Disparity in Selmer Ranks of Quadratic Twists of Elliptic Curves

Citation
Klagsbrun, Zev, Barry Charles Mazur, and Karl Rubin. 2013. "Disparity in Selmer Ranks of Quadratic Twists of Elliptic Curves." Annals of Mathematics 178 (1): 287–320.

Published Version
doi:10.4007/annals.2013.178.1.5

DISPARITY IN SELMER RANKS OF QUADRATIC TWISTS OF ELLIPTIC CURVES

ZEV KLAGSBRUN, BARRY MAZUR, AND KARL RUBIN

ABSTRACT. We study the parity of 2-Selmer ranks in the family of quadratic twists of an arbitrary elliptic curve E over an arbitrary number field K. We prove that the fraction of twists (of a given elliptic curve over a fixed number field) having even 2-Selmer rank exists as a stable limit over the family of twists, and we compute this fraction as an explicit product of local factors. We give an example of an elliptic curve E such that as K varies, these fractions are dense in $[0,1]$. More generally, our results also apply to p-Selmer ranks of twists of 2-dimensional self-dual $\mathbf{F}_p$-representations of the absolute Galois group of K by characters of order p.

CONTENTS

INTRODUCTION

The type of question that we consider in this paper has its roots in a conjecture of Goldfeld [6, Conjecture B] on the distribution of Mordell-Weil ranks in the family of quadratic twists of an arbitrary elliptic curve over $\mathbf{Q}$, and a result of Heath-Brown [7, Theorem 2] on the distribution of 2-Selmer ranks in the family of quadratic twists over $\mathbf{Q}$ of the elliptic curve $y^2 = x^3 - x$.

We study here the distribution of the parities of 2-Selmer ranks in the family of quadratic twists of an arbitrary elliptic curve E over an arbitrary number field K.

2010 *Mathematics Subject Classification.* Primary: 11G05, Secondary: 11G40.

This material is based upon work supported by the National Science Foundation under grants DMS-0700580, DMS-0757807, and DMS-0968831. Much of this work was carried out while the second and third authors were in residence at MSRI, and they would also like to thank MSRI for support and hospitality. We would also like to thank the referee for helpful comments.

For example, let $\rho(E/K)$ be the fraction of quadratic twists of E/K that have odd 2-Selmer rank. Precisely, for real numbers $X > 0$ let

$$\mathcal{C}(K,X) := \big\{\chi : G_K \to \{\pm 1\} : \chi \text{ is ramified only at primes } \mathfrak{q} \text{ with } \mathbf{N}\mathfrak{q} \le X\big\}$$

and define

$$\rho(E/K) := \lim_{X\to\infty} \frac{|\{\chi \in \mathcal{C}(K,X) : \dim_{\mathbf{F}_2} \mathrm{Sel}_2(E^\chi/K) \text{ is odd}\}|}{|\mathcal{C}(K,X)|}.$$

It follows from a result of Monsky [16, Theorem 1.5] along with root number calculations that $\rho(E/\mathbf{Q}) = 1/2$ for every elliptic curve $E/\mathbf{Q}$. It had already been noticed (see [4]) that this is not true when $\mathbf{Q}$ is replaced by an arbitrary number field K, because there are examples with $K \ne \mathbf{Q}$ for which $\rho(E/K) = 0$, and others with $\rho(E/K) = 1$. Our main theorem (see Theorem 7.6) evaluates $\rho(E/K)$.

Theorem A. *Suppose E is an elliptic curve defined over a number field K. Then for all sufficiently large X we have*

$$\rho(E/K) = \frac{|\{\chi \in \mathcal{C}(K,X) : \dim_{\mathbf{F}_2} \mathrm{Sel}_2(E^\chi/K) \textit{ is odd}\}|}{|\mathcal{C}(K,X)|} = (1-\delta(E/K))/2$$

where $\delta(E/K) \in [-1,1] \cap \mathbf{Z}[1/2]$ is given by an explicit finite product of local factors (see Definition 7.4).

We call $\delta(E/K)$ the "disparity" in the distribution of 2-Selmer ranks of twists of E. If K has a real embedding then $\delta(E/K) = 0$ so $\rho(E/K) = 1/2$ (see Corollary 7.10). On the other hand, Example 7.11 exhibits a particular elliptic curve $E/\mathbf{Q}$ such that as K varies, the set $\{\delta(E/K)\}$ is dense in $[-1,1]$, so $\{(1-\delta(E/K))/2\}$ is dense in $[0,1]$.

The finiteness of the 2-part of the Shafarevich-Tate group would imply that the parity of the 2-Selmer rank is the same as the parity of the Mordell-Weil rank. Thus one would expect that Theorem A holds with 2-Selmer rank replaced by Mordell-Weil rank. Further, Theorem A suggests a natural generalization of Goldfeld's conjecture (see Conjecture 7.12).

In a forthcoming paper [10], we will use the methods of this paper to make a finer study of the distribution of 2-Selmer ranks, inspired by the work of Heath-Brown [7], Swinnerton-Dyer [23], and Kane [9].

Our methods begin with those of [12] and [13]. Namely, we view all of the Selmer groups $\mathrm{Sel}_2(E^\chi/K)$ as subspaces of $H^1(K, E[2])$, defined by local conditions that vary with χ. In this way we can attach a Selmer group to a collection of local quadratic characters. The question of which collections of local characters arise from global characters is an exercise in class field theory (see §6).

To prove Theorem A, we show that the parity of $\dim_{\mathbf{F}_2} \mathrm{Sel}_2(E^\chi/K)$ depends only on the restrictions of χ to the decomposition groups at places dividing $2\Delta_E\infty$, where Δ_E is the discriminant of some model of E (see Proposition 7.2). (This is consistent with the behavior of the global root numbers of twists of E.) In particular the map that sends a character $\chi \in \mathrm{Hom}(G_K, \{\pm1\})$ to the parity of $\dim_{\mathbf{F}_2} \mathrm{Sel}_2(E^\chi/K)$ factors through the finite quotient $\prod_{v \mid 2\Delta_E\infty} \mathrm{Hom}(G_{K_v}, \{\pm1\})$. Using this fact we are able to deduce Theorem A.

There is another important ingredient in the proof of Theorem A. We make essential use of a recent observation of Poonen and Rains [17] that the local conditions that define the 2-Selmer groups we are studying are maximal isotropic subspaces for a natural quadratic form on the local cohomology groups $H^1(K_v, E[2])$. We use this in a crucial way in the proof of Theorem 3.9, which extends a result from [12] to include the case $p = 2$. Theorem 3.9 is a key ingredient in the proof of Theorem A.

Our methods apply much more generally than to 2-Selmer groups of elliptic curves, and throughout this paper we work in this fuller generality. Namely, suppose p is any prime, and T is a 2-dimensional $\mathbf{F}_p$-vector space with

- an action of the absolute Galois group G_K,
- a nondegenerate G_K-equivariant alternating $\boldsymbol{\mu}_p$-valued pairing, and
- a "global metabolic structure" (see Definition 3.3).

We also assume we are given "twisting data" (Definition 4.4) that allows us to define a family of Selmer groups $\mathrm{Sel}(T, \chi)$ as χ runs through characters of G_K of order p. We have analogues of Theorem A describing the distribution of $\dim_{\mathbf{F}_p} \mathrm{Sel}(T, \chi)$ in this setting.

For example, if E is an elliptic curve over K, then $T := E[p]$, the kernel of multiplication by p on E, comes equipped with all the structure we require. When $p > 2$ the Selmer groups $\mathrm{Sel}(E[p], \chi)$ are not Selmer groups of elliptic curves, but they are Selmer groups of $(p-1)$-dimensional abelian varieties over K that are twists of E in the sense of [14]. See §5, and see Theorem 8.2 for the analogue of Theorem A in this setting.

The layout of the paper is as follows. Let T be a Galois module as above. In §2 we derive some elementary properties of Lagrangian subspaces in quadratic vector spaces that we will need in the sequel. In §3 we define metabolic structures and Selmer groups in the generality we will need them. The key result is Theorem 3.9, which shows how the parity of the Selmer rank changes when we change some of the defining local conditions. In §4 we define the Selmer groups associated to twists of T, and in §5 we show how these Selmer groups reduce to classical Selmer groups of twists when $T = E[p]$ for an elliptic curve E/K.

Section 6 uses class field theory to allow us to go back and forth between global characters and collections of local characters. In §7 we study "parity disparity" when $p = 2$, and prove Theorem A, and in §8 we obtain similar but not identical results when $p > 2$.

1. Notation

Fix a number field K and a rational prime p. Let $\bar{K}$ denote a fixed algebraic closure of K, and $G_K := \mathrm{Gal}(\bar{K}/K)$. Let $\boldsymbol{\mu}_p$ denote the group of p-th roots of unity in $\bar{K}$.

Throughout this paper T will denote a two-dimensional $\mathbf{F}_p$-vector space with a continuous action of G_K, and with a nondegenerate G_K-equivariant alternating pairing corresponding to an isomorphism

$$\wedge^2 T \xrightarrow{\sim} \boldsymbol{\mu}_p. \tag{1.1}$$

We will use v (resp., $\mathfrak{q}$) for a place (resp., nonarchimedean place, or prime ideal) of K. If v is a place of K, we let K_v denote the completion of K at v, and K_v^{ur} its maximal unramified extension. We say that T is unramified at v if the inertia subgroup of G_{K_v} acts trivially on T, and in that case we define the unramified subgroup $H^1_{\mathrm{ur}}(K_v, T) \subset H^1(K_v, T)$ by

$$H^1_{\mathrm{ur}}(K_v, T) := H^1(K_v^{\mathrm{ur}}/K_v, T) = \ker[H^1(K_v, T) \to H^1(K_v^{\mathrm{ur}}, T)].$$

If $c \in H^1(K,T)$ and v is a place of K, we will often abbreviate $c_v := \mathrm{loc}_v(c)$ for the localization of c in $H^1(K_v,T)$.

We also fix a finite set Σ of places of K, containing all places where T is ramified, all primes above p, and all archimedean places.

2. Metabolic spaces

Fix for this section a finite dimensional $\mathbf{F}_p$-vector space V.

Definition 2.1. A *quadratic form* on V is a function $q : V \to \mathbf{F}_p$ such that

- $q(av) = a^2 q(v)$ for every $a \in \mathbf{F}_p$ and $v \in V$,
- the map $(v,w)_q := q(v+w) - q(v) - q(w)$ is a bilinear form.

If $X \subset V$, we denote by $X^\perp$ the orthogonal complement of X in V under the pairing $(\ ,\ )_q$. We say that (V,q) is a *metabolic space* if $(\ ,\ )_q$ is nondegenerate and V has a subspace X such that $X = X^\perp$ and $q(X) = 0$. Such a subspace X is called a *Lagrangian subspace* of V.

For this section, if W is an $\mathbf{F}_p$-vector space we let $\|W\| := \dim_{\mathbf{F}_p}(W)$.

Lemma 2.2. *Suppose (V,q) is a metabolic space, X is a Lagrangian subspace, and W is a subspace of V such that $q(W) = 0$. Then $W^\perp \cap X + W$ is a Lagrangian subspace of V.*

Proof. Exercise. See for example [17, Remark 2.4]. □

Lemma 2.3. *Suppose (V,q) is a metabolic space and X, Y, and Z are Lagrangian subspaces of V. Then*

$$\|(X+Y)\cap Z\| \equiv \|(X\cap Z) + (Y \cap Z)\| \pmod 2.$$

Proof. We adapt the proof of [12, Proposition 1.3] (see also [8, Lemma 1.5.7]). We define an alternating nondegenerate pairing on $((X+Y)\cap Z)/(X\cap Z + Y\cap Z)$, as follows.

Suppose $z, z' \in (X+Y)\cap Z$. Write $z = x+y$ and $z' = x'+y'$ with $x, x' \in X$ and $y \in Y$, and define

$$[z,z'] := (x,y')_q. \tag{2.1}$$

Note that x and y' are well-defined modulo $X \cap Y = (X+Y)^\perp$, so $[z,z']$ does not depend on the choice of x or y'. Thus $[\ ,\ ]$ is a well-defined bilinear pairing on $(X+Y)\cap Z$.

By definition we have

$$[z,z] = (x,y)_q = q(x+y) - q(x) - q(y).$$

Since X, Y, and Z are Lagrangian, and $x + y = z$, we have $q(x+y) = q(x) = q(y) = 0$, so $[z,z] = 0$ for every z, i.e., $[\ ,\ ]$ is alternating (and therefore also skew-symmetric).

If $z \in Y \cap Z$ then we can take $x = 0$ in (2.1), so $[z,z'] = 0$ for every z'. Using the skew-symmetry we deduce that $Y \cap Z$ is in the (left and right) kernel of the pairing $[\ ,\ ]$. Similarly $X\cap Z$, and hence $X\cap Z + Y\cap Z$, is in the kernel.

Conversely, if z is in the kernel of this pairing, then (still writing $z = x+y$ with $x \in X$ and $y \in Y$)

$$0 = [z,z'] = (x,y')_q = (x,z')_q = (x,z'+x'')_q$$

for every $z' \in (X+Y)\cap Z$ and $x'' \in X\cap Y$. Applying Lemma 2.2 with $W = X\cap Y$, $W^\perp = X+Y$ we see that

$$x \in ((X+Y)\cap Z + X\cap Y)^\perp = (X+Y)\cap Z + X\cap Y.$$

Thus, modifying x and y by an element of $X\cap Y$, we may assume that $x\in Z$, and then $y = z - x \in Z$ as well, so $z \in X\cap Z + Y\cap Z$.

This completes the proof that the pairing (2.1) is alternating and nondegenerate on $((X+Y)\cap Z)/(X\cap Z + Y\cap Z)$. A standard argument now shows that the dimension $\|((X+Y)\cap Z)/(X\cap Z+Y\cap Z)\|$ is even, and the lemma follows. □

Proposition 2.4. *Suppose (V,q) is a metabolic space and X, Y, and Z are Lagrangian subspaces of V. Then*

$$\|X\cap Y\| + \|Y\cap Z\| + \|X\cap Z\| \equiv \tfrac{1}{2}\|V\| = \|X\| = \|Y\| = \|Z\| \pmod 2.$$

Proof. For subspaces U, W of V we have $\|U\| + \|W\| = \|U+W\| + \|U\cap W\|$. This identity gives the two equalities below, and Lemma 2.3 gives the congruence:

$$\begin{aligned}\|X\cap Y\| + \|Y\cap Z\| + \|X\cap Z\| &= \|X\cap Y\| + \|X\cap Z + Y\cap Z\| + \|X\cap Y\cap Z\| \\ &\equiv \|X\cap Y\| + \|(X+Y)\cap Z\| + \|X\cap Y\cap Z\| \pmod 2 \\ &= \|(X+Y)\cap Z + X\cap Y\| + 2\|X\cap Y\cap Z\|.\end{aligned}$$

By Lemma 2.2, the subspace $(X+Y)\cap Z + X\cap Y$ is Lagrangian, and all Lagrangian subspaces have the same dimension $\frac{1}{2}\|V\|$, so this completes the proof. □

Corollary 2.5. *Suppose (V,q) is a metabolic space and X, Y, and Z are Lagrangian subspaces of V. Then*

$$\|X/(X\cap Y)\| + \|Y/(Y\cap Z)\| + \|Z/(X\cap Z)\| \equiv 0 \pmod 2.$$

Proof. This follows directly from Proposition 2.4. □

3. Metabolic structures and Selmer structures

In this section we define what we mean by a global metabolic structure $\mathbf{q}$ on T, and by a Selmer group for T and $\mathbf{q}$. The main result is Theorem 3.9, which shows how the parity of the Selmer rank changes when we change the defining local conditions.

