we can therefore always find such a τ. Let $\mathfrak{q}$ be any prime away from $2\Delta_E\mathfrak{p}_1\mathfrak{p}_2$ such that the image of $\mathrm{Frob}_{\mathfrak{q}}$ in $\mathrm{Gal}(NL/K)$ is τ. Because the restrictions of $\mathrm{Sel}_2(E/K)$, $\mathrm{Sel}_\phi(E/K)$, and $\mathrm{Sel}_{\hat{\phi}}(E'/K)$ to N/K are trivial, we get that all of $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(E/K))$, $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_\phi(E/K))$, and $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_{\hat{\phi}}(E'/K))$ are trivial.

As $\mathrm{Frob}_{\mathfrak{q}}$ in $\mathrm{Gal}(K(8\Delta_E\infty)/K)$ is trivial, $\mathfrak{q}$ has a totally positive generator π with $\pi \equiv 1 \pmod{8\Delta_E}$. Define quadratic extensions F_1/K and F_2/K by $F_1 = K(\sqrt{\pi})$ and $F_2 = K(\sqrt{\pi\pi'})$. Observe that all places above $2\Delta_E\infty$ split in both F_1/K and F_2/K. The only prime ramified in F_1/K is $\mathfrak{q}$ and the only primes ramified in F_2/K are $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{q}$. Further, because $\mathrm{Frob}_{\mathfrak{q}}\big|_L \neq 1$, we get that $\pi \notin (K_v^\times)^2$ and it follows that F_1/K_v and F_2/K_v are distinct ramified extensions of K_v.

Lastly, we have $\dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{q}\}}\mathrm{Sel}_2(E/K) = \dim_{\mathbb{F}_2}\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}\mathrm{Sel}_2(E/K)$ because $\mathrm{res}_{\mathfrak{q}}(\mathrm{Sel}_2(E/K)) = 0$. Applying Lemma 5.1, we get that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}\mathrm{Sel}_2(E/K)$ is contained in the diagonal of $E[2]/C \times E[2]/C$ since the restrictions to N/K of $\mathrm{Frob}_{\mathfrak{p}_1}$ and $\mathrm{Frob}_{\mathfrak{p}_2}$ are inverses of each other in $\mathrm{Gal}(N/K)$. By Lemma 5.4, $\mathrm{res}_{\mathfrak{p}_i}(\mathrm{Sel}_2(E/K)) \neq 0$ because $E'(K_{\mathfrak{p}_i})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and it therefore follows that $\mathrm{Loc}_{\{\mathfrak{p}_1,\mathfrak{p}_2\}}\mathrm{Sel}_2(E/K)$ is one-dimensional. □

10. Curves which acquire a cyclic 4-isogeny over $K(E[2])$

By Theorem 6.4, the Tamagawa ratio $\mathcal{T}(E^F/E'^F) = \frac{|\mathrm{Sel}_\phi(E^F/K)|}{|\mathrm{Sel}_{\hat\phi}(E'^F/K)|}$ is given by $\mathcal{T}(E^F/E'^F) = \prod_{v \text{ of } K} \frac{|H^1_{\phi^F}(K_v,C)|}{2}$. In the event that E does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over K but acquires such an isogeny over $M = K(E[2])$, we are able to replace this product with one taken over a finite set of places which are independent of F/K.

Proposition 10.1. *If E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over $M = K(E[2])$ but not over K and F/K is any quadratic extension, then*

$$\mathcal{T}(E^F/E'^F) = \prod_{v|2\Delta_E\infty} \frac{|H^1_{\phi^F}(K_v,C)|}{2} \text{ and} \tag{10.1}$$

$$\mathrm{ord}_2\mathcal{T}(E^F/E'^F) - \mathrm{ord}_2\mathcal{T}(E/E') = \sum_{v|2\Delta_E\infty} \dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v,C) - \dim H^1_{\phi}(K_v,C). \tag{10.2}$$

Proof. If E^F has good reduction at $v \nmid 2\infty$, then $|H^1_{\phi^F}(K_v,C)| = 2$, as $H^1_{\phi^F}(K_v,C)$ is equal to $H^1_u(K_v,C)$. If E has good reduction at $v \nmid 2\infty$ and v ramified in F/K, then combining Corollary 4.4 with Lemma 6.7 shows that $|H^1_{\phi^F}(K_v,C)| = 2$. Equation (10.1) then follows since the set of places $v \nmid 2$ where E^F has bad reduction is contained in the union of the set of places where E has bad reduction and the set of places ramified in F/K.