The cup product and the pairing (1.1) induce a pairing

$$H^1(K,T)\times H^1(K,T) \xrightarrow{\cup} H^2(K, T\otimes T) \longrightarrow H^2(K, \boldsymbol{\mu}_p).$$

If v is a place of K and K_v is the completion of K at v, then applying the same construction over the field K_v gives local pairings

$$H^1(K_v,T)\times H^1(K_v,T) \xrightarrow{\cup} H^2(K_v, T\otimes T) \longrightarrow H^2(K_v, \boldsymbol{\mu}_p).$$

For every v there is a canonical inclusion $H^2(K_v,\boldsymbol{\mu}_p) \hookrightarrow \mathbf{F}_p$ that is an isomorphism unless either $K_v = \mathbf{C}$, or $K_v = \mathbf{R}$ and $p > 2$. The local Tate pairing is the composition

$$\langle\ ,\ \rangle_v : H^1(K_v,T)\times H^1(K_v,T) \longrightarrow \mathbf{F}_p. \tag{3.1}$$

The Tate pairings satisfy the following well-known properties.

Theorem 3.1.

(i) *For every v, the pairing $\langle\ ,\ \rangle_v$ is symmetric and nondegenerate.*

(ii) *If $v \notin \Sigma$ then $H^1_{\mathrm{ur}}(K_v, T) \subset H^1(K_v, T)$ is equal to its own orthogonal complement under $\langle\ ,\ \rangle_v$.*
(iii) *If $c, d \in H^1(K, T)$, then $\langle c_v, d_v \rangle_v = 0$ for almost all v and $\sum_v \langle c_v, d_v \rangle_v = 0$.*

Proof. For (i) and (ii), see for example [15, Corollary I.2.3 and Theorem I.2.6]. The first part of (iii) follows from (ii), and the second from the fact that the sum of the local invariants of an element of the global Brauer group is zero. □

Definition 3.2. Suppose v is a place of K. We say that q is a *Tate quadratic form* on $H^1(K_v, T)$ if the bilinear form induced by q (Definition 2.1) is $\langle\ ,\ \rangle_v$. If $v \notin \Sigma$, then we say that q is *unramified* if $q(x) = 0$ for all $x \in H^1_{\mathrm{ur}}(K_v, T)$.

Definition 3.3. Suppose T is as above. A *global metabolic structure* $\mathbf{q}$ on T consists of a Tate quadratic form q_v on $H^1(K_v, T)$ for every place v, such that

(i) $(H^1(K_v, T), q_v)$ is a metabolic space for every v,
(ii) if $v \notin \Sigma$ then q_v is unramified,
(iii) if $c \in H^1(K, T)$ then $\sum_v q_v(c_v) = 0$.

Note that if $c \in H^1(K, T)$ then $c_v \in H^1_{\mathrm{ur}}(K_v, T)$ for almost all v, so the sum in Definition 3.3(iii) is finite.

Lemma 3.4. *If $p > 2$ then there is a unique Tate quadratic form q_v on $H^1(K_v, T)$ for every v, and a unique global metabolic structure on T.*

Proof. Since $p \neq 2$, for every v there is a unique Tate quadratic form q_v on $H^1(K_v, T)$, namely

$$q_v(x) := \tfrac{1}{2}\langle x, x \rangle_v.$$

If $v \notin \Sigma$ then q_v is unramified by Theorem 3.1(ii), and if $c \in H^1(K, T)$ then $\sum_v q_v(c_v) = \frac{1}{2}\sum_v \langle c_v, c_v \rangle_v = 0$ by Theorem 3.1(iii). □

Remark 3.5. Suppose $p = 2$ and $\mathbf{q} = \{q_v : v \text{ of } K\}$ is a global metabolic structure on T. If $c \in H^1(K, T)$ is such that $c_v \in H^1_{\mathrm{ur}}(K_v, T)$ for every $v \notin \Sigma$, then for every v we can define a new Tate quadratic form q'_v on $H^1(K_v, T)$ by

$$q'_v(x) := q_v(x) + \langle x, c_v \rangle_v.$$

It is straightforward to check (using Theorem 3.1) that $\mathbf{q}' := \{q'_v\}$ is again a global metabolic structure on T, and if $c \neq 0$ then $\mathbf{q}' \neq \mathbf{q}$.

Definition 3.6. Suppose v is a place of K and q_v is a quadratic form on $H^1(K_v, T)$. Let

$$\mathcal{H}(q_v) := \{\text{Lagrangian subspaces of } (H^1(K_v, T), q_v)\},$$

and if $v \notin \Sigma$

$$\mathcal{H}_{\mathrm{ram}}(q_v) := \{X \in \mathcal{H}(q_v) : X \cap H^1_{\mathrm{ur}}(K_v, T) = 0\}.$$

Lemma 3.7. *Suppose $v \notin \Sigma$ and q_v is a Tate quadratic form on $H^1(K_v, T)$. Let $d_v := \dim_{\mathbf{F}_p} T^{G_{K_v}}$. Then:*

(i) $\dim_{\mathbf{F}_p} H^1(K_v, T) = 2d_v$,
(ii) *every $X \in \mathcal{H}(q_v)$ has dimension d_v,*
(iii) *if $d_v > 0$ and q_v is unramified, then $|\mathcal{H}_{\mathrm{ram}}(q_v)| = p^{d_v - 1}$.*

Proof. Since $\langle\ ,\ \rangle_v$ is nondegenerate, every Lagrangian subspace of $H^1(K_v,T)$ has dimension $\frac{1}{2}\dim_{\mathbf{F}_p} H^1(K_v,T)$. Since $v \notin \Sigma$, Theorem 3.1(ii) shows that $H^1_{\mathrm{ur}}(K_v,T)$ is Lagrangian. We have $H^1_{\mathrm{ur}}(K_v,T) = T/(\mathrm{Frob}_v - 1)T$ (see for example [21, §XIII.1]), so the exact sequence

$$0 \longrightarrow T^{G_{K_v}} \longrightarrow T \xrightarrow{\mathrm{Frob}_v - 1} T \longrightarrow T/(\mathrm{Frob}_v - 1)T \longrightarrow 0$$

shows that $\dim_{\mathbf{F}_p} H^1_{\mathrm{ur}}(K_v,T) = d_v$. This proves (i) and (ii).

Assertion (iii) follows from a calculation of Poonen and Rains [17, Proposition 2.6(b,e)]. □

Definition 3.8. Suppose T is as above and $\mathbf{q}$ is a global metabolic structure on T. A *Selmer structure* $\mathcal{S}$ for $(T,\mathbf{q})$ (or simply for T, if $\mathbf{q}$ is understood) consists of

- a finite set $\Sigma_{\mathcal{S}}$ of places of K, containing Σ,
- for every $v \in \Sigma_{\mathcal{S}}$, a Lagrangian subspace $H^1_{\mathcal{S}}(K_v,T) \subset H^1(K_v,T)$.

If $\mathcal{S}$ is a Selmer structure, we set $H^1_{\mathcal{S}}(K_v,T) := H^1_{\mathrm{ur}}(K_v,T)$ if $v \notin \Sigma_{\mathcal{S}}$, and we define the *Selmer group* $H^1_{\mathcal{S}}(K,T) \subset H^1(K,T)$ by

$$H^1_{\mathcal{S}}(K,T) := \ker\big(H^1(K,T) \longrightarrow \bigoplus_v H^1(K_v,T)/H^1_{\mathcal{S}}(K_v,T)\big),$$

i.e., the subgroup of $c \in H^1(K,T)$ such that $c_v \in H^1_{\mathcal{S}}(K_v,T)$ for every v.

Theorem 3.9. *Suppose $\mathcal{S}$ and $\mathcal{S}'$ are two Selmer structures for T. Then*

$$\dim_{\mathbf{F}_p} H^1_{\mathcal{S}}(K,T) - \dim_{\mathbf{F}_p} H^1_{\mathcal{S}'}(K,T) \equiv \sum_{v \in \Sigma_{\mathcal{S}} \cup \Sigma_{\mathcal{S}'}} \dim_{\mathbf{F}_p} H^1_{\mathcal{S}}(K_v,T)/(H^1_{\mathcal{S}}(K_v,T) \cap H^1_{\mathcal{S}'}(K_v,T)) \pmod 2.$$

Proof. When $p > 2$, this is [12, Theorem 1.4]. We will prove this for all p using Proposition 2.4.

Let $\Sigma' := \Sigma_{\mathcal{S}} \cup \Sigma_{\mathcal{S}'}$. Define $V = \prod_{v \in \Sigma'} H^1(K_v,T)$, so $(V, \sum_v q_v)$ is a metabolic space. Let $\mathrm{loc}_{\Sigma'} : H^1(K,T) \to V$ denote the product of the localization maps. Define three subspaces of V

- $X := \prod_{v \in \Sigma'} H^1_{\mathcal{S}}(K_v,T)$,
- $Y := \prod_{v \in \Sigma'} H^1_{\mathcal{S}'}(K_v,T)$,
- Z is the image under $\mathrm{loc}_{\Sigma'}$ of $\ker(H^1(K,T) \to \bigoplus_{v \notin \Sigma'} H^1(K_v,T)/H^1_{\mathrm{ur}}(K_v,T))$.

The spaces X and Y are Lagrangian by definition of Selmer structure. That Z is also Lagrangian can be seen as follows. We have $Z^\perp = Z$ by Poitou-Tate global duality (see for example [15, Theorem I.4.10], [24, Theorem 3.1], or [19, Theorem 1.7.3]). If $z \in Z$, then $z = \mathrm{loc}_{\Sigma'}(s)$ with $s \in H^1(K,T)$ satisfying $s_v \in H^1_{\mathrm{ur}}(K_v,T)$ for every $v \notin \Sigma'$. Then $q_v(s_v) = 0$ if $v \notin \Sigma'$ by Definition 3.3(ii), so

$$\big(\sum_{v \in \Sigma'} q_v\big)(z) = \sum_{v \in \Sigma'} q_v(s_v) = \sum_{\text{all } v} q_v(s_v) = 0$$

by Definition 3.3(iii). Thus Z is Lagrangian.

Note that from the definitions we have exact sequences

$$0 \longrightarrow A \longrightarrow H^1_{\mathcal{S}}(K,T) \xrightarrow{\mathrm{loc}_{\Sigma'}} X \cap Z \longrightarrow 0$$

$$0 \longrightarrow A \longrightarrow H^1_{\mathcal{S}'}(K,T) \xrightarrow{\mathrm{loc}_{\Sigma'}} Y \cap Z \longrightarrow 0$$

where the kernel A in both sequences is

$$A = \ker\big(H^1(K,T) \longrightarrow \bigoplus_{v \notin \Sigma'} H^1(K_v,T)/H^1_{\mathrm{ur}}(K_v,T) \bigoplus_{v \in \Sigma'} H^1(K_v,T)\big)$$

Thus by Proposition 2.4 we have

$$\begin{aligned}\dim_{\mathbf{F}_p} H^1_{\mathcal{S}}(K,T) - \dim_{\mathbf{F}_p} H^1_{\mathcal{S}'}(K,T) &= \dim_{\mathbf{F}_p}(Y \cap Z) - \dim_{\mathbf{F}_p}(X \cap Z) \\ &\equiv \dim_{\mathbf{F}_p}(X/(X \cap Y)) \pmod 2.\end{aligned}$$

Since $X/(X \cap Y) = \prod_{v \in \Sigma'} H^1_{\mathcal{S}}(K_v,T)/(H^1_{\mathcal{S}}(K_v,T) \cap H^1_{\mathcal{S}'}(K_v,T))$, this completes the proof of the theorem. □

4. Twisted Selmer groups

Given T as above (and some additional "twisting data", see Definition 4.4), in this section we show how to attach to every character $\chi \in \mathrm{Hom}(G_K, \boldsymbol{\mu}_p)$ a Selmer group $\mathrm{Sel}(T,\chi)$. More generally, we attach a Selmer group $\mathrm{Sel}(T,\gamma)$ to every collection of local characters $\gamma = (\gamma_v)$ with $\gamma_v \in \mathrm{Hom}(G_{K_v}, \boldsymbol{\mu}_p)$ for v in some finite set containing Σ. Our main result is Theorem 4.11, which uses Theorem 3.9 to show how the parity of the Selmer rank changes when we change some of the γ_v.

Definition 4.1. If L is a field, define

$$\mathcal{C}(L) := \mathrm{Hom}(G_L, \boldsymbol{\mu}_p)$$

(throughout this paper, "Hom" will always mean continuous homomorphisms). If L is a local field, we let $\mathcal{C}_{\mathrm{ram}}(L) \subset \mathcal{C}(L)$ denote the subset of ramified characters. In this case local class field theory identifies $\mathcal{C}(L)$ with $\mathrm{Hom}(L^\times, \boldsymbol{\mu}_p)$, and $\mathcal{C}_{\mathrm{ram}}(L)$ is then the subset of characters nontrivial on the local units $\mathcal{O}_L^\times$. Let $\mathbf{1}_L \in \mathcal{C}(L)$ denote the trivial character.

There is a natural action of $\mathrm{Aut}(\boldsymbol{\mu}_p) = \mathbf{F}_p^\times$ on $\mathcal{C}(L)$, and we let $\mathcal{F}(L) := \mathcal{C}(L)/\mathrm{Aut}(\boldsymbol{\mu}_p)$. Then $\mathcal{F}(L)$ is naturally identified with the set of cyclic extensions of L of degree dividing p, via the correspondence that sends $\chi \in \mathcal{C}(L)$ to the fixed field $\bar{L}^{\ker(\chi)}$ of $\ker(\chi)$ in $\bar{L}$. If L is a local field, then $\mathcal{F}_{\mathrm{ram}}(L)$ denotes the set of ramified extensions in $\mathcal{F}(L)$.

Definition 4.2. For $1 \le i \le 2$ define

$$\mathcal{P}_i := \{\mathfrak{q} : \mathfrak{q} \notin \Sigma,\ \boldsymbol{\mu}_p \subset K_\mathfrak{q}, \text{ and } \dim_{\mathbf{F}_p} T^{G_{K_\mathfrak{q}}} = i\},$$

and $\mathcal{P}_0 := \{\mathfrak{q} : \mathfrak{q} \notin \Sigma \cup \mathcal{P}_1 \cup \mathcal{P}_2\}$. Define the *width* $w(\mathfrak{q}) \in \{0,1,2\}$ of a prime $\mathfrak{q}$ of K, $\mathfrak{q} \notin \Sigma$, by $w(\mathfrak{q}) := i$ if $\mathfrak{q} \in \mathcal{P}_i$.

Let $K(T)$ denote the field of definition of the elements of T, i.e., the fixed field in $\bar{K}$ of $\ker(G_K \to \mathrm{Aut}(T))$.

Lemma 4.3. *Suppose $\mathfrak{q}$ is a prime of K, $\mathfrak{q} \notin \Sigma$, and let $\mathrm{Frob}_\mathfrak{q} \in \mathrm{Gal}(K(T)/K)$ be a Frobenius element for some choice of prime above $\mathfrak{q}$. Then*
(i) *$\mathfrak{q} \in \mathcal{P}_2$ if and only if $\mathrm{Frob}_\mathfrak{q} = 1$,*
(ii) *$\mathfrak{q} \in \mathcal{P}_1$ if and only if $\mathrm{Frob}_\mathfrak{q}$ has order exactly p,*
(iii) *$\mathfrak{q} \in \mathcal{P}_0$ if and only if $\mathrm{Frob}_\mathfrak{q}^p \neq 1$.*

In particular $\mathcal{P}_2$ has positive density in the set of all primes of K, and $\mathcal{P}_1$ has positive density if and only if $p \mid [K(T):K]$.

Proof. Fix an $\mathbf{F}_p$-basis of T so that we can view $\mathrm{Frob}_\mathfrak{q} \in \mathrm{GL}_2(\mathbf{F}_p)$. Then by (1.1)

$$\boldsymbol{\mu}_p \subset K_\mathfrak{q} \iff \mathrm{Frob}_\mathfrak{q} \text{ acts trivially on } \boldsymbol{\mu}_p \iff \det(\mathrm{Frob}_\mathfrak{q}) = 1.$$

Since $\mathfrak{q} \notin \Sigma$, T is unramified at $\mathfrak{q}$, so $T^{G_{K_\mathfrak{q}}} = T^{\mathrm{Frob}_\mathfrak{q}=1}$, the subspace of T fixed by $\mathrm{Frob}_\mathfrak{q}$. We have $\dim_{\mathbf{F}_p} T^{\mathrm{Frob}_\mathfrak{q}=1} = 2$ if and only if $\mathrm{Frob}_\mathfrak{q} = 1$, and if $\det(\mathrm{Frob}_\mathfrak{q}) = 1$, then $\dim_{\mathbf{F}_p} T^{\mathrm{Frob}_\mathfrak{q}=1} = 1$ if and only if $\mathrm{Frob}_\mathfrak{q}$ has order p. This proves the lemma. □

Definition 4.4. Suppose T, Σ are as above, and $\mathbf{q}$ is a global metabolic structure on T. By *twisting data* we mean

(i) for every $v \in \Sigma$, a (set) map

$$\alpha_v : \mathcal{C}(K_v)/\mathrm{Aut}(\boldsymbol{\mu}_p) = \mathcal{F}(K_v) \longrightarrow \mathcal{H}(q_v),$$

(ii) for every $v \in \mathcal{P}_2$, a bijection

$$\alpha_v : \mathcal{C}_{\mathrm{ram}}(K_v)/\mathrm{Aut}(\boldsymbol{\mu}_p) = \mathcal{F}_{\mathrm{ram}}(K_v) \longrightarrow \mathcal{H}_{\mathrm{ram}}(q_v).$$

Remark 4.5. Note that if $v \in \mathcal{P}_2$ then $|\mathcal{F}_{\mathrm{ram}}(K_v)| = p = |\mathcal{H}_{\mathrm{ram}}(q_v)|$, the first equality by local class field theory (since by definition $v \nmid p$ and $\boldsymbol{\mu}_p \subset K_v^\times$) and the second by Lemma 3.7(iii).

On the other hand, if $v \in \mathcal{P}_1$ then $\mathcal{H}_{\mathrm{ram}}(q_v)$ has exactly one element by Lemma 3.7(iii), and if $v \in \mathcal{P}_0$ then either $H^1(K_v, T) = 0$ by Lemma 3.7(i), or $\boldsymbol{\mu}_p \not\subset K_v$ so $\mathcal{C}_{\mathrm{ram}}(K_v)$ is empty. Thus if $v \in \mathcal{P}_0 \cup \mathcal{P}_1$ then there is a unique map $\mathcal{C}_{\mathrm{ram}}(K_v) \to \mathcal{H}_{\mathrm{ram}}(q_v)$. That is why these maps do not need to be specified as part of the twisting data.

If $\chi \in \mathcal{C}(K)$ and v is a place of K, we let $\chi_v \in \mathcal{C}(K_v)$ denote the restriction of χ to G_{K_v}.

Definition 4.6. Let

$$\mathcal{D} := \{\text{squarefree products of primes } \mathfrak{q} \in \mathcal{P}_1 \cup \mathcal{P}_2\},$$

and if $\mathfrak{d} \in \mathcal{D}$ let $\mathfrak{d}_1$ (resp., $\mathfrak{d}_2$) be the product of all primes dividing $\mathfrak{d}$ that lie in $\mathcal{P}_1$ (resp., $\mathcal{P}_2$), so $\mathfrak{d} = \mathfrak{d}_1\mathfrak{d}_2$. For every $\mathfrak{d} \in \mathcal{D}$, define the *width* of $\mathfrak{d}$ by

$$w(\mathfrak{d}) := \sum_{\mathfrak{q} \mid \mathfrak{d}} w(\mathfrak{q}) = |\{\mathfrak{q} : \mathfrak{q} \mid \mathfrak{d}_1\}| + 2 \cdot |\{\mathfrak{q} : \mathfrak{q} \mid \mathfrak{d}_2\}|.$$

Let $\Sigma(\mathfrak{d}) := \Sigma \cup \{\mathfrak{q} : \mathfrak{q} \mid \mathfrak{d}\} \subset \Sigma \cup \mathcal{P}_1 \cup \mathcal{P}_2$ and

$$\mathcal{C}(\mathfrak{d}) := \{\chi \in \mathcal{C}(K) : \chi \text{ is ramified at all } \mathfrak{q} \text{ dividing } \mathfrak{d}, \text{ and unramified outside of } \Sigma(\mathfrak{d}) \cup \mathcal{P}_0\}.$$

Define a finite set

$$\Gamma_\mathfrak{d} := \prod_{v \in \Sigma} \mathcal{C}(K_v) \times \prod_{\mathfrak{q} \mid \mathfrak{d}_2} \mathcal{C}_{\mathrm{ram}}(K_\mathfrak{q}),$$

and let $\eta_\mathfrak{d} : \mathcal{C}(\mathfrak{d}) \to \Gamma_\mathfrak{d}$ and $\eta : \mathcal{C}(K) \to \Gamma_1$ denote the natural maps

$$\eta_\mathfrak{d}(\chi) := (\ldots, \chi_v, \ldots)_{v \in \Sigma(\mathfrak{d}_2)}, \quad \eta(\chi) := (\ldots, \chi_v, \ldots)_{v \in \Sigma}.$$

Note that $\mathcal{C}(K_v)$ is a group, and $\mathcal{C}_{\mathrm{ram}}(K_v)$ is not a group but it is closed under multiplication by unramified characters. Since $\mathcal{C}(\mathfrak{d})$ is the fiber over $\mathfrak{d}$ of the map $\mathcal{C}(K) \to \mathcal{D}$ that sends χ to the part of its conductor supported on $\mathcal{P}_1 \cup \mathcal{P}_2$, we have $\mathcal{C}(K) = \coprod_{\mathfrak{d} \in \mathcal{D}} \mathcal{C}(\mathfrak{d})$.

Definition 4.7. Given T, $\mathbf{q}$, and twisting data as in Definition 4.4, we define a Selmer structure $\mathcal{S}(\gamma)$ for every $\mathfrak{d} \in \mathcal{D}$ and $\gamma = (\gamma_v)_v \in \Gamma_\mathfrak{d}$ as follows.

- Let $\Sigma_{\mathcal{S}(\gamma)} := \Sigma(\mathfrak{d})$.
- If $v \in \Sigma$ then let $H^1_{\mathcal{S}(\gamma)}(K_v, T) := \alpha_v(\gamma_v)$.
- If $v \mid \mathfrak{d}_1$, let $H^1_{\mathcal{S}(\gamma)}(K_v, T)$ be the unique element of $\mathcal{H}_{\mathrm{ram}}(q_v)$.
- If $v \mid \mathfrak{d}_2$, let $H^1_{\mathcal{S}(\gamma)}(K_v, T) := \alpha_v(\gamma_v) \in \mathcal{H}_{\mathrm{ram}}(q_v)$.

If $\gamma \in \Gamma_\mathfrak{d}$ we will also write $\mathrm{Sel}(T, \gamma) := H^1_{\mathcal{S}(\gamma)}(K, T)$, and if $\chi \in \mathcal{C}(\mathfrak{d})$ then we define

$$\mathrm{Sel}(T, \chi) := \mathrm{Sel}(T, \eta_\mathfrak{d}(\chi)).$$

Remark 4.8. It is clear from the definition that $\mathrm{Sel}(T, \chi)$ depends only on the extension of K cut out by χ, i.e., $\mathrm{Sel}(T, \chi) = \mathrm{Sel}(T, \chi^i)$ for all $i \in \mathbf{F}_p^\times$. However, when we later count the twists $\mathrm{Sel}(T, \chi)$ with certain properties, it will be convenient to deal with $\mathcal{C}(K)$ rather than $\mathcal{F}(K)$ because $\mathcal{C}(K)$ is a group. In any case the natural map $\mathcal{C}(K) \twoheadrightarrow \mathcal{C}(K)/\mathrm{Aut}(\boldsymbol{\mu}_p) = \mathcal{F}(K)$ is $(p-1)$-to-one except for the single fiber consisting of the trivial character, so it is simple to go from counting results for $\mathcal{C}(K)$ to results for $\mathcal{F}(K)$. In particular, when $p = 2$ the natural map $\mathcal{C}(K) \to \mathcal{F}(K)$ is a bijection.

Remark 4.9 (Remarks about twisting data)**.** Our definition of twisting data is designed to ensure that for $v \notin \Sigma$, all subspaces $V \in \mathcal{H}_{\mathrm{ram}}(q_v)$ occur with equal frequency as we run over characters $\chi \in \mathcal{C}(K)$ that are ramified at v. That fact is all we require to prove our results in sections 7 and 8 about the rank statistics of $\mathrm{Sel}(T, \chi)$. In particular, the conclusions of Theorems 7.6 and 8.2 below do not depend on the choice of twisting data for $(T, \mathbf{q})$.

We will see in §5 that when E is an elliptic curve over K, p is a rational prime, and $T = E[p]$, then there is natural global metabolic structure on $E[p]$ and natural twisting data such that for every $\chi \in \mathcal{C}(K)$, $\mathrm{Sel}(E[p], \chi)$ is a classical Selmer group of a twist of E (an abelian variety twist, when $p > 2$). An analogous statement should hold for more general (self-dual) motives and their Bloch-Kato p-Selmer groups, so our results below should also apply to Bloch-Kato Selmer groups in families of twists.

Definition 4.10. If $v \in \Sigma$ and $\psi, \psi' \in \mathcal{C}(K_v)$, define

$$h_v(\psi, \psi') := \dim_{\mathbf{F}_p} \alpha_v(\psi)/(\alpha_v(\psi) \cap \alpha_v(\psi')).$$

Theorem 4.11. *Suppose $\mathfrak{d} \in \mathcal{D}$, $\gamma \in \Gamma_1$, and $\gamma' \in \Gamma_\mathfrak{d}$. Then*

$$\dim_{\mathbf{F}_p} \mathrm{Sel}(T, \gamma) - \dim_{\mathbf{F}_p} \mathrm{Sel}(T, \gamma') \equiv \sum_{v \in \Sigma} h_v(\gamma_v, \gamma'_v) + w(\mathfrak{d}) \pmod 2.$$

Proof. We will deduce this from Theorem 3.9. Suppose $\mathfrak{q} \mid \mathfrak{d}$. Then by definition $H^1_{\mathcal{S}(\gamma)}(K_\mathfrak{q}, T) = H^1_{\mathrm{ur}}(K_\mathfrak{q}, T)$ since $\mathfrak{q} \notin \Sigma_{\mathcal{S}(\gamma)}$, and $H^1_{\mathcal{S}(\gamma')}(K_\mathfrak{q}, T) \in \mathcal{H}_{\mathrm{ram}}(q_\mathfrak{q})$, so

$$H^1_{\mathcal{S}(\gamma)}(K_\mathfrak{q}, T) \cap H^1_{\mathcal{S}(\gamma')}(K_\mathfrak{q}, T) = 0.$$

Also by definition we have $H^1_{\mathcal{S}(\gamma)}(K_v, T) = \alpha_v(\gamma_v)$ if $v \in \Sigma$, and similarly for γ'. Now applying Theorem 3.9 with $\mathcal{S} = \mathcal{S}(\gamma)$ and $\mathcal{S}' = \mathcal{S}(\gamma')$ shows that

$$\begin{aligned}\dim_{\mathbf{F}_p} \mathrm{Sel}(T,\gamma) - \dim_{\mathbf{F}_p} \mathrm{Sel}(T,\gamma') \\ &\equiv \sum_{v\in\Sigma} \dim_{\mathbf{F}_p} \alpha_v(\gamma_v)/(\alpha_v(\gamma_v)\cap\alpha_v(\gamma'_v)) + \sum_{\mathfrak{q}\mid\mathfrak{d}} \dim_{\mathbf{F}_p}(H^1_{\mathrm{ur}}(K_\mathfrak{q}, T)) \\ &= \sum_{v\in\Sigma} h_v(\gamma_v,\gamma'_v) + \sum_{\mathfrak{q}\mid\mathfrak{d}} w(\mathfrak{q}) \pmod 2,\end{aligned}$$

using that if $\mathfrak{q} \in \mathcal{P}_1 \cup \mathcal{P}_2$ then $\dim_{\mathbf{F}_p} H^1_{\mathrm{ur}}(K_\mathfrak{q}, T) = w(\mathfrak{q})$ by Lemma 3.7(ii). This proves the theorem. □

Corollary 4.12. *Suppose $\mathfrak{d} \in \mathcal{D}$ and $\chi \in \mathcal{C}(\mathfrak{d})$. Then*

$$\dim_{\mathbf{F}_p} \mathrm{Sel}(T,\chi) \equiv \dim_{\mathbf{F}_p} \mathrm{Sel}(T,\eta(\chi)) + w(\mathfrak{d}) \pmod 2.$$

Proof. Let $\gamma = \eta(\chi)$ and $\gamma' = \eta_\mathfrak{d}(\chi)$. If $v \in \Sigma$ then $\eta(\chi)_v = \chi_v = \eta_\mathfrak{d}(\chi)_v$, so $h_v(\gamma_v, \gamma'_v) = 0$. Now the corollary follows from Theorem 4.11. □

5. Example: twists of elliptic curves

Fix for this section an elliptic curve E defined over K, a prime p, and let $T := E[p]$. We will show that this T comes equipped with the extra structure that we require, and that with an appropriate choice of twisting data, the Selmer groups $\mathrm{Sel}(E[p], \chi)$ are classical p-Selmer groups of twists of E.

The module $T = E[p]$ satisfies the hypotheses of §1, with the pairing (1.1) given by the Weil pairing. Let Σ be a finite set of places of K containing all archimedean places, all places above p, and all primes where E has bad reduction. Let $\mathcal{O}$ denote the ring of integers of the cyclotomic field of p-th roots of unity, and $\mathfrak{p}$ the (unique) prime of $\mathcal{O}$ above p.

If $p > 2$, there is a unique global metabolic structure $\mathbf{q}_E = (q_{E,v})$ on $E[p]$ (Lemma 3.4). For general p, there is a canonical global metabolic structure $\mathbf{q}_E$ on $E[p]$ constructed from the Heisenberg group, see [17, §4]. We recall this construction below when $p = 2$, in the proof of Lemma 5.2(ii).

We next define twisting data for $(E[p], \Sigma, \mathbf{q}_E)$ in the sense of Definition 4.4.

Definition 5.1. Suppose $\chi \in \mathcal{C}(K)$ (or $\chi \in \mathcal{C}(K_v)$) is nontrivial. If $p = 2$ we let E^χ denote the quadratic twist of E by χ. For general p, let F denote the cyclic extension of K (resp., K_v) of degree p corresponding to χ, and let E^χ denote the abelian variety denoted E_F in [14, Definition 5.1].

Concretely, if $\chi \in \mathcal{C}(K)$ and $\chi \neq \mathbf{1}_K$ then E^χ is an abelian variety of dimension $p-1$ over K, defined to be the kernel of the canonical map

$$\mathrm{Res}^F_K(E) \longrightarrow E$$

where $\mathrm{Res}^F_K(E)$ denotes the Weil restriction of scalars of E from F to K. The character χ induces an inclusion $\mathcal{O} \subset \mathrm{End}_K(E^\chi)$ (see [14, Theorem 5.5(iv)]).

For $\chi \in \mathcal{C}(K)$, let $\mathbf{q}_{E^\chi} = (q_{E^\chi,v})$ be the unique global metabolic structure on $E^\chi[\mathfrak{p}]$ if $p > 2$, and if $p = 2$ we let $\mathbf{q}_{E^\chi}$ be the canonical global metabolic structure on the elliptic curve E^χ.

If $p = 2$, then the two definitions above of E^χ agree, with $\mathcal{O} = \mathbf{Z}$, and $\mathfrak{p} = 2$.

Lemma 5.2. (i) *There is a canonical G_K-isomorphism $E^\chi[\mathfrak{p}] \cong E[p]$.*

(ii) *The isomorphism of (i) identifies* $q_{E^\chi,v}$ *with* $q_{E,v}$ *for every* v *and every* $\chi \in \mathcal{C}(K_v)$.