Equation (10.2) follows immediately from applying (10.1) to both E and E^F. □

Corollary 10.2. *Let E be as in Proposition* 10.1. *If E does not have constant* 2*-Selmer parity, then there must be some non-complex place $v \mid 2\Delta_E\infty$ and quadratic extension F_w/K_v with $\dim_{\mathbb{F}_2} H^1_{\phi}(K_v,C) \not\equiv \dim_{\mathbb{F}_2} H^1_{\phi^{F_w}}(K_v,C) \pmod 2$.*

Proof. Let E^F be a twist of E such that $d_2(E^F/K) \not\equiv d_2(E/K)$. By Theorem 6.5, we then get that $\mathrm{ord}_2\mathcal{T}(E/E') \not\equiv \mathrm{ord}_2\mathcal{T}(E^F/E'^F) \pmod 2$, so by Proposition 10.1, there is some place $v \mid 2\Delta_E\infty$ with $\dim_{\mathbb{F}_2} H^1_{\phi}(K_v,C) \not\equiv H^1_{\phi^F}(K_v,C) \pmod 2$. Note that v must not be complex as $H^1(\mathbb{C},C) = 0$. By part (i) of Lemma 2.7, v must not split in F/K. Taking w as the unique place of K lying above v gives the result. □

Because the product in (10.1) takes place over finitely many places and each term is bounded, we therefore see that $\mathcal{T}(E^F/E'^F)$ can only take finitely many values as F/K ranges over all quadratic extensions. This can affect the possible values of $d_2(E^F/K)$.

Let r_1 and r_2 denote the number of real and complex places of K respectively. As shown in Theorem 1 of [9], there are curves E defined over K for which $\mathrm{ord}_2\mathcal{T}(E^F/E'^F) \geq r_2$ for every F/K, which results in $d_2(E^F/K) \geq r_2$ for all quadratic twists of E. We now prove that the curves in [9] exhibit the worst possible behavior in this regard, made explicit in the following proposition.

Proposition 10.3. *If E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over M but not over K, then E has a twist E^F with $\mathrm{ord}_2\mathcal{T}(E^F/E'^F) \leq r_2$. Moreover, if E does not have constant 2-Selmer parity, then E has a twist $E^{F'}$ such that $\mathrm{ord}_2\mathcal{T}(E^{F'}/E'^{F'}) \leq r_2 + 1$ and $d_2(E^{F'}/K) \not\equiv d_2(E^F/K) \pmod 2$.*

Proposition 10.3 is a consequence of the following lemma.

Lemma 10.4. *Let E be as in Proposition* 10.3. *If v is a non-complex place of K, then we can always find a quadratic (or trivial) extension F_w/K_v such that $\dim_{\mathbb{F}_2} H^1_{\phi^{F_w}}(K_v, C) \leq \dim_{\mathbb{F}_2} H^1(K_v, C) - 1$.*

Proof. The case where E has additive reduction at $v \nmid 2$ is Lemma 3.3 in [9].

When E has multiplicative reduction at v with Kodaira type I_n, then by Theorem 5.4 in [5], E' will either have Kodaira type I_{2n} or $\mathrm{I}_{\frac{n}{2}}$. The result then follows from Lemma 3.4 in [9].