Proof. Assertion (i) follows directly from the definition of quadratic twist when $p = 2$ (or see the proof of (ii) below). For general p, see [14, Theorem 2.2(iii)] or [12, Proposition 4.1].

The isomorphism of (i) identifies the Weil pairings on $E^\chi[\mathfrak{p}]$ and $E[p]$, and hence it identifies the local Tate pairings on $H^1(K_v, E^\chi[\mathfrak{p}])$ and $H^1(K_v, E[p])$ for every v. Thus when $p > 2$, assertion (ii) follows from the uniqueness of the Tate quadratic form on T (Lemma 3.4). When $p = 2$, we use an explicit construction of the quadratic form $q_{E,v}$. Let $\bar{K}_v(E)$ denote the function field of E over $\bar{K}_v$. Following [3, Proposition 1.32] we define the Heisenberg (or theta) group

$$\Theta_E := \{(f, P) \in \bar{K}_v(E) \times E[2] : \text{the divisor of } f \text{ is } 2[P] - 2[O]\}$$

with group law

$$(f, P) \cdot (g, Q) := (\tau_Q^*(f)g, P + Q)$$

where τ_Q is translation by Q on E. The projection $\Theta_E \to E[2]$ induces an exact sequence

$$1 \longrightarrow \bar{K}_v^\times \longrightarrow \Theta_E \longrightarrow E[2] \longrightarrow 0. \tag{5.1}$$

We view Θ_E as an extension of $E[2]$ by $\mathbf{G}_m$, functorial in the sense that if E' is another elliptic curve over K_v and $\lambda : E \to E'$ is an isomorphism over $\bar{K}_v$, then λ induces an isomorphism $\lambda^* : \Theta_{E'} \to \Theta_E$ over $\bar{K}_v$ (that commutes with (5.1) in the obvious sense). It is easy to see that the map

$$\mathrm{Isom}(E, E') \longrightarrow \mathrm{Isom}(\Theta_{E'}, \Theta_E)$$

defined by $\lambda \mapsto \lambda^*$ is a G_{K_v}-equivariant homomorphism.

With this notation, $q_{E,v} : H^1(K_v, E[2]) \to H^2(K_v, \bar{K}_v^\times) \subset \mathbf{Q}/\mathbf{Z}$ is the connecting map of the long exact sequence of (nonabelian) Galois cohomology attached to (5.1).

Fix an isomorphism $\lambda : E \to E^\chi$ defined over the quadratic field cut out by χ. For every $\sigma \in G_{K_v}$ we have $\lambda^\sigma = \lambda \circ [\chi(\sigma)]$, where $[\chi(\sigma)] : E \to E$ is multiplication by $\chi(\sigma) = \pm 1$. Thus the isomorphism $\lambda^* : \Theta_{E^\chi} \to \Theta_E$ induced by λ satisfies $(\lambda^*)^\sigma = (\lambda^\sigma)^* = [\pm 1]^* \circ \lambda^*$.

Clearly $[-1]$ acts trivially on $E[2]$. Suppose $f \in \bar{K}_v(E)$ has divisor $2[P] - 2[O]$ with $P \in E[2] - O$. If we fix a Weierstrass model of E with coordinate functions X, Y, then f is a constant multiple of $X - X(P)$, so $f \circ [-1] = f$. Hence $[-1]^*$ is the identity on Θ_E, so in fact $(\lambda^*)^\sigma = \lambda^*$ for every $\sigma \in G_{K_v}$. Hence Θ_{E^χ} and Θ_E are isomorphic over K_v as extensions of $E[2]$, so by the definition above we have $q_{E^\chi,v} = q_{E,v}$. □

Definition 5.3. Let π denote any generator of the ideal $\mathfrak{p}$ of $\mathcal{O}$. If v is a place of K and $\chi \in \mathcal{C}(K_v)$, define $\alpha_v(\chi)$ to be the image of the composition of the Kummer "division by π" map with the isomorphism of Lemma 5.2(i)

$$\alpha_v(\chi) := \mathrm{image}\Big(E^\chi(K_v)/\mathfrak{p}E^\chi(K_v) \hookrightarrow H^1(K_v, E^\chi[\mathfrak{p}]) \xrightarrow{\sim} H^1(K_v, E[p])\Big).$$

Note that $\alpha_v(\chi)$ is independent of the choice of generator π.

Lemma 5.4. *For every place* v *and* $\chi \in \mathcal{C}(K_v)$, *we have* $\alpha_v(\chi) \in \mathcal{H}(q_{E,v})$.

Proof. If $p = 2$, then [17, Proposition 4.10] shows for every v that the image of $E^\chi(K_v)/2E^\chi(K_v)$ in $H^1(K_v, E^\chi[2])$ is a Lagrangian subspace for q_{v,E^χ}. If $p > 2$, then [12, Proposition A.7] (together with Lemma 3.4) shows that $\alpha_v(\chi)$ is a Lagrangian subspace for the (unique) Tate quadratic form on $H^1(K_v, E^\chi[\mathfrak{p}])$, and hence for q_{v,E^χ}. Now the lemma follows from Lemma 5.2(ii). □

As in Definition 4.10, let $h_v(\chi, \chi') := \dim_{\mathbf{F}_p}(\alpha_v(\chi)/(\alpha_v(\chi) \cap \alpha_v(\chi')))$.

Lemma 5.5. *Suppose v is a place of K, and $\chi \in \mathcal{C}(K_v)$. Let F/K_v be the cyclic extension cut out by χ. Then*

$$h_v(\mathbf{1}_v, \chi) = \dim_{\mathbf{F}_p} E(K_v)/N_{F/K_v}E(F).$$

Proof. When $p = 2$, this is due to Kramer [11, Proposition 7]. For general p this is [12, Corollary 5.3]. (That result is stated only for $p > 2$, but the proof for $p = 2$ is the same.) □

Lemma 5.6. *Suppose $p = 2$, $v \in \Sigma$, and $\psi \in \mathcal{C}(K_v)$. Let*

$$\alpha_v^\psi : \mathcal{C}(K_v) \longrightarrow \mathcal{H}(q_{E^\psi,v}) = \mathcal{H}(q_{E,v})$$

and $h_v^\psi(\mathbf{1}_v, \chi) := \dim_{\mathbf{F}_2}(\alpha_v^\psi(\mathbf{1}_v)/(\alpha_v^\psi(\mathbf{1}_v) \cap \alpha_v^\psi(\chi)))$ be as defined in Definitions 5.3 and 4.10, respectively, for E^ψ instead of E. Then

$$h_v^\psi(\mathbf{1}_v, \chi) = h_v(\psi, \chi\psi) \equiv h_v(\mathbf{1}_v, \psi) + h_v(\mathbf{1}_v, \chi\psi) \pmod 2.$$

Proof. It follows directly from Definition 5.3 that $\alpha_v^\psi(\chi) = \alpha_v(\chi\psi)$ for every $\chi \in \mathcal{C}(K_v)$. This proves the equality, and the congruence follows from Corollary 2.5 applied to the Lagrangian subspaces $\alpha_v(\mathbf{1}_v)$, $\alpha_v(\psi)$, and $\alpha_v(\psi\chi)$. □

Lemma 5.7. *Suppose $p > 2$, $v \in \mathcal{P}_2$, and $\chi \in \mathcal{C}(K_v)$ is nontrivial. If F is the cyclic extension of K_v corresponding to χ, then*

$$\alpha_v(\chi) = \mathrm{Hom}(\mathrm{Gal}(F/K_v), E[p]) \subset \mathrm{Hom}(G_{K_v}, E[p]) = H^1(K_v, E[p]).$$

Proof. Let $G := \mathrm{Gal}(F/K_v)$. Fix a generator σ of G, and let $\pi = 1 - \chi(\sigma) \in \mathcal{O}$, so $\pi\mathcal{O} = \mathfrak{p}$. Let $\mathcal{I} := (\sigma - 1)\mathbf{Z}[G]$ be the augmentation ideal of $\mathbf{Z}[G]$. By [14, Theorem 2.2(ii)], we have an isomorphism of $\mathcal{O}[G_{K_v}]$-modules

$$E^\chi[p] = \mathcal{I} \otimes_{\mathbf{Z}} E[p]$$

where $\gamma \in G_{K_v}$ acts by $\gamma^{-1} \otimes \gamma$ on $\mathcal{I} \otimes E[p]$, and π acts as multiplication by $(1 - \sigma) \otimes 1$ on $\mathcal{I} \otimes E[p]$. Since $v \in \mathcal{P}_2$, G_{K_v} acts trivially on $E[p]$, and G_F acts trivially on both $\mathcal{I}$ and $E[p]$. Hence

$$\begin{aligned} E^\chi(K_v)[p] = E^\chi[p]^{G_{K_v}} &= (\mathcal{I} \otimes_{\mathbf{Z}} E[p])^{G_{K_v}} \\ &= (\mathcal{I} \otimes_{\mathbf{Z}} E[p])^{\sigma=1} = (\mathcal{I} \otimes_{\mathbf{Z}} E[p])^{\pi=0} = E^\chi[\mathfrak{p}], \end{aligned} \tag{5.2}$$

$$E^\chi(F)[p] = E^\chi[p]^{G_F} = (\mathcal{I} \otimes_{\mathbf{Z}} E[p])^{G_F} = \mathcal{I} \otimes_{\mathbf{Z}} E[p] = E^\chi[p]. \tag{5.3}$$

Since $p > 2$, we have $\mathfrak{p}^2 \mid p$, so it follows from (5.2) that $E^\chi(K_v)[p^\infty] = E^\chi[\mathfrak{p}]$. Therefore since $v \nmid p\infty$, we have $E^\chi(K_v) \cong E^\chi[\mathfrak{p}] \times B$ with a profinite abelian group B such that $pB = B$, so we deduce from (5.3) that $E^\chi(K_v) \subset \pi E^\chi(F)$. Identifying $H^1(K_v, E[p])$ with $\mathrm{Hom}(G_{K_v}, E[p])$, it follows from Definition 5.3 that if $c \in \alpha_v(\chi) \subset \mathrm{Hom}(G_{K_v}, E[p])$, then $c(G_F) = 0$. Thus $\alpha_v(\chi) \subset \mathrm{Hom}(\mathrm{Gal}(F/K_v), E[p])$. By Lemma 3.7(ii) we have $\dim_{\mathbf{F}_p} \alpha_v(\chi) = 2 = \dim_{\mathbf{F}_p} \mathrm{Hom}(\mathrm{Gal}(F/K_v), E[p])$, which completes the proof. □

Proposition 5.8. *The maps α_v of Definition 5.3, for $v \in \Sigma$ and $v \in \mathcal{P}_2$, give twisting data as in Definition 4.4.*

Proof. It follows from the definition that $\alpha_v(\chi)$ depends only on the extension of K_v cut out by χ.

By Lemma 5.4, $\alpha_v(\chi) \in \mathcal{H}(q_{E,v})$ for every v and every $\chi \in \mathcal{C}(K_v)$. Thus α_v satisfies Definition 4.4(i) for $v \in \Sigma$.

Now suppose that $v \in \mathcal{P}_2$. If $\chi \in \mathcal{C}_{\mathrm{ram}}(K_v)$, then $\alpha_v(\chi) \cap H^1_{\mathrm{ur}}(K_v, T) = 0$ by [13, Lemma 2.11], so $\alpha_v(\chi) \in \mathcal{H}_{\mathrm{ram}}(q_{E,v})$. To complete the proof of the proposition we need only show that the map $\alpha_v : \mathcal{C}_{\mathrm{ram}}(K_v)/\mathrm{Aut}(\boldsymbol{\mu}_p) \to \mathcal{H}_{\mathrm{ram}}(q_{E,v})$ is a bijection. Since

$$|\mathcal{C}_{\mathrm{ram}}(K_v)/\mathrm{Aut}(\boldsymbol{\mu}_p)| = p = |\mathcal{H}_{\mathrm{ram}}(q_{E,v})|$$

by local class field theory and Lemma 3.7(iii), we only need to show the injectivity of α_v, and when $p > 2$ this follows from Lemma 5.7.

Suppose $p = 2$. Let $\psi, \chi \in \mathcal{C}(K_v)$ be a ramified and nontrivial unramified character, respectively. Then $\mathcal{C}_{\mathrm{ram}}(K_v) = \{\psi, \chi\psi\}$, so we need only show that $\alpha_v(\psi) \neq \alpha_v(\chi\psi)$.

Let F be the unramified quadratic extension of K_v. Since $v \in \mathcal{P}_2$, we have that $v \nmid 2$, E has good reduction at v, and G_{K_v} acts trivially on $E[2]$. Since ψ is ramified over F, E^ψ has additive reduction over F above v. Tate's algorithm [25] shows that $E^\psi(F)[2^\infty] = E^\psi(F)[2] = E^\psi(K_v)[2] = E[2]$, and so $E^\psi(K_v)$ and $E^\psi(F)$ are each isomorphic to the product of the Klein 4-group $E[2]$ with profinite abelian groups of odd order. Hence $\mathbf{N}_{F/K_v} E^\psi(F) = 2E^\psi(K_v)$, so by Lemmas 5.5 and 5.6

$$2 = h_v^\psi(\mathbf{1}_v, \chi) = h_v(\psi, \chi\psi) = \dim_{\mathbf{F}_2}(\alpha_v(\psi)/(\alpha_v(\psi) \cap \alpha_v(\chi\psi)))$$

and in particular $\alpha_v(\psi) \neq \alpha_v(\chi\psi)$. □

Proposition 5.9. *With the twisting data of Definition 5.3, and any generator π of $\mathfrak{p}$, for $\chi \in \mathcal{C}(K)$ we have that $\mathrm{Sel}(E[p], \chi) \cong \mathrm{Sel}_\pi(E^\chi/K)$, the usual π-Selmer group of E^χ/K. In particular when $p = 2$, $\mathrm{Sel}(E[2], \chi) = \mathrm{Sel}_2(E^\chi/K)$ is the classical 2-Selmer group of E^χ/K.*

Proof. Let $\mathfrak{d} \in \mathcal{D}$ be such that $\chi \in \mathcal{C}(\mathfrak{d})$. By definition

$$\mathrm{Sel}_\pi(E^\chi/K) \cong \{c \in H^1(K, E[p]) : c_v \in \alpha_v(\chi) \text{ for every } v\}$$

with $\alpha_v(\chi)$ as in Definition 5.3. Thus we need to show that $H^1_{\mathcal{S}(\gamma)}(K_v, T) = \alpha_v(\chi)$ for every v, where $\gamma := \eta_\mathfrak{d}(\chi) \in \Gamma_\mathfrak{d}$.

If $v \in \Sigma$, or if $v \mid \mathfrak{d}$ and $v \in \mathcal{P}_2$, then this is the definition of $H^1_{\mathcal{S}(\gamma)}(K_v, T)$. If $v \in \mathcal{P}_0$ and χ is ramified at v, then $H^1(K_v, T) = 0$ by Lemma 3.7(i), and if $v \notin \Sigma$ and χ is unramified at v, then $\alpha_v(\chi) = H^1_{\mathrm{ur}}(K_v, T)$ by [1, Lemma 4.1], so in those cases we also have $H^1_{\mathcal{S}(\gamma)}(K_v, T) = \alpha_v(\chi)$.

It remains only to check those v such that $v \mid \mathfrak{d}$ and $v \in \mathcal{P}_1$. In that case $\alpha_v(\chi) \cap H^1_{\mathrm{ur}}(K_v, T) = 0$ by [13, Lemma 2.11], so $\alpha_v(\chi) \subset \mathcal{H}_{\mathrm{ram}}(q_{E,v})$. But in this case $|\mathcal{H}_{\mathrm{ram}}(q_{E,v})| = 1$ by Lemma 3.7(iii), and $H^1_{\mathcal{S}(\gamma)}(K_v, T)$ is the unique element of $\mathcal{H}_{\mathrm{ram}}(q_{E,v})$ by definition, so $H^1_{\mathcal{S}(\gamma)}(K_v, T) = \alpha_v(\chi)$ in this case also. This completes the proof. □

Remark 5.10. Definition 5.1 of E^χ shows that E^χ depends only on the field cut out by χ, not on the choice of character χ itself. As mentioned in Remark 4.8, it is easier to count characters of order p than cyclic extensions of degree p, because the set of characters is a group.

If F/K is the cyclic extension cut out by $\chi \neq \mathbf{1}_K$, then the short exact sequence $0 \to E^\chi \to \mathrm{Res}_K^F(E) \to E \to 0$ of Definition 5.1 gives an identity of Mordell-Weil ranks

$$\mathrm{rank}(E(F)) = \mathrm{rank}(\mathrm{Res}_K^F(E)(K)) = \mathrm{rank}(E(K)) + \mathrm{rank}(E^\chi(K)).$$

In particular if $\mathrm{Sel}(E[p], \chi) = 0$, then by Proposition 5.9 we have $\mathrm{rank}(E(F)) = \mathrm{rank}(E(K))$.

6. Local and global characters

For the rest of this paper we fix T and Σ as in §1, a global metabolic structure $\mathbf{q}$ on T as in Definition 3.3, and twisting data as in Definition 4.4. Recall that $K(T)$ is the field of definition of the elements of T, i.e., the fixed field in $\bar{K}$ of $\ker(G_K \to \mathrm{Aut}(T))$.

For the rest of this paper we assume also that

$$\mathrm{Pic}(\mathcal{O}_{K,\Sigma}) = 0, \tag{6.1}$$

and

$$\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^p \longrightarrow \prod_{v \in \Sigma} K_v^\times/(K_v^\times)^p \quad \text{is injective,} \tag{6.2}$$

where $\mathcal{O}_{K,\Sigma}$ is the ring of Σ-integers of K, i.e., the elements that are integral at all $\mathfrak{q} \notin \Sigma$.

Lemma 6.1. *Conditions* (6.1) *and* (6.2) *can always be satisfied by enlarging* Σ *if necessary.*

Proof. First, enlarge Σ if necessary by adding primes $\mathfrak{q}$ whose classes generate the ideal class group of $\mathcal{O}_K$. After this we will have (6.1). Further increases will preserve this condition.

Let f_Σ denote the natural map $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^p \to \prod_{v\in\Sigma} K_v^\times/(K_v^\times)^p$, and suppose $u \in \ker(f_\Sigma)$ is nontrivial. The kernel of $K^\times/(K^\times)^p \to K(\boldsymbol{\mu}_p)^\times/(K(\boldsymbol{\mu}_p)^\times)^p$ is $H^1(K(\boldsymbol{\mu}_p)/K, \boldsymbol{\mu}_p) = 0$, so $u \notin (K(\boldsymbol{\mu}_p)^\times)^p$ and $[K(\boldsymbol{\mu}_p, u^{1/p}) : K(\boldsymbol{\mu}_p)] = p$. Let $\mathfrak{q}$ be a prime of K whose Frobenius automorphism in $\mathrm{Gal}(K(\boldsymbol{\mu}_p, u^{1/p})/K)$ has order p. Then $u \notin (K_\mathfrak{q}^\times)^p$, so $f_{\Sigma\cup\{\mathfrak{q}\}}(u) \neq 1$.

Let $\Sigma' := \Sigma \cup \{\mathfrak{q}\}$. Since $\mathrm{Pic}(\mathcal{O}_\Sigma) = 0$, there is a $\lambda \in \mathcal{O}_{K,\Sigma'}$ such that $\mathrm{ord}_\mathfrak{q}(\lambda) = 1$. Thus $\mathcal{O}_{K,\Sigma'}^\times = \mathcal{O}_{K,\Sigma}^\times \times \langle\lambda\rangle$, where $\langle\lambda\rangle$ is the infinite cyclic group generated by λ. The map $\langle\lambda\rangle/\langle\lambda^p\rangle \to K_\mathfrak{q}^\times/(K_\mathfrak{q}^\times)^p$ is injective, so $\ker(f_{\Sigma'}) \subsetneq \ker(f_\Sigma)$ and the inclusion is strict because $\ker(f_\Sigma)$ contains u and $\ker(f_{\Sigma'})$ does not. Replacing Σ by Σ', we can continue in this way until $\ker(f_\Sigma) = 1$, i.e., until (6.2) holds. □

Lemma 6.2. *Define the subgroup* $\mathcal{A} \subset K^\times/(K^\times)^p$ *by*

$$\mathcal{A} := \ker(K^\times/(K^\times)^p \to K(T)^\times/(K(T)^\times)^p).$$

Then there is a canonical isomorphism

$$\mathcal{A} \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p)), \boldsymbol{\mu}_p)^{\mathrm{Gal}(K(T)/K)},$$

and $\mathcal{A}$ *is cyclic, generated by an element* $\Delta \in \mathcal{O}_{K,\Sigma}^\times$.

Proof. The inflation-restriction sequence of Galois cohomology, together with the fact that $H^1(F,\boldsymbol{\mu}_p) = F^\times/(F^\times)^p$ for every field F of characteristic different from p, shows that

$$\mathcal{A} = \ker(H^1(K,\boldsymbol{\mu}_p) \to H^1(K(T),\boldsymbol{\mu}_p)) = H^1(K(T)/K,\boldsymbol{\mu}_p).$$

Since $[K(\boldsymbol{\mu}_p):K]$ is prime to p, the Hochschild-Serre spectral sequence gives an isomorphism

$$\begin{aligned}\mathcal{A} = H^1(K(T)/K,\boldsymbol{\mu}_p) \xrightarrow{\sim} H^1(K(T)/K(\boldsymbol{\mu}_p),\boldsymbol{\mu}_p)^{\mathrm{Gal}(K(T)/K)}\\ = \mathrm{Hom}(\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p)),\boldsymbol{\mu}_p)^{\mathrm{Gal}(K(T)/K)}.\end{aligned}$$

Since $\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$ is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbf{F}_p)$, we see that $\mathrm{Hom}(\mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p)),\boldsymbol{\mu}_p)$ has order 1 or p. Thus $\mathcal{A}$ is cyclic.

Let $I_{K,\Sigma}$ (resp., $I_{K(T),\Sigma}$) denote the group of fractional ideals of K (resp., $K(T)$) prime to Σ. We have a commutative diagram

$$\begin{array}{ccccccc} 1 \to \mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^p & \longrightarrow & K^\times/(K^\times)^p & \longrightarrow & I_{K,\Sigma}/I_{K,\Sigma}^p & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \\ & & K(T)^\times/(K(T)^\times)^p & \longrightarrow & I_{K(T),\Sigma}/I_{K(T),\Sigma}^p & & \end{array}$$

in which the top row is exact by (6.1). Since $K(T)/K$ is unramified outside of Σ, the right-hand vertical map is injective, so $\mathcal{A}$ (the kernel of the left-hand vertical map) is contained in the image of of $\mathcal{O}_{K,\Sigma}^\times$. This completes the proof of the lemma. □

Lemma 6.3. *Suppose $p \le 3$, E is an elliptic curve over K, and $T = E[p]$. Then we can take the element Δ of Lemma 6.2 to be the discriminant Δ_E of (any model of) E.*

Proof. Since Σ contains all primes where E has bad reduction, we have $\Delta_E \in \mathcal{O}_{K,\Sigma}^\times \cdot (K^\times)^{12}$. By Lemma 6.2, $\mathcal{A} = \{1\}$ if $p \nmid [K(E[p]):K]$.

Suppose first that $p = 2$. Then $\Delta_E \in (K(E[2])^\times)^2$ and $[K(E[2]) : K(\sqrt{\Delta_E})]$ divides 3. Thus $\Delta_E \in (K^\times)^2$ if and only if $2 \nmid [K(E[2]):K]$, so Δ_E generates $\mathcal{A}$.

Similarly, when $p = 3$, computing the discriminant of the universal elliptic curve with full level 3 structure (see for example [20, §1.1]) shows that $\Delta_E \in (K(E[3])^\times)^3$ and that $[K(E[3]) : K(\boldsymbol{\mu}_3, \sqrt[3]{\Delta_E})]$ divides 8, so again Δ_E generates $\mathcal{A}$. □

Fix once and for all a $\Delta \in \mathcal{O}_{K,\Sigma}^\times$ as in Lemma 6.2. Recall (Definition 4.6) that $\Gamma_1 := \prod_{v\in\Sigma}\mathcal{C}(K_v)$, and more generally $\Gamma_\mathfrak{d} := \prod_{v\in\Sigma}\mathcal{C}(K_v) \times \prod_{\mathfrak{q}|\mathfrak{d}_2}\mathcal{C}_{\mathrm{ram}}(K_\mathfrak{q})$ for $\mathfrak{d} \in \mathcal{D}$. For each v, local class field theory identifies $\mathcal{C}(K_v)$ with $\mathrm{Hom}(K_v^\times,\boldsymbol{\mu}_p)$.

Definition 6.4. Define a "sign" homomorphism $\mathrm{sign}_\Delta : \Gamma_1 \to \boldsymbol{\mu}_p$ by

$$\mathrm{sign}_\Delta(\ldots,\gamma_v,\ldots) := \prod_{v\in\Sigma}\gamma_v(\Delta).$$

Composing with the natural maps $\Gamma_\mathfrak{d} \to \Gamma_1$ and $\mathcal{C}(K) \to \Gamma_1$, we will extend sign_Δ to $\Gamma_\mathfrak{d}$ for every $\mathfrak{d} \in \mathcal{D}$, and to $\mathcal{C}(K)$.

Lemma 6.5. *Suppose $\mathcal{A}$ is nontrivial, i.e., $\Delta \notin (K^\times)^p$.*

(i) *If $\mathfrak{q} \in \mathcal{P}_2$ and $\chi_\mathfrak{q} \in \mathcal{C}(K_\mathfrak{q})$, then $\chi_\mathfrak{q}(\Delta) = 1$.*
(ii) *If $\mathfrak{q} \in \mathcal{P}_1$ and $\chi_\mathfrak{q} \in \mathcal{C}(K_\mathfrak{q})$, then $\chi_\mathfrak{q}(\Delta) = 1$ if and only if $\chi_\mathfrak{q}$ is unramified.*

(iii) *If* $p = 2$, $\mathfrak{q} \in \mathcal{P}_0$, *and* $\chi_\mathfrak{q} \in \mathcal{C}(K_\mathfrak{q})$, *then* $\chi_\mathfrak{q}(\Delta) = 1$.

Proof. By Lemma 4.3(i), if $\mathfrak{q} \in \mathcal{P}_2$ then $\mathrm{Frob}_\mathfrak{q}$ fixes $K(T)$, so $\mathrm{Frob}_\mathfrak{q}$ fixes $\Delta^{1/p}$, so $\Delta \in (K_\mathfrak{q}^\times)^p$. This proves (i). Similarly, if $p = 2$ and $\mathfrak{q} \in \mathcal{P}_0$ then Lemma 4.3(iii) shows that $\mathrm{Frob}_\mathfrak{q} \in \mathrm{Gal}(K(T)/K)$ has order 3. Thus again $\mathrm{Frob}_\mathfrak{q}$ fixes $\sqrt{\Delta}$, so $\Delta \in (K_\mathfrak{q}^\times)^2$. This proves (iii).

If $\mathfrak{q} \in \mathcal{P}_1$ then Lemma 4.3(ii) shows that $\mathrm{Frob}_\mathfrak{q} \in \mathrm{Gal}(K(T)/K)$ has order exactly p, and in particular $\mathrm{Frob}_\mathfrak{q} \in \mathrm{Gal}(K(T)/K(\boldsymbol{\mu}_p))$. But since $\Delta \notin (K^\times)^p$, the degree $[K(T) : K(\boldsymbol{\mu}_p, \Delta^{1/p})]$ is prime to p. Thus $\mathrm{Frob}_\mathfrak{q}$ does not fix $\Delta^{1/p}$, so $\Delta \notin (K_\mathfrak{q}^\times)^p$. Therefore Δ generates $\mathcal{O}_\mathfrak{q}^\times/(\mathcal{O}_\mathfrak{q}^\times)^p \cong \mathbf{Z}/p\mathbf{Z}$, where $\mathcal{O}_\mathfrak{q}$ is the ring of integers of $K_\mathfrak{q}$. It follows that for $\chi_\mathfrak{q} \in \mathcal{C}(K_\mathfrak{q})$, we have $\chi_\mathfrak{q}(\Delta) = 1$ if and only if $\chi_\mathfrak{q}(\mathcal{O}_\mathfrak{q}^\times) = 1$. This is (ii). □

Lemma 6.6. *Suppose G and H are abelian groups, and $J \subset G \times H$ is a subgroup. Let π_G and π_H denote the projection maps from $G \times H$ to G and H, respectively. Let* $J_0 := \ker(J \xrightarrow{\pi_G} G/G^p)$.

(i) *The image of the natural map* $\mathrm{Hom}((G \times H)/J, \boldsymbol{\mu}_p) \to \mathrm{Hom}(H, \boldsymbol{\mu}_p)$ *is* $\mathrm{Hom}(H/\pi_H(J_0), \boldsymbol{\mu}_p)$.
(ii) *If* $J/J^p \to G/G^p$ *is injective, then* $\mathrm{Hom}((G \times H)/J, \boldsymbol{\mu}_p) \to \mathrm{Hom}(H, \boldsymbol{\mu}_p)$ *is surjective.*

Proof. We have an exact sequence of $\mathbf{F}_p$-vector spaces

$$0 \longrightarrow \pi_H(J_0)H^p/H^p \longrightarrow H/H^p \longrightarrow (G \times H)/J(G \times H)^p.$$

Assertion (i) follows by applying $\mathrm{Hom}(\,\cdot\,, \boldsymbol{\mu}_p)$, and (ii) follows directly from (i). □

Lemma 6.7. (i) *The natural map* $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^p \to \prod_{\mathfrak{q} \notin \Sigma} \mathcal{O}_\mathfrak{q}^\times/(\mathcal{O}_\mathfrak{q}^\times)^p$ *is injective.*
(ii) *The kernel of the natural map* $\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^p \to \prod_{\mathfrak{q} \in \mathcal{P}_2} \mathcal{O}_\mathfrak{q}^\times/(\mathcal{O}_\mathfrak{q}^\times)^p$ *is* $\mathcal{A}$.

Proof. Suppose $\alpha \in \mathcal{O}_{K,\Sigma}^\times$, $\alpha \notin (\mathcal{O}_{K,\Sigma}^\times)^p$. Then $\alpha \notin (K(\boldsymbol{\mu}_p)^\times)^p$. If $\mathfrak{q} \notin \Sigma$ is any prime whose Frobenius in $\mathrm{Gal}(K(\boldsymbol{\mu}_p, \alpha^{1/p})/K(\boldsymbol{\mu}_p))$ is nontrivial, then $\alpha \in \mathcal{O}_\mathfrak{q}^\times$ but $\alpha \notin (\mathcal{O}_\mathfrak{q}^\times)^p$. Thus α is not in the kernel of the map of (i), and (i) follows.

Now suppose $\alpha \notin \mathcal{A}$. Then $\alpha^{1/p} \notin K(T)$, so we can choose a nontrivial automorphism $\sigma \in \mathrm{Gal}(K(T, \alpha^{1/p})/K(T))$. Suppose $\mathfrak{q} \notin \Sigma$ is a prime whose Frobenius in $\mathrm{Gal}(K(T, \alpha^{1/p})/K)$ is σ. Then $\mathfrak{q} \in \mathcal{P}_2$ by Lemma 4.3(i), and $\alpha \in \mathcal{O}_\mathfrak{q}^\times$ but $\alpha \notin (\mathcal{O}_\mathfrak{q}^\times)^p$. This shows that the kernel of the map of (ii) is contained in $\mathcal{A}$, and $\mathcal{A}$ is contained in the kernel by Lemma 6.5(i). □

Proposition 6.8. (i) *The natural homomorphism* $\mathcal{C}(K) \to \Gamma_1$ *is surjective.*
(ii) *If* $\mathfrak{q} \notin \Sigma$ *and* $\boldsymbol{\mu}_p \subset K_\mathfrak{q}^\times$, *then there is a* $\chi \in \mathcal{C}(K)$ *ramified at* $\mathfrak{q}$ *and unramified outside of* Σ *and* $\mathfrak{q}$.
(iii) *There is a finite subgroup of* $\mathcal{C}(K)$, *containing only characters unramified outside of* Σ *and* $\mathcal{P}_2$, *whose image in* Γ_1 *is* $\ker(\mathrm{sign}_\Delta)$.