If $K_v = \mathbb{R}$, we pick a model $y^2 = x^3 + ax^2 + bx$ with coefficients in K_v such that $(0,0) \in \ker\phi$. Up to squares in K_v, the discriminants of E and E' are given by $a^2 - 4b$ and b respectively. As $M = M'$, we therefore get that $a^2 - 4b$ and b have the same sign. By Proposition 7.6 in [5], $|H^1_\phi(K_v, C)| = |E'(K_v)/\phi(E(K_v))| = 1$ if both a and b are positive or if b is negative. We therefore see that at least one of $H^1_\phi(K_v, C)$ and $H^1_{\phi^{\mathbb{C}}}(K_v, C)$ is trivial.[1]

When E has additive reduction at $v \mid 2$, we begin by showing that E' has some twist E'^{F_w} such that $E'^{F_w}(K_v)$ has no points of order four. For any twist E'^{F_w} of E', we get that the points of order four on $E'^{F_w}(K_v)$ are contained in $E'(F_w)^{\sigma=-1}$, where $\mathrm{Gal}(F_w/K_v) = \langle\sigma\rangle$. Therefore, $E'^{F_w}(K_v)$ will contain a point of order four if and only if there is a point $R \in E'[4]$ such that $R \in E'(F_w)$ with $\sigma(R) = -R$. In such a case, we have $F_w = K_v(R)$. Because K_v has at least eight quadratic extensions (including the trivial one) and $E'[4]$ only has six cyclic subgroups of order four, there must be some F_w/K_v such that $E'^{F_w}(K_v)$ has no points of order four.

As $|E(K_v)[2]| = |E'(K_v)[2]|$, there exists some $Q \in E^{F_w}(K_v)[2] \setminus \hat{\phi}(E'^{F_w}[2])$. Both pre-images of Q under $\hat{\phi}$ have order four in $E'^{F_w}[4]$. Since $E'^{F_w}(K_v)$ has no points of order four, Q has non-trivial image in $H^1(K_v, C')$, showing that $H^1_{\hat{\phi}^{F_w}}(K_v, C') \neq 0$. By Lemma 6.2, we then have $H^1_{\phi^{F_w}}(K_v, C) \neq H^1(K_v, C)$. □

Proof of Proposition 10.3. For each non-complex $v \mid 2\Delta_E\infty$ we use Lemma 10.4 to find a quadratic (or trivial) extension F_w/K_v such that $H^1_{\phi^{F_w}}(K_v, C) \neq H^1(K_v, C)$.

[1] Applying the same logic to E', we find that at least one of $H^1_{\hat{\phi}}(K_v, C')$ and $H^1_{\hat{\phi}^{\mathbb{C}}}(K_v, C')$ is trivial. Combined with Lemma 6.2, this shows that exactly one of $H^1_\phi(K_v, C)$ and $H^1_{\phi^{\mathbb{C}}}(K_v, C)$ is trivial.

Define an idele $\mathbf{x}$ of K by $\mathbf{x} = (x_v)$, where x_v is an element of K_v such that F_w is given by $F_w = K_v(\sqrt{x_v})$ for each non-complex place v above $2\Delta_E\infty$ and $x_v = 1$ at all other places v of K. Let $\mathbf{d}$ be the formal product of all places v above $\Delta_E\infty$ and let $\gamma = [\mathbf{x}, MK(8\mathbf{d})]$ be the image of $\mathbf{x}$ under the global Artin map. If $\mathfrak{p}$ is taken to be a prime of K away from $2\Delta_E$ such that $\mathrm{Frob}_\mathfrak{p}$ in $MK(8\mathbf{d})$ is γ, then $\mathfrak{p}$ is principal with a generator π such that $K_v(\sqrt{\pi}) = F_w$ for every non-complex place $v \mid 2\Delta_E\infty$. Setting $F = K(\sqrt{\pi})$, we get $\dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C) \le \dim_{\mathbb{F}_2} H^1(K_v, C) - 1$ for all non-complex $v \mid 2\Delta_E\infty$. Combining this with (10.1), the fact that $\dim_{\mathbb{F}_2} H^1(K_v, C) = 2$ for all $v \nmid 2\infty$, and some basic algebraic number theory, we obtain