Proof. Let $\mathbf{A}_K^\times$ denote the ideles of K. Global class field theory and (6.1) show that

$$\mathcal{C}(K) = \mathrm{Hom}(\mathbf{A}_K^\times/K^\times, \boldsymbol{\mu}_p) = \mathrm{Hom}((\textstyle\prod_{v \in \Sigma} K_v^\times \times \prod_{\mathfrak{q} \notin \Sigma} \mathcal{O}_\mathfrak{q}^\times)/\mathcal{O}_{K,\Sigma}^\times, \boldsymbol{\mu}_p). \tag{6.3}$$

For (i), we apply Lemma 6.6(ii) with

$$G := \prod_{\mathfrak{q} \notin \Sigma} \mathcal{O}_{\mathfrak{q}}^{\times}, \quad H := \prod_{v \in \Sigma} K_v^{\times}, \quad J := \mathcal{O}_{K,\Sigma}^{\times}.$$

Then $J/J^p \to G/G^p$ is injective by Lemma 6.7(i), so Lemma 6.6(ii) and (6.3) show that

$$\mathcal{C}(K) \twoheadrightarrow \mathrm{Hom}(\textstyle\prod_{v \in \Sigma} K_v^{\times}, \boldsymbol{\mu}_p) = \Gamma_1$$

is surjective.

For (ii), we apply Lemma 6.6(ii) with

$$G := \prod_{v \in \Sigma} K_v^{\times}, \quad H := \prod_{v \notin \Sigma} \mathcal{O}_v^{\times}, \quad J := \mathcal{O}_{K,\Sigma}^{\times}.$$

Assumption (6.2) says that the map $J/J^p \to G/G^p$ is injective, so by Lemma 6.6(ii) and (6.3) we have that

$$\mathcal{C}(K) \twoheadrightarrow \mathrm{Hom}(\textstyle\prod_{v \notin \Sigma} \mathcal{O}_v^{\times}, \boldsymbol{\mu}_p) \tag{6.4}$$

is surjective. If $\boldsymbol{\mu}_p \subset K_{\mathfrak{q}}^{\times}$ then we can fix an element $\psi \in \mathrm{Hom}(\prod_{v \notin \Sigma} \mathcal{O}_v^{\times}, \boldsymbol{\mu}_p)$ such that $\psi(\mathcal{O}_{\mathfrak{q}}^{\times}) \neq 1$ but $\psi(\mathcal{O}_v^{\times}) = 1$ if $v \neq \mathfrak{q}$, and let $\chi \in \mathcal{C}(K)$ be a character that maps to ψ under (6.4). Then χ satisfies (ii).

For (iii), we apply Lemma 6.6(i) with

$$G := \prod_{\mathfrak{q} \in \mathcal{P}_2} \mathcal{O}_{\mathfrak{q}}^{\times}, \quad H := \prod_{v \in \Sigma} K_v^{\times} \times \prod_{\mathfrak{q} \in \mathcal{P}_0 \cup \mathcal{P}_1} \mathcal{O}_{\mathfrak{q}}^{\times}, \quad J := \mathcal{O}_{K,\Sigma}^{\times}.$$

Lemma 6.7(ii) shows that $\ker(\mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^p \to G/G^p)$ is generated by Δ. Now we deduce from (6.3) and Lemma 6.6(i) that the image of

$$\mathcal{C}(K) \to \mathrm{Hom}(\prod_{v \in \Sigma} K_v^{\times} \times \prod_{\mathfrak{q} \in \mathcal{P}_0 \cup \mathcal{P}_1} \mathcal{O}_{\mathfrak{q}}^{\times}, \boldsymbol{\mu}_p)$$

is $\mathrm{Hom}((\prod_{v \in \Sigma} K_v^{\times} \times \prod_{\mathfrak{q} \in \mathcal{P}_0 \cup \mathcal{P}_1} \mathcal{O}_{\mathfrak{q}}^{\times})/\langle \Delta \rangle, \boldsymbol{\mu}_p)$. Restricting to characters unramified at $\mathcal{P}_0 \cup \mathcal{P}_1$ proves (iii), since $\ker(\mathrm{sign}_{\Delta}) = \mathrm{Hom}((\prod_{v \in \Sigma} K_v^{\times})/\langle \Delta \rangle, \boldsymbol{\mu}_p)$. □

7. Parity disparity ($p = 2$)

Fix T and Σ as in §1, a global metabolic structure $\mathbf{q}$ on T as in Definition 3.3, and twisting data as in Definition 4.4. In this section we let $p = 2$ and we study how the parity of $\dim_{\mathbf{F}_2} \mathrm{Sel}(T, \chi)$ varies as χ varies. The main result is Theorem 7.6. When $T = E[2]$ with an elliptic curve E/K, Theorem 7.6 specializes to Theorem A of the Introduction, and we make Theorem A more explicit in Proposition 7.9, Corollary 7.10, and Example 7.11.

Suppose throughout this section that $p = 2$ and that (6.1) and (6.2) are satisfied. Let $\Delta \in \mathcal{O}_{K,\Sigma}^{\times}$ be as in Lemma 6.2.

If $\chi \in \mathcal{C}(K)$, let $r(\chi) := \dim_{\mathbf{F}_2} \mathrm{Sel}(T, \chi)$, where $\mathrm{Sel}(T, \chi)$ is given by Definition 4.7, the Selmer group for the twist of T by χ. If $T = E[2]$ with the natural twisting data, then $r(\chi) = \dim_{\mathbf{F}_2} \mathrm{Sel}_2(E^{\chi}/K)$ by Proposition 5.9.

Recall the function $h_v(\chi, \chi') := \dim_{\mathbf{F}_2} \alpha_v(\chi)/(\alpha_v(\chi) \cap \alpha_v(\chi'))$ of Definition 4.10.

Definition 7.1. For every $v \in \Sigma$, define a map (of sets) $\omega_v : \mathcal{C}(K_v) \to \{\pm 1\}$ by

$$\omega_v(\chi_v) := (-1)^{h_v(\mathbf{1}_v, \chi_v)} \chi_v(\Delta).$$

Proposition 7.2. *Suppose* $\chi \in \mathcal{C}(K)$. *Then*

$$r(\chi) \equiv r(\mathbf{1}_K) \pmod 2 \iff \prod_{v\in\Sigma} \omega_v(\chi_v) = 1.$$

Proof. We will deduce this from Theorem 4.11. Fix $\mathfrak{d} \in \mathcal{D}$ such that $\chi \in \mathcal{C}(\mathfrak{d})$. If $\mathfrak{q} \in \mathcal{P}_0 \cup \mathcal{P}_2$, then $\chi_\mathfrak{q}(\Delta) = 1$ by Lemma 6.5(i,iii). If $\mathfrak{q} \in \mathcal{P}_1$, then $\chi_\mathfrak{q}(\Delta) = -1$ if $\mathfrak{q} \mid \mathfrak{d}$, and $\chi_\mathfrak{q}(\Delta) = 1$ if $\mathfrak{q} \nmid \mathfrak{d}$, by Lemma 6.5(ii). Therefore

$$\prod_{\mathfrak{q}\notin\Sigma} \chi_\mathfrak{q}(\Delta) = (-1)^{|\{\mathfrak{q}:\mathfrak{q}\,\in\,\mathcal{P}_1 \text{ and } \mathfrak{q}\,\mid\,\mathfrak{d}\}|} = (-1)^{w(\mathfrak{d})}$$

so by Theorem 4.11,

$$r(\chi) \equiv r(\mathbf{1}_K) \pmod 2 \iff \prod_{v\in\Sigma} (\omega_v(\chi_v)\chi_v(\Delta)) \prod_{v\notin\Sigma} \chi_v(\Delta) = 1.$$

Global class field theory shows that $\prod_v \chi_v(\Delta) = 1$, and the proposition follows. □

Definition 7.3. Define a (set) function $\mathcal{C}(K) \to \mathbf{Z}_{>0}$ measuring the "size" of a character χ by

$$||\chi|| := \max\{\mathbf{N}\mathfrak{q} : \chi \text{ is ramified at } \mathfrak{q}\}$$

If $X > 0$, let $\mathcal{C}(K, X) \subset \mathcal{C}(K)$ be the subgroup

$$\mathcal{C}(K, X) := \{\chi \in \mathcal{C}(K) : ||\chi|| < X\}.$$

Definition 7.4. For every $v \in \Sigma$ define

$$\delta_v := \frac{1}{|\mathcal{C}(K_v)|} \sum_{\chi\in\mathcal{C}(K_v)} \omega_v(\chi), \quad \text{and} \quad \delta := (-1)^{r(\mathbf{1}_K)} \prod_{v\in\Sigma} \delta_v.$$

Note that $-1+2/|\mathcal{C}(K_v)| \le \delta_v \le 1$ for every v (since $\omega_v(\mathbf{1}_v) = 1$) and $\delta \in [-1, 1]$.

Lemma 7.5.

$$\frac{|\{\gamma \in \Gamma_1 : \prod_{v\in\Sigma} \omega_v(\gamma_v) = 1\}|}{|\Gamma_1|} = \frac{1 + \prod_{v\in\Sigma} \delta_v}{2}.$$

Proof. Let $N = |\{\gamma \in \Gamma_1 : \prod_{v\in\Sigma} \omega_v(\gamma_v) = 1\}|$. Since $\Gamma_1 = \prod_{v\in\Sigma} \mathcal{C}(K_v)$, we have

$$N - (|\Gamma_1| - N) = \sum_{\gamma\in\Gamma_1} \prod_{v\in\Sigma} \omega_v(\gamma_v) = \prod_{v\in\Sigma} \Bigl(\sum_{\gamma_v\in\mathcal{C}(K_v)} \omega_v(\gamma_v) \Bigr)$$

and dividing both sides by $|\Gamma_1| = \prod_{v\in\Sigma} |\mathcal{C}(K_v)|$ yields $2N/|\Gamma_1| - 1 = \prod_{v\in\Sigma} \delta_v$. The lemma follows. □

Theorem 7.6. *For all sufficiently large* X,

$$\frac{|\{\chi \in \mathcal{C}(K, X) : \dim_{\mathbf{F}_2} \mathrm{Sel}(T, \chi) \textit{ is even}\}|}{|\mathcal{C}(K, X)|} = \frac{1 + \delta}{2}.$$

Proof. Suppose X is large enough so that the natural group homomorphism $\eta : \mathcal{C}(K, X) \to \Gamma_1$ is surjective (this holds for all sufficiently large X by Proposition 6.8(i)). By Proposition 7.2, the parity of $r(\chi)$ depends only on $\eta(\chi)$. Since η is a homomorphism, all of its fibers have the same size, so by Proposition 7.2

$$\frac{|\{\chi \in \mathcal{C}(K, X) : r(\chi) \equiv r(\mathbf{1}_K) \pmod 2\}|}{|\mathcal{C}(K, X)|} = \frac{|\{\gamma \in \Gamma_1 : \prod_{v\in\Sigma} \omega_v(\gamma_v) = 1\}|}{|\Gamma_1|}.$$

Now the theorem follows from Lemma 7.5. □

Remark 7.7. As the proof shows, the equality of Theorem 7.6 holds with $\mathcal{C}(K,X)$ replaced by any subset $\mathcal{B} \subset \mathcal{C}(K)$ having the property that there is a subgroup $A \subset \mathcal{C}(K)$ such that the natural map $A \to \Gamma_1$ is surjective and $A\mathcal{B} = \mathcal{B}$.

For the rest of this section, we fix an elliptic curve E/K and take $T = E[2]$ with the natural twisting data of Definition 5.3. In this setting Proposition 5.9 shows that Theorem 7.6 specializes to Theorem A of the Introduction. Proposition 7.9 below computes the δ_v for $E[2]$, in all cases when $v \nmid 2$, and in certain cases when $v \mid 2$. We first need the following lemma.

Lemma 7.8. *Suppose $v \in \Sigma$ and $\psi \in \mathcal{C}(K_v)$. Let ω_v be as in Definition 7.1, and let ω_v^ψ be the corresponding quantity defined with the elliptic curve E^ψ over K_v in place of E. Then for every $\chi \in \mathcal{C}(K_v)$, we have*

$$\omega_v^\psi(\chi)\omega_v^\psi(\psi) = \omega_v(\chi\psi).$$

Proof. Let $h_v^\psi(\mathbf{1}_v, \chi)$ be as given by Definition 4.10 for E^ψ in place of E. Then by Lemma 5.6,

$$\begin{aligned}\omega_v^\psi(\chi)\omega_v^\psi(\psi) &= (-1)^{h_v^\psi(\mathbf{1}_v,\chi)}\chi(\Delta)(-1)^{h_v^\psi(\mathbf{1}_v,\psi)}\psi(\Delta) \\ &= (-1)^{h_v(\mathbf{1}_v,\psi)+h_v(\mathbf{1}_v,\chi\psi)+h_v(\mathbf{1}_v,\psi)}\chi\psi(\Delta) = \omega_v(\chi\psi).\end{aligned}$$

□

Proposition 7.9. *Suppose E is an elliptic curve over K, and $T = E[2]$ with the natural twisting data. For every $v \in \Sigma$, let $m_v^\pm := |\{\gamma \in \mathcal{C}(K_v) : \omega_v(\gamma) = \pm 1\}|$, and let $c_v := |K_v^\times/(K_v^\times)^2|$, so $c_v = 4$ if $v \nmid 2\infty$. Then we have the following table, where if $v \nmid \infty$ then "type" denotes the Kodaira type of the Néron model.*

type of v	m_v^+	m_v^-	δ_v
real	1	1	0
complex	1	0	1
split multiplicative	1	$c_v - 1$	$2/c_v - 1$
type I_ν *or* I_ν^*, $\nu > 0$, *not split multiplicative*	$c_v - 1$	1	$1 - 2/c_v$
good reduction or type I_0^*, $v \nmid 2$	4	0	1
type II, IV, II*, IV*, $\Delta \in (K_v^\times)^2$, $v \nmid 2$	4	0	1
type II, IV, II*, IV*, $\Delta \notin (K_v^\times)^2$, $v \nmid 2$	2	2	0
type III, III*, $-1 \in (K_v^\times)^2$, $v \nmid 2$	4	0	1
type III, III*, $-1 \notin (K_v^\times)^2$, $v \nmid 2$	2	2	0

Proof. Most of the entries in the table follow directly from calculations of Kramer [11], using Lemma 5.5. For every v, we have $\omega_v(\mathbf{1}_v) = 1$, and by definition $\delta_v = (m_v^+ - m_v^-)/c_v$.

Case 1: v archimedean. If v is complex then there is nothing to check. Suppose v is real, and let $\chi : K_v^\times \to \pm 1$ be the sign character, the nontrivial element of $\mathcal{C}(K_v)$. By Lemma 5.5 and [11, Proposition 6], we have

$$(-1)^{h_v(\mathbf{1}_v,\chi)} = -\chi(\Delta) \tag{7.1}$$

so $\omega_v(\chi) = -1$. Thus $m_v^+ = m_v^- = 1$.

Case 2: v split multiplicative. In this case Lemma 5.5 and [11, Proposition 1] show that if $\chi \in \mathcal{C}(K_v)$ is nontrivial, then (7.1) holds, so $\omega_v(\chi) = -1$. Thus $m_v^+ = 1$ and $m_v^- = c_v - 1$.

Case 3: v type I_ν or I_ν^*, $\nu > 0$, not split multiplicative. In this case there is a $\psi \in \mathcal{C}(K_v)$, $\psi \neq \mathbf{1}_v$, such that E^ψ is split multiplicative (see for example [22, §1.12]). Case 2 showed that $\omega_v^\psi(\psi) = -1$, and so by Case 2 and Lemma 7.8 we have $m_v^+ = c_v - 1$, $m_v^- = 1$.

Case 4: v good reduction or type I_0^*, $v \nmid 2$. If E has good reduction at v, then Lemma 5.5 and [11, Proposition 3] show that $(-1)^{h_v(\mathbf{1}_v,\chi)} = \chi(\Delta)$ for every $\chi \in \mathcal{C}(K_v)$, so $\omega_v(\chi) = 1$. If E has reduction type I_0^*, then E has a quadratic twist with good reduction, so by Lemma 7.8 we again have $\omega_v(\chi) = 1$ for every χ. In either case $m_v^+ = c_v = 4$, $m_v^- = 0$.

Case 5: v type II, IV, II*, or IV*, $v \nmid 2$. In this case the number of connected components of the Néron model is odd, and E has additive reduction at v, so $E(K_v)$ is 2-divisible. Hence $\alpha_v(\chi)$ is zero for every χ, so $h_v(\mathbf{1}_v, \chi) = 0$, so $\omega_v(\chi) = \chi(\Delta)$. Thus if $\Delta \in (K_v^\times)^2$, then $m_v^+ = c_v = 4$ and $m_v^- = 0$, and if $\Delta \notin (K_v^\times)^2$, then $m_v^+ = m_v^- = 2$.

Case 6: v type III or III*, $v \nmid 2$. Suppose $\chi \in \mathcal{C}(K_v)$, $\chi \neq \mathbf{1}_v$, and let F be the corresponding quadratic extension of K_v. In this case Tate's algorithm [25] shows that

$$E(K_v)[2] \cong \mathbf{Z}/2\mathbf{Z}, \quad E(K_v) = E(K_v)[2] \times B, \quad E(F) = E(F)[2] \times B'$$

with profinite abelian groups B, B' of odd order, and $\mathrm{ord}_v(\Delta)$ is odd. If $F \neq K_v(\sqrt{\Delta})$, then $E(F)[2] = E(K_v)[2]$, so $\mathbf{N}_{F/K_v}E(F) = 2E(K_v) = B$, so $h_v(\mathbf{1}_v, \chi) = 1$ by Lemma 5.5. If $F = K_v(\sqrt{\Delta})$, then $E(F)[2] = E[2]$ and $\mathbf{N}_{F/K_v}E(F) = E(K_v)$, so $h_v(\mathbf{1}_v, \chi) = 0$ by Lemma 5.5.

Fix $u \in \mathcal{O}_v^\times$, $u \notin (\mathcal{O}_v^\times)^2$. We have $\mathcal{C}(K_v) = \{\mathbf{1}_v, \chi_\Delta, \chi_u, \chi_{\Delta u}\}$, where χ_a is the quadratic character corresponding to $K_v(\sqrt{a})$. The discussion above showed that $h_v(\mathbf{1}_v, \mathbf{1}_v) = h_v(\mathbf{1}_v, \chi_\Delta) = 0$ and $h_v(\mathbf{1}_v, \chi_u) = h_v(\mathbf{1}_v, \chi_{\Delta u}) = 1$. We have $\chi_u(\Delta) = -1$, since $K_v(\sqrt{u})/K_v$ is unramified and $\mathrm{ord}_v(\Delta)$ is odd. With $F = K_v(\sqrt{\Delta})$ we have

$$\chi_\Delta(\Delta) = 1 \iff \Delta \in \mathbf{N}_{F/K_v}F^\times \iff -1 \in \mathbf{N}_{F/K_v}F^\times \iff -1 \in (K_v^\times)^2,$$

and with $F = K_v(\sqrt{\Delta u})$ we have

$$\begin{aligned}\chi_{\Delta u}(\Delta) = 1 \iff \Delta \in \mathbf{N}_{F/K_v}F^\times &\iff -u \in \mathbf{N}_{F/K_v}F^\times \\ &\iff -u \in (K_v^\times)^2 \iff -1 \notin (K_v^\times)^2,\end{aligned}$$

Combining these facts gives the entries in the last two rows of the table. □

Corollary 7.10. (i) *If K has a real embedding, then for all sufficiently large X we have*

$$|\{\chi \in \mathcal{C}(K,X) : r(\chi) \text{ is odd}\}| = |\{\chi \in \mathcal{C}(K,X) : r(\chi) \text{ is even}\}| = \frac{|\mathcal{C}(K,X)|}{2}.$$

(ii) *If K has no real embeddings, E/K is semistable, and E has multiplicative reduction at all primes above 2, then for all sufficiently large X*

$$\frac{|\{\chi \in \mathcal{C}(K,X) : r(\chi) \text{ is even}\}|}{|\mathcal{C}(K,X)|} = \frac{1+\delta}{2} \notin \{0, \tfrac{1}{2}, 1\}.$$

Proof. If K has a real place v, then Proposition 7.9 shows that $\delta_v = 0$, so (i) follows from Theorem 7.6.

Under the hypotheses of (ii), Proposition 7.9 shows that

- $\delta_v = 1$ for every archimedean place and every place of good reduction,
- $|\delta_v| = \frac{1}{2}$ for every place $v \nmid 2$ of bad reduction, since $c_v = 4$,
- $|\delta_v| = 1 - 2^{-[K_v:\mathbf{Q}_p]-1} \in [\frac{3}{4}, 1)$ if $v \mid 2$, since $c_v = [K_v : \mathbf{Q}_p] + 2$.

Thus $\delta \notin \{0, \pm 1\}$ so (ii) follows from Theorem 7.6 as well. □

Example 7.11. *Let E be the elliptic curve labelled* 50B1 *in* [2]*:*

$$y^2 + xy + y = x^3 + x^2 - 3x - 1$$

and let K be a finite extension of $\mathbf{Q}(\sqrt{-2})$, unramified at 5*. Then for all sufficiently large X,*

$$\frac{|\{\chi \in \mathcal{C}(K, X) : r(\chi) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = \frac{1}{2} + \frac{(-1)^{[K:\mathbf{Q}(\sqrt{-2})]}}{2} \prod_{v|2} (1 - 2^{-[K_v:\mathbf{Q}_2]-1}).$$

As K varies, these values are dense in the interval $[0, 1]$*.*

Proof. The discriminant of E is $-2^5 \cdot 5^2$, which is a square in K, so $\Delta = 1$ in $K^\times/(K^\times)^2$. Over $\mathbf{Q}_2$, E has split multiplicative reduction, so E has split multiplicative reduction at every prime of K above 2. Over $\mathbf{Q}_5$, E has Kodaira type II, and since $K/\mathbf{Q}$ is unramified at 5, E has Kodaira type II at all primes of K above 5. Further, since K is unramified at 5 we have $E(K)[2] = 0$.

Let $w(E/K_v)$ denote the local root number of E over K_v. We have $w(E/K_v) = 1$ if $v \nmid 2 \cdot 5 \cdot \infty$. By [18, Theorem 2] we have $w(E/K_v) = -1$ if $v \mid 2$ or $v \mid \infty$, and $w(E/K_v) = 1$ if $v \mid 5$. Thus the global root number $w(E/K)$ is given by

$$w(E/K) = \prod_v w(E/K_v) = (-1)^{n_\infty + n_2}$$

where n_2 (resp., $n_\infty = [K : \mathbf{Q}(\sqrt{-2})]$) is the number of places of K above 2 (resp., above ∞). By [5, Theorem 1.3] (the “2-Selmer parity conjecture”), combined with the Cassels pairing (see for example [12, Proposition 2.1]), it follows that $\dim_{\mathbf{F}_2} \mathrm{Sel}_2(E/K) \equiv n_\infty + n_2 \pmod 2$.

The field K has no real embeddings, and E has good reduction at all primes of K not dividing 10. Hence Proposition 7.9 shows that the δ of Definition 7.4 is given by $\delta = (-1)^{n_\infty+n_2} \prod_{v|2}(2/|K_v^\times/(K_v^\times)^2| - 1)$. For each v dividing 2 we have

$$|K_v^\times/(K_v^\times)^2| = 2^{[K_v:\mathbf{Q}_2]+2}$$

so the desired formula follows from Theorem 7.6.

To prove the final assertion, suppose L is a finite extension of $\mathbf{Q}$, unramified at 5, in which 2 splits completely, and let $t := [L : \mathbf{Q}]$. Let $K := L(\sqrt[2m]{-2})$ with $m \geq 1$. Then K is unramified at 5, $[K : \mathbf{Q}(\sqrt{-2})] = tm$, $n_2 = [L : \mathbf{Q}] = t$, and $[K_v : \mathbf{Q}_2] = 2m$ if $v \mid 2$. In this case the quantity in the formula of the theorem is

$$\frac{1}{2} + \frac{(-1)^{tm}}{2}(1 - 2^{-2m-1})^t.$$

As m and t vary, the sets

$$\{\log((1 - 2^{-2m-1})^t) : tm \text{ even}\}, \quad \{\log((1 - 2^{-2m-1})^t) : tm \text{ odd}\}$$

are both dense in $\mathbf{R}_{\leq 0}$. It follows from the continuity of the exponential function that the set $\{(-1)^{tm}(1-2^{-2m-1})^t\}$ is dense in $[-1, 1]$. This completes the proof. □

Note that the Selmer rank and Mordell-Weil rank of E^χ are related by

$$\mathrm{rank}(E^\chi(K)) \geq r(\chi) - \dim_{\mathbf{F}_2} E(K)[2]$$

and if the 2-part of the Shafarevich-Tate group Ш(E/K) is finite, then

$$\mathrm{rank}(E^\chi(K)) \equiv r(\chi) - \dim_{\mathbf{F}_2} E(K)[2] \pmod 2.$$

Thus by Theorem 7.6 we expect that $\mathrm{rank}(E^\chi(K))$ is odd (and therefore at least one) for exactly $(1-(-1)^{\dim_{\mathbf{F}_2} E(K)[2]}\delta)/2$ of the twists E^χ. This leads to the following generalization of Goldfeld's conjecture [6, Conjecture B], which follows from Theorem 7.6 if we assume

- the 2-parts of the Shafarevich-Tate groups of twists of E are all finite,
- twists of rank at least 2 are rare enough that they do not affect the average rank.

Conjecture 7.12. *The average rank of the quadratic twists of E/K is given by*

$$\lim_{X\to\infty} \frac{\sum_{\chi\in\mathcal{C}(K,X)} \mathrm{rank}(E^\chi(K))}{|\mathcal{C}(K,X)|} = \frac{1-(-1)^{\dim_{\mathbf{F}_2} E(K)[2]}\delta}{2}.$$

Example 7.13. This example shows that the fraction of even ranks given by Theorem 7.6 does depend on the way we have chosen to order the twists. Let $\mathcal{C}(K,X)$ be as above, and consider also another natural ordering

$$\mathcal{C}'(K,X) := \{\chi_d : d \in \mathcal{O}_K : |\mathbf{N}d| < X\}$$

where χ_d is the character of $K(\sqrt{d})/K$. Let E be the elliptic curve 38B1 in [2]

$$y^2 + xy + y = x^3 + x^2 + 1$$

and $K = \mathbf{Q}(i)$. Then $r(\mathbf{1}_K) = 0$, and E has split multiplicative reduction at the primes $(1+i)$ and (19), and good reduction everywhere else. We have $|\mathcal{C}(K_{1+i})| = 2^4$ and $|\mathcal{C}(K_{19})| = 2^2$, and according to Proposition 7.9 we have $\omega_v(\chi_v) = 1$ if and only if $\chi_v = \mathbf{1}_v$, for $v = (1+i)$ or (19) and $\chi_v \in \mathcal{C}(K_v)$.

If $X > \mathbf{N}(19) = 19^2$, then the images of the characters χ in the group $\mathcal{C}(K,X)$ are uniformly distributed in $\mathcal{C}(K_{1+i}) \times \mathcal{C}(K_{19})$. Hence under the map

$$\mathcal{C}(K,X) \longrightarrow \mathcal{C}(K_{1+i}) \times \mathcal{C}(K_{19}) \xrightarrow{\omega_{1+i}\times\omega_{19}} \{\pm 1\} \times \{\pm 1\}$$

exactly $\frac{1}{16}\cdot\frac{1}{4} = \frac{1}{64}$ of them map to $(1,1)$ and $\frac{15}{16}\cdot\frac{3}{4} = \frac{45}{64}$ of them map to $(-1,-1)$. Hence by Proposition 7.2, $r(\chi)$ is even for exactly $\frac{23}{32} = \frac{1}{2} + \frac{7}{32}$ of the $\chi \in \mathcal{C}(K,X)$. This is the content of Theorem 7.6 in this case.

Now consider the density using $\mathcal{C}'(K,X)$ instead of $\mathcal{C}(K,X)$. The quadratic characters of K correspond bijectively to squarefree integers $d \in \mathbf{Z}[i]$ modulo ± 1, and $\mathcal{C}'(K,X)$ corresponds to d with $\mathbf{N}d < X$. These characters no longer map uniformly to $\mathcal{C}(K_{1+i})\times\mathcal{C}(K_{19})$; for example, the fraction of characters unramified at (19) (i.e., the fraction of squarefree d's that are not divisible by 19) is $19^2/(19^2+1)$, not $1/2$. Of those that are unramified, half of the d's are squares modulo 19. Reasoning in this way we see that under the map

$$\mathcal{C}'(K,X) \longrightarrow \mathcal{C}(K_{1+i}) \times \mathcal{C}(K_{19}) \xrightarrow{\omega_{1+i}\times\omega_{19}} \{\pm 1\} \times \{\pm 1\}$$

the fraction mapping to $(1,1)$ is

$$\left(\frac{1}{8}\cdot\frac{2}{2+1}\right)\cdot\left(\frac{1}{2}\cdot\frac{19^2}{19^2+1}\right) = \frac{1}{12}\cdot\frac{361}{724} = \frac{361}{8688},$$

and the fraction mapping to $(-1,-1)$ is $\frac{11}{12}\cdot\frac{363}{724}=\frac{1331}{2896}$. We conclude by Proposition 7.2 that

$$\lim_{X\to\infty}\frac{|\{\chi\in\mathcal{C}'(K,X):r(\chi)\text{ is even}\}|}{|\mathcal{C}'(K,X)|}=\frac{361}{8688}+\frac{1331}{2896}=\frac{2177}{4344}=\frac{1}{2}+\frac{5}{4344}.$$

8. Parity ($p>2$)

In this section suppose that $p>2$ and that (6.1), (6.2) are satisfied. We will study how the parity of $\dim_{\mathbf{F}_p}\mathrm{Sel}(T,\chi)$ varies as χ varies.

Recall that $\mathcal{C}(K)=\coprod_{\mathfrak{d}\in\mathcal{D}}\mathcal{C}(\mathfrak{d})$. If $\chi\in\mathcal{C}(\mathfrak{d})$, let

$$w(\chi):=w(\mathfrak{d}),\qquad r(\chi):=\dim_{\mathbf{F}_p}\mathrm{Sel}(T,\chi),$$

where $\mathrm{Sel}(T,\chi)$ is given by Definition 4.7, the Selmer group for the twist of T by χ. Similarly, if $\gamma\in\Gamma_{\mathfrak{d}}$ we let $r(\gamma):=\dim_{\mathbf{F}_p}\mathrm{Sel}(T,\gamma)$.

Let $\eta:\mathcal{C}(K)\to\Gamma_1$ be the natural homomorphism.

Definition 8.1. Define

$$\rho:=\frac{|\{\gamma\in\Gamma_1:r(\gamma)\text{ is odd}\}|}{|\Gamma_1|}.$$

Note that ρ cannot be $1/2$, since $|\Gamma_1|$ is odd. The main result of this section is the following.