$$\begin{aligned}(10.3)\quad \mathrm{ord}_2\mathcal{T}(E^F/E'^F) &= \sum_{v|2\Delta_E\infty} \Big(\dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C) - 1\Big) \\ &\le -(r_1 + r2) + \sum_{v|2} \big(\dim_{\mathbb{F}_2} H^1(K_v, C) - 2\big) = -(r_1 + r2) + \sum_{v|2} [K_v : \mathbb{Q}_2] \\ &= -(r_1 + r_2) + [K : \mathbb{Q}] = r_2,\end{aligned}$$

where the fact that $\dim_{\mathbb{F}_2} H^1(K_v, C) = [K_v : \mathbb{Q}_2] + 2$ for $v \mid 2$ follows from the identification of $H^1(K_v, C)$ with $K_v^\times/(K_v^\times)^2$ and by applying Proposition 6 in Section II.3 of [12]. If E does not have constant 2-Selmer parity, then Corollary 10.2 tells us that there must be some non-complex place $v \mid 2\Delta_E\infty$ and quadratic extension $F_{w'}/K_v$ with $\dim_{\mathbb{F}_2} H^1_\phi(K_v, C) \not\equiv \dim_{\mathbb{F}_2} H^1_{\phi^{F'_w}}(K_v, C) \pmod 2$. The above construction with $F_{w'}/K_v$ in place of F_w/K_v gives the result. □

Proof of Theorem 1.4. In the case that E does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over $M = K(E[2])$, Theorem 1.4 follows from Theorem 1.2. (If E has a place of multiplicative reduction or if K has a real place, then the fact that E does not have constant 2-Selmer parity follows from the discussion immediately following the statement of Theorem 1.2.) We will therefore assume that E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over M but not over K.

By Theorem 1.6, it suffices to exhibit a single twist E^F of E with $d_2(E^F/K) = r$.

Suppose that $r < d_2(E/K)$ and $r \equiv d_2(E/K) \pmod 2$ and let $r_0 = 0$ if $d_2(E/K)$ is even and $r_0 = 1$ if $d_2(E/K)$ is odd. If $r > \mathrm{Max}(\mathrm{ord}_2\mathcal{T}(E/E'), r_0)$, then iteratively applying Corollary 8.6 gives a twist E^F with $d_2(E^F/K) = r$.

If $r > d_2(E/K)$ and $r \equiv d_2(E/K) \pmod 2$, then we may iteratively apply Proposition 9.2 to E to find a twist E^F with $d_2(E^F/K) = r$. As in the proof of Theorem 1.2, we observe that while any one application of Proposition 9.2 is not guaranteed to increase $d_2(E^F/K)$ relative to $d_2(E/K)$, enough applications of Proposition 9.2 will necessarily result in a twist E^F with $d_\phi(E^F/K) > d_2(E/K)+2$. As $d_2(E^F/K) \ge d_\phi(E^F/K)-2$, it must be the case that iteratively applying Proposition 9.2 to E will eventually result in increasing $d_2(E^F/K)$ relative to $d_2(E/K)$.

We next want to show that if K has a real place or E has a place of multiplicative reduction, then E has a twist E^F with $d_2(E^F/K) \not\equiv d_2(E/K)$ and $\mathrm{ord}_2\mathcal{T}(E^F/E'^F) - \mathrm{ord}_2\mathcal{T}(E/E') = \pm 1$. The theorem then follows from applying the above to E^F in place of E. We construct such an E^F via an adelic construction.

Let v be either a real place of K or a prime where E has multiplicative reduction. Let $u = -1$ if $K_v = \mathbb{R}$ and let u be a non-square in $K_v^\times$ such that $K_v(\sqrt{u})/K_v$ is unramified if v is prime. Define an idele $\mathbf{x}$ of K by $\mathbf{x} = (x_w)$ where $x_v = u$ and

$x_w = 1$ for all $w \mid 2\Delta_E\infty$ different from v. Proceeding as in the proof of Proposition 10.3, we get a quadratic extension F/K such that all $w \mid 2\Delta_E\infty$ other than v split in F/K and $F_v = \mathbb{R}$ if v is real and F_v/K_v is unramified if v is prime. By (10.2),

$$\operatorname{ord}_2\mathcal{T}(E^F/E'^F) - \operatorname{ord}_2\mathcal{T}(E/E') = \dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C) - \dim H^1_{\phi}(K_v, C).$$