Theorem 8.2. (i) *If $p\nmid[K(T):K]$, then for all sufficiently large X*

$$\frac{|\{\chi\in\mathcal{C}(K,X):r(\chi)\text{ is odd}\}|}{|\mathcal{C}(K,X)|}=\rho.$$

(ii) *If $p\mid[K(T):K]$, then*

$$\lim_{X\to\infty}\frac{|\{\chi\in\mathcal{C}(K,X):r(\chi)\text{ is odd}\}|}{|\mathcal{C}(K,X)|}=\frac{1}{2}.$$

Proof of Theorem 8.2(i). By Corollary 4.12, $r(\chi)\equiv r(\eta(\chi))+w(\chi)\pmod 2$ for every χ. Since $p\nmid[K(T):K]$, Lemma 4.3(ii) shows that $w(\chi)$ is even for every χ, so $r(\chi)$ is odd if and only if $r(\eta(\chi))$ is odd. By Proposition 6.8(i), for all X sufficiently large, η restricts to a surjective homomorphism of finite groups $\mathcal{C}(K,X)\to\Gamma_1$. In particular all fibers have the same size, so for large X

$$|\{\chi\in\mathcal{C}(K,X):r(\chi)\text{ is odd}\}|=|\{\gamma\in\Gamma_1:r(\gamma)\text{ is odd}\}|\ \frac{\mathcal{C}(K,X)}{|\Gamma_1|}$$

which proves assertion (i) of the theorem. □

The rest of this section is devoted to the proof of Theorem 8.2(ii). Order the primes of K not in Σ by norm, $\mathbf{N}\mathfrak{q}_1\le\mathbf{N}\mathfrak{q}_2\le\cdots$. For every n, let $C_n\subset\mathcal{C}(K)$ be the subgroup

$$C_n:=\{\chi\in\mathcal{C}(K):\chi\text{ is unramified outside of }\Sigma\cup\{\mathfrak{q}_1,\ldots,\mathfrak{q}_n\}\}.$$

For every $\gamma\in\Gamma_1$ define

$$s_n(\gamma):=\frac{|\{\chi\in C_n:\eta(\chi)=\gamma\text{ and }w(\chi)\text{ is even}\}|}{|\{\chi\in C_n:\eta(\chi)=\gamma\}|}-\frac{1}{2}.$$

We will show that $\lim_{n\to\infty}s_n(\gamma)=0$ for every $\gamma\in\Gamma_1$.

Lemma 8.3. (i) *If $\boldsymbol{\mu}_p\not\subset K_{\mathfrak{q}_n}^\times$, then $C_n=C_{n-1}$.*

(ii) *If* $\boldsymbol{\mu}_p \subset K_{\mathfrak{q}_n}^\times$, *then there is a* $\psi \in C_n$, *ramified at* $\mathfrak{q}_n$ *and unramified at* $\mathfrak{q}_1, \dots, \mathfrak{q}_{n-1}$, *such that* $C_n = \coprod_{i=0}^{p-1} \psi^i C_{n-1}$. *If* $\chi \in C_{n-1}$ *then*

$$w(\psi^i\chi) = \begin{cases} w(\chi) & \text{if } p \mid i \\ w(\chi) + k & \text{if } p \nmid i \text{ and } \mathfrak{q}_n \in \mathcal{P}_k. \end{cases}$$

Proof. If $\boldsymbol{\mu}_p \not\subset K_{\mathfrak{q}_n}^\times$ then by local class field theory no character of order p can ramify at $\mathfrak{q}_n$, so $C_n = C_{n-1}$. If $\boldsymbol{\mu}_p \subset K_{\mathfrak{q}_n}^\times$, then by Proposition 6.8(ii) there is a character $\psi \in C_n$ ramified at $\mathfrak{q}_n$ and unramified at $\mathfrak{q}_1, \dots, \mathfrak{q}_{n-1}$. The restriction of ψ generates $\mathrm{Hom}(\mathcal{O}_{\mathfrak{q}_n}^\times, \boldsymbol{\mu}_p)$, so ψ generates C_n/C_{n-1}. If $\mathfrak{q}_n \in \mathcal{P}_k$ and $p \nmid i$ then $w(\psi^i\chi) = w(\psi^i) + w(\chi) = k + w(\chi)$. This proves the lemma. ☐

Let $\Delta \in \mathcal{O}_{K,\Sigma}^\times$ be as in Lemma 6.2, and let $\mathrm{sign}_\Delta : \Gamma_1 \to \boldsymbol{\mu}_p$ be the homomorphism $\gamma \mapsto \prod_{v \in \Sigma} \gamma_v(\Delta)$ of Definition 6.4.

Lemma 8.4. *There is an* $N \in \mathbf{Z}_{>0}$ *such that if* $n \geq N$ *then* $s_n(\gamma)$ *depends only on* n *and* $\mathrm{sign}_\Delta(\gamma)$.

Proof. By Proposition 6.8(iii), if n is large enough then for every $\gamma \in \Gamma_1$ with $\mathrm{sign}_\Delta(\gamma) = 1$, there is a character $\psi_\gamma \in C_n$ ramified only at primes in $\Sigma \cup \mathcal{P}_2$, such that $\eta(\psi_\gamma) = \gamma$.

Suppose $\gamma_1, \gamma_2 \in \Gamma_1$ and $\mathrm{sign}_\Delta(\gamma_1) = \mathrm{sign}_\Delta(\gamma_2)$. Let $\gamma := \gamma_1^{-1}\gamma_2$. Then multiplication by ψ_γ gives a bijection

$$\{\chi \in C_n : \eta(\chi) = \gamma_1\} \longrightarrow \{\chi \in C_n : \eta(\chi) = \gamma_2\}.$$

Further, since ψ_γ is unramified at primes in $\mathcal{P}_1$ we have $w(\chi) \equiv w(\psi_\gamma\chi) \pmod 2$ for every $\chi \in C_n$. Thus $s_n(\gamma_1) = s_n(\gamma_2)$, which proves the lemma. ☐

Define $S_n = \frac{1}{|\Gamma_1|} \sum_{\gamma \in \Gamma_1} s_n(\gamma)$, the average of the $s_n(\gamma)$.

Lemma 8.5. *Suppose* $n > N$ *with* N *as in Lemma 8.4. If* $\boldsymbol{\mu}_p \not\subset K_{\mathfrak{q}_n}^\times$ *let* $\psi := \mathbf{1}_K \in C_n$, *and if* $\boldsymbol{\mu}_p \subset K_{\mathfrak{q}_n}^\times$ *let* $\psi \in C_n$ *be as in Lemma 8.3(ii). In either case let* $\varepsilon := (-1)^k$ *where* $\mathfrak{q}_n \in \mathcal{P}_k$, *and* $\bar{\psi} := \eta(\psi) \in \Gamma_1$. *Then*

$$s_n(\gamma) = \begin{cases} \frac{1+\varepsilon(p-1)}{p} s_{n-1}(\gamma) & \text{if } \mathrm{sign}_\Delta(\bar{\psi}) = 1, \\ \frac{1-\varepsilon}{p} s_{n-1}(\gamma) + \varepsilon S_{n-1} & \text{if } \mathrm{sign}_\Delta(\bar{\psi}) \neq 1. \end{cases}$$

Proof. If $\boldsymbol{\mu}_p \not\subset K_{\mathfrak{q}_n}^\times$, then $\bar{\psi} = \mathbf{1}$, $C_n = C_{n-1}$ by Lemma 8.3(i), and $\mathfrak{q}_n \in \mathcal{P}_0$ by definition, so $\varepsilon = 1$ and $s_n(\gamma) = s_{n-1}(\gamma)$ for every γ. Thus the formula of the lemma holds in this case.

Suppose now that $\boldsymbol{\mu}_p \subset K_{\mathfrak{q}_n}^\times$, so ψ is ramified at $\mathfrak{q}_n$. Then for every $\gamma \in \Gamma_1$, $\chi \in C_{n-1}$, and $0 \leq i < p$, Lemma 8.3(ii) shows that

$$\eta(\psi^i\chi) = \gamma \text{ and } w(\psi^i\chi) \text{ is even} \iff \begin{cases} i = 0,\ \eta(\chi) = \gamma, \text{ and } w(\chi) \text{ is even, or} \\ i \neq 0,\ \eta(\chi) = \bar{\psi}^{-i}\gamma, \text{ and } (-1)^{w(\chi)} = \varepsilon. \end{cases}$$

Thus, using that $C_n = \coprod_{i=0}^{p-1} \psi^i C_{n-1}$ by Lemma 8.3(ii), we have

$$1/2 + s_n(\gamma) = \frac{(1/2 + s_{n-1}(\gamma)) + \sum_{i=1}^{p-1}(1/2 + \varepsilon s_{n-1}(\bar{\psi}^i\gamma))}{p}$$

or equivalently

$$s_n(\gamma) = \frac{(1-\varepsilon)s_{n-1}(\gamma) + \varepsilon \sum_{i=0}^{p-1} s_{n-1}(\bar{\psi}^i\gamma)}{p}. \tag{8.1}$$

If $\mathrm{sign}_\Delta(\bar\psi) = 1$ then $s_n(\bar\psi^i\gamma) = s_{n-1}(\gamma)$ for every i by Lemma 8.4, and (8.1) becomes $s_n(\gamma) = \frac{1+(p-1)\varepsilon}{p} s_{n-1}(\gamma)$. If $\mathrm{sign}_\Delta(\bar\psi) \neq 1$ then $\mathrm{sign}_\Delta(\bar\psi)$ generates $\boldsymbol{\mu}_p$, so (using Lemma 8.4)

$$\sum_{i=0}^{p-1} s_{n-1}(\bar\psi^i\gamma) = \frac{p}{|\Gamma_1|}\sum_{\varphi\in\Gamma_1} s_{n-1}(\varphi) = pS_{n-1}.$$

Now the final equality of the lemma follows from (8.1). □

Corollary 8.6. *If $p \mid [K(T):K]$ and $\gamma \in \Gamma_1$, then $\lim_{n\to\infty} s_n(\gamma) = 0$.*

Proof. Averaging over $\gamma \in \Gamma_1$ in Lemma 8.5 shows that

$$S_n = \begin{cases} S_{n-1} & \text{if } \varepsilon = 1 \\ \frac{2-p}{p} S_{n-1} & \text{if } \varepsilon = -1. \end{cases}$$

If $p \mid [K(T):K]$, then $\mathcal{P}_1$ is infinite by Lemma 4.3, and $\varepsilon = -1$ whenever $\mathfrak{q}_n \in \mathcal{P}_1$, so we deduce that $\lim_{n\to\infty} S_n = 0$. Applying Lemma 8.5 again proves the corollary. □

Proof of Theorem 8.2(ii). By Corollary 4.12, $r(\chi) \equiv r(\eta(\chi)) + w(\chi) \pmod 2$ for every χ, so

$$r(\chi) \text{ is odd} \iff w(\chi) \not\equiv r(\eta(\chi)) \pmod 2. \tag{8.2}$$

We may assume (Proposition 6.8(i)) that n is large enough so that the map $\eta : C_n \to \Gamma_1$ is surjective. Using (8.2), for every $\gamma \in \Gamma_1$ we have

$$\frac{|\{\chi \in C_n : \eta(\chi) = \gamma \text{ and } r(\chi) \text{ is odd}\}|}{|\{\chi \in C_n : \eta(\chi) = \gamma\}|} = 1/2 - (-1)^{r(\gamma)} s_n(\gamma).$$

Since $p \mid [K(T):K]$, Corollary 8.6 shows that $\lim_{n\to\infty} s_n(\gamma) = 0$, so

$$\lim_{n\to\infty} \frac{|\{\chi \in C_n : \eta(\chi) = \gamma \text{ and } r(\chi) \text{ is odd}\}|}{|\{\chi \in C_n : \eta(\chi) = \gamma\}|} = 1/2.$$

This holds for every $\gamma \in \Gamma_1$, so

$$\lim_{X\to\infty} \frac{|\{\chi \in \mathcal{C}(K,X) : r(\chi) \text{ is odd}\}|}{|\mathcal{C}(K,X)|} = \lim_{n\to\infty} \frac{|\{\chi \in C_n : r(\chi) \text{ is odd}\}|}{|C_n|} = 1/2.$$

This completes the proof of Theorem 8.2 □

Remark 8.7. Fix an elliptic curve E/K, and let p vary. If E does not have complex multiplication, then Serre's theorem [22] shows that $p \mid [K(T):K]$ for all but finitely many p, so Theorem 8.2(ii) shows that for all but finitely many p, half of the twists by characters of order p have even p-Selmer rank and half have odd p-Selmer rank.

References

[1] J.W.S. Cassels, Arithmetic of curves of genus 1. VIII. *J. Reine Angew. Math.* **217** (1965) 180-199.

[2] J.E. Cremona, Algorithms for modular elliptic curves. Cambridge University Press, Cambridge (1992).

[3] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, M. Stoll, Explicit n-descent on elliptic curves. I. Algebra. *J. Reine Angew. Math.* **615** (2008) 121-155.

[4] T. Dokchitser, V. Dokchitser, Elliptic curves with all quadratic twists of positive rank. *Acta Arith.* **137** (2009) 193–197.

[5] T. Dokchitser, V. Dokchitser, Regulator constants and the parity conjecture. *Invent. Math.* **178** (2009) 23-71.
[6] D. Goldfeld, Conjectures on elliptic curves over quadratic fields. In: Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979, M. B. Nathanson, ed.), *Lecture Notes in Math.* **751**, Springer-Verlag, Berlin (1979), 108–118.
[7] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem II. *Invent. Math.* **118** (1994) 331–370.
[8] B. Howard, The Heegner point Kolyvagin system. *Compositio Math.* **140** (2004) 1439–1472.
[9] D. Kane, On the ranks of the 2-Selmer groups of twists of a given elliptic curve, to appear. http://arxiv.org/abs/1009.1365
[10] Z. Klagsbrun, B. Mazur, K. Rubin, Distribution of Selmer ranks of quadratic twists of elliptic curves, to appear.
[11] K. Kramer, Arithmetic of elliptic curves upon quadratic extension, *Transactions Amer. Math. Soc.* **264** (1981) 121–135.
[12] B. Mazur, K. Rubin, Finding large Selmer rank via an arithmetic theory of local constants, *Annals of Mathematics* **166** (2007) 579–612.
[13] B. Mazur, K. Rubin, Ranks of twists of elliptic curves and Hilbert's tenth problem, *Inventiones Math.* **181** (2010) 541–575.
[14] B. Mazur, K. Rubin, A. Silverberg, Twisting commutative algebraic groups. *J. Algebra* **314** (2007) 419-438.
[15] J.S. Milne, Arithmetic duality theorems, *Perspectives in Math.* **1**, Academic Press, Orlando (1986).
[16] P. Monsky, Generalizing the Birch-Stephens theorem. I. Modular curves. *Math. Z.* **221** (1996) 415–420.
[17] B. Poonen, E. Rains, *Random maximal isotropic subspaces and Selmer groups. J. Amer. Math. Soc.* **25** (2012) 245–269.
[18] D. Rohrlich, Galois theory, elliptic curves, and root numbers, *Compositio Math.* **100** (1996) 311–349.
[19] K. Rubin, Euler Systems. *Annals of Math. Studies* **147**, Princeton: Princeton University Press (2000).
[20] K. Rubin, A. Silverberg, Families of elliptic curves with constant mod p representations. In: Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), *Ser. Number Theory* **I**, Int. Press, Cambridge, MA (1995) 148-161.
[21] J-P. Serre, Cohomologie galoisienne, *Lecture Notes in Mathematics* **5**, Springer-Verlag, Berlin-New York (1965).
[22] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
[23] H.P.F. Swinnerton-Dyer, The effect of twisting on the 2-Selmer group. *Math. Proc. Cambridge Philos. Soc.* **145** (2008) 513–526.
[24] J. Tate, Duality theorems in Galois cohomology over number fields, in: *Proc. Intern. Cong. Math.*, Stockholm (1962) 234–241.
[25] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular functions of one variable (IV), *Lecture Notes in Math.* **476**, New York: Springer-Verlag (1975) 33–52.

Department of Mathematics, University of Wisconsin - Madison, Madison, WI 53706, USA
E-mail address: klagsbru@math.wisc.edu

Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
E-mail address: mazur@math.harvard.edu

Department of Mathematics, UC Irvine, Irvine, CA 92697, USA
E-mail address: krubin@math.uci.edu