The fact that $\dim_{\mathbb{F}_2} H^1_{\phi^F}(K_v, C) - \dim H^1_{\phi}(K_v, C) = \pm 1$ follows from footnote 1 for v real and Lemma 3.4 in [9] for v prime. Finally, we obtain $d_2(E^F/K) \not\equiv d_2(E/K)$ as a consequence of Theorem 6.5. □

Proof of Theorem 1.3. In the case that E does not have a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over $M = K(E[2])$, Theorem 1.3 follows from Theorem 1.2. If E has a cyclic 4-isogeny whose kernel contains $E(K)[2]$ defined over M but not over K, then Theorem 1.3 follows from combining Theorem 1.4 with Proposition 10.3. □

Proof of Theorem 1.7. Theorem 1.7 is an immediate consequence of combining Theorem 1.4 with the fact that $\mathcal{T}(E/E') = \mathcal{T}(E'/E)^{-1}$. □

Acknowledgements

The author would like to express his utmost gratitude to Karl Rubin for the guidance and assistance he provided while undertaking this research. The author would also like to thank Matthew Gealy and Danny Goldstein for recommending the formulation of Lemma 4.2. Lastly, the author would like to thank the referee for suggesting a number of revisions to this work which resulted in a much stronger paper.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[2] Armand Brumer and Kenneth Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), no. 4, 715–743. MR0457453 (56 #15658)

[3] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199. MR0179169 (31 #3420)

[4] Tim Dokchitser and Vladimir Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64, DOI 10.1515/CRELLE.2011.060. MR2831512 (2012h:11084)

[5] Tim Dokchitser and Vladimir Dokchitser, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), no. 6, 4339–4358, DOI 10.1090/S0002-9947-2014-06271-5. MR3324930

[6] E. V. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43** (2008), no. 4, 293–303, DOI 10.1016/j.jsc.2007.11.001. MR2402033 (2009c:11080)

[7] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370, DOI 10.1007/BF01231536. With an appendix by P. Monsky. MR1292115 (95h:11064)

[8] Daniel Kane, *On the ranks of the 2-Selmer groups of twists of a given elliptic curve*, Algebra Number Theory **7** (2013), no. 5, 1253–1279, DOI 10.2140/ant.2013.7.1253. MR3101079

[9] Zev Klagsbrun, *Elliptic curves with a lower bound on 2-Selmer ranks of quadratic twists*, Math. Res. Lett. **19** (2012), no. 5, 1137–1143, DOI 10.4310/MRL.2012.v19.n5.a14. MR3039836

[10] Zev Klagsbrun, Barry Mazur, and Karl Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320, DOI 10.4007/annals.2013.178.1.5. MR3043582

[11] Zev Klagsbrun, Barry Mazur, and Karl Rubin, *A Markov model for Selmer ranks in families of twists*, Compos. Math. **150** (2014), no. 7, 1077–1106, DOI 10.1112/S0010437X13007896. MR3230846

[12] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR1282723 (95f:11085)

[13] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575, DOI 10.1007/s00222-010-0252-0. MR2660452 (2012a:11069)

[14] Ken Ono and Christopher Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), no. 3, 651–660, DOI 10.1007/s002220050275. MR1660945 (2000a:11077)

[15] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005)

[16] Alexei Skorobogatov and Peter Swinnerton-Dyer, *2-descent on elliptic curves and rational points on certain Kummer surfaces*, Adv. Math. **198** (2005), no. 2, 448–483, DOI 10.1016/j.aim.2005.06.005. MR2183385 (2006g:11129)

[17] Peter Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Math. Proc. Cambridge Philos. Soc. **145** (2008), no. 3, 513–526, DOI 10.1017/S0305004108001588. MR2464773 (2010d:11059)

[18] Lawrence C. Washington, *Galois cohomology*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 101–120. MR1638477

Center for Communications Research, 4320 Westerra Court, San Diego, California 92121

E-mail address: zdklags@ccrwest.org